



Titre: Randomness in Fiber-Based Photonics for Secure Communications
Title:

Auteur: Frédéric Monet
Author:

Date: 2023

Type: Mémoire ou thèse / Dissertation or Thesis

Référence: Monet, F. (2023). Randomness in Fiber-Based Photonics for Secure Communications [Thèse de doctorat, Polytechnique Montréal]. PolyPublie.
Citation: <https://publications.polymtl.ca/53393/>

 **Document en libre accès dans PolyPublie**
Open Access document in PolyPublie

URL de PolyPublie: <https://publications.polymtl.ca/53393/>
PolyPublie URL:

Directeurs de recherche: Raman Kashyap
Advisors:

Programme: Génie physique
Program:

POLYTECHNIQUE MONTRÉAL

affiliée à l'Université de Montréal

Randomness in fiber-based photonics for secure communications

FRÉDÉRIC MONET

Département de génie physique

Thèse présentée en vue de l'obtention du diplôme de *Philosophiæ Doctor*

Génie physique

Avril 2023

© Frédéric Monet, 2023.

POLYTECHNIQUE MONTRÉAL

affiliée à l'Université de Montréal

Cette thèse intitulée :

Randomness in fiber-based photonics for secure communications

présentée par **Frédéric MONET**

en vue de l'obtention du diplôme de *Philosophiæ Doctor*

a été dûment acceptée par le jury d'examen constitué de :

Frédéric LEBLOND, président

Raman KASHYAP, membre et directeur de recherche

Jean-Jacques LAURIN, membre

Jens SCHMID, membre externe

DEDICATION

To my parents, who always encouraged me to accomplish my dreams

ACKNOWLEDGEMENTS

First and foremost, I would like to thank my research director, Raman Kashyap, for his constant support and guidance. These last few years have been an extraordinary learning experience, and Raman consistently pushed me to try out new crazy ideas and learn new skills, leading this PhD in a direction that none of us expected at the beginning. His advice and mentorship helped shape me as a researcher, but also as the human being I am today.

I wish to thank my colleagues at Fabulas, past and present, who turned this journey into an extraordinary adventure. I would like to especially thank Sébastien Loranger and Victor Lambin-Iezzi, who were two amazing mentors that taught me everything about research and photonics when I started my graduate studies, and turned the little undergraduate boy I was into a man. I also need to express special thanks to Jean-Sébastien Boisvert, who recruited me into this laboratory with a lucky dice roll, and consistently offered both technical and mental support throughout these years. I'd also like to thank the other fabulous Fabulas people with whom I worked and interacted during this PhD: Amirhossein, Antoine, Pierre, Jyothis, Yalina, Antsar, Anthony, Yannick, Qingtao and Jacynthe, as well as the new generation who's inheriting this laboratory: Foroogh, Ehsan, Mahshid and Reyhane.

I would also like to acknowledge the amazing support of our devoted technicians and support staff, from Poly-Grames: Jules Gauthier, Steve Dubé, Jean-Sébastien Décarie, Louis-Philippe Carignan, Traian Antonescu and Rachel Lortie, and from Engineering Physics: Jean-Paul Lévesque and Mikael Leduc. Without their technical skills, none of the results presented in this thesis would have been possible.

This achievement was only possible with the help and support of my friends and family, in particular my parents Sophie Monet and Alain Charpentier, who taught me the importance of persevering to achieve my goals, as well as my amazing partner Florence Maas-Gariépy, with whom I shared every day the highs and lows of a PhD.

Finally, I would like to thank the Vanier Canada Graduate Scholarship Program and the Fonds de Recherche du Québec – Nature et Technologie for their financial support.

RÉSUMÉ

Dans notre ère d'information, une quantité croissante d'informations personnelles et de nos communications est transmise par l'Internet, qui est sujet aux cyberattaques, à l'espionnage et aux intrusions. La sécurité de nos communications est donc une préoccupation croissante pour toutes les entités qui traitent des informations sensibles comme les gouvernements, les institutions bancaires, les agences de renseignement et même le grand public. Pour garantir la confidentialité de nos informations, les systèmes de télécommunications s'appuient désormais sur des protocoles cryptographiques qui chiffrent les messages à l'aide de clés secrètes, garantissant ainsi que seul le destinataire prévu peut déchiffrer les informations contenues dans le message. Ces clés secrètes sont basées sur des nombres aléatoires, qui sont généralement générés par des algorithmes complexes afin de garantir qu'ils présentent la non-reproductibilité et la non-périodicité requises. Cependant, ces protocoles de communication n'offrent pas une sécurité absolue, et présentent certaines faiblesses qui peuvent être exploitées par certains attaquants. Par exemple, les algorithmes générant les nombres aléatoires sont déterministes et pourraient potentiellement être reproduits ou simulés, ce qui mettrait en danger la confidentialité des communications.

Pour résoudre ce problème, de nouvelles techniques sont conçues pour améliorer les protocoles de communication sécurisés, par exemple en intégrant un niveau physique supplémentaire de sécurité en plus des algorithmes cryptographiques. De plus, comme alternative aux nombres pseudo-aléatoires algorithmiques, les sources physiques d'entropie sont étudiées pour générer de véritables nombres aléatoires basés sur des processus physiques, comme le bruit d'une diode. Dans cette thèse, l'utilisation de l'aléatoire dans les dispositifs photoniques à base de fibres est étudiée comme une solution potentielle pour améliorer la sécurité des protocoles cryptographiques existants. La recherche est orientée selon deux axes principaux. Le premier axe est basé sur la fabrication de nouveaux dispositifs physiques basés sur l'aléatoire, qui sont ensuite utilisés à plusieurs étapes du protocole de communication. Le second axe se concentre sur le développement d'une nouvelle source d'entropie, ainsi que l'évaluation de son potentiel pour la génération de nombres aléatoires.

Pour répondre au premier axe de recherche, un nouveau type de réseau aléatoire est développé, appelé *Random Optical Grating by Ultraviolet or ultrafast laser Exposure* (ROGUE). Ce type de réseau possède des caractéristiques uniques qui le rendent parfaitement adapté aux applications de

communications sécurisées. En effet, chaque ROGUE possède une signature spectrale complexe, basée sur le bruit, qui agit comme une empreinte digitale unique. Cette empreinte unique est alors utilisée pour authentifier l'identité de l'utilisateur, ou peut alternativement être utilisée comme la clé secrète au cœur des protocoles cryptographiques. Le premier article de cette thèse décrit la méthodologie utilisée pour fabriquer ces réseaux, tandis que le second article présente comment ce ROGUE agit en tant que *Physical Unclonable Function* (PUF) de haute qualité, ce qui permet de multiples applications potentielles dans les communications sécurisées. La réponse spectrale unique du ROGUE et sa facilité de fabrication en font également un candidat parfait pour d'autres applications, dont certaines sont étudiées au cours de cette thèse, comme la détection distribuée et la reconstruction de forme d'instruments chirurgicaux minimalement invasifs.

Dans le deuxième axe de recherche, l'aléatoire en optique fibrée est investigué sous la forme de lasers aléatoires, un type émergent de lasers aux propriétés intéressantes. En effet, au lieu d'être basés sur une cavité fixe, les lasers aléatoires utilisent comme rétroaction la diffusion inhérente de milieux amorphes, formant des cavités aléatoires qui peuvent commencer à laser lorsque le gain optique est suffisant. Dans cette thèse, un laser Raman aléatoire à rétroaction distribuée est développé, où un rouleau de fibre optique utilise à la fois la diffusion de Rayleigh comme rétroaction et la diffusion Raman comme gain optique. Ce laser aléatoire, couplé à d'autres effets d'optique non linéaire tels que l'instabilité de modulation, est démontré comme une nouvelle source d'entropie qui peut aboutir à la génération ultra-rapide de nombres aléatoires. Le troisième article décrit l'architecture de la cavité laser, et démontre sa capacité à générer des bits aléatoires à des vitesses comparables à l'état de l'art actuel. Dans le quatrième article de cette thèse, une modification mineure de la structure de la cavité entraîne la génération d'un supercontinuum, qui permet la génération de nombres aléatoires sur plusieurs canaux parallèles. Ceci fournit également une plateforme très intéressante permettant d'étudier les liens entre l'entropie générée et le multiplexage de canaux de génération de nombres aléatoires.

Enfin, une discussion résume les avantages et inconvénients de chaque dispositif développé au cours de cette thèse, et comment ils peuvent être intégrés dans les protocoles cryptographiques existants. La synergie entre ces dispositifs est également décrite, en discutant de leur potentiel d'utilisation simultanée pour différentes applications au sein d'un même protocole de communication, ou même d'être combinés en un seul dispositif aux capacités uniques.

ABSTRACT

In the current information era, an increasing quantity of our personal information and communications is transmitted by the Internet, which is prone to cyber-attacks, spying and intrusions. The security of our communications is therefore a growing concern to all entities transacting sensitive information like governments, banking institutions, intelligence agencies and even the general public. To ensure the privacy of our information, telecommunications systems now rely on cryptographic protocols that encrypt messages using secret keys, making sure only the intended receiver can decrypt the information embedded in the message. These secret keys are based on random numbers, which are typically generated by complex algorithms to ensure they have the required non-reproducibility and non-periodicity. However, these communication protocols do not offer absolute security, and have certain weaknesses that can be exploited by some attackers. For example, the algorithms generating the random numbers are deterministic, and could be potentially reverse-engineered or simulated, putting at risk the privacy of the communications.

To address this issue, researchers are devising novel techniques to improve the secure communications protocols, for instance by integrating an additional physical layer of security on top of the cryptographic algorithms. Additionally, as an alternative to the algorithmic pseudo-random numbers, physical sources of entropy are investigated to generate *true* random numbers based on physical processes, such as from the noise in a diode. In this thesis, the use of randomness in fiber-based photonic devices is investigated as a potential solution to improve the security of existing cryptographic protocols. The research is oriented along two main axes. The first axis is based on the fabrication of new physical devices based on randomness, which are then used at multiple steps in the communication protocol. The second axis aims at developing a novel source of entropy, and evaluating its potential for random number generation.

To address the first research axis, a novel type of random grating is developed, named the Random Optical Grating by Ultraviolet or ultrafast laser Exposure (ROGUE). This type of grating has unique characteristics that makes it perfectly well suited for secure communications applications. Indeed, each ROGUE has a complex, noise-based spectral signature that acts as a unique fingerprint. This unique fingerprint is then used to authenticate the user's identity, or can alternatively used as the secret key at the heart of cryptographic protocols. The first article of this

thesis describes the methodology used to fabricate these gratings, while the second article presents how this ROGUE acts as a high-quality Physical Unclonable Function (PUF), which has multiple applications in secure communications. The ROGUE's unique spectrum and ease of fabrication also makes it a perfect candidate for other applications, some of which are investigated during the course of this thesis like distributed sensing and shape reconstruction of minimally invasive surgical instruments.

In the second axis of research, randomness in fiber-based optics is employed in the form of random lasers, an emerging type of lasers with exciting properties. Indeed, instead of relying on a fixed cavity structure, random lasers rely on the inherent scattering of diffusive media as feedback, forming random cavities that can start lasing when provided with enough gain. In this thesis, a random distributed feedback Raman laser is developed, where an optical fiber bundle provides both Rayleigh scattering as feedback and Raman scattering as optical gain. This random laser, coupled with other nonlinear optics effects such as modulation instability, demonstrates a novel entropy source that can result in high-speed random number generation (RNG). The third article describes the laser cavity architecture, and demonstrates its capacity to generate random bits at rates comparable to the current state-of-the-art. In the fourth article of this thesis, a minor change in the cavity structure results in the generation of a supercontinuum, which enables the generation of random numbers across multiple parallel channels. This also provides a very interesting platform allowing the study of the links between the entropy generated and RNG channel multiplexing.

Finally, a discussion summarizes the advantages and drawbacks of each device developed during this PhD, and how they can be integrated into existing cryptographic protocols. The synergy between these devices is also be described, as they can be used simultaneously for different applications within a single communications protocol, or even combined into a single device with unique capabilities.

TABLE OF CONTENTS

DEDICATION	III
ACKNOWLEDGEMENTS	IV
RÉSUMÉ.....	V
ABSTRACT	VII
TABLE OF CONTENTS	IX
LIST OF TABLES	XV
LIST OF FIGURES.....	XVI
LIST OF SYMBOLS AND ABBREVIATIONS.....	XXVII
LIST OF APPENDICES	XXIX
CHAPTER 1 INTRODUCTION.....	1
1.1 Motivation	1
1.2 Problematic.....	5
1.3 Objectives.....	5
1.4 Organisation of the thesis.....	7
CHAPTER 2 LITERATURE REVIEW.....	9
2.1 Fiber Bragg gratings.....	9
2.1.1 Fiber Bragg grating theory	9
2.1.2 Fiber Bragg grating fabrication	12
2.1.3 Random fiber Bragg gratings	18
2.2 Nonlinear Optics	20
2.2.1 Stimulated Raman scattering.....	21
2.2.2 Modulation instability	24
2.2.3 Raman self-frequency shift	28

2.3	Fiber Lasers	29
2.3.1	Conventional FBG fiber laser cavity.....	30
2.3.2	Distributed feedback (DFB) fiber lasers	31
2.3.3	Random lasers	32
2.4	Strain and temperature sensing	37
2.4.1	Quasi-distributed sensing	38
2.4.2	Distributed sensing.....	39
2.5	Random number generation	43
2.5.1	Pseudo-random number generation.....	44
2.5.2	Physical random number generation	45
2.6	Authentication and secure communications.....	46
2.6.1	Conventional secure communications and authentication protocols	47
2.6.2	Physical Unclonable Functions	48
2.6.3	Alternative secure communications systems.....	52
CHAPTER 3	METHODOLOGY	53
3.1	Methodology of the overall research.....	53
3.1.1	FBG Writing.....	53
3.1.2	OFDR Measurements	56
3.1.3	Random Raman fiber laser	58
3.1.4	Random number generation	59
3.2	Organisation of the articles	61
CHAPTER 4	ARTICLE 1: THE ROGUE: A NOVEL, NOISE-GENERATED RANDOM GRATING	63
4.1	Introduction	63

4.2	Methods.....	65
4.2.1	ROGUE fabrication.....	65
4.2.2	Noise level and accuracy measurements	66
4.2.3	Interpolation technique.....	68
4.3	Fabrication and Modeling of the ROGUE	69
4.4	Advantages for OFDR Distributed Sensing	73
4.4.1	Results of the interpolation	73
4.4.2	ROGUE noise level and accuracy in OFDR sensing	75
4.4.3	Spatial resolution in noise level	77
4.4.4	ROGUE gain and loss compensation	78
4.5	Discussion	79
4.6	Conclusion.....	82
4.7	Funding.....	82
4.8	Acknowledgement.....	82
CHAPTER 5	ARTICLE 2: NON FUNGIBLE GRATINGS AS PHYSICAL UNCLONABLE FUNCTIONS	83
5.1	Introduction	83
5.2	Fabrication Methods.....	85
5.2.1	ROGUE Writing.....	85
5.2.2	PUF Fabrication	86
5.3	PUF Performance	88
5.3.1	Hamming Distance Distributions	88
5.3.2	False positive and negative probabilities	90
5.3.3	Temperature Dependence.....	91

5.3.4	Other interrogation parameters.....	93
5.3.5	Alternative Digitization Algorithm	94
5.4	Discussion	96
5.5	Conclusion.....	99
5.6	Supplementary Material	101
5.6.1	Temperature and Strain Compensation Algorithm	101
CHAPTER 6 ARTICLE 3: A SIMPLE HIGH-SPEED RANDOM NUMBER GENERATOR WITH MINIMAL POST-PROCESSING USING A RANDOM RAMAN FIBER LASER 105		
6.1	Introduction	105
6.2	Random Raman fiber laser emission.....	107
6.3	Statistical randomness evaluation	110
6.4	Physical entropy estimation	112
6.5	Methods.....	115
6.6	Funding.....	116
6.7	Acknowledgment	116
6.8	Disclosures.	116
6.9	Author Contributions.....	116
6.10	Supplementary Material	117
6.10.1	Random laser output power distributions at different pump powers	117
6.10.2	Spectrum of NZ-DS and TF optical fibers	118
CHAPTER 7 ARTICLE 4: ON MULTIPLEXING IN PHYSICAL RANDOM NUMBER GENERATION, AND CONSERVED TOTAL ENTROPY CONTENT 120		
7.1	Introduction	120
7.2	Single-Channel Random Number Generation.....	123

7.2.1	Random Supercontinuum Generation	123
7.2.2	Single-Channel Random Number Generation.....	124
7.2.3	Physical Entropy Evaluation	125
7.3	Parallel RNG	127
7.3.1	Cross-correlations across channels.....	128
7.3.2	Mutual Information between channels.....	131
7.3.3	Channel widths and conserved total entropy.....	132
7.4	Discussion	134
7.5	Methods.....	135
7.6	Funding.....	137
7.7	Acknowledgment	137
7.8	Disclosures.	137
7.9	Data Availability	137
7.10	Author Contributions.....	137
7.11	Supplementary Material	138
7.11.1	Mutual Information for all 8 bits.....	138
CHAPTER 8	ADDITIONAL RESULTS.....	140
8.1	Shape reconstruction of a Continuum Dexterous Manipulator	140
8.2	ROGUE-based localization and random lasers	143
8.3	Fabrication of high-quality FBGs and lasers.....	147
8.3.1	Optimization of the FBG Apodization	147
8.3.2	Fabrication of DFB lasers in Tm-doped fiber	150
CHAPTER 9	GENERAL DISCUSSION.....	155
9.1	Review of the objectives	155

9.1.1	Fabrication of a novel, noise-based random grating	155
9.1.2	Secure communications using random gratings	159
9.1.3	Demonstrate the robustness to changing environmental conditions	162
9.1.4	Development of novel entropy sources for RNG using random lasers	164
9.1.5	Investigation of the limits of the RNG schemes developed	168
9.2	Overall discussion	170
CHAPTER 10 CONCLUSION AND RECOMMENDATIONS		172
REFERENCES		177
APPENDICES		191

LIST OF TABLES

Table 6.1 Results of the NIST SP 800-22 for the random bit sequence generated at 1.28 Tbps .	112
Table 7.1 Results of the NIST SP 800-22 for the random bit sequence generated at 120 Gbps..	125
Table 7.2 RNG Potential of different channel's optical bandwidth $\delta\lambda$	133
Table 8.1 Writing parameters used for the DFB	151
Table 9.1 Comparison of the different random gratings properties	158
Table 9.2 Comparison of the different fiber-based PUF architectures	160
Table 9.3 Comparison of the different RNG schemes discussed in this thesis	167

LIST OF FIGURES

Figure 1.1 (a) Typical communication system between Alice and Bob, who both act as transmitter (TX) and receiver (RX). Alice can use Bob's public key to encrypt her messages to him, which Bob can then decrypt using his secret key, and vice-versa. (b) The malicious attacker Mallory can act as man-in-the-middle, issuing her own set of public and private keys, and can then intercept the communications between Alice and Bob, or even impersonate them.	2
Figure 2.1 (a) Uniform FBG refractive index profile and (b) associated Fourier transform. (c) Apodized FBG refractive index profile, where the visibility $v(z)$ is tuned to induce the apodization, and (d) associated Fourier transform.	11
Figure 2.2 Simulated spectra of a 100 mm uniform FBG with a Gaussian apodization, where the apodization is achieved by varying either the refractive index modification $\Delta n(z)$ (orange) or the visibility $v(z)$ (blue).	12
Figure 2.3 Behind-the-mask FBG inscription technique. Orders ± 1 diffracted by the phase mask interfere on the optical fiber, resulting in the FBG inscription.	14
Figure 2.4 (a) Talbot interferometer scheme, where the FBG is inscribed by an interference pattern formed by the two overlapping ± 1 diffraction orders. (b) Lloyd interferometer scheme, where the FBG is inscribed by the interference of the UV beam with its reflection.	15
Figure 2.5 Continuous FBG writing techniques, using a modified Talbot interferometer writing scheme. The phase of the interference pattern is tuned synchronously with the fiber movement by applying a sawtooth wave to (a) a piezoelectric element or (b) a pair of phase modulators. Figure taken with permission from [17].	16
Figure 2.6 Femtosecond laser FBG inscription process, where an ultrafast laser is focused into the core of an optical fiber, allowing the inscription of each FBG period. The gratings periods can either consist of (a) single spots in the point-by-point technique (PbP), (b) lines in the line-by-line technique (LbL) or (c) planes in the plane-by-plane technique (Pl-b-Pl). Taken with permission from [19].	17
Figure 2.7 Energy level diagram describing, for an optical pump wave ω_P , the Raman scattering generating (a) the Stokes wave ω_S and (b) the Anti-Stokes wave ω_{AS}	22

Figure 2.8 Raman gain spectra in silica optical fiber, for a pump wavelength of 1 μm . Figure reproduced with permission from [32], © Elsevier 2005. This figure is adapted from the published work of Stolen and Ippen [33], reproduced here with the permission of AIP Publishing.....	23
Figure 2.9 MI gain spectrum, for $\beta_2 = -10 \text{ ps}^2/\text{km}$, $\gamma = 2 \text{ W/km}$, and various pump powers.	28
Figure 2.10 (a) Fabry-Perot fiber laser cavity, consisting of two FBGs: a high-reflective (HR) grating and an output coupler (OC), placed on both sides of the gain fiber. (b) Ring fiber laser cavity, where the pump is injected in the cavity through a WDM coupler. Part of the signal exits the cavity through an output coupler (OC), while the rest remains in the cavity for further amplification. An isolator (optional) can be used to ensure single-direction operation.	31
Figure 2.11 Schematic illustrating the glass slides experiment of Berry and Klein [47]. For a sufficiently large number of glass slides, all the light paths including multiple reflections, such as paths a and b , will cancel each other destructively, leaving only the ballistic path c remaining.....	33
Figure 2.12 (a) Normalized linear spectrum of a random Raman laser, both below (blue) and above threshold (orange) (b) Evolution of both the Lévy α parameter (blue) and the output power (orange) as a function of pump power.	35
Figure 2.13 OFDR sensing algorithm. (a) A tunable laser scan measures the intensity profile as a function of wavelength (or frequency). (b) A Fourier transform is performed to obtain the temporal intensity profile. A certain gauge length (dashed window) is selected, defining the spatial resolution. (c) An inverse Fourier transform is performed to have the spectrum associated to this specific location. (d) This spectrum is compared with a reference value, by (e) performing a cross-correlation computation. The position of this peak provides (f) the spectral shift for this specific position (blue), which is proportional to strain or temperature fluctuations. This process is repeated along the entire length of the fiber (gray).	42
Figure 2.14 Schematic of an optical PUF, relying on the speckle pattern obtained after propagation of coherent radiation through a scattering medium.....	49
Figure 3.1 Schematics of the Fabulas installations [132].....	53

Figure 3.2 Fabulas FBG writing station, shown here with the piezoelectric-based modulation....55

Figure 3.3 Optical circuit of the commercial OFDR instrument (Luna OBR 4600). A tunable laser source (TLS) is separated in a Mach-Zehnder interferometer scheme, with the device under test (DUT) in one arm. The interference between the reflection from the DUT and the other arm of the interferometer is separated by a polarization beam splitter (PBS), and the amplitude and phase of the two polarizations is measured by detectors.....57

Figure 3.4 Random distributed feedback Raman fiber laser cavity. The cavity can be closed on one side by a highly reflective FBG, or alternatively can be removed, in which case the feedback is replaced by the 4% Fresnel reflection of a fiber end facet. All other fiber end facets are angled-cleaved to avoid parasitic reflections. The random feedback is provided by the optical fiber bundle, and can be enhanced by the addition of a ROGUE. The pump and output powers are monitored by power-meters (PMs), while the output spectrum is measured by an optical spectrum analyzer (OSA). The pump and output signals are separated by wavelength division multiplexer (WDM) couplers. 58

Figure 4.1 Talbot interferometer used for the fabrication of the ROGUE. The phase mask above generates different diffraction orders. The first two orders (+1 and -1) are reflected by mirrors onto the fiber, where an interference fringe pattern is created. The UV exposure increases the refractive index periodically, creating an FBG. By changing the angle of the mirrors, the interference fringe pattern (and thus the FBG wavelength) can be modified. The random electrical wave applied to the piezoelectric element induces imperfect overlap of the interference pattern, creating a ROGUE. 66

Figure 4.2: Cross-correlation result (a) before and (b) after the *sinc* interpolation. The fiber used is a standard SMF-28 fiber inscribed with a ROGUE, interrogated over a 42.90 nm bandwidth with a 10 mm gauge length. The original dataset of (a) has 521 points, while the interpolation of (b) is performed by adding 2,000 padding zeroes to the data. 69

Figure 4.3 : (a) Schematic illustration showing the difference between a regular in-phase FBG, exhibiting a very narrow bandwidth (typical full-width at half-maximum (FWHM) taken from [131]), and a ROGUE, composed of multiple out-of-phase μ FBGs of different lengths, resulting in a much wider bandwidth. Experimental measurements for a 1-meter-long

ROGUE written in SMF-28 fiber are presented (b) in the temporal domain, showing over 30 dB in backscattered amplitude enhancement, and (c) in the spectral domain, where an 8 nm FWHM (41 nm full width) can be observed. Rayleigh scattering baseline can be observed out-of-band of the grating, at around -60 dB. The ROGUE was written using 37 mW of 213 nm UV laser power, at a writing speed of 0.2 mm/s. Measurements were made with the largest bandwidth of 88.24 nm available on the OBR4600. 70

Figure 4.4 : Gain of the backscattering signal of the ROGUE as a function of writing speed vs untreated fiber. The ROGUE was written using a noise amplitude of 5 V (~10 periods) and a frequency bandwidth of 20 Hz. A SMF-28 fiber from Corning (orange) and a SM1500 fiber from Fibercore (green) were tested, using 22 mW (solid line) and 37 mW (dashed line) of laser power. 0 dB corresponds to the signal level of untreated fiber both for SMF-28 and SM1500). Measurements made on the OBR4600 using a 21.16 nm scanning bandwidth, the bandwidth most suitable for sensing, as will be shown in the next sections. The gain was measured in the temporal domain (see Figure 4.3(b)). 71

Figure 4.5 : FWHM bandwidth of the ROGUE, as a function of length. The experimental data is limited to 400 mm, with models using the parameters $k_1 = 500 \text{ m}^{-1}$ and $k_2 = 1.4\text{e}4 \text{ m}^{-1}$. The μFBG were considered as uniform gratings, with a central wavelength of 1555 nm. The phase and amplitude of each μFBG is random. The bandwidth asymptotically approaches 7 nm for a ROGUE length $> 100 \text{ mm}$ for an average μFBG length of $72.5 \mu\text{m}$ 73

Figure 4.6: Calculated spectral shift as a function of the elongation, where the method is compared between the OBR's internal algorithm and the one described earlier, using a number N of padding zeroes. Solid black curve is the applied strain value. (a) is taken right after the cross-correlation, and (b) is taken after applying an additional quadratic fit. Measurements were made using the OBR4600 from Luna with a 42.90 nm bandwidth, the largest available bandwidth on the OBR for sensing. 74

Figure 4.7: RMS noise level in a uniform and stable environment of 300 mm of both unexposed SMF-28 fiber and ROGUE written in SMF-28. The fibers are placed in an insulated box, averaged over 15 measurements. A 30 dB enhanced ROGUE was used for these measurements. 75

Figure 4.8: RMS strain error while stretching the fiber as a function of scanning bandwidth, for both unexposed fiber and ROGUE. The spectral shift is calculated for the 20 μm stretching, across 80 mm of sensing fiber along the 1.15 m fiber length. It can be observed that, using a ROGUE, a scanning bandwidth of only 5.24 nm is sufficient to achieve better accuracy to the one obtained with unexposed SMF-28. A 30 dB enhanced ROGUE was used for these measurements. 76

Figure 4.9: RMS noise level as a function of gauge length, for both unexposed fiber and ROGUE, when placed in an insulated box, averaged over 15 measurements, for bandwidths of 5.24 and 42.90 nm. The gauge length is varied from 0.5 mm to 200 mm. As can be seen, a ROGUE scanned with a 5.24 nm bandwidth requires a gauge length of only 2 mm to beat the noise level of SMF-28 with a 42.90 nm bandwidth and a 10 mm gauge length. A 30 dB enhanced ROGUE was used for these measurements. 77

Figure 4.10 : Strain RMS error calculated over a 20 μm stretching and 80 mm of sensing fiber along the 1.15 m fiber length. (a) Spectral shift accuracy as a function of ROGUE gain (linear scale in y). The ROGUES were written using 21 mW of UV power, by varying the writing speed from 0.05 mm/s to 10 mm/s. The 0 dB gain value represents an unexposed SMF-28 fiber. 78

Figure 4.11: Spectral shift accuracy for three ROGUES of different gains, as a function of optical loss induced *before* the ROGUE by an optical attenuator (logarithmic scale in y). 79

Figure 5.1 Continuous ROGUE writing setup 86

Figure 5.2 ROGUE backscatter signal both shown (a) in the spatial domain, where an improvement in backscattered signal of 20 dB above the unexposed fiber can be observed, and (b) in the spectral domain, where the random structure of the backscattered spectrum is shown, as well as its broad 12 nm full width at first zeros (FWFZ) bandwidth. The PUF generation algorithm is also displayed in (c-d), over a 2 nm bandwidth. From the initial spectrum (c), a discrete derivative is applied, resulting in the signal (d). Positive derivatives are attributed a “1” bit (red), and negative derivatives a “0” bit (blue). The resulting bit sequence is shown at the bottom of (d). 87

Figure 5.3 Hamming Distance distributions, for both (a) the ROGUE-inscribed PUFs and (b) the TF PUFs. In both cases, the *intra* distribution is shown in blue, while the *inter* distribution is in orange. Binomial distribution fits were applied to all the distributions, are displayed in dashed lines. The false positive and false negative probabilities are also displayed, depending on the detection threshold, for both (c) the ROGUE-inscribed PUFs and (d) the TF PUFs. False positive probabilities are in blue, while false negative probabilities are in orange. 89

Figure 5.4 (a) Hamming distance for the *intra* case, for different ROGUE strengths, normalized by the bit signature's length, as a function of the temperature variation. The *inter* case is also shown in the dashed black line. The error bars correspond to one standard deviation. (b) False identification probabilities associated with the normalized Hamming distances. 92

Figure 5.5 Probability of false identification for the ROGUE PUFs, for different PUF lengths and scanned bandwidth. The face color is interpolated from the experimental data points (black squares).....94

Figure 5.6 (a) Fitted binomial p values for both *intra* (blue) and *inter* (orange) distributions, for each of the bits of the 64-bit double representation, for $L = 20$ mm. Only bits 5 to 25 are shown, although the behaviour observed extends on both sides. The dashed line identifies the threshold at which the *inter* distribution reaches $p = 0.50 \pm 0.02$. (b) False identification probability P_{FI} depending on the digitization used, for the first three PUF lengths, with the 5.24 nm scanned bandwidth. The star marker is the probability computed using the derivative algorithm described earlier.....95

Figure 5.7 ROGUE Spectrum (a-c-e) and Cross-Correlation between reference and sample measurements (b-d-f) for different interpolation regimes. Subfigures (a-b) use only the raw data of the 10-mm ROGUE, (c-d) use the raw data using a 40-mm scanned window, including the 10-mm ROGUE and (e-f) use an additional 10^5 padding zeros added numerically. The inset in (b-d-f) displays the central peak, where the improvement in resolution can be better observed. 102

Figure 5.8 Normalized Hamming Distance (a-c-e) and associated false identification probabilities (b-d-f) for different interpolation regimes. Subfigures (a-b) use only the raw data of the 10-

mm ROGUE, (c-d) use the raw data using a 40-mm scanned window, including the 10-mm ROGUE and (e-f) use an additional 10^5 padding zeros added numerically.....	103
Figure 6.1 Output spectra of the random laser at various pump powers. The inset on the left shows the laser linewidth broadening.	108
Figure 6.2 (a) Lévy α parameter fitted from experimental data (solid blue) and laser output power (dashed orange), as a function of input pump power. (b) Histogram of the output power at 5.6 W pump power, sampled over 10 million points. (c) Sample time sequence of the output power, at 5.6 W pump power.	109
Figure 6.3 Autocorrelation of the first 10 μ s for the raw signal (blue) and the 5 LSBs. Inset (a) shows that no correlation exists between the truncated bits after the first delay of 4 ps (since the ACF drops to 0 instantly), while inset (b) shows that taking the 5 LSBs removes all further existing correlation.	110
Figure 6.4 Representation of a 160 Mb bit stream. (a) Histogram displaying the distribution amongst the 5 LSBs. (b) Bit map with the first 500 x 500 random bits shown in a 2D array, where bits “0” are converted to black and bits “1” are converted to white.....	111
Figure 6.5 RF Spectra of the random laser over a 45 GHz span at a 5.6 W pump power. The inset shows the various peaks observed at lower pump powers, while as pump power is increased, the spectrum flatness is also improved.....	113
Figure 6.6 Schematic of the experimental setup, with LAS 1480 nm CW laser, WDM wavelength division multiplexer, HR-FBG highly reflective fiber Bragg grating, OF optical fiber bundle, PD photodiode and OSC oscilloscope.	115
Figure 6.7 Reflexion (blue) and transmission (orange) spectrum of the FBG, showing the 21.5 pm full width at first zeroes (FWFZ) bandwidth, centered at 1571.86 nm.	116
Figure 6.8 Histograms of the output power at increasing pump powers. As pump power increases, the distribution is shown to shift from Gaussian (a), to Lévy-like distributions (b-d), with a return to Gaussian (e-f).	117
Figure 6.9 Comparison of the spectrum when using (a) NZ-DS optical fiber and (b) standard telecommunication fiber.....	119

Figure 7.1 Output spectra of the random laser, both in (a) backward direction and (b) forward direction. At high pump power, the random supercontinuum can be observed. The pump (P), first Stokes (S1) and second Stokes (S2) lines are identified on both spectra. 124

Figure 7.2 (a) Single-channel's optical spectrum, displaying the narrow -10 dB bandwidth of 0.39 nm. (b) RF spectrum of the single channel, displaying a 5.3 GHz bandwidth at -3 dB. (c) Sample time sequence, measured at 40 GSa/s. (d) Histogram of the channel output, sampled over 2 million points. 126

Figure 7.3 Cross-correlation values using (a) the raw data and (b) the same data after applying a self-delayed XOR operation, as a function of the channels' spectral spacing. The region highlighted in red corresponds to spectral separations considered uncorrelated. The cross-correlation is also computed after extraction of a number of LSBs, using (c) the raw data and (d) the same data after applying a self-delayed XOR operation. The *inter* values (dashed line) displays the cross-correlation measured between two separate measurements as comparison. 129

Figure 7.4 Mutual information between the two channels, as a function of the LSB position, where 1 is the least significant bit and 8 the most significant one, for various spectral separations. The mutual information is computed from (a) the digitized raw data and (b) after performing a self-delayed XOR operation. In both cases, the sequence was digitized using 8 bits, and consisted of 10^5 samples. The sequence length is inversely proportional to the mutual information limit of detection, observed in the *inter* case as 10^{-5} 131

Figure 7.5 Cross-correlation values as a function of wavelength detuning, for different channel spectral widths. 134

Figure 7.6 (a) Experimental setup for the random laser, with LAS the pump laser, OC the optical coupler, OF the optical fiber bundle, PM the power meter used to measure the output power, BS and FS, respectively measure the backward and forward spectra of the laser. (b) Experimental setup for the parallel channel demultiplexer. The supercontinuum SC is split in two channels by a 50:50 optical coupler OC, and each channel's central wavelength is defined by its own FBG (Ports 1 and 2). The optical signal of each channel is converted to an electrical signal by a pair of high-speed photodiodes PD (Port 3 and 4). The spectral separation between

the channels can be tuned by applying strain on one FBG, using the translation stages TS, where on top of each one a fiber clamp FC (*FiberViceTM*, *PhotoNova Inc*) holds the fiber. An optical spectrum analyzer OSA monitors the spectral separation between the two channels (Port 5).....136

Figure 7.7 Mutual information for all LSB positions (blue), compared to that bit's probability of being equal to 1 (orange), in the case where there was no spectral separation between the two channels. LSB position 1 is the least significant bit, and 8 is the most significant bit. 138

Figure 7.8 (a) Histogram of a Gaussian distribution, binned using 4 bits. (b) Probability of all bits being equal to 1, depending on the LSB position. 139

Figure 8.1 (a) The FBG fiber triplet, where each fiber is glued in a groove engraved in a nitinol wire, and contains three FBGs. (b) The ROGUE fiber triplet, where the fibers are extruded in a polymer coating. (c) The CDM during articulation and (d) its tip, showing the actuation cables pulling the CDM, and the FBG and ROGUE triplets. (e) The nitinol notch pattern in the CDM design. Taken from [170]. 141

Figure 8.2 Pictures of the CDM bending experiments, taken (a) in free environment and (b) when interacting with an obstacle. The red markers are used with a pair of stereo cameras to provide a ground truth for the shape reconstruction. Taken from [170]. 142

Figure 8.3 (a) ROGUE full-width at half-maximum (FWHM) bandwidth for different inscription's spot sizes (blue), compared with the FWHM of a single grating written with the same spot size (orange). (b) Simulated ROGUE bandwidth (blue) and reflectivity (orange) as a function of the randomness factor α 144

Figure 8.4 Localization effects observed in the ROGUE. The reflectivity (orange) starts following the fit in the dashed black line (which is the equivalent of an exponential decay of the transmission) for the same ROGUE length at which the bandwidth (blue) localizes to that of the single grating. 145

Figure 8.5 (a) Output of the laser as a function of pump power, both with and without the ROGUE, using a 3 km length of standard telecommunications fiber as a cavity. (b) Lévy α parameter with the ROGUE confirming the laser is truly operating in a random regime. Here P_{th} is

defined by the intersection of the linear fit, rather than by the α parameter. (c) Spectrum of the ROGUE's transmission (black) and of the laser while applying different values of strain to the FBG, highlighting the laser's tunability across the ROGUE's broad bandwidth. 146

Figure 8.6 (a) Required apodization voltage to achieve a certain grating strength κ , depending on the assumption of a linear or *sinc* relationship. (b) Resulting applied voltage to achieve a cosine apodization for a 10 mm grating, depending on a linear or *sinc* relationship. 149

Figure 8.7 Comparison of the apodization quality when assuming the apodization voltage and the coupling strength κ_{ac} have a linear relationship (blue) and a *sinc* relationship (orange), both for (a) experimentally measured data and (b) simulated spectra. All gratings are 10 mm long with a cosine apodization, written at a central wavelength of 1558 nm. 150

Figure 8.8 (a) The DFB apodization displayed as the normalized coupling coefficient κ as a function of length, as well as the π phase shift located at 55 mm. (b) Reflection and transmission spectra of the simulated DFB. 152

Figure 8.9 Cavity design for the single-frequency, single-polarization fiber laser, where the pump goes through the Wavelength Division Multiplexer (WDM) coupler and pumps the π phase shifted (π -PS) grating. The active Tm-doped fiber is highlighted in red. In the forward direction, the Fabry-Perot FBG (FPFBG) written in telecommunications fiber reflects the fast-axis mode towards the laser. The fiber is held by two fiber holders, and placed on a metallic plate whose temperature is controlled by two thermoelectric coolers (TEC), to ensure uniform temperature across the entire cavity. The reverse output of the laser is filtered by the WDM coupler, and is split in two ports by a power coupler (PC), where output P2 is used to monitor the output power, while output P1 is used to characterize the optical/electrical spectrum with an optical/electrical spectrum analyzer (O/ESA), or to ensure it is operating in a single mode with the scanning Fabry-Perot (FP) interferometer. An isolator before the PC ensures that no backreflection destabilises the laser, while forward output P3 is cleaved at an angle for the same reason. Taken with permission from [207]. 153

Figure 8.10 DFB output spectra, when operating at a pump power of 361 mW, using (a) an optical spectrum analyzer and (b) a scanning Fabry-Perot interferometer. The mode's full width at

half-maximum (FWHM) of 8 MHz can be observed in (b). Adapted with permission from [207]. 154

LIST OF SYMBOLS AND ABBREVIATIONS

ACF	Autocorrelation Function
ADC	Analog to Digital Converter
ASE	Amplified Spontaneous Emission
AWG	Arrayed Waveguide Grating
BOTDA	Brillouin optical time domain analysis
BOTDR	Brillouin optical time domain reflectometry
CDM	Continuum Dexterous Manipulator
CRP	Challenge-Response Pair
CW	Continuous Wave
DFB	Distributed Feedback
FBG	Fiber Bragg Grating
FUT	Fiber Under Test
FWFZ	Full Width at First Zeros
FWHM	Full Width at Half Maximum
GVD	Group-Velocity Dispersion
HR	High Reflectivity
HTTPS	Hypertext Transfer Protocol Secure
JHU	Johns Hopkins University
LSB	Least Significant Bit
MI	Modulation Instability
NFT	Non-Fungible Token
NIST	National Institute of Standards and Technology
NZ-DS	Non-Zero Dispersion Shifted

OBR	Optical Backscatter Reflectometer
OFDR	Optical Frequency Domain Reflectometry
OTDR	Optical Time Domain Reflectometry
PDF	Probability Density Function
PM	Polarization Maintaining
PRNG	Pseudo-Random Number Generation
PUF	Physical Unclonable Function
RF	Radio Frequency
RFID	Radio-Frequency Identification
RMS	Root Mean Square
RNG	Random Number Generation
ROGUE	Random Optical Grating by Ultraviolet or ultrafast laser Exposure
RSA	Rivest-Shamir-Adleman
SNR	Signal to Noise Ratio
SPM	Self-Phase Modulation
SRS	Stimulated Raman Scattering
SRAM	Static Random Access Memory
TLS	Transport Layer Security
TF	Telecommunications Fiber
UV	Ultraviolet
WDM	Wavelength Division Multiplexing
XOR	Exclusive OR
ZDW	Zero-Dispersion Wavelength

LIST OF APPENDICES

Appendix A	List of publications and awards	191
Appendix B	Mathematical developments	194

CHAPTER 1 INTRODUCTION

Recent developments in high speed telecommunications have affected life on planet Earth in a profound manner. While enabled today by lasers and optical fibres, the etymology of telecommunications simply refers to the act of communicating at a distance, which is far from a novel concept. Smoke signals were used by natives in North America and China to send messages across long distances [1], while ancient African tribes communicated through talking drums [2]. As the legend of Philippiades says, even the original marathon was an act of telecommunications, as a Greek warrior ran the 42 kilometers separating the battleground of Marathon towards the city of Athens to claim Greece's victory over the Persian army [3]. With telecommunications came the problems of privacy and security of the message, which led to complex schemes of encryption, using for instance the concept of the "one-time pad" where a deciphering key was destroyed after delivery. The concept of cryptography (to ensure that the information sent across communications channel remains secret to everyone but the intended receiver) is therefore just as old as telecommunications, with evidence of substitution ciphers such as the Atbash cipher, used by Hebrews hundreds of years before Jesus Christ, or the famed Caesar cipher, used by Julius Caesar himself in private communication [4].

Since the times of Ancient Greece and Rome, both telecommunications and cryptography have greatly evolved, but the intrinsic desire to send information securely across long distances has remained the same. While cryptographic techniques are incredibly more complex nowadays, the computing powers available to potential eavesdroppers have risen just as quickly, which makes the search for novel ways of securing transmitted information a crucial endeavor. This is especially true in our increasingly digital world, where all our communications, financial information and now even our meetings take place on the Internet. While this is very convenient for a large number of reasons, it also exposes us to very severe consequences, if the encryption protocols currently used to protect our information were to be compromised.

1.1 Motivation

Most of today's communications, whether through telephone [5], television [6] or the Internet [7], use optical fibers as a medium to transmit information from one emitter to a receiver. This information is converted to a series of ones and zeros (bits), which are encoded by modulating the

laser light injected into the optical fibers. The information carried by the laser then travels at the speed of light (in glass!) to reach its destination, where it can be decoded by the receiver. However, while it travels through the fiber optic network, this information is vulnerable to ill-intentioned third parties, who might tap into the fiber network and could then eavesdrop on the communications, or even attempt to impersonate other users. To ensure the security of the communications, the binary data is encrypted using advanced cryptographic protocols. Most communications protocols, like the Internet's Hypertext Transfer Protocol Secure (HTTPS) [8], use a public-key cryptography system, where each user generates a pair of cryptographic keys: one public key that can be shared with other users, and one private key that is kept secret. Other users can then use the public key to encrypt their messages, and these messages can then only be decrypted with the corresponding private key. This ensures that only the desired user can decrypt the sent messages. This process is displayed in Figure 1.1(a). Typically, this is done by software, before the digital bits are converted to modulation patterns of the laser light sent in the optical fiber.

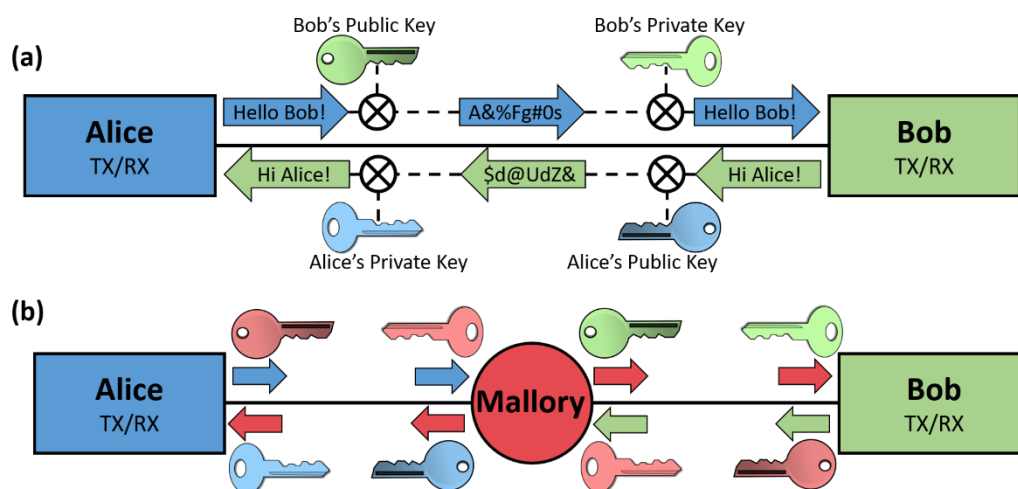


Figure 1.1 (a) Typical communication system between Alice and Bob, who both act as transmitter (TX) and receiver (RX). Alice can use Bob's public key to encrypt her messages to him, which Bob can then decrypt using his secret key, and vice-versa. (b) The malicious attacker Mallory can act as man-in-the-middle, issuing her own set of public and private keys, and can then intercept the communications between Alice and Bob, or even impersonate them.

One of the most widely used public-key cryptosystem is the Rivest-Shamir-Adleman (RSA) algorithm, named for its inventors who designed it at the Massachusetts Institute of Technology in

1977 [9]. It is based on the difficulty of factoring large numbers, and uses the product of two very large prime numbers $n = p \times q$ as the public key, while the private key can be computed from the original numbers p and q . Therefore, anyone with the computing capabilities of factoring the large number n is then able to recover p and q , and therefore of decrypting the private communications. This is the reason why these algorithms use very long numbers that are generated randomly, so that factoring such numbers by brute force requires a prohibitively large computational load. While a potential attacker could harness large computing powers and attempt to break such encryption over extended periods, the RSA algorithm and other public-key cryptosystems have other weaknesses that are potentially easier to exploit.

One of the main weaknesses of such schemes is their susceptibility to man-in-the-middle attacks. In a man-in-the-middle attack, a malicious attacker, usually referred to as Mallory, can insert herself between Alice and Bob and intercept their communication. Mallory can then give Alice and Bob her own public key, so that when Alice wants to communicate with Bob, she encrypts her messages with what she believes to be Bob's public key, but is in fact Mallory's. Then, Mallory can decrypt Alice's communication, and relay it to Bob by encrypting it with Bob's real public key, so that the two can communicate without realizing her presence. This allows Mallory to eavesdrop on their communication, but also to potentially tamper with their messages, and even to eventually impersonate them. This is schematised in Figure 1.1(b). To prevent man-in-the-middle attacks, secure communications protocol typically add an additional layer of cryptographic security. For example, the Transport Layer Security (TLS) used in HTTPS relies on a third party, the certificate authority, who provides digital certificates to each participant. Before initiating communications, Alice and Bob can thus verify each other's identity by asking the certificate authority to authenticate the other's certificate, ensuring they are indeed conversing with each other. As such, the security of the communications against man-in-the-middle attacks is entirely dependent on the certificate authority. If it were to be compromised, then the communication channel would no longer be secure. While relying on a third party to protect against man-in-the-middle attacks can be sufficient for most communications, it is certainly not acceptable for high-stakes information, and there is therefore a need to develop systems that can ensure authentication without relying on a certificate authority.

Another potential point of failure of public-key cryptosystems relies on the random numbers used as the basis of the RSA algorithm. Indeed, random numbers are typically generated by computer algorithms, which only have the appearance of randomness. Rather than being truly random, such algorithms are deterministic, and the numbers they return are thus pseudo-random numbers, and could be replicated by a potential attacker, if he could reverse-engineer the algorithm. This risk is perfectly illustrated by the story of Daniel Corriveau, who won 600,000\$ at Keno (a lottery-like gambling game) at the Montreal casino in 1994, by exploiting a flaw in the system's pseudo-random number generation (PRNG) [10]. After carefully noting the winning numbers every day, Mr. Corriveau observed that certain sequences repeated themselves. When the known sequence began, Mr. Corriveau simply played the numbers he had noted, allowing him to win the 200,000\$ prize three times in a row, before the casino stopped the game after the third time. While the Keno's PRNG system should not have repeated itself before decades, the machine was reset every morning in the same state, and thus repeated the same numbers every day. This allowed Mr. Corriveau to take advantage of it, once he figured out the pattern [11].

While modern-day PRNG systems are significantly more advanced, and should not be expected to fail against such naïve attacks, this story illustrates two important points. First, if there is a pattern to be found, and the stakes are sufficiently high, a highly motivated individual with the time and resources will find this pattern and profit from it. In the case of Montreal's Keno game, the stakes were relatively small. However, breaking RSA encryption is on an entirely different level, as this would jeopardize all secure communications, financial information, industrial secrets, etc. With such high stakes, it is obvious that potential attackers are working on much more complex algorithms to crack this encryption than a college student noting numbers on reams of paper. The second conclusion to take from this story is that the complexity of the system generating the pseudo-random numbers is irrelevant if it is susceptible to human error. In this story, a sequence that should not repeat itself before decades ended up on a daily loop because the engineers who designed the system did not consider that the casino would shut down every night. This is another argument against algorithmic PRNG: these algorithms are designed by humans, and used by humans. If the randomness of the algorithm depends on the humans surrounding it, this adds a supplementary point of failure potentially much more fallible than the algorithm itself.

1.2 Problematic

The problematic that will be addressed in this thesis is the following: How can we improve the security of existing public-key cryptosystems to ensure data confidentiality on the communications channels? This problematic will be investigated along two main axes. In the first axis, we will investigate how an additional physical layer of security can complement existing software-based encryption techniques, resulting in improved security. This physical layer system will rely on the use of unique randomly fabricated fiber Bragg gratings (FBGs) that will act as a fingerprint authenticating the identity of their user, and should be impossible (or at least very challenging) to reproduce, even with the knowledge of their fabrication technique. Over the course of this research axis, the fabrication and implementation of these unique random FBGs will be investigated. As optical fiber is sensitive to temperature and strain variations, it will be important for real-life implementation to characterize how this unique signature will vary as a function of these parameters. Indeed, environmental fluctuations are sure to induce strain or temperature changes in the sensor. It will thus be important to monitor these fluctuations and ensure that they can be compensated.

The second axis of research will be oriented at finding alternate sources of randomness to provide true physical random numbers to generate the secure keys used in public-key cryptosystems. Indeed, as mentioned in the previous section, the deterministic algorithms used in PRNG make it susceptible to reverse engineering, which then compromises the entire system's security. Therefore, researchers have begun developing novel techniques to generate random numbers based on the true randomness of physical phenomena, which are impossible to predict. In this PhD, we will investigate a novel source of randomness for physical random number generation (RNG) based on random fiber lasers. We will explore how this source can be fabricated and optimized to maximize the RNG output, and investigate the theoretical and physical limits of entropy generation.

1.3 Objectives

The objectives of this thesis are separated along the two main research axes identified earlier. The first two objectives will be focused on the development of the novel authentication scheme based on random gratings. The last two objectives involve the development of new sources of randomness

for high-speed random number generation, which can then be used to encrypt the transmitted data. The four objectives are the following ones:

1. Fabricate a novel, noise-based random grating

The first step to develop the novel physical layer security system is by fabricating random gratings that have the desired qualities of randomness, complexity and uniqueness. The goal of this objective is to demonstrate how such gratings can be fabricated, and to properly characterize the fabrication methodology.

2. Demonstrate how this random grating can be used for secure communications

This objective is to explore the ways the novel random grating developed in the previous objective can be used in existing communications systems to improve their security, and to demonstrate that it has all the required characteristics for this application.

3. Demonstrate the random grating's robustness to changing environmental conditions

The goal of this objective is to demonstrate that, while temperature or strain variations will affect the grating's unique signature, these fluctuations can (a) be measured and (b) compensated for, so that the system is robust to changing environmental conditions.

4. Develop novel systems for high-speed generation of random numbers using random lasers

Random lasers have unique properties making them perfectly well suited for random number generation. However, there are only a few demonstrations of random lasers used for generation of random bits, and the RNG rates produced by such lasers are for the moment far below the current state-of-the-art. The goal of this objective is thus to demonstrate that random lasers have the potential for generating random numbers at rates comparable to state-of-the-art chaotic semiconductor lasers.

5. Investigate the limits of the true randomness generated by the random lasers

In order to ensure that the random bits generated by the novel random laser sources developed in the previous objective can be used for secure communications, it is important to ensure that the bits generated are truly random. A detailed evaluation of the quality of the randomness,

combined with theoretical explanations is therefore important to properly evaluate the potential of these novel sources.

1.4 Organisation of the thesis

In the next section of this thesis, a detailed literature review will be presented on the various subjects investigated during this PhD. First, a review of the theory on fiber Bragg grating will be presented, as well as the main methods of fabrication, and the state of the art on random fiber Bragg gratings. Then, the nonlinear optics concepts relevant to the random laser component of this PhD thesis will be presented, as well as the required concepts on fiber lasers, and current state of the art on random fiber lasers. The last sections of this literature review will be focused on the applications targeted during the course of this PhD, namely distributed sensing applications, physical layer security and authentication for the random gratings and random number generation for the random fiber laser.

After this literature review, an introductory chapter will be presented to place into context the articles of this thesis. This chapter will introduce the overall methodology used during this PhD, as well as the links between the articles. After this chapter, the four articles of this thesis will be presented:

- The first article will present the fabrication of the ROGUE (Random Optical Grating by Ultraviolet or ultrafast laser Exposure), as well as its application in distributed sensing. This article addresses the first objective by explaining how those gratings are manufactured. This article also partially addresses the third objective by describing how the ROGUE can be used as a strain and temperature sensor.
- The second article demonstrates how the random gratings fabricated in the first article have all the necessary characteristics to be used as Physical Unclonable Functions. It also provides a proof of concept where the ROGUEs are used as authentication devices, accomplishing the second objective of this thesis. The third objective of this thesis is also achieved through this article, by demonstrating that the sensing algorithm developed in the first article can be used to recover the initial unique PUF signature in the presence of strain

or temperature fluctuations, so that the ROGUE acts simultaneously both as a PUF as well as a sensor.

- The third article presents the first demonstration of a random Raman distributed feedback fiber laser used for random number generation, and how it can generate random bits at speeds comparable to the current state of the art. This article is directly related to the third objective, and also addresses in part the fourth objective.
- The final article investigates the generation of random numbers across multiplexed channels in a slightly modified version of the laser presented in the second article. The alternate cavity design explored in this article addresses the third objective. Additionally, we investigate the ability of various statistical tests found in literature to ensure independence across channels, and demonstrate that the total entropy generated by a single laser source remains constant, regardless of the number of channels it is separated into, thus addressing the fourth objective.

An additional chapter will follow these four articles, presenting results not published in the articles, but that are direct applications of the methodologies and prototypes developed in this PhD. The subsequent chapter will provide a general discussion giving an overview of all the work displayed in this thesis and how it addressed the four objectives identified. Finally, a concluding chapter will mark the end of this thesis.

CHAPTER 2 LITERATURE REVIEW

2.1 Fiber Bragg gratings

Fiber Bragg gratings (FBGs) are periodic structures inscribed in an optical fiber. They consist of a refractive index modulation pattern, typically inscribed in the core of the optical fiber. Every change in refractive index leads to a Fresnel reflection, resulting in a backward propagating wave. In FBGs, due to the typically low refractive index contrast, the reflectivity at each interface is usually very small, but it quickly adds up as a function of the grating's length. Due to the periodic structure of the modulation, there is a specific wavelength where the reflected waves from all the Fresnel interfaces add up constructively. This resonant wavelength is defined as the Bragg wavelength. For sufficiently long gratings, the reflected waves at wavelengths outside the resonance will interfere destructively, resulting in a narrow reflection spectrum centered on the Bragg wavelength. This Bragg wavelength will depend on the inscribed pattern periodicity as well as the propagation characteristics of the mode guided in the optical fiber, more specifically its effective refractive index.

2.1.1 Fiber Bragg grating theory

The refractive index of an FBG as a function of position is defined as

$$n(z) = n_0 + \overline{\Delta n}(z) \left(1 + v(z) \cos \left(\frac{2\pi z}{\Lambda} + \phi(z) \right) \right). \quad (2.1)$$

This refractive index periodic modulation will have an impact on the waves propagating in the optical waveguide, which can be understood by inserting this expression into the wave equation

$$\nabla^2 E = \mu_0 \epsilon_0 \frac{\partial^2 E}{\partial t^2} + \mu_0 \frac{\partial^2 P}{\partial t^2}. \quad (2.2)$$

In single mode fibers, this modulation will allow coupling of the light from the propagating mode towards the counter propagating mode, but only for a specific Bragg wavelength, given by

$$\lambda_B = 2n_{eff}\Lambda. \quad (2.3)$$

While the full mathematical derivation leading to this equation is available in Appendix B, the relationship between the reflected light's wavelength and the index modulation period can also be

understood intuitively, by simply considering the conservation of momentum. Indeed, the reflected wave's momentum $-\beta$ must be equal to the incident wave's momentum β , minus the grating's momentum $2\pi/\Lambda$. This intuitive explanation can also be expanded to coupling between different modes in multimode fibers, for example for long period gratings, where the two modes are co-propagating. In this case, the difference between the two modes' momentum must be the same as the long period grating's momentum to enable coupling between the modes.

The simplest FBG, the uniform FBG, is defined by a constant amplitude modulation and a constant phase, such that $\overline{\Delta n}$, v and ϕ are all constants. The reflectivity of one such grating is defined by the power reflection coefficient $|\rho|^2$. At its peak, the reflectivity of a uniform FBG is

$$|\rho|^2 = \tanh^2(\kappa_{ac}L) \quad (2.4)$$

with κ_{ac} defined as

$$\kappa_{ac} = \frac{n_0 \omega \varepsilon_0 \overline{\Delta n} v \xi \xi^*}{2} = \frac{2\pi n_{eff} \overline{\Delta n} v \eta}{\lambda} \quad (2.5)$$

The uniform FBG's full width at first zeroes (FWFZ) bandwidth is given by

$$\Delta\lambda = \frac{\lambda_B^2}{\pi n_{eff} L} \sqrt{(\kappa_{ac}L)^2 + \pi^2} \quad (2.6)$$

The refractive index profile associated with this type of FBG can be observed in Figure 2.1(a), while its reflectivity spectrum is shown in Figure 2.1(b). On each side of the central reflection lobe (corresponding to the Bragg wavelength), additional side-lobes can be observed. While these side-lobes can be computed from the analytical solution of the uniform FBG, there is also an intuitive explanation for their existence, due to the finite length of the FBG. Indeed, for a weak FBG, the associated reflectivity spectrum can be approximated by the Fourier transform of the refractive index spatial profile (while this approximation is no longer valid for very strong FBGs, for the purpose of the following illustration, this case will not be considered, and the conclusions remain valid). For a uniform FBG of infinite length, the refractive index profile is thus a sinusoidal wave, spanning from $-\infty$ to ∞ . The Fourier transform of a sinusoidal wave is simply a Dirac delta function, centered at the wave's frequency. However, such an FBG is impossible in practice, and a real FBG is bounded by a certain length. Therefore, the refractive index profile of a real uniform FBG is that of a sinusoidal wave multiplied by a rectangular function, whose length equals that of the FBG. As

per the convolution theorem, the Fourier transform of the product of two functions equal the convolution of both functions' Fourier transform. Therefore, the reflection spectrum of a finite FBG is the convolution of a Dirac delta function and a cardinal sine (which is the Fourier transform of a rectangular function). This thus corresponds to a cardinal sine (*sinc* function), centered at the Bragg wavelength, which explains the side-lobes observed in Figure 2.1(b).

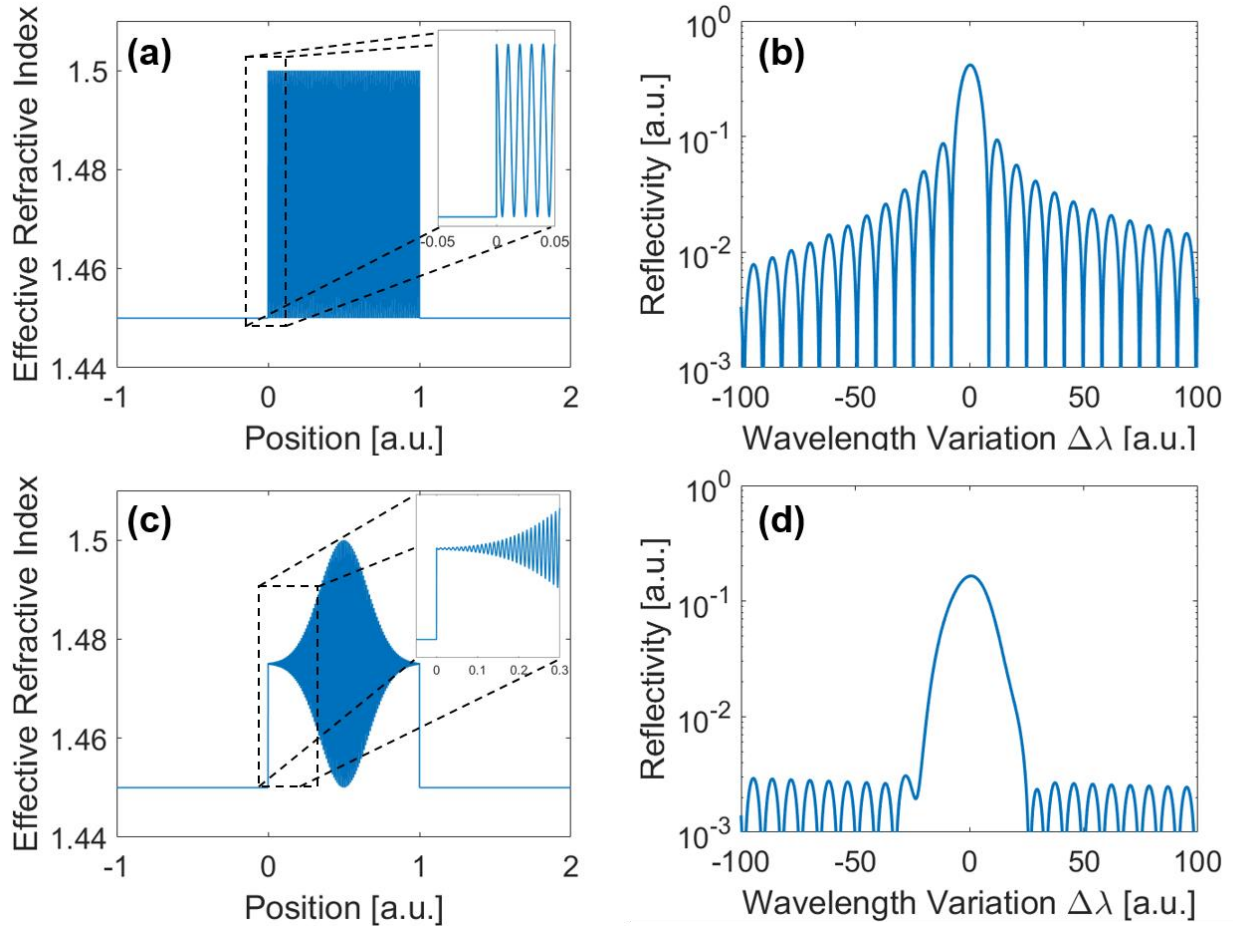


Figure 2.1 (a) Uniform FBG refractive index profile and (b) associated Fourier transform. (c) Apodized FBG refractive index profile, where the visibility $v(z)$ is tuned to induce the apodization, and (d) associated Fourier transform.

These side-lobes are often detrimental to the required spectrum, and thus various techniques have been developed to eliminate or at least mitigate them. One such technique is the use of *apodization*. Indeed, as explained above, the side-lobes of the *sinc* function occur because of the rectangular function delimiting the FBG length. Therefore, by using a different type of function, one could

affect the size and position of these side-lobes. For example, a Gaussian function's Fourier transform is also a Gaussian function. Therefore, varying the amplitude profile of the refractive index modulation allows control over the spectral side-lobes, as illustrated in Figure 2.1(c-d). From Equation (2.1), this can be achieved by one of two ways, either by directly varying the modulation amplitude $\overline{\Delta n}(z)$, or by varying the grating's visibility $v(z)$. In practice, it is much easier to change $\overline{\Delta n}(z)$, as it can be tuned by simply changing the inscription laser's output power, but it has the negative effect of also changing the average refractive index, as the start and end of the FBG will have a smaller average index than the central part. This variation of the average index will, as per Equation (2.3), induce a change in Bragg wavelength along the grating's length, introducing a non-linear *chirp*. While relatively small, this chirp will be detrimental for high-quality FBGs. Therefore, it is preferable to tune the visibility $v(z)$ of the grating instead, as this will keep the average refractive index, and thus the Bragg wavelength, constant. The difference this will have on the apodization quality is displayed in Figure 2.2.

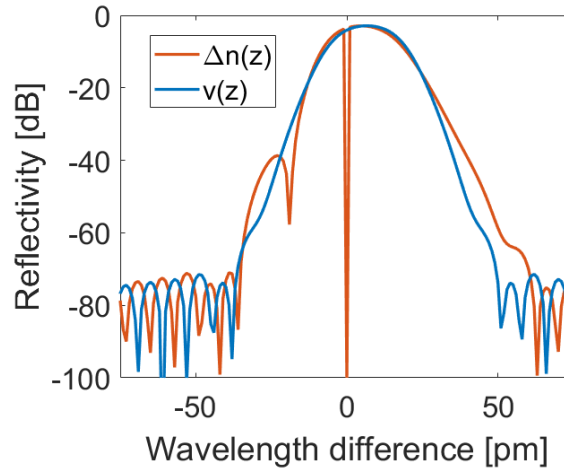


Figure 2.2 Simulated spectra of a 100 mm uniform FBG with a Gaussian apodization, where the apodization is achieved by varying either the refractive index modification $\overline{\Delta n}(z)$ (orange) or the visibility $v(z)$ (blue).

2.1.2 Fiber Bragg grating fabrication

There are many techniques allowing the fabrication of FBGs. While the main results of this thesis are not directly related to the FBG fabrication process, FBG writing was an important part of the work done during this PhD. In this section, the three main FBG fabrication techniques will be

quickly reviewed: writing behind the phase mask, the holographic interferometer and writing point-by-point. But first, it is important to understand how the refractive index of optical fibers can be modified.

2.1.2.1 Laser sources used for FBG inscription

Two main types of laser sources are used to induce refractive index changes in optical fibers: ultraviolet (UV) light and infrared femtosecond pulses. In the first case, lasers at wavelengths ranging from 193 nm (ArF excimer laser) to 266 nm (4th harmonic of a Nd:YAG (1064 nm) semiconductor laser) are typically used, as this is the window where photosensitivity in fibers is the highest. The material used to make standard telecommunications fibers, fused silica (SiO_2), is transparent in this region, but is not sufficiently photosensitive and as such dopants need to be incorporated in the optical fiber core to ensure photosensitivity. Germanium oxide (GeO_x) is the most typically used dopant, but other co-dopants such as boron (B) or tin (Sn) can also be used.

In the case where the desired fiber's dopant concentration is insufficient, hydrogen loading can enhance the photosensitivity. Hydrogen loading is achieved by placing the fiber in a high-pressure hydrogen environment for multiple days or weeks (depending on the pressure), so that the hydrogen atoms can diffuse inside the fiber all the way to the core. However, the OH defects generated after UV exposure have an absorption band at 1.4 μm , close to the C-band (1.5 μm) typically used for telecommunications. Therefore, deuterium is generally favored, as this absorption band is then shifted to 1.9 μm [12]. Fibers with low photosensitive dopants concentration, such as Corning's standard telecommunications fiber (SMF-28), greatly benefit from deuterium loading.

On the other hand, ultrashort infrared pulses do not require the use of specialized fibers. Indeed, the very high power intensity at the focal spot leads to multi-photon absorption, which can then induce refractive index modifications through multiple effects such as generation of plasmas, thermal effects and formation of nan gratings [13]. This allows femtosecond laser sources to be used to write FBGs in fibers that are typically non-photosensitive to UV irradiation, such as pure silica fibers [14]. Most polymer coatings used to protect optical fibers are also transparent to infrared radiations, meaning that the coating does not have to be removed prior to FBG inscription. This allows the fiber to retain its physical properties and robustness, without requiring an additional step of recoating. While certain types of fiber use polymers that are transparent to the UV to allow

UV inscription of FBGs through the coating [15], these are far from the norm. Furthermore, femtosecond laser-written FBGs are more resistant to high temperature (over 900°C) [16].

2.1.2.2 FBG Fabrication techniques

The most simple FBG fabrication technique is called behind-the-mask, as illustrated in Figure 2.3. This technique can be realized both with UV and femtosecond infrared radiation. In this technique, the fiber is placed behind a phase mask, towards which the laser is directed perpendicularly. After propagation through the phase mask, various diffraction orders are created. Typically, phase masks are designed to maximize the amount of energy in the ± 1 orders. The interference between these two orders will create an interference pattern in the fiber, which will result in FBG inscription at a wavelength

$$\lambda_B = n_{eff} \Lambda_{PM} \quad (2.7)$$

with Λ_{PM} the phase mask period. The laser will then scan over the phase mask length to fabricate the entire grating. This technique is very robust and repeatable, and complex FBG designs (apodization, chirp, etc.) can be achieved, depending on the phase mask used. However, this technique is not versatile, and every FBG design must have its own associated phase mask. Furthermore, FBG length is limited by the available phase masks, which become prohibitively expensive for lengths of more than a few centimeters.

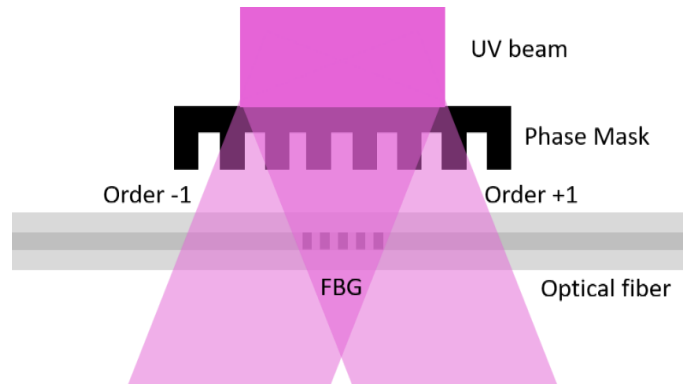


Figure 2.3 Behind-the-mask FBG inscription technique. Orders ± 1 diffracted by the phase mask interfere on the optical fiber, resulting in the FBG inscription.

The same fringe pattern can be achieved by using holographic techniques, by building an interferometer system such as the Talbot interferometer scheme presented in Figure 2.4(a) or the

Lloyd interferometer presented in Figure 2.4(b). These systems typically rely on UV laser sources. In the case of the Talbot interferometer, a phase mask is also used to separate the beam in the ± 1 orders, and they are recombined on the optical fiber by a pair of mirrors. The advantage of this technique is that the FBG wavelength can be tuned by either (a) rotating the mirrors in the Talbot interferometer scheme, or (b) adjusting the incident angle of the laser in the Lloyd interferometer scheme. This will modify the angle of the intersecting UV beams, resulting in a Bragg wavelength

$$\lambda_B = \frac{n_{eff}\lambda_{UV}}{\sin(\theta)} \quad (2.8)$$

where λ_{UV} is the inscription laser's wavelength. Therefore, a single phase mask can be used for multiple designs, which provides versatility. However, the additional complexity makes this type of system less repeatable than the behind-the-mask technique and better suited for research facilities than for mass production. These interferometer designs also require lasers with long coherence lengths to ensure the beams interfere properly. Just as with the behind-the-mask technique, the Talbot interferometer scheme allows the inscription of FBGs longer than the beam size by scanning the phase mask, however these are subject to the same length limitations.

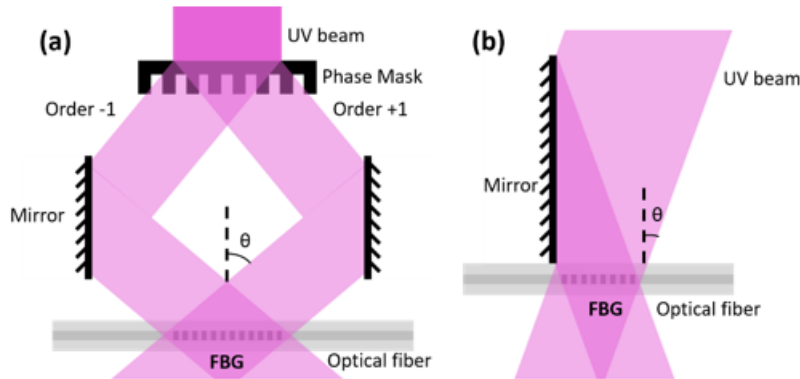


Figure 2.4 (a) Talbot interferometer scheme, where the FBG is inscribed by an interference pattern formed by the two overlapping ± 1 diffraction orders. (b) Lloyd interferometer scheme, where the FBG is inscribed by the interference of the UV beam with its reflection.

Two FBG writing stations were developed by previous students in our laboratory to allow the continuous writing of FBGs of unlimited lengths, based on modified versions of the Talbot interferometer scheme. In both cases, an air-bearing stage moves the fiber under the interference pattern of the two intersecting UV beams. In the first case (Figure 2.5(a)), the phase mask is

mounted on a piezoelectric element. By applying a voltage on the piezoelectric element, the phase mask's phase (and thus, the phase of the interference pattern) follows the displacement of the moving optical fiber, ensuring the FBG does not self-erase. After the fiber has moved a number of periods M , the voltage drops to zero, resetting the phase of the interference pattern to its initial value. The frequency of the applied sawtooth wave will define the Bragg wavelength of the FBG that is written, such that

$$\lambda_B = \frac{2n_{eff}v}{Mf} \quad (2.9)$$

where v is the fiber's velocity and f is the sawtooth wave's frequency. Due to the mechanical movement of the piezoelectric element, the sawtooth frequency is limited to 20 Hz, so for writing speeds greater than 10 $\mu\text{m/s}$, the number of periods M needs to be greater than 1. This process is very similar in the second case (Figure 2.5(b)), where the phase of the interference pattern is controlled by a pair of phase modulators in a push-pull configuration. However, the Pockels electro-optic effect at the basis of the phase modulator does not have the same inertia limitations as the piezoelectric element, allowing the use of much higher sawtooth wave frequencies, so that M can be set equal to 1. This results in higher quality gratings and apodization [17]. Furthermore, the use of phase modulators induces no mechanical movement or vibrations that can affect FBG quality.

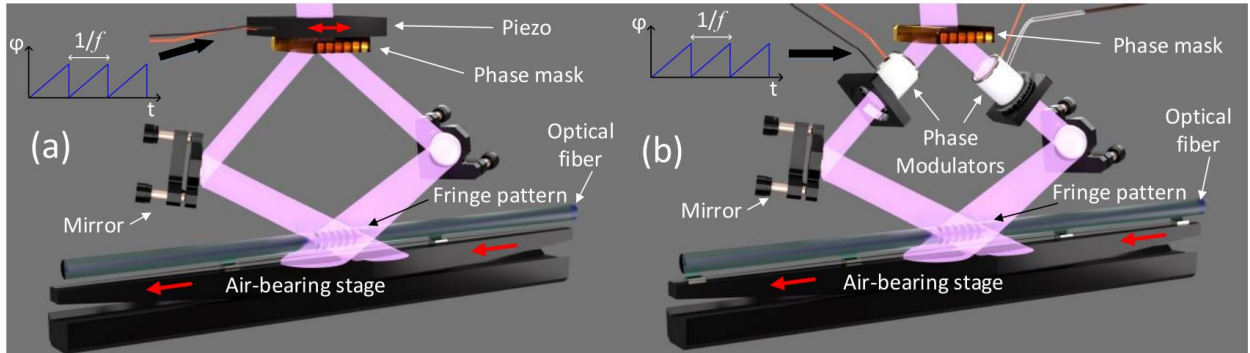


Figure 2.5 Continuous FBG writing techniques, using a modified Talbot interferometer writing scheme. The phase of the interference pattern is tuned synchronously with the fiber movement by applying a sawtooth wave to (a) a piezoelectric element or (b) a pair of phase modulators. Figure taken with permission from [17].

An alternative technique allowing the inscription of continuous FBGs is the point-by-point technique. This technique can be used with UV lasers, but has recently been increasingly explored using femtosecond lasers. As each grating plane is written individually, it is the most versatile technique, allowing the inscription of any grating structure that can be imagined. However, it is highly dependent on precise alignment and accuracy of the translation stage. For this reason, most point-by-point FBG inscription demonstrate higher order FBGs, as this divides the accuracy requirements by the order of the grating. These are also typically relatively short gratings.

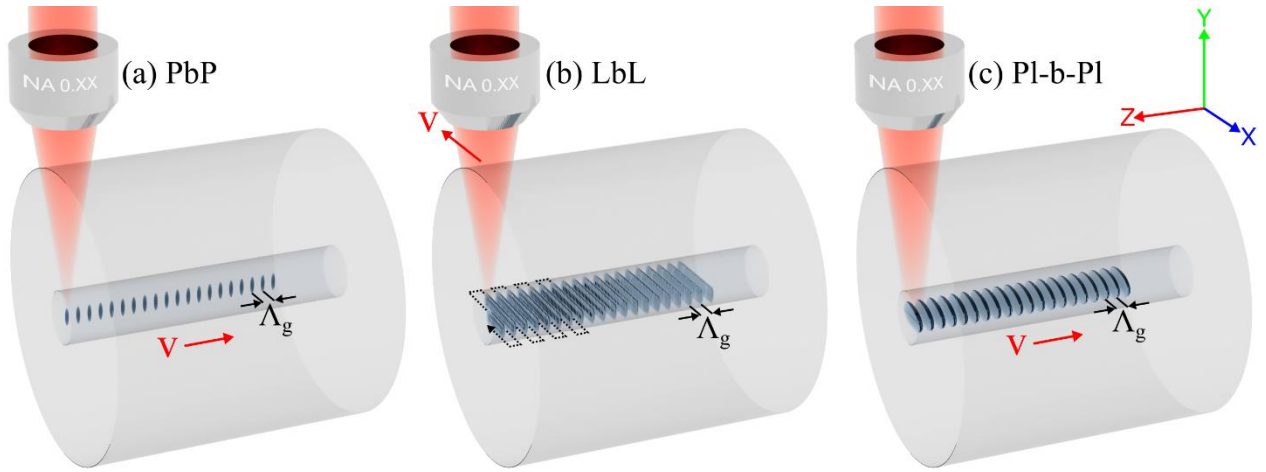


Figure 2.6 Femtosecond laser FBG inscription process, where an ultrafast laser is focused into the core of an optical fiber, allowing the inscription of each FBG period. The gratings periods can either consist of (a) single spots in the point-by-point technique (PbP), (b) lines in the line-by-line technique (LbL) or (c) planes in the plane-by-plane technique (Pl-b-Pl). Taken with permission from [18].

Recent advances in our group demonstrated high-quality, long (>100 mm) FBG fabrication at the first order, with arbitrary complex phase and amplitude profiles using femtosecond infrared laser inscription [19]. However, these impressive results require the capabilities of a unique manufacturing station, with a complex alignment technique and the use of the advanced functionalities of an expensive air-bearing stage controller. Furthermore, femtosecond laser-written FBGs typically suffer from higher losses than UV-written ones, which can be detrimental in many applications. Variants of the point-by-point technique include the line-by-line technique, where the laser is translated in the transverse direction to write a line covering the core diameter, and the plane-by-plane technique, where the laser is translated both in the transverse and longitudinal

directions, resulting in the inscription of a plane covering the entire core area. These various techniques are illustrated in Figure 2.6.

2.1.3 Random fiber Bragg gratings

A fiber Bragg grating is characterized by a periodic modulation of the refractive index. Therefore, a random FBG may seem like an oxymoron, or at the very least counter-productive. However, random gratings have found applications in studying light localization [20, 21], random lasing [22-24] and sensing [25, 26]. Random FBGs are a relatively novel and niche field of study, and as such there is no consensus on a universal definition. A random FBG can be best described as a standard FBG containing a certain number of phase errors that introduce disorder within their ordered structure. Since FBGs are one-dimensional photonic crystals, these phase errors could be viewed as discontinuities in the photonic crystalline structure. This disorder can lead to very unusual and unique properties in photonic crystals, just like in conventional crystals (the observation of electron localization in disordered crystals by Anderson [27] awarded him the 1977 Nobel Prize in Physics).

The first demonstrations of random gratings could be attributed to Shapira *et al.* [20], although their work was concentrated on an array of randomly-spaced uniform gratings, rather than random gratings. Nonetheless, their work demonstrated that, for a sufficiently large random array of uniform FBGs, the overall structure would demonstrate the same effects of localization in 1D than had been observed by Anderson in 3D random electronic lattices. The same type of array was used in later work by Lizárraga *et al.* to demonstrate random lasing, a consequence of light localization [22]. The first demonstration of a continuous random Bragg grating was achieved by Mathieu Gagné from our group, where he demonstrated a continuous 30 cm FBG written in erbium (Er)-doped fiber, and containing randomly spaced random phase shifts [23]. This unique grating could also be used for studying light localization and random lasing. The properties and advantages of random lasers will be discussed in section 2.3.3 of this thesis.

Random gratings based on a femtosecond point-by-point FBG writing technique were also developed by Xu *et al.* [25], where each grating plane was randomly spaced from the previous one. This resulted in an FBG with a very broad bandwidth of over 200 nm. This broad bandwidth was then subdivided into three separate sections, which allowed simultaneous sensing of temperature, axial strain and surrounding refractive index. However, this came with very high losses

(~ 100 dB/m), due to the large scattering and absorption caused by the index modifications. Indeed, this is not surprising, based on the work of Mafi on Anderson localization in partially random gratings and the associated conserved area theorem [21].

Mafi described the idea of a partially random grating as one where the phase difference between two grating planes would be picked from a uniform random distribution between $\bar{\phi} - \alpha\pi$ and $\bar{\phi} + \alpha\pi$, where $\bar{\phi}$ would be the average phase difference between the two grating planes, and α would be the disorder level. A uniform, deterministic FBG would have a disorder parameter $\alpha = 0$, and the Bragg wavelength of that grating would be the one where $\bar{\phi}$ corresponds to π , whereas a completely random grating would have a disorder parameter $\alpha = 1$. Mafi then plotted the transmission of such gratings as a function of average phase difference $\bar{\phi}$, and found that while the curve itself changed depending on the value of the disorder parameter, the integral of such a curve remained constant [21]. Viewed in terms of reflectivity spectrum, it is akin to saying that as that disorder parameter increases, the FBG bandwidth also increases, but its reflectivity decreases, such that the area under the curve remains constant.

Therefore, a completely random grating with $\alpha = 1$ such as the one achieved by Xu *et al.* [25] provides a very broadband enhancement in spectrum, but the enhancement is also diluted over this broad spectrum. This means that in order to provide a meaningful enhancement in signal, the index modification must be very large, which incurs high losses in the form of absorption (due to the damage caused by the high intensity of the femtosecond laser irradiation required to induce such high refractive index changes) and non-directional scatter outside the fiber core due to the shape of this refractive index modification. Using Mafi's theoretical work, it is thus possible to compute the exact amount of randomness required to achieve the desired bandwidth, which would optimize the backscattered signal by concentrating the reflectivity in the part of the spectrum that is desired. However, such gratings would require the ability to precisely choose the position of each grating plane, something that had not really been demonstrated using point-by-point writing techniques until recently by our group [19], but which could be the subject of future work.

2.2 Nonlinear Optics

Nonlinear optical effects play an important role in many of the concepts explored throughout this PhD. For the purpose of this thesis, only the nonlinear effects most relevant to the work presented will be explored. These effects are: stimulated Raman scattering, which provides gain for the lasers presented in Chapter 6 and Chapter 7, modulation instability (MI), which provides entropy to the random number generation process in the same chapters, and Raman self-frequency shift, which generates the supercontinuum obtained in Chapter 7. Before delving into the specific nonlinear effects, let us consider the origin of these nonlinear effects.

It is generally considered that the polarization P induced by an electric dipole is linear with the applied electrical field E . While true in the majority of cases, this approximation is only the first term of a more general Taylor series expansion of the relationship between P and E . This generalized relationship would be

$$P = \epsilon_0 (\chi^{(1)} \cdot E + \chi^{(2)} \cdot E^2 + \chi^{(3)} \cdot E^3 + \dots) \quad (2.10)$$

where $\chi^{(j)}$ is the j -th order susceptibility. The linear susceptibility $\chi^{(1)}$ is the most dominant contribution to P , and the $\chi^{(j)}$ contribution rapidly decreases as the susceptibility order increases. Therefore, observing the higher order effects requires increasingly large electric fields. Additionally, the even orders of the susceptibility are only nonzero for media that lack an inversion symmetry. Since SiO_2 is a symmetric molecule, much like most other glass molecules, the $\chi^{(2)}$ effects (such as second-harmonic generation or the Pockels effect) are non-existent in typical optical fibers, unless their symmetry is somehow broken, for example through optical poling [28]. Since this is not the subject of this thesis, this section will concentrate on third order nonlinear effects, as these are the dominant ones in fiber optics (the intensities in guided optics are generally not sufficiently high for 5th order nonlinear processes to be a concern).

Third order nonlinear effects can be separated into two categories: the elastic effects (four-wave mixing, self-phase modulation and cross-phase modulation) and the inelastic effects (stimulated Raman scattering and stimulated Brillouin scattering). The former are defined as elastic since there is no transfer of energy between the optical field and the medium. On the other hand, inelastic effects involve either giving or taking energy from the medium by interacting with vibrational

excitation modes, either through optical phonons (stimulated Raman scattering) or acoustic phonons (stimulated Brillouin scattering). Stimulated Raman scattering is at the core of many experiments realized in this thesis, and will be presented in Section 2.2.1. Two additional effects will be considered, as they hold special importance to the results observed in this thesis: modulation instability and Raman self-frequency shift. These effects occur due to amplitude fluctuations, and the interaction of self-phase modulation, Raman scattering and group-velocity dispersion, which will be introduced prior to discussing these effects.

2.2.1 Stimulated Raman scattering

Stimulated Raman scattering (SRS) is a very important third order nonlinear effect that relies on the vibrational states of the propagation medium to provide a frequency shift to the photons, either up (anti-Stokes) or down (Stokes shift), which corresponds to that of the vibrational state's frequency. Being a third order nonlinear effect, SRS is not restricted to media with a broken centrosymmetric crystalline structure. However, Raman scattering has a selection rule, where it can only exist in transitions that induce a change in molecular polarizability. Luckily, this is the case for optical fibers, and they are therefore susceptible to Raman scattering effects. SRS is heavily used in fiber amplifier and fiber laser design and fabrication, as it allows transferring the energy of a standard laser pump to an otherwise impossible to reach wavelength. For example, most typical fiber lasers are doped with rare-earth ions to provide gain in a certain region of the spectrum (for instance, ytterbium near 1 μm or erbium around 1.5 μm). However, there are no gain medium that provides gain in between these two regions. Therefore, SRS can be used to bridge the gap between these two wavelengths. Since fused silica's Raman gain is maximal at approximately 13.2 THz, this corresponds at 1 μm to a shift of around 100 nm. To span the entire region from 1 to 1.5 μm , the SRS signal can be cascaded from one order to the next, each time incurring a ~ 13 THz shift in frequency. However, it is important to note that, while SRS allows the fabrication of lasers and amplifiers at wavelengths difficult to reach otherwise, it can also be detrimental, as it can deplete the energy of a high-power laser propagating through an optical fiber. It is therefore very important to understand the mechanisms governing its generation when working with high-power fiber lasers. To understand the SRS effect, it is important to first consider the origin of spontaneous Raman scattering, which can be best understood with the energy diagram presented in Figure 2.7. In the

Raman Stokes scattering presented in Figure 2.7(a), the incident wave, with frequency ω_P , excites a molecule from the ground state g to the excited state n . The wave does not have enough energy to populate the excited state n' , it therefore transits by a virtual state associated with n' (represented by the dashed line). Since the energy difference between the virtual state and the excited state n is smaller than with the ground state g , the Stokes wave ω_S has lower frequency than the incident wave. The reverse is possible, where the photon excites a molecule from the excited vibrational state n towards the ground state g , generating a wave with a higher frequency ω_{AS} , a process which is referred to as the Anti-Stokes emission. Anti-Stokes emission is typically much weaker than the Stokes emission, since, in thermal equilibrium, the population of the excited state is smaller than the population of the ground state. Spontaneous Raman scattering is a relatively weak process with a small cross-section (even in condensed matter, this cross-section is of the order of 10^{-6} cm^{-1} [29]). However, for strong pump fields, the emitted photons by spontaneous Raman scattering will be amplified by the Raman gain provided by the pump, resulting in stimulated Raman scattering (SRS). This amplification quickly builds up as the light propagates through the optical fiber, such that a very important fraction of the pump light can be transferred towards the Stokes wave [30].

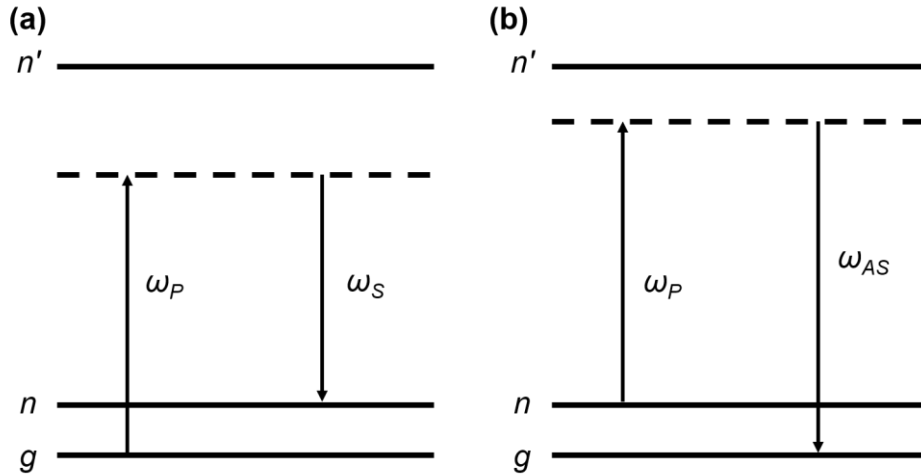


Figure 2.7 Energy level diagram describing, for an optical pump wave ω_P , the Raman scattering generating (a) the Stokes wave ω_S and (b) the Anti-Stokes wave ω_{AS} .

The Raman gain is dependent on the frequency difference between the pump and the Stokes wave. In standard fused silica optical fibers, it is maximal for a spectral detuning of 13.2 THz, and its central peak has a very broad full width at half-maximum (FWHM) of approximately 6 THz [31],

as can be observed in Figure 2.8. Since spontaneous Raman scattering generates photons at all the wavelengths covered by the Raman gain bandwidth, all these photons will be amplified. However, both the spontaneous generation and the stimulated amplification will be maximal for the wavelength corresponding to the Raman gain peak, and as such it quickly becomes dominant over the other frequency components. Past a certain threshold (the Raman threshold), this component builds up exponentially.

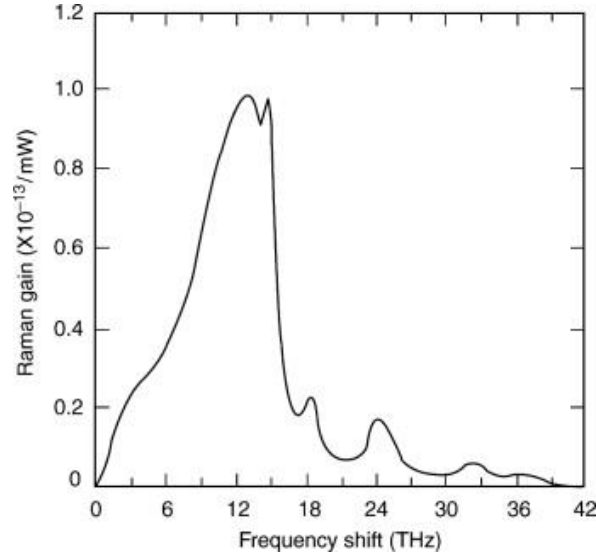


Figure 2.8 Raman gain spectra in silica optical fiber, for a pump wavelength of 1 μm . Figure reproduced with permission from [32], © Elsevier 2005. This figure is adapted from the published work of Stolen and Ippen [33], reproduced here with the permission of AIP Publishing. For CW pumping, the Raman generation of the Stokes wave can be derived from this set of coupled equations

$$\frac{dI_S}{dz} = g_R(\Omega)I_P I_S - \alpha_S I_S \quad (2.11a)$$

$$\frac{dI_P}{dz} = -\frac{\omega_P}{\omega_S} g_R(\Omega)I_P I_S - \alpha_P I_P \quad (2.11b)$$

where I_S and I_P are the Stokes and pump intensities, α_S and α_P are the Stokes and pump fiber losses and $g_R(\Omega)$ is the Raman gain coefficient for a frequency shift $\Omega = \omega_P - \omega$. Near the threshold, pump depletion (the first term on the right-hand side of Equation (2.11b)) can be neglected, as the energy transfer is minimal below threshold. This simplifies Equation (2.11b), which can then be solved analytically to

$$I_P = I_0 \exp(-\alpha_P z), \quad (2.12)$$

with I_0 the initial pump power at $z = 0$. This solution can then be inserted into Equation (2.11a), which can easily be solved to

$$I_S(L) = I_S(0) \exp(g_R(\Omega) I_0 L_{eff} - \alpha_S L) \quad (2.13)$$

with $L_{eff} = (1 - \exp(-\alpha_P L)) / \alpha_P$, the effective interaction length stemming from the pump absorption α_P , which decreases the interaction length. It can be observed that Equation (2.13) requires an input Stokes intensity $I_S(0)$. In the case of a seeded process, where the SRS process is initiated by a second laser at a wavelength within the Raman gain bandwidth, this intensity is a known value. However, when the process stems from spontaneous Raman scattering, it can be approximated as the injection of a single photon at the input of the fiber [31]. Thus, Equation (2.13) can be expressed as the amplification of every frequency component integrated over the Raman gain spectrum, such that, for a single mode fiber

$$P_S(L) = \int \hbar \omega \exp(g_R(\omega_P - \omega) I_0 L_{eff} - \alpha_S L) d\omega \quad (2.14)$$

These equations consider the generation of the Stokes wave during propagation of the pump wave in an optical fiber. This amplification process can also be harnessed to achieve lasing, by building a cavity at the Stokes wavelength. This will be further described in Section 2.3.

2.2.2 Modulation instability

The propagation of optical pulses inside single-mode fibers can be described by the nonlinear Schrödinger equation. For optical pulses with input pulse widths $T_0 > 5$ ps, this equation can be simplified to

$$i \frac{\partial A}{\partial z} = -\frac{i\alpha}{2} A + \frac{\beta_2}{2} \frac{\partial^2 A}{\partial T^2} - \gamma |A|^2 A \quad (2.15)$$

where A is the amplitude of the pulse envelope, α is the fiber loss, β_2 is the group-velocity dispersion coefficient, γ is the nonlinear parameter and $T = t - z/v_g$, which can be understood as time in a frame of reference travelling at the speed of the pulse. The first term describes the effect of the fiber loss, while the second term govern the dispersion effects, and the third term is related to nonlinear effects. A normalized amplitude U can be defined to encompass the fiber losses effect, such that

$$A(z, T) = \sqrt{P_0} \exp(-\alpha z/2) U(z, T) \quad (2.16)$$

The equation (2.15) can thus be rewritten as

$$i \frac{\partial U}{\partial z} = \frac{\text{sgn}(\beta_2)}{2L_D} \frac{\partial^2 U}{\partial \tau^2} - \frac{\exp(-\alpha z)}{L_{NL}} |U|^2 U \quad (2.17)$$

with $\tau = T/T_0$, and the two characteristic lengths

$$L_D = \frac{T_0^2}{|\beta_2|} \quad (2.18a)$$

$$L_{NL} = \frac{1}{\gamma P_0} \quad (2.18b)$$

The magnitude of L_D and L_{NL} in proportion to the propagation length L allows the identification of the pulse propagation regimes. If L is much smaller than both L_D and L_{NL} , then the pulse will be affected by neither dispersion nor nonlinearity. However, when L becomes comparable to either of these parameters (or both), it becomes important to consider these effects.

2.2.2.1 Dispersion in optical pulses

Let us first consider the case where $L \sim L_D < L_{NL}$. In this scenario, the propagation is long enough that dispersion starts being important, but nonlinear effects do not need to be considered. In that case, the last term of Equation (2.17) can be neglected. This equation can be solved by the Fourier-transform, whose solution in the Fourier domain is

$$\tilde{U}(z, \omega) = \tilde{U}(0, \omega) \exp\left(\frac{i}{2} \beta_2 \omega^2 z\right) \quad (2.19)$$

Taking the inverse Fourier transform, the pulse envelope can be obtained in the time domain. As can be seen from Equation (2.19), the different spectral components ω will accumulate different phases as they propagate. This will result in the pulse duration increasing, as, depending on the sign of β_2 , either the longer wavelengths (normal dispersion, $\beta_2 > 0$) or the shorter wavelengths (anomalous dispersion, $\beta_2 < 0$) will propagate faster. In either cases, this will result in a chirp, meaning that the instantaneous frequency of the pulse will change throughout its duration.

2.2.2.2 Self-phase modulation (SPM)

On the contrary, in the case where $L \sim L_{NL} < L_D$, the nonlinear term of Equation (2.17) dominates, while the dispersion term can be neglected. In this case, the solution of Equation (2.17) is thus

$$U(L, T) = U(0, T) \exp(i\phi_{NL}(L, T)) \quad (2.20)$$

where $U(0, T)$ is the normalized field amplitude at $z = 0$, and ϕ_{NL} is the nonlinear phase, defined as

$$\phi_{NL}(L, T) = |U(0, T)|^2 (L_{eff}/L_{NL}) \quad (2.21)$$

with $L_{eff} = (1 - \exp(-\alpha L))/\alpha$. The time dependance of ϕ_{NL} will generate a spectral broadening, as the instantaneous optical frequency is the derivative of the phase. The difference between the pulse's initial central frequency ω_0 and the instantaneous optical frequency is

$$\delta\omega(T) = -\frac{\partial\phi_{NL}}{\partial T} = -\left(\frac{L_{eff}}{L_{NL}}\right) \frac{\partial}{\partial T} |U(0, T)|^2 \quad (2.22)$$

The symmetrical spectral broadening resulting from SPM will depend on the peak value of $\delta\omega$. As can be seen from Equation (2.22), the SPM-induced spectral broadening depends on the effective propagation length L_{eff} , and thus the pulse's spectrum continuously broadens as the pulse propagates. SPM also induces a chirp, as $\delta\omega$ varies along the pulse's duration. Indeed, at the leading edge of the pulse, $\delta\omega$ will be negative, resulting in the generation of longer wavelengths (red shift), while at the trailing edge, $\delta\omega$ will be positive, generating shorter wavelengths (blue shift). Additionally, the shape of the pulse will influence the magnitude of this effect, as evidenced by the derivative of $|U|^2$ with respect to T . Pulses with sharp edges and flat tops will generate a more important chirp located only at the edges, while the chirp occurring in Gaussian pulses will be weaker, but occur throughout the entire pulse duration.

2.2.2.3 Modulation instability

Modulation instability (MI) occurs when a high power CW wave propagates in an optical fiber. The amplitude A of CW light is constant through time, and therefore is not dependent on T . Therefore, the nonlinear phase ϕ_{NL} induced by SPM from Equation (2.21) is also independent of T , which implies that SPM does not induce any chirp or the generation of new frequencies, as the derivative with respect to T will be zero. In this case, SPM would only induce a phase shift, which would be dependent on the input power. The amplitude A could thus be written as

$$A(z) = \sqrt{P_0} \exp(i\gamma P_0 z) \quad (2.23)$$

However, that is only true in the case of a perfectly constant amplitude. To ensure the robustness of this conclusion, it should be tested in the presence of small perturbations. Therefore, a perturbation to the steady-state solution of Equation (2.23) is introduced, such that it can now be expressed as

$$A(z) = (\sqrt{P_0} + a) \exp(i\gamma P_0 z) \quad (2.24)$$

Inserting this solution in the nonlinear Schrödinger Equation (2.15) yields solution for a in the form

$$a(z, T) = a_1 \exp(i(Kz - \Omega T)) + a_2 \exp(-i(Kz - \Omega T)) \quad (2.25)$$

with K the wave number of the perturbation, and Ω its frequency. This solution has a non-trivial solution only for

$$K = \pm \frac{1}{2} |\beta_2 \Omega| \sqrt{\Omega^2 + \text{sgn}(\beta_2) \Omega_c^2} \quad (2.26a)$$

with
$$\Omega_c^2 = \frac{4\gamma P_0}{|\beta_2|} \quad (2.26b)$$

From Equations (2.25) and (2.26), it can be seen that the stability of this solution depends on the sign of β_2 . Indeed, in the case of normal dispersion ($\beta_2 > 0$), K is real for every Ω , and the system is stable against all perturbations. However, in the case of anomalous dispersion ($\beta_2 < 0$), K is imaginary for $\Omega < \Omega_c$. Therefore, from Equation (2.25), the perturbation a will grow exponentially for an imaginary K . As such, the solution found in Equation (2.23) is inherently unstable for propagation in media with anomalous dispersion. This effect is called modulation instability (MI) because it creates a temporal modulation of the amplitude and turns the continuous wave into a pulse train. The MI gain is given by

$$g(\Omega) = |\beta_2 \Omega| \sqrt{\Omega_c^2 - \Omega^2} \quad (2.27)$$

where the additional factor of 2 comes from the conversion from amplitude in Equation (2.25) to power gain, and Ω is the frequency difference with the pump frequency. This gain only exists for $|\Omega| < \Omega_c$. As can be seen in Figure 2.9, the MI gain spectrum is composed of two symmetrical lobes on either side of the pump frequency. The gain is maximal for a frequency of

$$\Omega_{max} = \pm \left(\frac{2\gamma P_0}{|\beta_2|} \right)^{1/2}. \quad (2.28)$$

As can be gathered from Equation (2.28), the position of this maxima is dependent on the fiber nonlinearity parameter γ and the input pump power P_0 , but more importantly, it has the GVD parameter β_2 in the denominator. Therefore, when pumping very close to the zero-dispersion wavelength (ZDW), $|\beta_2|$ will be very small, resulting in a very large Ω_{max} . This large Ω_{max} will result in the generation of a train of ultrashort pulses, whose duration is inversely related to Ω_{max} .

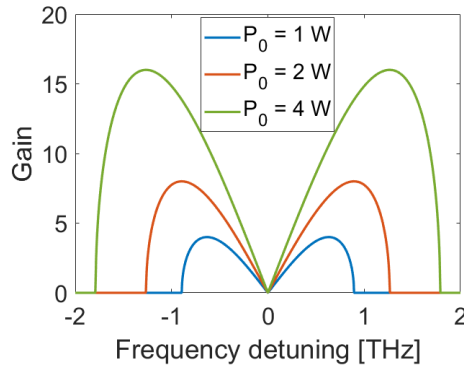


Figure 2.9 MI gain spectrum, for $\beta_2 = -10$ ps²/km, $\gamma = 2$ W/km, and various pump powers.

2.2.3 Raman self-frequency shift

As mentioned earlier, the nonlinear Schrödinger equation formulated in Equation (2.15) is only valid for pulse durations above 5 ps. However, for very short durations, this approximation is no longer valid. The first term that must be added is the term governing the Raman self-frequency shift, also known as intrapulse Raman scattering. To take this effect into account, an additional term must be added to Equation (2.17), resulting in

$$i \frac{\partial U}{\partial z} = \frac{\text{sgn}(\beta_2)}{2L_D} \frac{\partial^2 U}{\partial \tau^2} - \frac{\exp(-\alpha z)}{L_{NL}} |U|^2 U + \frac{\tau_R}{L_{NL}} U \frac{\partial |U|^2}{\partial \tau} \quad (2.29)$$

with $\tau_R = T_R/T_0$, where T_R can be related to the slope of the Raman gain spectrum. Experimentally, T_R has been found to be approximately 3 fs in silica optical fibers near 1.55 μm . This additional term will induce a frequency shift

$$\Delta\omega_R(z) = -8|\beta_2|T_R z / (15T_0^4) \quad (2.30)$$

This frequency shift is dependent on the pulse duration T_0 , and the propagation distance z . It is important to note that the negative sign of the frequency shift means that the pulse's spectrum shifts only in one direction, towards the longer wavelengths side, in contrast with other nonlinear effects such as SPM or MI, which are symmetric on both sides of the pump wavelength. Raman self-frequency is an important effect for supercontinuum generation [34-36], as it can provide broadening of the initial pump's spectrum towards the longer wavelength side.

Raman self-frequency shift, as its name suggests, originates from Raman stimulated scattering. For very short pulses, the spectral width of the pulse becomes sufficiently large than the high-frequency (smaller wavelength) spectral components of the pulse can act as a pump generating Raman gain that amplifies the low-frequency (longer wavelength) components of the pulse. This process continues throughout the propagation of the pulse, where the energy from the high-frequency components is continually transferred to the low-frequency components, inducing the spectral shift characterized by Equation (2.31).

Most pulsed laser sources in optical fiber have pulses whose durations are not short enough for this effect to need to be considered. However, as mentioned earlier, by pumping near to the zero-dispersion wavelength (ZDW), MI will induce a train of ultrashort pulses. The duration of these pulses will be dependent on the pump power and fiber nonlinearity, but most importantly is inversely proportional to the GVD parameter, which can be very small near the ZDW. For example, MI was used in a mode-locked fiber ring laser configuration to generate a soliton pulse train, with 660 GHz repetition rate and 420 fs pulse width [37]. This pulse width would be short enough so that the Raman self-frequency shift term is no longer negligible, which would result in a shift towards the longer wavelengths after propagation.

2.3 Fiber Lasers

Fiber lasers are an important application of both fiber Bragg gratings (FBGs) and nonlinear optics. They were also a very important part of the work done during this PhD. A conventional laser is defined by two important characteristics: a gain medium and a cavity (although cavity-less lasers will be discussed later). In fiber lasers, the cavity is typically based on two reflectors, which can be FBGs, but also fiber couplers, dichroic mirrors, etc., while the gain medium is usually also optical fiber itself. The gain is provided either by rare-earth ions doped in the optical fiber or by

nonlinear optics phenomena, such as the Raman effect introduced in section 2.2.1. Rare-earth doped fibers rely on ions such as erbium, ytterbium or thulium that are doped in the fiber preform before it is pulled into optical fiber. Lasers based on nonlinear optics effects do not require a special fiber composition and can be based on standard telecommunications fiber, although the nonlinear effects are stronger in smaller core fibers, since the power density is higher. Before describing the more complex types of cavities used in this thesis, the more conventional fiber laser cavity based on FBGs will be detailed. Afterwards, the two types of lasers that were fabricated during this thesis will be introduced, i.e. the distributed feedback (DFB) laser and the random laser.

2.3.1 Conventional FBG fiber laser cavity

The most typical fiber laser cavity consists of two fiber Bragg gratings (FBGs), placed on both sides of the gain medium. Sometimes the FBGs are written in the same optical fiber as the gain medium, and sometimes a different type of fiber is used and spliced to the gain medium. Figure 2.10(a) displays such a cavity. In most cases, to ensure single-direction output, one of the FBGs, named the output coupler (OC), is weaker than the other FBG, named the high-reflective (HR) grating. These two gratings form a Fabry-Perot cavity, which has certain modes of resonance. The spectral spacing between these modes is given by

$$\Delta f = c/2n_g L \quad (2.31)$$

where c is the speed of light in the vacuum, n_g is the group index of the optical fiber and L is the distance between the two reflectors. To ensure lasing can occur, the gain spectrum must overlap with at least one of these modes. This is typically not an issue, as usually the gain spectrum is much larger than the spectral spacing between the modes. The lasing threshold is reached when the optical gain is balanced by the optical losses, as demonstrated by Equation (2.32). These losses are the combination of the fiber losses α and the mirror losses.

$$R_1 R_2 \exp(2(G - \alpha L)) = 1 \quad (2.32)$$

where R_1 and R_2 are the reflectivity of the two reflectors and G is the total gain in the cavity. Fiber lasers are always pumped by another pump laser, and the gain is dependent on the pump power. The relationship between gain and pump power is dependent on the type of gain medium used. For instance, for a Raman fiber laser, the lasing threshold can be found from

$$R_1 R_2 \exp \left(-2\alpha_s L + 2g_R \int_0^L P_p(z) dz \right) = 1 \quad (2.33)$$

Another very interesting type of laser cavity is the ring cavity, which is usually fabricated using a fiber Wavelength Division Multiplexing (WDM) coupler. This coupler allows separation of the signal and pump wavelengths. An isolator can be added inside the ring cavity to ensure unidirectional operation of the laser. Like Fabry-Perot cavities, ring cavities can only support certain resonant modes. These modes can be computed by a modified version of Equation (2.31), where the ring cavity circumference replaces the cavity length $2L$. Equation (2.32) can also be adapted to the ring cavity, by replacing the mirror losses with the output coupler's loss. Figure 2.10(b) displays an example of a ring cavity.

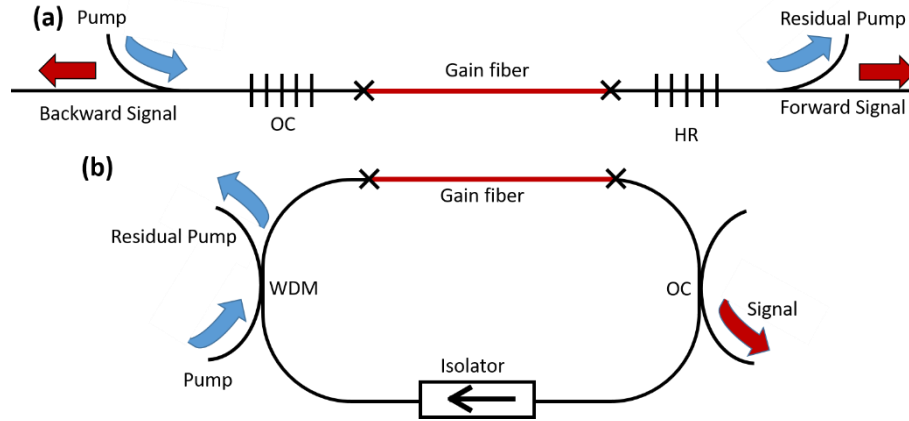


Figure 2.10 (a) Fabry-Perot fiber laser cavity, consisting of two FBGs: a high-reflective (HR) grating and an output coupler (OC), placed on both sides of the gain fiber. (b) Ring fiber laser cavity, where the pump is injected in the cavity through a WDM coupler. Part of the signal exits the cavity through an output coupler (OC), while the rest remains in the cavity for further amplification. An isolator (optional) can be used to ensure single-direction operation.

2.3.2 Distributed feedback (DFB) fiber lasers

Distributed feedback (DFB) fiber lasers use a continuous feedback mechanism instead of a fixed reflection like that of a mirror, where the reflection occurs only at the surface. Fiber Bragg gratings are a good example of distributed feedback, due to the accumulation of small reflections adding up

over the entire grating's length. For example, when pump power is sufficient, the two transmission modes between the main bandgap and the side-lobes of uniform FBGs can start lasing [38].

A special case of the DFB laser that is of particular interest to this thesis is the π -shifted DFB laser. This special type of laser uses a single FBG, where a π phase shift is inserted in the center of the grating. This phase shift induces a resonance within its bandgap that can lase with sufficiently high gain. The resulting structure can be thought of as two FBGs on both sides of a cavity measuring only half a wavelength. However, due to the distributed feedback of the FBG, the length of the gain medium is greater than that half-wavelength, as the light penetrates part of the FBG before being reflected. The advantage of this configuration is that the resonance has a very high quality (Q) factor, which ensures a low lasing threshold and a very narrow linewidth, as well as single-frequency operation.

The Q factor of the laser is maximal when the phase shift is placed in the center. However, this results in laser emission from both ends of the grating, which is rarely desired. To encourage a unidirectional output for the laser, the phase shift is often moved off-center. This is the equivalent of having a shorter (and thus less reflective) grating on one side, acting as an OC, and a longer (and more reflective) grating on the other side, acting as an HR. However, this has the disadvantage of reducing the Q factor of the laser. π -shifted DFB fiber lasers have been fabricated in all sorts of gain fibers, relying on both rare-earth ions [39, 40] and nonlinear effects such as stimulated Raman [41] and Brillouin scattering [42] for gain.

2.3.3 Random lasers

Another special type of lasers that has recently attracted a lot of interest is the random laser. Instead of fixed cavities like the ones discussed above, random lasers use scattering of non-homogenous media as a feedback mechanism. Random lasers have unique properties that make them perfectly well suited for specialized applications. Since they do not rely on a fixed and well-defined cavity, they can be manufactured very cheaply in a variety of media. This property can even be used as a diagnostic tool, for example by using human tissue as gain media, and evaluating the lasing properties [43]. Furthermore, due to their incoherent nature, they can provide speckle-free images when used for imaging [44]. Their distributed feedback also allows them to provide lasing without the time-delay signature typical of standard cavity lasers, which is detrimental for random number

generation [45], as well as other chaos-based systems [46]. Random lasing relies on an important concept named light localization.

2.3.3.1 Light localization

As photons are randomly scattered in the medium, some of them will form closed loops where they will come back to their initial position. If the scattering is sufficiently important, the effects of light localization will start taking place, where light will be localized to these specific modes. This effect is akin to the electron localization effects observed by Philip Anderson in random lattices [27], where electrons would stop diffusing in the presence of enough randomness and remain localized in a certain region. Indeed, in a high-scattering disorganized media, the electron's wavefunction will be scattered in all directions at random points within the lattice. The superposition of all these scattered wavefunctions will add up and cancel each other by destructive interference, such that the electron will not be scattered, and will remain localized.

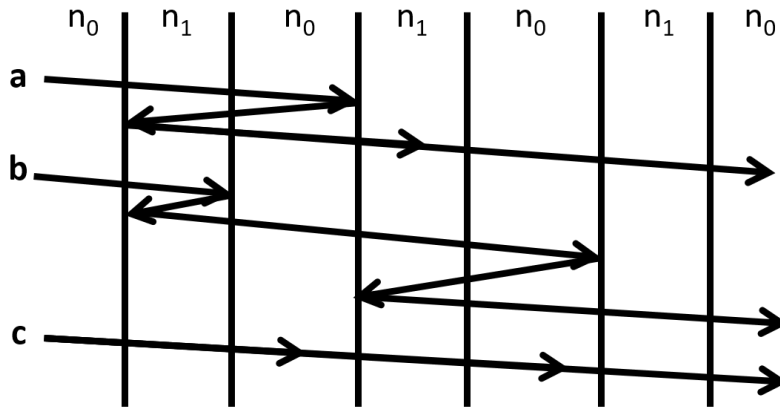


Figure 2.11 Schematic illustrating the glass slides experiment of Berry and Klein [47]. For a sufficiently large number of glass slides, all the light paths including multiple reflections, such as paths **a** and **b**, will cancel each other destructively, leaving only the ballistic path **c** remaining.

In optics, this phenomenon can be best observed in one dimension, by measuring the transmission of light through a stack of transparent glass slides, as was demonstrated by Berry and Klein in 1997 [47]. Indeed, as light propagates through a number of randomly spaced glass slides, at each interface part of the light will be transmitted, with the complex transmission coefficient t , and part of it will be reflected, with reflection coefficient r . After propagating through the entire stack of N

slides, the transmission will be dependent on the ballistic transmission t^N , but also on the multiple reflections occurring within the stack, as schematized in Figure 2.11, and the phase relationships between these multiple reflections. The localization theory claims that, for a sufficiently large number of glass slides, these multiple reflections will cancel each other, so that the transmission will simply have an exponential decay t^N . Indeed this is what was observed by Berry and Klein. A similar behaviour can be observed in 2D by propagating a beam of light in a disordered photonic lattice, composed of a multitude of neighbouring waveguides placed in a non-periodic arrangement [48]. While propagating through the medium, one would expect that the beam would expand, as it couples to adjacent waveguides, and indeed, this is what happens without the presence of disorder. However, when the 2D photonic lattice has a very large disorder, the beam remains collimated, as the light coupling with the other waveguides interferes destructively. It is possible to take advantage of this effect, for instance when designing imaging fiber optics bundle. Indeed, it has been shown that using disordered waveguides instead of a periodic arrangement results in improvement of the quality of the image transport [49]. Light localization also makes random lasers possible.

2.3.3.2 Random lasers

Random lasers can be obtained by combining light localization with a gain medium. Indeed, in optically pumped highly-scattering media, certain modes will be localized, and be amplified, which will lead to lasing. This was first theorized by Vladilen Letokhov in 1968 [50], but only demonstrated in 1994 by Lawandy *et al.* [51]. To do so, Lawandy used a laser dye solution, to which he added suspended microparticles to provide the required scattering to induce localization. The transition between the broadband amplified spontaneous emission (ASE) spectra and the narrow localized mode was then used as the criterion to identify the lasing threshold, as demonstrated in Figure 2.12(a). However, this criterion has since been refined. Indeed, as random lasing became better understood, theoretical work on the random laser's intensity temporal dynamics demonstrated that the probability density function (PDF) of a random laser could be described by a Lévy α -stable distribution, which is a generalization of the Gaussian distribution. This family of distributions is described by the Fourier transform of the PDF in k -space, such that

$$\bar{P}(k) = \exp\{-|ck|^\alpha(1 - i\beta \operatorname{sgn}(k)\Phi(k)) + ikv\}. \quad (2.34)$$

The most important parameter of Equation (2.34) is the Lévy index α , which defines the shape of the distribution, and varies between the values of 0 to 2. A Lévy index $\alpha = 2$ defines a Gaussian distribution, while $0 < \alpha < 2$ implies a Lévy-like distribution, which is a distribution that is characterized by an exponential tail. The other parameters of Equation (2.34) are $\beta \in [-1,1]$, which describes the skewness of the distribution, $\nu \in (-\infty, \infty)$, which describes the location and $c \in (0, \infty)$, which describes the scale, while the function $\Phi(k) = -(2/k)\ln|k|$ for $\alpha = 1$, or $\Phi(k) = \tan(\pi\alpha/2)$ for $\alpha \neq 1$ [52]. The parameter α found from the emission's PDF can thus be used to define the regime of the random laser. Indeed, the spontaneous emission of a random laser below the threshold will have a Gaussian temporal PDF, with $\alpha = 2$, while at the threshold, the Lévy index will drop quickly below 2, and a gradual increase towards a value of $\alpha = 2$ will characterize the operation above threshold. This has been observed in many types of random lasers [53, 54], and is now being recognized as a universal identifier for random lasing threshold [55]. The evolution of the α parameter as a function of pump power is shown in Figure 2.12(b).

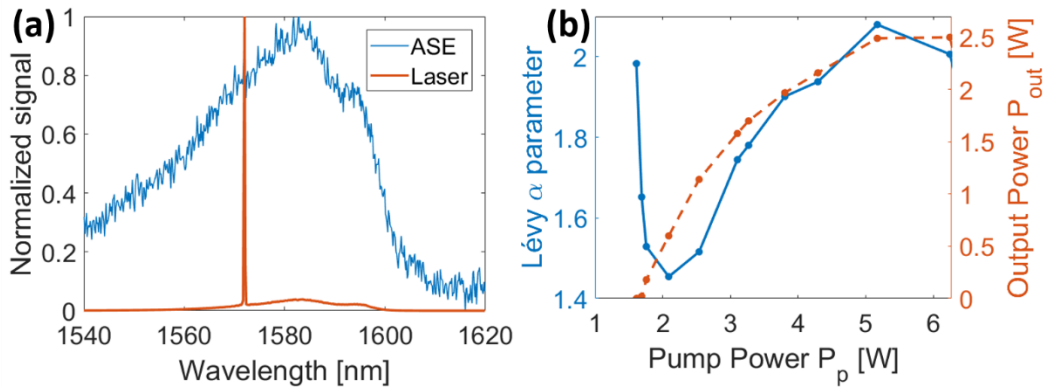


Figure 2.12 (a) Normalized linear spectrum of a random Raman laser, both below (blue) and above threshold (orange) (b) Evolution of both the Lévy α parameter (blue) and the output power (orange) as a function of pump power.

2.3.3.3 Random fiber lasers

The first demonstration of a random fiber laser was achieved by de Matos *et al.* in 2007 [56], and relied on a rhodamine laser dye solution with TiO_2 nanoparticles placed inside a hollow-core photonic crystal fiber. While technically a fiber laser, it is more similar to a dye laser placed inside

an optical fiber. The first demonstration of a “real” random fiber laser was obtained by Lizárraga *et al.* [22] based on localization in a random array of fixed length fiber Bragg gratings (FBGs) written in erbium-doped fiber, shortly followed by a demonstration in our group relying on a random FBG written in the same type of fiber [23]. The same technique was later successfully used with gain provided by Raman stimulated scattering [24].

However, these techniques required the inscription of complex structures into the optical fiber core to provide the scattering necessary to achieve localization. In 2010, Turitsyn *et al.* proposed an alternative technique, relying on the inherent Rayleigh scattering of standard optical fibers instead. This scattering, combined with the nonlinear stimulated Raman scattering, could induce lasing in an optically pumped fiber bundle, resulting in the first random distributed feedback laser [57]. This very elegant technique had the advantage of relying solely on the optical fiber, both for the feedback mechanism as well as the gain. Since this demonstration, random distributed feedback lasers have been demonstrated with other types of gain such as rare-earth doped fibers [58, 59] and Brillouin stimulated scattering [60]. Additionally, Raman emission can be easily cascaded to higher orders, allowing easy access to difficult to reach wavelengths, while also obtaining record-high energy conversion, almost at the limit imposed by the quantum defect. Recent demonstrations have achieved more than 97% spectral purity for a 4th order cascaded Raman random distributed feedback laser [61], and over 90% for the 8th order [62]. Random distributed feedback fiber lasers can operate either in an open cavity scheme, where the Rayleigh backscatter is the unique source of feedback of the laser, or in a half-open cavity scheme, where the cavity is closed on one side by a conventional reflection. This reflection can originate from a mirror, an FBG or simply the 4% Fresnel reflection of a fiber end facet. When fabricating a random distributed feedback laser, it is important to ensure that all fiber ends are properly cleaved at an angle, as otherwise the reflections from the facets can form a cavity, which could lase at a lower threshold, and prevent random lasing.

The random distributed feedback laser can be described by the following set of equations

$$\pm \frac{dP_p^\pm}{dz} = -\alpha_p P_p^\pm - g_R \frac{\nu_p}{\nu_s} P_p^\pm (P_s^- + P_s^+) \quad (2.35a)$$

$$\pm \frac{dP_s^\pm}{dz} = -\alpha_s P_s^\pm + g_R (P_p^+ + P_p^-) P_s^\pm + \varepsilon P_s^\mp \quad (2.35b)$$

where $P_{p,s}$ are respectively the pump and Stokes wave powers, $\alpha_{p,s}$ are the losses at the pump and signal wavelengths, g_R is the Raman gain coefficient, $\nu_{p,s}$ are the frequencies of the pump and signal waves and $\varepsilon = \alpha_s Q$ represents the signal being backscattered by the Rayleigh scattering and captured by the fiber's numerical aperture (with $Q \sim 10^{-3}$ being the proportion of scattered light captured by the core, and is related to the fiber's geometry). This last factor is neglected for the pump, while the $\pm$ refers to the direction of propagation. These equations consider the case of bidirectional pumping; for unidirectional pumping $P_p^- = 0$.

To compute the lasing threshold, instead of using the reflectivity of two fixed mirrors as in a normal cavity, one must calculate the integral of all the virtual mirrors of reflectivity εdz along the fiber's length. For a laser with bidirectional pumping, of length $2L$, this problem can be simplified by considering the symmetry of the fiber. Indeed, this is the equivalent of considering only the region where z is spanning from 0 to L , and placing a 100% reflective mirror at $z = 0$. In that case, the threshold will be found when the gain equals the losses for the roundtrip, such that

$$1 = \varepsilon \int_0^L \exp(-2\alpha_s z + 2g_R \int_0^z P_p(x) dx) dz \quad (2.36)$$

where $P_p = P_p^+ + P_p^-$. This symmetry can be also enacted in real-life, by placing a 100% FBG at the position $z = 0$, resulting in a half-open cavity. This has the advantage of reducing the cavity length by a factor of 2 (or alternatively, reducing the required pump power by the same amount). In the case of unidirectional pumping, the symmetry of the problem is broken. Therefore, to compute the threshold, one must consider all the cavities of length l , formed of two virtual mirrors εdz placed at z and εdl placed at $z + l$. Therefore, the threshold is given by

$$1 = \varepsilon^2 \int_0^L \int_0^{L-z} \exp(-2\alpha_s l + 2g_R \int_z^{z+l} P_p(x) dx) dl dz \quad (2.37)$$

2.4 Strain and temperature sensing

Optical fibers are sensitive to both strain and temperature changes. While this sensitivity can be problematic in certain applications, it can also be viewed as an opportunity, making optical fibers very interesting candidates for sensing applications. Over the years, multiple sensing techniques have been developed. These techniques can be separated into two categories: quasi-distributed sensing methods and fully distributed sensing methods.

2.4.1 Quasi-distributed sensing

Quasi-distributed sensing is achieved through fiber Bragg gratings (FBGs) written at discrete locations along the fiber length. It is referred to as “quasi”-distributed because the sensing can only occur within the FBG’s length, and as such this sensing technique cannot detect what happens in between each FBG. To better understand how FBGs can achieve sensing, let us go back to Equation (2.3), and consider how a change in a parameter X would affect the Bragg wavelength.

$$\lambda_B = 2n_{eff}\Lambda$$

$$\frac{d\lambda_B}{dX} = 2\Lambda \frac{dn_{eff}}{dX} + 2n_{eff} \frac{d\Lambda}{dX} \quad (2.38a)$$

$$\Delta\lambda_B = \frac{d\lambda_B}{dX} \Delta X = \lambda_B \left(\frac{1}{n_{eff}} \frac{dn_{eff}}{dX} + \frac{1}{\Lambda} \frac{d\Lambda}{dX} \right) \quad (2.38b)$$

As can be seen, when a certain parameter X is changed, the Bragg wavelength can be affected either by the dependance of n_{eff} or Λ to this parameter X . For temperature changes, the variation in length ($d\Lambda/dT$) is much less important than the variation in refractive index (dn_{eff}/dT), and can thus be neglected. The opposite is true when applying strain to the sensor, where the variation in refractive index ($dn_{eff}/d\varepsilon$) can be neglected when compared to the variation in length ($d\Lambda/d\varepsilon$) [63]. Therefore, both strain and temperature variations will affect the Bragg wavelength of an FBG. Depending on the type of fiber used and the ambient temperature, the temperature dependence of the FBG’s wavelength will be around 6-10 pm/°C, while its strain dependence will be around 1.2 pm/ $\mu\varepsilon$ [64]. While strain and temperature affect different properties of the optical fiber, their effect on the Bragg wavelength is the same, meaning that it is very difficult for a single FBG to discriminate between these two effects. To achieve this, it is generally necessary to use multiple modalities, such as combining an FBG with a long period grating [65], or by measuring different regions of the spectrum using a very broadband random grating [25].

A typical quasi-distributed sensing scheme uses multiple FBGs written at slightly different wavelengths at different points along the fiber, and uses a broadband source or a tunable laser to scan the entire spectrum. The reflected wavelengths of each FBG can then be used to monitor the strain or temperature fluctuations locally. However, to ensure there is no confusion between the sensors, the wavelengths of each individual FBG must be separated by a certain spectral separation

$\delta\lambda$ corresponding to the expected range of temperature/strain variations. This, thus, limits the number of sensors that can be interrogated in this fashion.

To address this limitation, more advanced techniques have been developed to enable sensing on a larger number of weak FBGs all written at the same wavelength. This makes fabrication of the sensors easier, as each FBG is identical and can therefore be mass-produced without requiring realignment or changing the phase mask in between each inscription. However, it requires a more complex interrogator, which can increase costs. The most typically used technique is optical time domain reflectometry (OTDR), which sends laser pulses in the optical fiber, and monitors the time delay between the launch and return of the pulse to identify each FBG, while the wavelength variation of the FBG is used to monitor strain/temperature. This allowed in one demonstration the measurement of 1,000 identical weak FBGs in the same fiber over a one kilometer sensing length [66]. However, the sensing resolution of this technique is limited by the pulse length, typically in the order of the nanosecond, resulting in a spatial resolution in the tens of centimeters.

2.4.2 Distributed sensing

Optical fibers themselves can be used for sensing, without even requiring FBG inscription. These techniques rely on either elastic or inelastic scattering naturally occurring inside the optical fiber, and are referred to as “distributed” techniques as they can provide sensing at every point throughout the entire length of the fiber. Furthermore, their spatial resolution is given not by the physical spacing in between each sensor, but rather by the interrogator and the modalities used. These techniques rely on even simpler sensors (using only standard, unmodified optical fiber), but increase the complexity of the interrogator. Inelastic scattering-based techniques use either Raman or Brillouin scattering to achieve sensing, while elastic scattering is based on Rayleigh scattering.

Raman-based distributed sensing relies on spontaneous Raman scattering, which is naturally occurring in many media, including optical fibers. It measures both the Stokes and anti-Stokes waves emitted by the optical fiber as a pump light pulse is propagating. As described in section 2.2.1, the anti-Stokes radiation will be dependent on the electrons/vibrational states that are already located in the excited states when the pulse arrives, while the Stokes radiation occurs with electrons or vibrational states that are in the fundamental state, and reach an excited state. At thermal equilibrium, the proportion of excited electrons/vibrational states versus those at the

fundamental level follows a Boltzmann distribution, and is therefore dependent on the temperature. As such, the temperature can be inferred by measuring the ratio of anti-Stokes to Stokes power level [67]. This technique is quite interesting, as it is insensitive to strain, and directly measures the absolute temperature, rather than being a relative measurement like the quasi-distributed techniques discussed above. However, spontaneous Raman scattering is a very weak effect that can be difficult to measure, and the large spectral separation between the pump and the Raman bands means it has to be measured optically, rather than electronically. Additionally, just like in OTDR, the spatial resolution is given by the pulse duration, and is thus relatively large.

Brillouin scattering can also be used to monitor temperature in a distributed fashion. While Raman-based sensing uses the ratio of Stokes/anti-Stokes intensities, Brillouin-based sensing directly measures the Stokes wave's frequency. Indeed, the Brillouin frequency is dependent on the speed of acoustic phonons, which depends on both temperature and strain. The simplest technique, Brillouin Optical Time Domain Reflectometry (BOTDR), is similar to OTDR and Raman-based sensing, in the sense that it uses a pump pulse light, and uses the time delay to measure distances [68]. However, because the Brillouin frequency shift is relatively small (about 10 GHz in silica fiber), this shift can be measured electronically, by beating the scattered Brillouin light with the pump. The beat frequency can then be related to a strain or temperature variation. More complex techniques, like Brillouin Optical Time Domain Analysis (BOTDA) and Brillouin Optical Correlation Domain Analysis (BOCDA) were later developed to improve the sensing and spatial resolution, as well as the signal to noise ratio [69, 70].

Finally, elastic scattering (Rayleigh scattering) can also be used for sensing. Very similarly to an FBG, the Rayleigh backscatter of an optical fiber can be measured by OTDR techniques. Measuring the light intensity can provide insights into the attenuation characteristics of the fiber, which can for example be useful to detect if a fiber is broken, and where [71]. However, the Rayleigh scatter has the same frequency as the initial pump light, and thus the light frequency cannot provide information on the perturbations. Monitoring the temperature or strain variations in the fiber thus requires more complex analysis, by measuring not only the intensity of the backscattered light, but also the phase. Indeed, just like in Equation (2.38), strain and temperature will affect the phase of the propagating light, as this phase is dependent on both refractive index

and length. Therefore, changes in phase of the backscattered light will be related to fluctuations of temperature or strain. This process is called ϕ -OTDR [72].

Alternatively, the frequency spectrum of the backscattered Rayleigh light can be measured by a tunable laser source, through a process called Optical Frequency Domain Reflectometry (OFDR). The Fourier transform of this frequency spectrum can then be computed, to obtain the intensity signal and associated phase as a function of length, just as one would obtain by a ϕ -OTDR measurement. However, in this case, the spatial resolution is no longer limited by the pulse duration, but rather by the spectral resolution of the tunable laser. This yields spatial resolutions in the order of the centimeter or even millimeter [73, 74].

To perform these measurements, the tunable laser source scans the fibre over a certain scanning bandwidth and measures the backscattered amplitude and phase. This results in a signal in the frequency domain I_j , where j represents every point along the frequency scan. This signal can afterwards be converted in the temporal domain by a Fourier transform

$$\tilde{I}_m = \frac{1}{N} \sum_{j=0}^{N-1} I_j \exp\left(-imj \frac{2\pi}{N}\right) \quad (2.39)$$

where N is the total number of data points acquired and m represents the position in the temporal domain. Knowing the group index and light velocity in the fibre, the temporal signal can then be converted in spatial information. This yields information on the reflectivity of the light all along the fibre. The step size of this signal is directly dependent on the frequency scan bandwidth, and is given by

$$L_{res} = \frac{\pi}{2n\Delta k} \approx \frac{\lambda^2}{2n\Delta\lambda} \quad (2.40)$$

with λ the central wavelength of the scan, and $\Delta\lambda$ the total range of the wavelength scan. In order to achieve sensing, the algorithm uses this signal and compares it with a reference measurement made prior to this sample measurement. A certain gauge length window is selected in the fibre, over which an inverse Fourier transform is performed on both reference and sample signals to transfer them both back to the frequency domain

$$I'_j = \frac{1}{2\pi N'} \sum_{m=m_1}^{m_2} \tilde{I}_m \exp\left(ijm \frac{2\pi}{N'}\right) \quad (2.41)$$

where $N' = m_2 - m_1 + 1$ is the number of points selected in the gauge length window. This results in a Rayleigh scatter spectrum that is associated to the specific portion of the fiber identified. Just like for an FBG, strain and temperature variations will induce a shift in this spectrum. To compute the magnitude of this shift, a cross-correlation between reference and sample signals is then performed. The position of the cross-correlation peak gives the spectral shift between reference and sample signals, which can then be associated to a temperature or strain variation, as per Equation (2.38b).

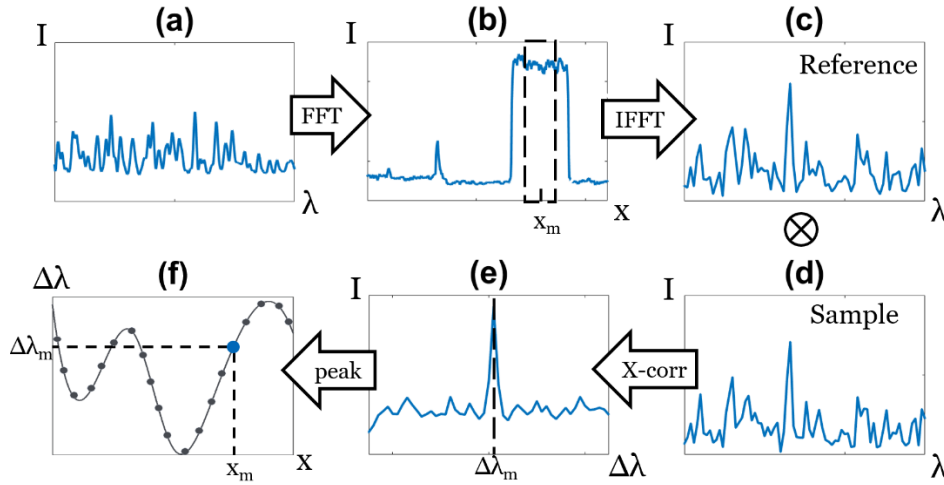


Figure 2.13 OFDR sensing algorithm. (a) A tunable laser scan measures the intensity profile as a function of wavelength (or frequency). (b) A Fourier transform is performed to obtain the temporal intensity profile. A certain gauge length (dashed window) is selected, defining the spatial resolution. (c) An inverse Fourier transform is performed to have the spectrum associated to this specific location. (d) This spectrum is compared with a reference value, by (e) performing a cross-correlation computation. The position of this peak provides (f) the spectral shift for this specific position (blue), which is proportional to strain or temperature fluctuations. This process is repeated along the entire length of the fiber (gray).

The spectral resolution is directly linked to the selected number of points N' through the Fourier transform uncertainty principle. Simply put, the larger the gauge length window selected, the better the spectral shift accuracy can be. However, this will lead to a decreased sensing spatial

resolution [73]. All those steps are then performed for a number n of sensors inside a certain sensing region. The computation time increases linearly with the number of sensors selected, but an increased number of sensors yields a more distributed measurement along the fiber. The maximum number of possible sensors is given by the step size, defined in Equation (2.40). This process is schematized in Figure 2.13.

2.5 Random number generation

Random numbers are heavily used in various domains. They are at the basis of Monte Carlo simulations (named after the famous Monaco casino), where they can help predict uncertain outcomes by probabilistically simulating a wide variety of events based on a number of random variables, and computing the probability of each outcome. However, the quantity of uncorrelated random numbers required to accurately simulate a problem scales very quickly with the problem's complexity, and with the required accuracy [75]. Machine learning algorithms also make use of random numbers to train their models, for example in deep learning algorithms to build their neuron layer model [76], or in decision-making algorithms to improve their computing speeds [77]. Random numbers also play an important part in secure communications systems. Since absolute security can only be implemented by single-use encryption keys [78], absolutely secure communications require the generation of random numbers at the same rate as the communication bitrate, so that the encryption key may be refreshed in real time. The secret keys generated from these random numbers are at the basis of various cryptosystems, such as the famous Rivest–Shamir–Adleman (RSA) cryptosystem [9], but also in other cryptosystems such as the Digital Signature Algorithm proposed by the National Institute of Standards and Technology (NIST) in the US [79], or the Diffie-Hellman algorithm [80]. Most authentication protocols also use in their process randomly generated numbers to prevent replay attacks [81, 82].

However, these complex problems require large quantities of very high-quality random numbers. The importance of the quality of the random bits was made obvious during what is now known as the “Ferrenberg affair”. In 1992, Alan Ferrenberg and his colleagues discovered that Monte Carlo simulations using a well-established pseudo-random number generation (PRNG) algorithm returned solutions to a statistical mechanics problem that differed from the known analytical solution [83]. While the numbers generated by this PRNG algorithm passed all the required

statistical tests, there were still some hidden correlations in the numbers. This caused the Monte Carlo simulation to converge towards inexact solutions. Ferrenberg's publication led to a major shift of mentalities at the time, since Monte Carlo simulations could no longer be trusted on their own, and had to be combined with empirical testing to ensure their solution was correct. This also led researchers to investigate novel sources of randomness to provide higher-quality random numbers that would not have such shortcomings.

2.5.1 Pseudo-random number generation

Pseudo-random number generation (PRNG) uses complex mathematical algorithms to generate unpredictable bit sequences, which can then be used in any application requiring randomness as an input. The idea of generating random numbers from deterministic algorithms for computing is almost as old as the idea of computing itself. Indeed, one of the first PRNG algorithm was proposed by John von Newmann, one of the pioneers of computing. His method relied on an initial seed n -digit number, which was then squared, resulting in a $2n$ -digit number. The n middle digits of this new number were then selected as the new seed for the next iteration, thus producing n random digits at each step. However, von Newmann himself recognized that such deterministic algorithms could not produce *true* randomness. He famously said "Any one who considers arithmetical methods of producing random digits is, of course, in a state of sin." [84]. This did not stop mathematicians and computer scientists to design novel algorithms attempting to generate better PRNG algorithms, such as linear-congruential generators [85] or shift-register algorithms [86]. At the same time, mathematicians formalized statistical tests to ensure the quality of these pseudo-random numbers. Knuth described the first statistical test suite for testing real random numbers [87]. It later became the standard that a random number sequence generated by one of these methods and tested by the Knuth statistical test suite was viewed as sufficiently random. This is why Ferrenberg's discovery was so shocking to the computer scientists' community, 40 years after the first PRNG algorithms of von Newmann. Following his publication, Ferrenberg himself put up von Newmann's declaration about sin over his door, frustrated and discouraged by the failures of the PRNG algorithms [84]. Following the "Ferrenberg affair", more complex statistical test suites have been developed, such as the NIST statistical test suite [88] or the DIEHARD battery of tests [89]. However, even with these more complex tests, there is still a concern about the

existence of undetected correlations within the generated numbers, and empirical testing of the generated pseudo-random numbers in Monte Carlo simulations, with comparisons to known solutions, remains important to ensure their quality.

2.5.2 Physical random number generation

As an alternative to the deterministic algorithms used for PRNG, random number generation (RNG) based on physical phenomena has been investigated to provide better sources of randomness. This is sometimes referred to as *true* or *truly* random number generation, because the source of entropy comes from the inherent randomness of the phenomena used for RNG, and not from an arithmetical method. While interest in them was propelled by the “Ferrenberg affair”, physical RNG systems were investigated decades prior, and are in fact about as old as algorithmic PRNG. Indeed, electrical noise has been used to pick the winners of the United Kingdom’s Premium Bonds since 1956, through a machine called ERNIE (Electronic Random Number Indicator Equipment) [90], which could pick 50 digits every second. However, algorithmic PRNG were preferred, due to their higher random bit rate. Since the regain of interest in physical methods for RNG, multiple techniques for producing them have been investigated. Processes based on quantum properties, such as quantum optics for instance [91], provide absolute certainty over the true randomness of the generated numbers, since they draw their entropy from their intrinsic quantum nature. This is actually how the 5th generation of ERNIE currently operates. However, while the rate at which the random bits are generated is sufficient for some applications (like picking Premium Bonds winners), it is limited to the hundreds of megabit per second (Mbps) or a few gigabit per second (Gbps) [91], which is not sufficient for applications that require a very large number of random bits. Random lasers have also been used for RNG, using the randomness intrinsic to their cavity and mode of operation. However, here too, the bitrates are similar, in the Mbps to Gbps speeds [45, 92]. Currently, most physical RNG systems rely on chaotic semiconductor lasers, which have been demonstrated to generate random bits at rates of hundreds of Gbps [93].

To increase the rates at which random bits are generated, various post-processing steps have been investigated in literature. One of the most typically used technique relies on converting the analog signal containing the random information into a digital signal, using a multi-bit analog-to-digital

converter (ADC). Then, from the multiple bits thus generated, the least significant bits (LSBs) are extracted. This allows to multiply the sampling rate by the number of LSBs, thus increasing the RNG rate [93]. Other more complex techniques rely on deterministic operations on the generated bits, such as a self-delayed exclusive OR (XOR) operation [94, 95], or the use of numerical derivatives to artificially increase the number of extracted bits [96, 97]. While all these physical RNG systems were able to pass statistical tests such as the NIST test suite, it is known from the PRNG research that it is not sufficient to properly ascertain the *true* randomness of a bit sequence. For this purpose, Hart *et al.* published recommendations on the best practices for evaluating the *true* randomness potential of the investigated RNG scheme [98]. In his article, he argued that the entropy content of the physical source should be evaluated, to provide an upper theoretical bound on the RNG potential. Furthermore, he argued against the use of deterministic operations such as self-delayed XOR and numerical derivatives, as they cannot increase the physical entropy of a system, and can thus only produce at best high-quality pseudo-random bits. This is somewhat reminiscent of von Newmann’s comment about sinning.

Following this article, novel techniques to increase the generated RNG rates of photonic systems have been developed, by multiplexing the RNG across multiple parallel channels. This has been demonstrated for instance by combining chaotic lasers into multiple detection channels [99]. Other techniques rely on the separation of a single laser source into independent channels, using some physical property. For example, an optical source with a wide spectrum could be separated into multiple separate spectral channels [100-102]. The same idea can be applied spatially, where the multimode emission of a laser could be separated into individual spatial channels [103], or by separating the polarization of an unpolarized light source [104]. However, while there are recommendations on the best practices to ensure *true* randomness for single-channel RNG, there is no equivalent for multiplexed RNG at the moment.

2.6 Authentication and secure communications

The goal of this thesis is not to generate and describe novel protocols for secure communications and authentication, but rather to develop the tools that could then be used to build such protocols. However, it is important to have a basic understanding of the way these protocols operate, so that the tools developed during this thesis are appropriate for this task. Therefore, this section will

briefly cover the conventional secure communications and authentication protocols, as well as the concept of Physical Unclonable Functions (PUFs), and how they could be integrated to improve the security of such protocols.

2.6.1 Conventional secure communications and authentication protocols

The security of communications channels is generally achieved by encrypting the messages using a secret key. However, this requires both transmitter and emitter to agree on a shared key beforehand, which they can then use for encryption. This is often not possible, especially when the two parties do not know each other. Therefore, secure communications protocols have been implemented to allow key exchanges between two parties over public communications channels. One of the first key exchange protocols was proposed in 1976 by Diffie and Hellman [80], and relies on the discrete logarithm problem. In this protocol, the two participants, Alice and Bob, agree on a modulus p and a base g over a public channel. Alice then chooses a secret integer a , and sends Bob the number $A = g^a \bmod p$, while Bob also chooses his own secret integer b , and sends Alice the number $B = g^b \bmod p$. From Bob's number B , Alice can compute the secret key $s = B^a \bmod p$, and similarly Bob can compute from Alice's number $s = A^b \bmod p$. This way, they both have access to the same secret key s , which can then be used as an encryption key. However, a potential eavesdropper would only have access to p , g , A and B . From these values, obtaining either a , b or s is very computationally expensive, and scales quickly with the number of digits used, so that even a modern supercomputer is unable to compute the encryption key in a practical amount of time.

Since Diffie and Hellman's article describing this protocol, various other protocols have been developed, such as the RSA protocol described in the introduction [9], or the NIST's Digital Signature Algorithm [79]. For both these algorithms, all users have a pair of cryptographic keys, one public that they can share with other users, and one private that they use to decrypt messages that are sent to others after encryption using the public key. All these algorithms are designed such that eavesdroppers need to perform a prohibitive number of computations to obtain the secret key, while it is very easy for the receiver to decrypt the data using their key. However, a brute force attack is not the only potential attack on these types of protocols. Random numbers are at the core of the various secret numbers used in these protocols, and the importance of using a truly random RNG source has been explained in the previous section. If a potential attacker could replicate the

RNG source used to generate the secret keys, the secrecy of the communications would be jeopardized. Another potential issue is the man-in-the-middle attack, where a malicious attacker infiltrates the channel and provides its own public key, pretending to be either Alice or Bob. Preventing this requires the use of additional authentication protocols, and of another layer of trust in certificate authorities.

Certificate authorities (CA) issue digital certificates that link the identity of a user with its public key. Therefore, before initiating communications, both Alice and Bob can verify with a CA that the public key they gave each other corresponds to their respective identity. In web browsers, this is operated seamlessly, and every time a user logs in to a certain web page (for instance, to access banking information), a digital certificate associated with a CA is issued. Before the user is asked to enter his personal information, the web browser sends a query to the CA to verify that the certificate is valid, and that the public key is indeed associated with the user's bank. However, CAs are not perfect, and can sometimes be compromised. Fraudulent individuals have in the past been able to obtain illegitimate certificates from a CA, allowing them to impersonate corporations such as Microsoft [105] or Google [106], giving them the ability to send users false updates. Since communications with CAs are also based on public key cryptosystems, it is vital that CAs protect their own secret keys. Indeed, someone with access to the secret key of a CA could then forge certificates and pretend to be anybody. Therefore, secure key storage is a very important potential point of failure for CAs. Finally, CAs are private corporations that have a track record of not always being transparent when bugs are found, or when certificates are compromised [106]. Therefore, it is worth investigating other authentication protocols that could be more decentralized, which could increase the security of web users' private information.

2.6.2 Physical Unclonable Functions

Physical Unclonable Functions (PUFs), or physical one-way functions as they were first named by Pappu *et al.* [107] in 2002, are physical devices that can be used to generate secure cryptographic keys based on their intrinsic randomness. The first demonstration of PUFs by Pappu *et al.* relied on the interaction of a collimated beam of coherent light and the randomness of a scattering medium. After the beam propagation through the inhomogeneous medium, a speckle pattern is formed on a screen, as schematized in Figure 2.14. This speckle pattern will be dependent on the

light wavelength and angle of illumination, and cannot be easily simulated or duplicated. Pappu then described a protocol for authentication in cryptographic communications systems that would make use of these advantages.

Since this demonstration, PUFs of all kinds have been demonstrated. In optics, PUFs were proposed based on plasmonic nanoparticles [108], laser speckle [109] and polymer optical fiber [110]. However, they raised a lot of interest in silicon electronics, as they can be readily integrated into more complex integrated circuit chips. There are several examples of PUF architectures based on electronic integrated circuits, such as arbiter PUFs [111] or ring-oscillator PUFs [112]. PUFs are generally separated into two categories: the *weak* and the *strong* PUFs. This distinction is established by the number of unique challenges supported by a PUF. Each challenge will result in a unique, unpredictable response, defining a challenge-response pair (CRP). In the case of the speckle-based PUF described by Pappu, the different challenges would be the illumination angle, wavelength, etc., while the response would be the obtained speckle pattern. A PUF that has a small CRP domain (i.e. a limited number of unique challenges and responses) will be defined as a *weak* PUF, while a PUF with a very large CRP domain (so large that it would be impossible for an attacker to entirely map it out) will be considered a *strong* PUF [113]. It is important to note that this definition does not mean that *weak* PUFs are less secure than *strong* PUFs, but rather that they support different types of applications.

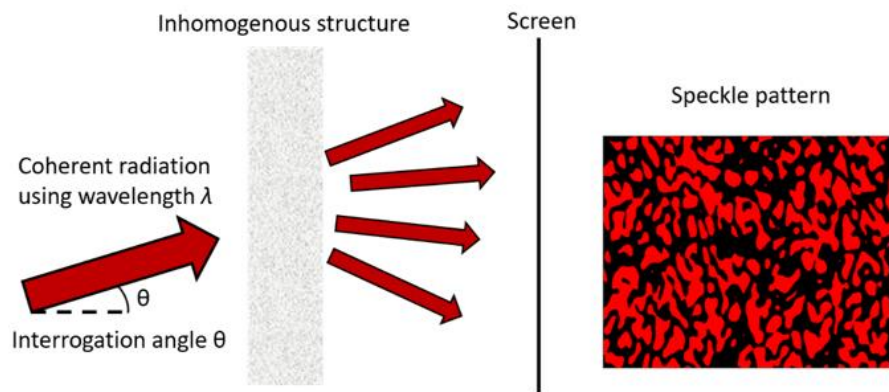


Figure 2.14 Schematic of an optical PUF, relying on the speckle pattern obtained after propagation of coherent radiation through a scattering medium.

One of the most typically used PUF is based on the power-on state of Static Random Access Memory (SRAM) [114-116]. When SRAM is powered on, each bit of the SRAM array can either

exist in the “0” or “1” state. Theoretically, feedback towards either state should cancel out, and the cell should stay in a metastable state between the “0” and the “1” as long as no write operation is applied. However, due to imperfections in the manufacturing process, each cell will have a preferred state when powered on. Thus, when powering on the SRAM, reading the SRAM will result in a repeatable string of “0”s and “1”s that will be unique to this specific SRAM array. This is thus an example of a *weak* PUF that has a single CRP, where the challenge is powering up the SRAM, and the response is the string of bits obtained. This unique signature could then be used as a cryptographic key in secure communications protocols.

However, due to the presence of noise such as environmental fluctuations, certain bits will be less repeatable than others. This is problematic, as if even a single bit of the cryptographic key is wrong, then the entire cryptographic communications system fails. While the least stable bits can be identified and discarded from the cryptographic key generation protocol [117], most SRAM PUF systems use some form of error correction [118]. One of the most interesting technique to generate a repeatable cryptographic key from a noisy response is the use of fuzzy extractors [119]. Fuzzy extractors have been developed to generate secure keys from biometric readings. Just like SRAM or other types of PUFs, biometric readings are also subject to noise, and therefore the same pitfalls are experienced when trying to use them as identifiers. The fuzzy extractor is an operation that takes a noisy information and extracts a reliable key. This operation is error-tolerant, meaning that so long as the input is reasonably close to the original, the extracted key will be identical. While initially designed to be used for biometric authentication, they are perfectly compatible with PUFs since they target the exact same problem. However, one issue with fuzzy extractors is that they are computationally expensive, and most of the computational burden is on the device, rather than on the reader. This led to the development of other algorithms, which were named reverse fuzzy extractors, that shift this burden towards the reader [120]. This is helpful, especially for the development of Internet of Things, where PUFs are envisioned as a prime candidate for authentication of the various connected devices, but where each device has limited computational capacities [115].

In recent years, various protocols based around PUFs have been developed for generation of secure keys and authentication. Most authentication protocols use *strong* PUFs rather than *weak* PUFs. These protocols typically have two phases. First, in the enrollment phase, the server is given the

PUF, and can generate a table of CRPs, which is then securely stored. The PUF is then deployed to the client. Whenever the server is asked to authenticate the client, it issues a challenge from the list of CRPs, and measures the response. If the response is within a certain tolerance threshold, the PUF is authenticated. To avoid replay attacks, each challenge can be issued only once. The *strong* PUFs used in these protocols need to have an extended CRP domain that is large enough so that it cannot be entirely mapped by a potential attacker, which could then reproduce the response of a known challenge [113]. However, there are other types of attacks that can target PUFs without testing all potential challenges by brute force. For example, these types of protocols can be vulnerable to modeling or machine learning attacks, where an attacker tries to reverse-engineer the PUF's behaviour from a subset of CRPs, and then emulate it [121].

The unique signatures of *weak* PUFs could also be used for authentication. However this is potentially less secure, as in this case the only barrier a potential attacker would face is the physical constraints of reproducing or emulating the PUF. Depending on the PUF fabrication process, this can be more or less difficult, but it then becomes a technological challenge rather than a mathematical challenge. Therefore, *weak* PUFs are generally used for cryptographic key generation. Most conventional encryption protocols use digital cryptographic keys that are stored in non-volatile memory. However, if this secure key is leaked or hacked, the entire cryptographic protocol is exposed to potential eavesdropper. Therefore, *weak* PUFs can act as physical key storage to replace the need to store the key in non-volatile memory. Whenever the key is needed, it can be extracted from the PUF and written in volatile memory during the operation, which can afterwards be flushed to ensure it remains secure [113]. This cryptographic key can then be used in conjunction with standard cryptographic protocols, thus enabling encryption/decryption or authentication based on a *weak* PUF [122]. This key storage application is especially relevant for certain entities that place paramount importance in private key security, such as the certificate authorities (CAs) mentioned in the previous section. While this type of protocol ensures that the secure key is not stored in memory, and is therefore not at risk of hacking, it also opens the possibility of a different kind of side-channel attack [123]. Indeed, an attacker that has physical access to the PUF can then also extract the cryptographic key and decrypt the messages. Therefore, proper care must be taken to ensure that nobody but the allowed user can physically gain access to the PUF and read its signature.

2.6.3 Alternative secure communications systems

Other types of secure communications systems have been proposed to improve the security of communications over public channels. One such example is quantum key distribution, which uses entangled photon pairs [124]. In this scheme, both transmitter and receiver measure the polarization of one of the entangled photons, and this information is used to build a random key. This random key can then be used to encrypt messages in the same manner as the other methods discussed previously. An eavesdropper attempting to also gain knowledge of the secret key would disturb the quantum states in such a way that it would be instantaneously detected, allowing evasive action to be taken. While this telecommunication technique is perfectly secure, quantum key distribution systems suffer some major disadvantages. Sending entangled photons over long distances is difficult, and the achievable bitrates are generally low [125]. Since single photons cannot be amplified, the detectors must achieve record low background noise to be able to measure entangled photons over lengths of only a few hundreds of kilometers [126]. Scaling this system to the demands of our telecommunications networks, therefore, remains very challenging.

An alternative secure communication protocol relies on chaos. While chaotic systems are incredibly unpredictable, they are not really random, and two identical systems in the same initial state will evolve in an identical fashion. Such systems can therefore be used to encrypt information within a chaotic waveform that looks random from the outside, but which can be interpreted by an identical system, synchronized to the transmitter. The first demonstrations were achieved using electrical oscillating systems [127], but were limited to relatively low bitrates. In the optical domain, the broader bandwidth of chaotic lasers enabled bitrates comparable to those of telecommunication networks. This was first proposed by Colet *et al.* in the 1990s [128], and was demonstrated in the Athens metropolitan optical fiber network in 2005 [129]. Chaotic semiconductor lasers are typically used for this application, since they can generate very broad chaotic bandwidths. However, the optical feedback used to generate their chaotic operation leaves a time-delay signature, which can be exploited by a potential attacker to reproduce the lasers. Indeed, if the lasers used for encryption were reverse-engineered, an attacker would be also able to decrypt the encoded messages, putting the security of the transmission at risk. As such, even though these alternative protocols have great potential for improving the telecommunications' security, they also have drawbacks that make their implementation challenging.

CHAPTER 3 METHODOLOGY

This chapter describes the methodology used during this thesis. While each article has a dedicated section to its own methodology, the goal of this chapter is to provide an overall view on the main methodology that guided this PhD, as well as detailing the different instruments and protocols that were used. The last section of this chapter will describe the organisation of the articles in the following chapters.

3.1 Methodology of the overall research

3.1.1 FBG Writing

Fiber Bragg grating (FBG) fabrication was an important part of this PhD. Most of the FBGs used throughout this thesis were fabricated using the Fabulas writing station, a state-of-the-art FBG writing setup that was developed by previous students of my laboratory, and demonstrated FBG inscription of unparalleled quality [41, 130, 131].

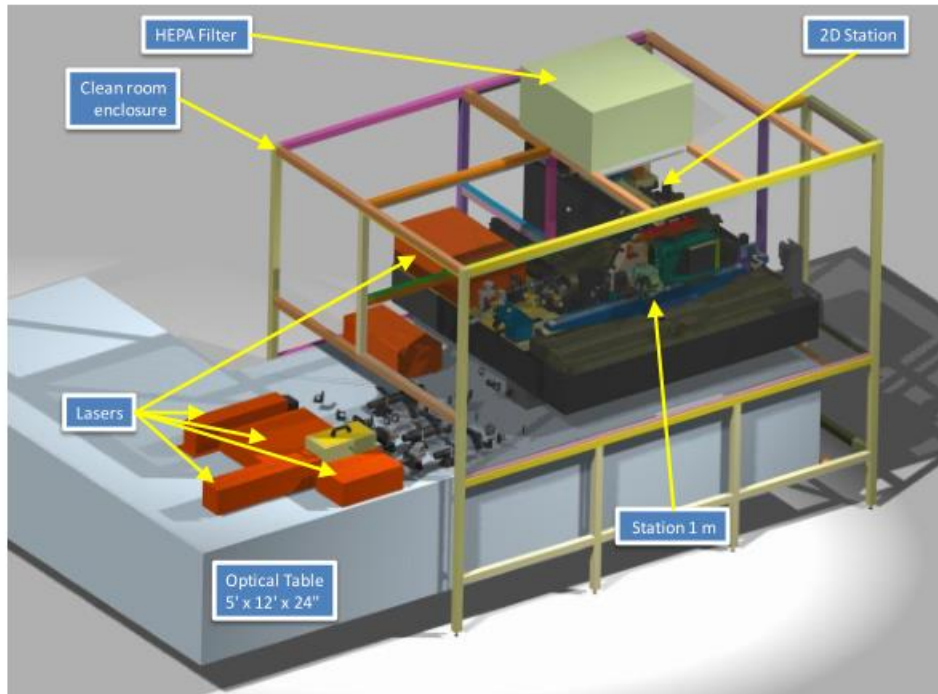


Figure 3.1 Schematics of the Fabulas installations [132]

The Fabulas FBG writing station is part of the Fabulas installations, which also includes a 3D laser-based micromachining station that can be used for laser ablation and waveguide inscription. The Fabulas facilities (shown in Figure 3.1) have access to a large number of lasers, which can be used on either station. These include a PHAROS femtosecond laser (Light Conversion), which emits 250 fs pulses at a wavelength of 1030 nm, and two solid-state UV lasers, a 266 nm wavelength laser originating from the 4th harmonic of an Nd:YVO₄ laser (Spectra-Physics) and a 213 nm wavelength laser originating from the 5th harmonic of another Nd:YVO₄ laser (Xiton Photonics). While FBGs can be inscribed in optical fibers by all these lasers, and they were all used by the author at some point during the course of this PhD, the work presented in this thesis relied on the latter, due to the enhanced photosensitivity of germanium-doped silica fiber to 213 nm light [133].

The Fabulas FBG writing station can be used with multiple writing heads, depending on the type of laser used for the inscription, and the complexity of the required FBGs. These writing heads include one dedicated to femtosecond laser inscription, using a specially designed microscope objective for focusing into the core of the optical fiber, as well as multiple writing heads for continuous UV laser inscription based on a modified Talbot interferometer scheme described in section 2.1.2. As mentioned in this section, the phase modulation is achieved either by a piezoelectric element, on which the phase mask is mounted, or by electro-optic phase modulators in a push-pull configuration. All the FBGs presented in this thesis were fabricated with the writing head relying on piezoelectric-based modulation. This writing scheme is presented in Figure 3.2.

In this station, a meter-long air bearing stage (Aerotech) allows smooth translation of the fiber as it is moving under the illuminating UV beams. An optical Fabry-Perot encoder (Renishaw) provides a closed-loop feedback on the stage's position with nanometer resolution. The phase modulation is achieved by applying a sawtooth voltage on the piezoelectric element, so that the interference pattern inscribed in the fiber remains in phase as the fiber moves. In the current configuration, the maximum voltage that can be applied to the phase mask corresponds to a phase change of 19 periods, while its cut-off frequency is limited to 20 Hz. Applying a higher frequency on the piezoelectric element induces a degradation of the sawtooth wave, which results in poor FBG quality. Apodization of the FBG is achieved by tuning the visibility v of the grating, by applying an additional phase function on the piezoelectric element. In this case, either a sawtooth or triangle wave is sent to the phase mask at the highest frequency possible (here 20 Hz), with an

amplitude depending on the level of apodization required. When using a peak-to-peak amplitude $V_{2\pi}$ corresponding to the voltage required to achieve a 2π phase change, the piezoelectric element will induce self-erasure of the grating ($v = 0$), while a zero amplitude will result in a visibility $v = 1$. To achieve a grating with a Gaussian apodization for instance, the amplitude of this apodization function is continuously updated as the grating is written. The relationship between the amplitude of the apodization function and the grating's visibility is further detailed in section 8.3.1.

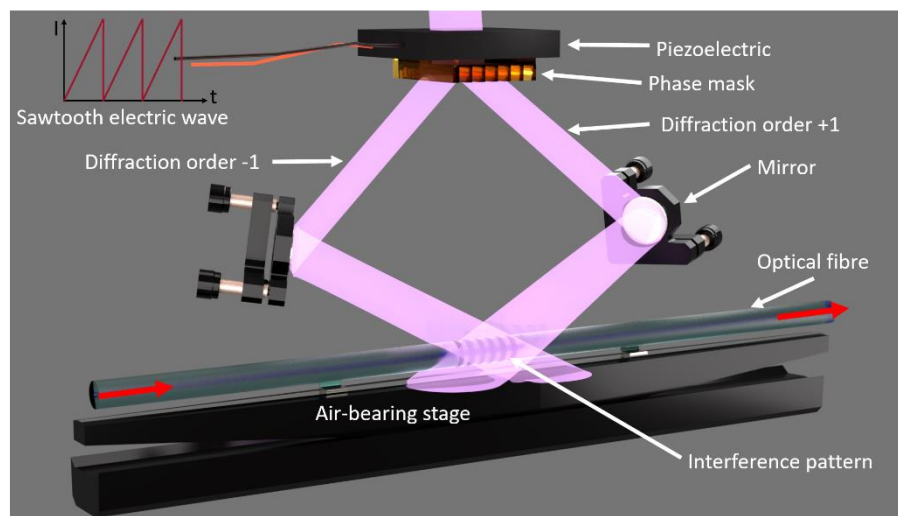


Figure 3.2 Fabulas FBG writing station, shown here with the piezoelectric-based modulation

The phase of the FBG inscribed can be also changed either by tuning the voltage applied on the piezoelectric element, or by changing the speed of the air-bearing stage. Indeed, to fabricate π -shifted gratings, a DC voltage corresponding to a π phase change ($V_{2\pi}/2$) can be applied to the piezoelectric element during the writing process, to open a bandpass within the grating's bandgap. This is used to fabricate distributed feedback lasers for instance. Similarly, chirped gratings can be fabricated by this writing station, either by slowly varying the velocity of the stage, or the frequency of the sawtooth wave applied on the piezoelectric element. Changing either of these parameters, as per Equation (2.9), changes the wavelength of the inscribed grating. As such, a linear dynamical variation of one of these quantities results in a linearly chirped grating.

To achieve random grating inscription, the same FBG writing station is used, but by replacing the sawtooth function with a noise signal. This results in the inscription of noise-based gratings, which were named Random Optical Grating by Ultraviolet or ultrafast laser Exposure (ROGUEs). Indeed, while these gratings were inscribed by a UV laser, they can just as easily be fabricated by a

femtosecond laser (and indeed, this was demonstrated by my colleague Anthony Roberge in later work [18]). In this UV-based writing station, the strength of these random gratings depends on the random phase function that is applied on the piezoelectric element. Indeed, if no function is applied, the gratings would simply self-erase as the fiber is translated under the interference pattern formed by the intersecting UV beams. Experimentally, the gratings' strength was maximal when the noise signal's amplitude was largest, and when its frequency was highest (up to the 20 Hz limit, after which the gratings' strength decreased, as driving the piezoelectric element above its cut-off frequency induces damping of the noise signal). While a good proof of concept, it is somewhat counter-intuitive to use a state-of-the-art FBG writing station to write noise-based gratings. Furthermore, the length of the ROGUEs that could be inscribed with this station is limited to one meter by the linear stage. Therefore, a dedicated ROGUE writing station was later assembled, and is described in Chapter 5.

3.1.2 OFDR Measurements

OFDR was used as a tool at multiple points during this thesis, either for FBG characterization, distributed sensing measurements or PUF signature measurements. In all cases, a commercial optical backscatter reflectometer (OBR 4600, Luna Inc.) was used. The optical circuit of this instrument is displayed in Figure 3.3. As explained in section 2.4.2, a tunable laser source scans a certain wavelength span, and the backscattered signal is polarization-separated and measured by interferometry. This results in a measurement of the complex transfer function of the device under test (DUT) $H(\omega) = \rho(\omega)e^{i\varphi(\omega)}$, with phase φ , amplitude ρ and polarization information. The transfer function is essentially the DUT's complex reflectivity spectrum. A Fourier transform is then computed to recover the DUT's impulse response $h(t)$, i.e. its amplitude and phase profile as a function of length. Performing an inverse Fourier transform of specific portions of the fiber allows the computation of this section's reflection spectrum. This system allows characterization of optical fiber components with a spectral resolution of 0.1 pm, and covers the C and L bands (1530 to 1610 nm). This instrument also has a built-in distributed sensing software that can be used to measure strain and temperature fluctuations.

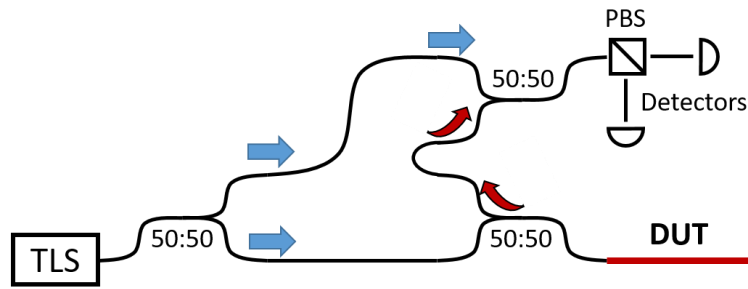


Figure 3.3 Optical circuit of the commercial OFDR instrument (Luna OBR 4600). A tunable laser source (TLS) is separated in a Mach-Zehnder interferometer scheme, with the device under test (DUT) in one arm. The interference between the reflection from the DUT and the other arm of the interferometer is separated by a polarization beam splitter (PBS), and the amplitude and phase of the two polarizations is measured by detectors.

The distributed sensing is achieved by computing the cross-correlation of a reference spectrum with a sample measurement, at each sensing point along the DUT's length. During characterization of the ROGUE's capabilities for distributed sensing, it was discovered that the OBR's built-in sensing software had a nonlinear response for very small perturbations (this is discussed in detail in section 4.4.1). To correct for this nonlinearity, a custom sensing software built in Matlab was designed to properly characterize the ROGUE's sensitivity and noise level in post-processing, based on the raw data measured by the OBR. This algorithm is based on interpolation of the measured signal, and an additional quadratic fit is performed on the interpolated data for more accuracy. The algorithm is described in detail in Chapter 4.

The PUF signatures were also measured by the same OFDR instrument. Here the spectral response of a PUF is converted into a digital fingerprint that is unique to this specific PUF. In a similar fashion, enrollment of the PUF is achieved by a first reference measurement, and authentication of the PUF is achieved by comparing the subsequent measured signature with that of the reference. A LabView program was designed to automate the PUF measurement, sending commands directly to the OBR, and converting the response into the digital signature. This enabled the characterization of the temporal stability of the PUF signature across multiple measurements. The Matlab software developed for distributed sensing was also used to compensate the temperature and strain fluctuations experienced by the ROGUE PUFs, ensuring their unique signature could be recovered

even with large environmental changes. The PUF measurements and the data processing algorithm are described in Chapter 5.

3.1.3 Random Raman fiber laser

The two random Raman fiber laser schemes developed during this PhD rely on a half-open distributed feedback cavity. A conventional reflector closes one side of the cavity, while the feedback from the other side of the cavity comes from the inherent Rayleigh backscatter of standard optical fiber. This optical fiber also provides the Raman gain used to generate random lasing. This cavity is pumped by a commercial 1480 nm CW laser (IPG Photonics), which relies on the cascaded Raman Stokes conversion of an ytterbium fiber laser. In the first iteration, this reflector was a highly-reflective fiber Bragg grating, written at a specific wavelength corresponding to the peak of the Raman gain of the pump laser (near 1580 nm). This wavelength defines the laser emission, and can be tuned to longer wavelengths by straining the FBG.

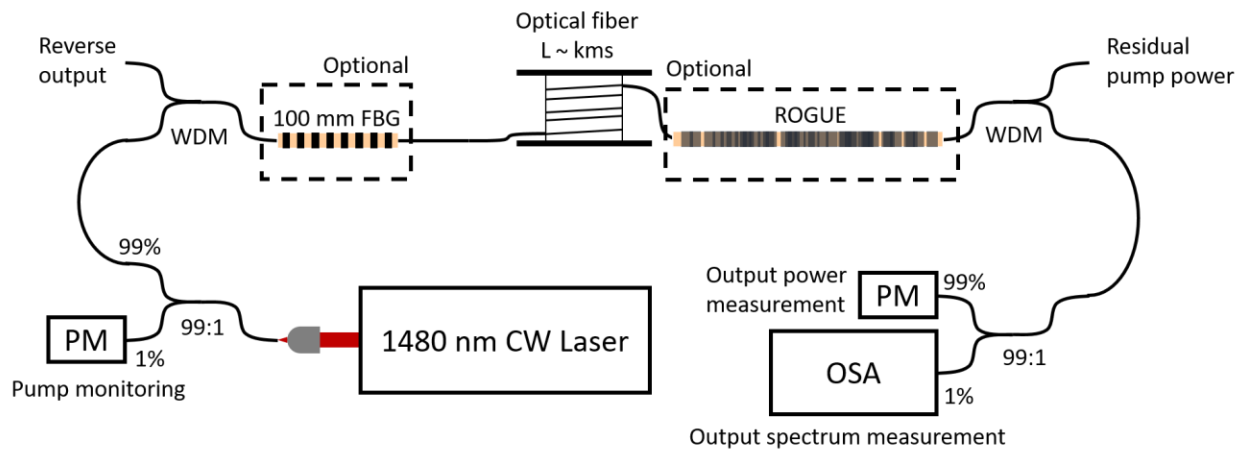


Figure 3.4 Random distributed feedback Raman fiber laser cavity. The cavity can be closed on one side by a highly reflective FBG, or alternatively can be removed, in which case the feedback is replaced by the 4% Fresnel reflection of a fiber end facet. All other fiber end facets are angled-cleaved to avoid parasitic reflections. The random feedback is provided by the optical fiber bundle, and can be enhanced by the addition of a ROGUE. The pump and output powers are monitored by power-meters (PMs), while the output spectrum is measured by an optical spectrum analyzer (OSA). The pump and output signals are separated by wavelength division multiplexer (WDM) couplers.

The cavity initially relied on standard SMF-28 telecommunications fiber (Corning). Using this fiber, modulation instability effects were observed, but were relatively weak. In subsequent cavity designs, this fiber was replaced by a non-zero dispersion shifted fiber, the SMF-LS (Corning), since its zero-dispersion wavelength (ZDW) was close (~ 1560 nm) to the lasing wavelength. Lasing near the ZDW of the cavity greatly increased the magnitude of the modulation instability, and resulted in the RNG scheme covered in Chapter 6. In the second iteration, the FBG was removed and replaced by the 4% reflection of a cleaved fiber facet. This broadband reflection no longer constrained the lasing wavelength, and allowed interesting nonlinear effects to take place in the cavity, such as Raman self-frequency shift. These results are described in Chapter 7.

The potential of ROGUEs for random lasing was also investigated in this type of laser cavity. Indeed, the enhanced scattering of the ROGUE was put to use by placing it at the end of the cavity. The random feedback offered a decreased lasing threshold, while maintaining the random lasing properties of the random laser. These results are presented in section 8.2 of this thesis.

3.1.4 Random number generation

The random output of this random laser was then converted to the electrical domain by a high-speed photodiode, with a cut-off frequency of 70 GHz. This analog electrical signal was then converted to a digital signal by the analog-to-digital converter (ADC) of a real-time oscilloscope. The bits thus generated were then extracted from the oscilloscope and post-processed using Matlab. Various post-processing techniques were experimented, including least significant bit (LSB) extraction, self-delayed exclusive-OR (XOR) operations and numerical derivatives. For every investigated post-processing algorithm, a random bit file was generated, containing at least one hundred bit sequences of a million bits (1 Mb) each. This bit file was then tested with the NIST randomness test suite [134], which is an open-source software running on Linux. This test suite runs 15 statistical tests that try to identify different types of patterns within the bit sequence. These types of tests include basic tests such as computing the frequency of ones and zeros (which should be very close to $\frac{1}{2}$), but also more advanced tests based on discrete Fourier transform analysis, or on the rank of disjoint sub-matrices formed from the original bit sequence.

These statistical tests all have the purpose of evaluating the null hypothesis H_0 that the sequence is indeed random. The result of the test returns a p -value, which is the probability that the sequence

is random. If the p -value is below a certain score, the bit sequence is considered non-random, and the null hypothesis is rejected. However, even a truly random bit sequence will have a certain probability of appearing to have non-random properties, which will make it fail the test. This probability is defined as the significance level α , which is typically set for cryptographic applications to 0.01. To mitigate this, every one of these 15 tests is executed on multiple bit sequences (at least 100, if possible 1,000 bit sequences). If the number of bit sequences that pass each statistical test is below a certain threshold, the null hypothesis is then rejected. This threshold is dependent on the number of bit sequences tested. For 100 bit sequences, at least 96 must pass each statistical test, while that threshold increases to 980 when 1,000 sequences are tested.

While statistical tests such as those of the NIST test suite can provide an estimate of the achievable bitrate of a given RNG source, they cannot distinguish between true randomness and high-quality pseudo-random numbers. Therefore, the physical entropy content of true RNG sources must be evaluated to provide a theoretical explanation for the randomness generated. The maximum entropy of a system is given by

$$h_0 = \min(\tau^{-1}, 2BW)(N_\epsilon - D_{KL}(p(x)||u(x))) \quad (3.1)$$

This entropy limit depends on three important parameters. The first one is given by the first term, which depends on the limiting bandwidth (BW) of the system. The limiting bandwidth can be that of the entropy source, but also that of the various instruments used to convert the entropy signal into digital bits. In the current case, these are the photodiode and the ADC of the oscilloscope. The sampling rate τ^{-1} of the ADC can also be the limiting factor, and must be at least twice the limiting bandwidth (as per the Nyquist theorem). The second term is highly dependent on the digitization N_ϵ of the ADC, i.e. the number of bits that the analog signal is converted to. An ADC that can extract more bits per sample can generate greater entropy. However, the number of bits that can be extracted from a single sample depends not only on the ADC digitization, but also on the entropy source's probability density function (PDF). Indeed, the ideal distribution for RNG purposes is a uniform distribution $u(x)$. However, since most entropy sources have a PDF that is not uniform, the theoretical entropy content is not directly given by N_ϵ , but must also consider the source's PDF $p(x)$. Therefore, the Kullback-Leibler divergence D_{KL} from the uniform distribution to the source's PDF must be computed. This divergence is computed by

$$D_{KL}(p(x)||u(x)) = \sum_{x \in X} p(x) \log_2 \left(\frac{p(x)}{u(x)} \right) \quad (3.2)$$

where the probability of every value x is compared to the probability of a uniform distribution spanning the entire domain where $p(x)$ is non-zero. As such, D_{KL} is a value in bits that describes how the experimental distribution $p(x)$ diverges from a uniform distribution, and is equal to 0 bit when $p(x)$ follows a uniform distribution.

3.2 Organisation of the articles

The results of this thesis are structured in four articles, oriented along the two main research axes of this thesis: the development of a physical layer of security for secure communications, and the physical generation of random numbers through novel entropy sources. The first two articles are directly related to the first research axis, while the last two articles address the second research axis of this thesis.

The physical layer of security that is proposed in this thesis is based on the inscription of random fiber Bragg gratings in the core of optical fibers. The first article, “**The ROGUE: A novel, noise-generated random grating**”, describes the fabrication process of these gratings (related to the first Objective of this thesis), and their application for distributed sensing. This article was published in *Optics Express* in May 2019. In this article, random noise is added to a Talbot interferometer FBG fabrication station during the FBG fabrication process. The resulting random FBGs that are inscribed exhibit a wide, very noisy bandwidth, with a significant scattering improvement. The capabilities of the ROGUE for sensing were also investigated in this article, in order to address the third Objective of this thesis, evaluating the robustness of these new random gratings to changing environmental conditions. These fluctuations were monitored by OFDR distributed sensing, using a commercially available OFDR interrogator.

The second Objective of this thesis was then investigated in the second article, “**Non-Fungible gratings as Physical Unclonable Functions**”, which was submitted in the *Journal of Selected Topics in Quantum Electronics* in October 2022. This article demonstrated that the ROGUE’s spectral signature could be used as a Physical Unclonable Function (PUF), which can find applications in multiple secure communications protocols in the form of secret key generation and

authentication. The distributed sensing algorithm developed in the first article was then integrated to this measurement, to measure and compensate the temperature/strain variations that the PUF could be subjected to, so that its response could be constant even in the face of large environmental fluctuations. This addressed the third Objective of this thesis.

The last two articles were related to the second axis of research of this thesis. The fourth Objective was addressed by the development of a novel physical entropy source, a random distributed feedback Raman fiber laser. The third article of this thesis, **“A simple, high-speed random number generator with minimal post-processing using a random Raman fiber laser”**, demonstrated the potential of random Raman lasers for RNG. This article was published in *Scientific Reports* in June 2021. In this article, the use of a half-open cavity random distributed feedback laser was shown to generate random bits at rates comparable with that of the state-of-the-art chaotic semiconductor lasers. The intrinsic randomness of the localized modes of this laser is further enhanced by important modulation instability effects. Both statistical testing of the random bits and physical entropy evaluation are carried out on the laser’s output, to test the limitations of this RNG source, as per the fifth Objective.

The last two Objectives were further investigated in the fourth article of this thesis, **“On multiplexing in physical Random Number Generation, and conserved total entropy content”**, which was submitted to *Scientific Reports* in November 2022. In this article, a slightly modified version of the random Raman fiber laser presented in the third article was used, to generate a random supercontinuum. Random number generation across multiplexed channels was then studied using this random supercontinuum. This allowed to address the fourth Objective of this thesis, by providing an additional method to generate random bits, but this time across multiple independent channels. As per the fifth Objective, the limitations of this technique were also investigated, to provide recommendations on the best practices for multiplexed RNG. This helps ensure that the random bits generated are *truly* random, so that they can reliably be used for encryption in secure communications protocols.

CHAPTER 4 ARTICLE 1: THE ROGUE: A NOVEL, NOISE-GENERATED RANDOM GRATING

Authors: Frédéric Monet, Sébastien Loranger, Victor Lambin-Iezzi, Antoine Drouin, Samuel Kadoury, Raman Kashyap

Published in: Optics Express 27(10), 13895-13909, May 13, 2019.

We propose a novel device defined as Random Optical Grating by Ultraviolet or ultrafast laser Exposure (ROGUE), a new type of fiber Bragg grating (FBG), exhibiting a weak reflection over a large bandwidth, which is independent of the length of the grating. This FBG is fabricated simply by dithering the phase randomly during the writing process. This grating has an enhanced backscatter, several orders of magnitude above typical Rayleigh backscatter of standard SMF-28 optical fiber. The grating is used in distributed sensing using optical frequency domain reflectometry (OFDR), allowing a significant increase in signal to noise ratio for strain and temperature measurement. This enhancement results in significantly lower strain or temperature noise level and accuracy error, without sacrificing the spatial resolution. Using this method, we show a sensor with a backscatter level 50 dB higher than standard unexposed SMF-28, which can thus compensate for increased loss in the system.

4.1 Introduction

Optical fiber distributed sensing has been investigated over the past years as a way to replace sensors based on fiber Bragg gratings (FBG) that can only perform sensing on discrete, pre-determined points along the fiber [67, 135, 136]. Many techniques based on different types of elastic and inelastic scattering mechanisms have also been developed over the years. Raman scattering-based sensing in the time domain typically allows spatial resolutions of around 1 m over a sensing length of several kilometers, as well as a resolution of a few degrees Celsius [135, 137]. Brillouin scattering techniques, such as Brillouin optical time domain reflectometry or analysis (BOTDR/A), were able to push this distributed sensing distance limit to over 100 km, with a spatial resolution of a few meters and a similar temperature resolution [69, 138]. Encoding techniques have allowed to further reduce the resolution to only 2 cm over a 2.2 km sensing range [70]. Finally, techniques using Rayleigh scatter can achieve much greater resolution, while sacrificing the

sensing dynamic range. Phase optical time-domain reflectometry (ϕ -OTDR) can obtain resolutions of the order of the milli-Kelvins over a few kilometers of fiber, along with a spatial resolution of under 1 m [72]. Optical frequency domain reflectometry (OFDR) can achieve the highest spatial resolution of all techniques (centimeters or even millimeters scale) while maintaining good temperature resolution (under 1°C), at the expense of the scanning range, typically limited to the hundreds of meters [73, 139], or a few kilometers at best [140].

As such, OFDR has been under investigation for various applications requiring a very high spatial resolution, such as shape sensing [15, 141, 142], structural health monitoring [143] and flow rate measurements [144]. OFDR has also been used with many different types of fibers for specific applications, such as polymer optical fibers for their better mechanical properties [145] or photonic crystal fibers for their lower radiation-induced attenuation [146]. Many methods have been developed to increase the OFDR accuracy, e.g. optimization of the interpolation method used to recover the strain or temperature information [147], or ways to increase the backscattered signal, using ultrafast laser exposition [148], chirped FBGs written into the sensing fiber [15] or simply by UV exposition of the optical fiber [149]. These methods result in enhanced signal to noise ratio, hence increasing the resolution of measurements in cases where a very high strain or temperature sensitivity is needed or where significant loss in the optical system needs to be compensated for. However, since the spatial resolution is related to the bandwidth of the returned signal, any improvement on the signal strength must be performed on a large bandwidth to avoid resolution loss.

In this paper, we present a novel, noise-driven random Bragg grating, with the unusual property of possessing a large bandwidth which is independent of its length, contrary to uniform FBGs, whose bandwidth is inversely proportional to its length. This new type of structure presents a backscatter cross-section orders of magnitude higher than SMF-28 optical fiber, making it ideal for sensing applications. The technique to achieve those properties consists of adding noise during writing of the FBG, so as to fabricate a Random Optical Grating by Ultraviolet or ultrafast laser Exposure (ROGUE), a grating with a spectrum similar to a very broadband, very short FBG, but that can actually span an indefinite length. This can be modeled as a series of very small, randomly out-of-phase FBGs. As such, this results in a weakly reflective grating with a reflectivity that is much higher than typical Rayleigh backscatter, while at the same time maintaining a large bandwidth,

unlike a typical long weak FBG [150]. An in-depth analysis of how these ROGUE gratings enhance the accuracy and precision of strain and temperature sensing, while still maintaining a good spatial resolution, is also presented.

Although the subject of random, out-of-phase FBGs has been studied in the past for applications such as localization [20, 21] and random lasing [22, 23], this was done using strong gratings, and thus cannot be used efficiently for sensing over long distances. The subject of this paper being related to the use of the ROGUE as a sensor, localization will not be discussed here, but is the subject of an upcoming future article.

4.2 Methods

4.2.1 ROGUE fabrication

The ROGUEs were written in the fiber using a Talbot interferometer configuration with a phase-mask. The fiber core is exposed to a 213 nm wavelength laser, using the 5th harmonic of a 1064 nm Q-switched laser (Xiton Photonics), as shown in Figure 4.1. The spot size was $\sim 100 \mu\text{m}$, with a 30 kHz repetition rate and 7 ns pulse duration. The fiber coating was removed prior to ROGUE inscription. When writing a long FBG, the fiber is moved continuously at a constant speed under the phase mask using a nanometer-precision air-bearing stage (Aerotech). An electrical sawtooth wave is applied to a piezoelectric element driving the phase mask to move the fringe pattern synchronously with the moving fiber, hence preserving and controlling the FBG phase, as detailed in reference [130]. However, the objective is not to write an in-phase grating, as this would lead to a very narrow reflection bandwidth. Therefore, no sawtooth wave is sent to the piezo. In theory, the grating should self-erase as the fiber is moved under the fixed UV fringe pattern and no gain in backscatter signal would be obtained except for pure UV enhancement of the Rayleigh scatter, described in reference [149]. However, the UV exposure is not completely uniform because of noise in the system, hence the erasure of the grating is not perfect. As a result, a random interference pattern will appear in the fiber, leading to enhanced reflectivity over a certain bandwidth at the Bragg wavelength determined by the UV fringe patterns.

In order to increase the reflectivity of the grating, all that is needed is to increase the noise. To do so, we simply replaced the sawtooth wave by a random electrical signal. This way, the ROGUE is

no longer dependent on the small environmental noise in the system, but rather on the noise output of the function generator. The amplitude and frequency of this noise are much greater than the environmental noise, and as such it increases the backscattered signal by orders of magnitude, since it creates a larger number of micro-gratings (μ FBGs). The phase-mask movement amplitude and the noise bandwidth were optimized to reach the highest ROGUE reflection amplitude for the same UV exposure to values of ~ 10 periods (5V) and 20 Hz respectively. The latter is mostly limited by the response time of the piezoelectric element. The applied noise amplitude and bandwidth were found to influence the amount of backscatter, but had no effect on the bandwidth of the backscattered spectrum, which is dependent on the average μ FBG length and can be modified by changing the spot size.

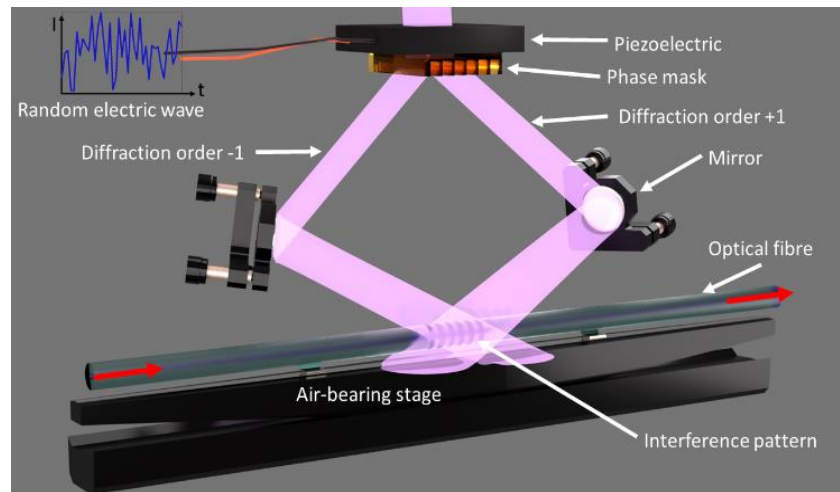


Figure 4.1 Talbot interferometer used for the fabrication of the ROGUE. The phase mask above generates different diffraction orders. The first two orders (+1 and -1) are reflected by mirrors onto the fiber, where an interference fringe pattern is created. The UV exposure increases the refractive index periodically, creating an FBG. By changing the angle of the mirrors, the interference fringe pattern (and thus the FBG wavelength) can be modified. The random electrical wave applied to the piezoelectric element induces imperfect overlap of the interference pattern, creating a ROGUE.

4.2.2 Noise level and accuracy measurements

In order to characterize the increase in accuracy and precision provided by the use of ROGUES with the enhanced scatter, two sets of experiments were performed. In the first experiment, the

precision is evaluated by a measurement of the root mean square (RMS) noise level of strain from a uniform and stable fiber under test (FUT). The fiber was placed inside an insulated box, to remove environmental fluctuations and vibrations. A reference measurement is first taken, and 15 sample measurements are then performed sequentially, to average out idler points. The strain is calculated at every point along the fiber's length using the algorithm described by Froggatt et al. [73], and using an interpolation inspired from the one described by Cui et al. [147] to improve strain resolution beyond what can be achieved with our OFDR commercial optical backscatter reflectometer (described below). The RMS error between measurement and expected value (zero strain) was calculated across all data points in the selected 300 mm of the fiber, and averaged over the 15 measurements. In order to avoid problems related to the dynamic range of the OFDR unit, two different fibers were used, one in which a ROGUE was inscribed, and another that was left untreated. Both fibers were stripped of their coatings, to ensure repeatability of the measurement.

The second set of experiments was performed to evaluate the accuracy of the strain measurement. A reference measurement was first taken before any strain is applied. Then the 1.15 m fiber is stretched over 20 μm by increments of 1 μm using a nanometer-precision Aerotech stage, leading to strains ranging from 0 to 17.4 $\mu\epsilon$. A measurement is performed after every 1 μm increment, when the fiber is static, and the strain is calculated using the same algorithm as for the noise level. The accuracy error is the difference between measured strain and the expected value of strain for a given stretch. The total calculated error is the RMS accuracy error of each sensing point of the FUT (80 mm in length) at each stretch point. Again, two different fibers were used to avoid the dynamic range issue described earlier.

All OFDR measurements were performed using a commercial optical backscatter reflectometer (OBR4600) from Luna. Only the raw data from the OBR was used and the rest of the data processing was performed independently using our own software. All the scanning bandwidths available on the OBR software were tested, and the central wavelength of the scan was the same for all measurements, i.e. the central wavelength of the ROGUES (1555 nm). Except when explicitly specified, a gauge length of 10 mm was used for data processing, and the sensor spacing (distance between every sensing point) was set at 1 mm. Tests were performed on SMF-28 fiber from Corning, and a SM1500(4.2/125) fiber from Fibercore, a highly Ge doped fiber. Due to its high Germanium concentration, the SM1500 is more photosensitive than the regular SMF-28. It

also exhibits 4.1 dB more backscattered signal prior to any UV exposure. Both fibers were loaded with molecular deuterium in order to increase photosensitivity, although this technique would still be effective without deuterium, provided the fiber is photosensitive enough (just like regular FBG inscription). The measurements were performed in the weeks following the ROGUE's inscription, to ensure deuterium out-diffusion.

4.2.3 Interpolation technique

The OFDR method is detailed by Froggatt *et al.* [73] for temperature and strain sensing. In order to improve the accuracy of the results given by the OBR4600, an interpolation method similar to the one described by Cui *et al.* [147] was implemented, as a way to overcome the Fourier uncertainty principle inherent to the calculation. Basically, by adding a number N of padding zeroes at one end of the spatial domain data of both reference and sample signals before performing the Fourier transform and cross-correlation of the two data sets, the spectral resolution is artificially enhanced, allowing more points in the cross-correlation peak. Those points come from a *sinc* interpolation that is performed by the Fourier transform of the dataset with the added zeroes. Indeed, since the Fourier transform of a rectangle is a *sinc* function, performing the Fourier transform on this new dataset results in a *sinc* interpolation on the original dataset. Although this peak does not get narrower (the Fourier limitation remains), the extra points inside the peak allow us to measure more accurately small displacements of the peak.

Figure 4.2 shows the result of this interpolation on the quality of the cross-correlation peak. Before the interpolation on Figure 4.2(a), the cross-correlation peak is defined by a single point at 0 GHz. At this point, even performing a fit on the neighboring points would result in a bad approximation of the real spectral shift, because of the wide separation in between each point. However, after adding 2,000 padding zeroes, the peak is much better defined, and thus the spectral resolution increases significantly, as shown on Figure 4.2(b).

In addition to the technique presented by Cui *et al.* [147], an additional quadratic fit was implemented on the processed data, in order to find the maximum of the cross-correlation peak more accurately to values in between interpolation points. The quadratic fit was performed over the maximum cross-correlation value and its two nearest neighbors. Since a quadratic fit over three

data points can be resolved analytically, it adds very little to the calculation time and increases the spectral resolution without additional padding zeroes.

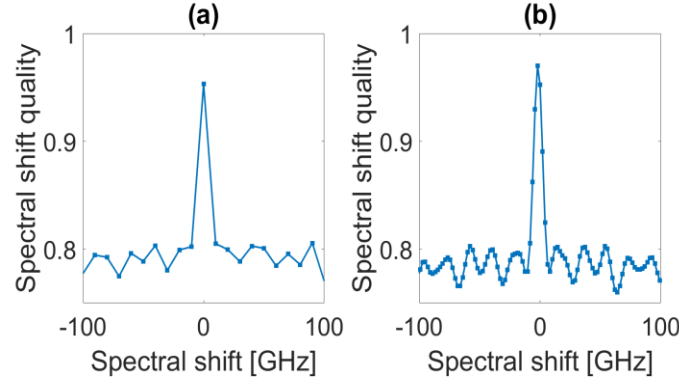


Figure 4.2: Cross-correlation result (a) before and (b) after the *sinc* interpolation. The fiber used is a standard SMF-28 fiber inscribed with a ROGUE, interrogated over a 42.90 nm bandwidth with a 10 mm gauge length. The original dataset of (a) has 521 points, while the interpolation of (b) is performed by adding 2,000 padding zeroes to the data.

However, the downside of this method is that it increases the calculation time. The number N of padding zeroes must thus be sufficient to achieve the desired resolution, ideally down to the experimental noise limit, without using an unnecessary high number of zeroes to limit calculation time. For an OFDR measurement using a 5 nm bandwidth, the processing time goes from 83 ms using 10^3 zeroes to 633 ms with 10^6 zeroes. While not a limiting factor in the current application, choosing the correct number of zeroes can become critical when applied to real-time measurements.

4.3 Fabrication and Modeling of the ROGUE

Figure 4.3(a) compares the expected spectra of a meter-long fiber Bragg grating to the one of a ROGUE. Being composed of multiple μ FBGs, the ROGUE FWHM will remain constant regardless of the grating's length, whereas a typical FBG bandwidth will decrease with length (typically 2 pm for a 1 m grating [131]). Using our technique, ROGUES of strength ranging from under 5 up to 50 dB of backscattered intensity were written. Figure 4.3(b) and (c) shows the results of such a ROGUE in both temporal and spectral domains, written in standard SMF-28 fiber and measured with OFDR. While the exposed region in Figure 4.3(b) shows more noise than the SMF-

28 region, this does not influence sensing accuracy, as it is based on the change in backscatter signature of the fiber. It therefore does not matter if this signature is mostly flat or noisy.

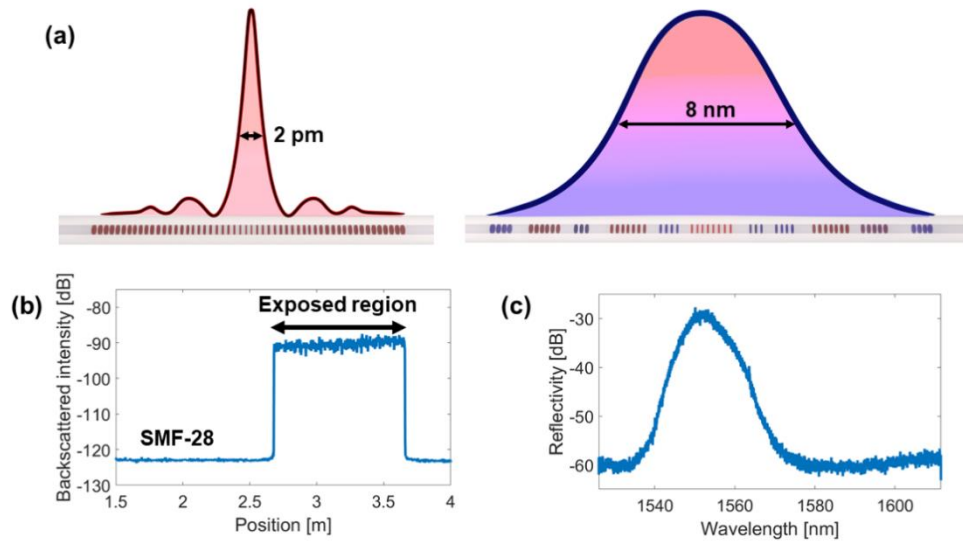


Figure 4.3 : (a) Schematic illustration showing the difference between a regular in-phase FBG, exhibiting a very narrow bandwidth (typical full-width at half-maximum (FWHM) taken from [131]), and a ROGUE, composed of multiple out-of-phase μ FBGs of different lengths, resulting in a much wider bandwidth. Experimental measurements for a 1-meter-long ROGUE written in SMF-28 fiber are presented (b) in the temporal domain, showing over 30 dB in backscattered amplitude enhancement, and (c) in the spectral domain, where an 8 nm FWHM (41 nm full width) can be observed. Rayleigh scattering baseline can be observed out-of-band of the grating, at around -60 dB. The ROGUE was written using 37 mW of 213 nm UV laser power, at a writing speed of 0.2 mm/s. Measurements were made with the largest bandwidth of 88.24 nm available on the OBR4600.

The loss induced by the writing of the ROGUE was evaluated by measuring the backscattered intensity of an unexposed SMF-28 fiber portion placed after the exposed region across an 88 nm bandwidth scan (the largest available on our OBR). By comparing the backscattered intensity before and after writing the ROGUE, the loss can be estimated. Averaging over an 800 mm-long section of fiber, after the writing of the 1 meter-long ROGUE shown in Figure 4.3(b) and (c), the induced loss was estimated at 0.15 dB/m.

The effect of speed and power on the backscatter signal gain is shown in Figure 4.4. It can be shown that decreasing the writing speed leads at first to a slow, steady increase in gain, until writing speeds of under 0.3 mm/s, when the gain starts increasing rapidly. It can be also observed that, for SMF-28, the use of additional power has more impact at fast-writing speeds than for the SM1500. This can be explained by the saturation of the refractive index change of the fiber. Since this SM1500 is significantly more photosensitive, it requires a lower UV exposure in order to achieve the same results. For the lowest writing speed, an average refractive index increase of 4.8×10^{-3} was measured for the SM1500 fiber with an interferometric microscopy system, while the refractive index modification of the SMF-28 was always under 10^{-4} , below the resolution of our system. This larger refractive index modification resulted in additional losses, and we estimate losses for this type of fiber with this writing speed to be around 1 dB/m. When taking into account the intrinsically higher 4.1 dB backscatter in SM1500, using this writing speed on the SM1500 results in a sensor showing more than 50 dB higher backscatter than regular SMF-28.

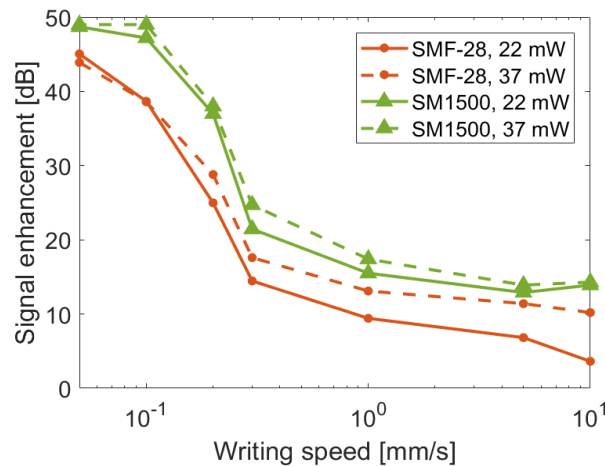


Figure 4.4 : Gain of the backscattering signal of the ROGUE as a function of writing speed vs untreated fiber. The ROGUE was written using a noise amplitude of 5 V (~10 periods) and a frequency bandwidth of 20 Hz. A SMF-28 fiber from Corning (orange) and a SM1500 fiber from Fibercore (green) were tested, using 22 mW (solid line) and 37 mW (dashed line) of laser power. 0 dB corresponds to the signal level of untreated fiber both for SMF-28 and SM1500).

Measurements made on the OBR4600 using a 21.16 nm scanning bandwidth, the bandwidth most suitable for sensing, as will be shown in the next sections. The gain was measured in the temporal domain (see Figure 4.3(b)).

The ROGUE was simulated using a probabilistic model describing the position and length of uniform μ FBGs, each defined with a random phase. A stochastic process using two distributions was used, the distribution X describing the distance between the end of a μ FBG and the beginning of the next one, and the distribution Y describing the length of each μ FBG.

The beginning of the first μ FBG is x_1 , generated from the distribution

$$X_1 = X \quad (4.1)$$

The end of this μ FBG is y_1 , and is conditional to the value of x_1 . As such, y_1 is generated from

$$Y_1 | x_1 = Y + x_1 \quad (4.2)$$

Based on Equations (4.1) and (4.2), the beginning and ending positions of all μ FBGs can be found sequentially by knowing the value of the previous point. As such, the beginning position x_n and ending position y_n of every μ FBG are generated from

$$X_n | y_{n-1} = X + y_{n-1} \quad (4.3)$$

$$Y_n | x_n = Y + x_n \quad (4.4)$$

In the current case, two exponential distributions were chosen for X and Y , with two different parameters k_1 and k_2 . This stochastic process is similar to a Poisson process [151, 152], the difference lying in the use of two different parameters instead of a single one. These parameters were fitted to experimental data, and can be related to respectively the gratings' density (or the distance between each μ FBG) and the gratings' average lengths. The complex reflectivity of a single μ FBG in the fiber is given by [153]

$$\rho = \frac{-\kappa_{ac} \sinh(\alpha L)}{\delta \sinh(\alpha L) - i\alpha \cosh(\alpha L)}, \quad (4.5)$$

with

$$\delta = \kappa_{dc} + \frac{1}{2} \left(\Delta\beta - \frac{d\phi(z)}{dz} \right), \quad (4.6)$$

$$\alpha = \sqrt{|\kappa_{ac}|^2 - \delta^2}, \quad (4.7)$$

where κ_{ac} and κ_{dc} are the AC and DC components of the coupling constant, $\Delta\beta$ is the difference in propagation constants between grating and incident light, ϕ is the phase of the grating, z is the position along the grating and L is the grating length. By adding the complex reflectivity of all the μ FBGs together using the stochastic process described earlier for their length and position, the total reflectivity can thus be simulated. Results are shown in Figure 4.5.

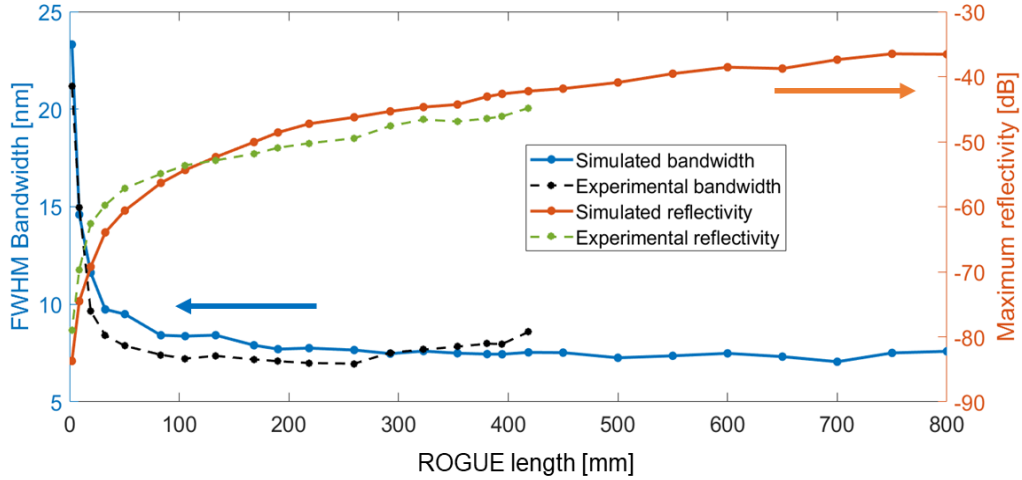


Figure 4.5 : FWHM bandwidth of the ROGUE, as a function of length. The experimental data is limited to 400 mm, with models using the parameters $k_1 = 500 \text{ m}^{-1}$ and $k_2 = 1.4\text{e}4 \text{ m}^{-1}$. The μ FBG were considered as uniform gratings, with a central wavelength of 1555 nm. The phase and amplitude of each μ FBG is random. The bandwidth asymptotically approaches 7 nm for a ROGUE length > 100 mm for an average μ FBG length of 72.5 μm .

4.4 Advantages for OFDR Distributed Sensing

4.4.1 Results of the interpolation

Figure 4.6 presents the signal of a ROGUE acquired directly from the OBR, as the fiber is being strained (solid blue curve) using a 42.90 nm bandwidth and compared with the expected spectral shift (solid black curve). As can be seen in Figure 4.6(a), the spectral shift given by the OBR internal calculation (solid blue curve) is at first much smaller than the applied value, until it suddenly jumps to a much higher value, only to again start increasing much slower than the real value. As such, the results given by the OBR have a very poor sensing resolution (greater than

8 $\mu\epsilon$). However, by using the interpolation method described previously on the raw measurement data, we can increase the accuracy of the results. These results were obtained with a varying number of padding zeroes added after the gauge length window. As can be seen, for $N \leq 1,000$, the resolution obtained by performing the *sinc* interpolation is actually worse than the one given by the OBR's calculation. However, if the number of padding zeroes is increased further, the interpolation increases the spectral shift resolution. We demonstrate here that in order to achieve the best possible resolution using solely a *sinc* interpolation, a number of padding zeroes above 10^5 must be used, since the spectral shift still varies noticeably while increasing the number of zeroes at this point. It should be noted that we have no information on the exact nature of the OBR's algorithm, as this is propriety information of Luna.

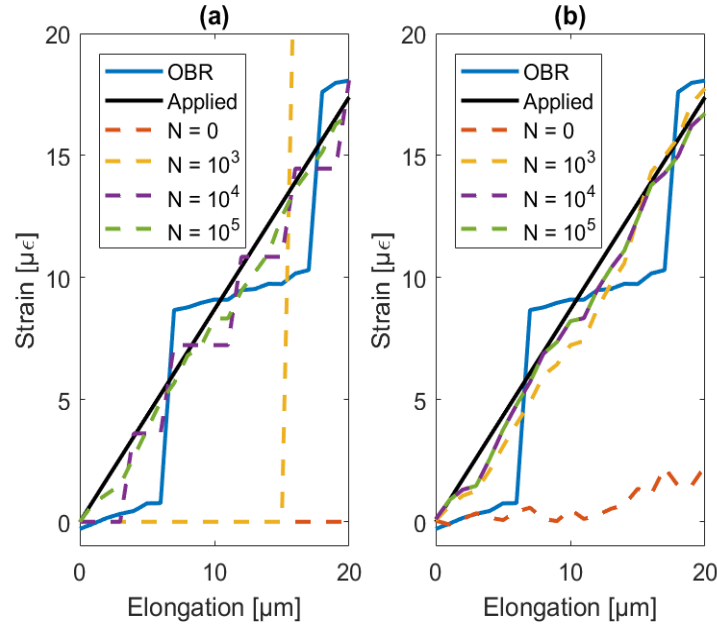


Figure 4.6: Calculated spectral shift as a function of the elongation, where the method is compared between the OBR's internal algorithm and the one described earlier, using a number N of padding zeroes. Solid black curve is the applied strain value. (a) is taken right after the cross-correlation, and (b) is taken after applying an additional quadratic fit. Measurements were made using the OBR4600 from Luna with a 42.90 nm bandwidth, the largest available bandwidth on the OBR for sensing.

In Figure 4.6(b), the additional quadratic fit was added to the data treatment. It can be seen that this implementation decreases the number of padding zeroes needed to achieve the best available

resolution by a significant amount. Indeed, using a number of padding zeroes as small as 1,000 yields a spectral shift comparable to the theoretical value, and increasing the number of padding zeroes above 10^4 results in no noticeable increase in resolution, as can be seen on Figure 4.6(b), where the curves of both $N = 10^4$ and $N = 10^5$ are actually superposed on top of each other. This is because the resolution is no longer limited by the algorithm, but rather by the intrinsic experimental sources of error, such as laser repeatability, environmental fluctuations, etc. As such, the required number of padding zeroes decreases by an order of magnitude when the *sinc* interpolation is combined with a quadratic fit. However, it should be noted that the calculation time using 10^4 padding zeroes is 2.6 times longer than when using no padding zeroes (23 times longer with 10^5).

4.4.2 ROGUE noise level and accuracy in OFDR sensing

The noise level experiment described earlier was performed on both regular unexposed SMF-28 fiber and ROGUE. The results are presented in Figure 4.7. It can be observed that, for the unexposed fiber, the RMS error decreases when the bandwidth is increased. This is to be expected, since an increase in bandwidth leads to more data points in the same gauge length, due to the smaller step size, hence a higher quality cross-correlation.

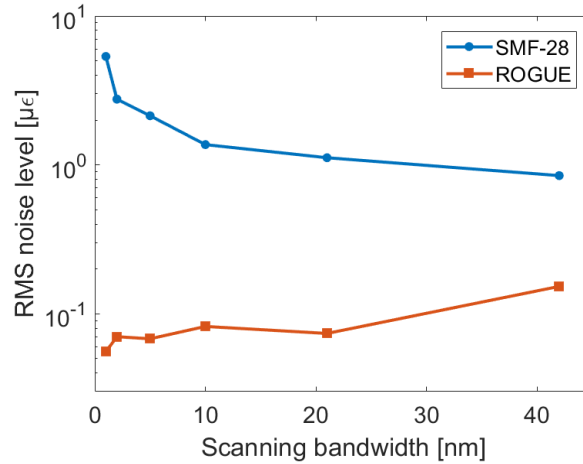


Figure 4.7: RMS noise level in a uniform and stable environment of 300 mm of both unexposed SMF-28 fiber and ROGUE written in SMF-28. The fibers are placed in an insulated box, averaged over 15 measurements. A 30 dB enhanced ROGUE was used for these measurements.

However, surprisingly, the opposite happens in the case of the ROGUE. This is most likely due to the fact that, contrary to the unexposed fiber, most of the signal comes from a narrower spectrum. As such, using a smaller scanning bandwidth increases the signal to noise ratio (SNR), because only the portion of the spectrum where the ROGUE is inscribed is probed during the laser scan, while the data with low SNR is ignored. Although there is less data, the available data is of higher quality, hence the lower noise level. However, scanning across too narrow a bandwidth limits the maximum strain or temperature that can be sensed, limits the spatial resolution and will decrease accuracy, as described in the following section.

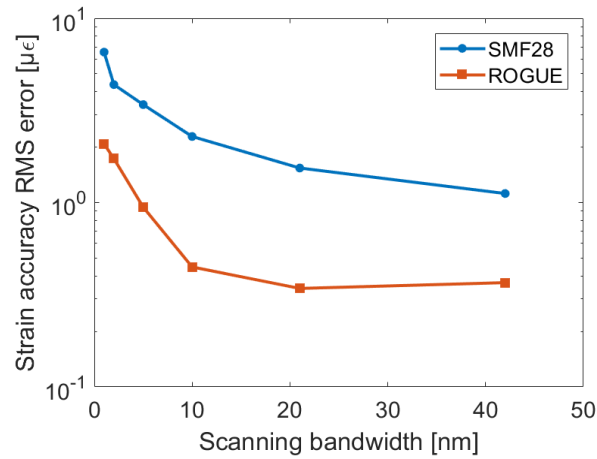


Figure 4.8: RMS strain error while stretching the fiber as a function of scanning bandwidth, for both unexposed fiber and ROGUE. The spectral shift is calculated for the 20 μm stretching, across 80 mm of sensing fiber along the 1.15 m fiber length. It can be observed that, using a ROGUE, a scanning bandwidth of only 5.24 nm is sufficient to achieve better accuracy to the one obtained with unexposed SMF-28. A 30 dB enhanced ROGUE was used for these measurements.

Afterwards, the accuracy experiment was performed on those fibers, and is shown in Figure 4.8. The behavior for the ROGUE is very similar to the unexposed fiber, but the error is almost an order of magnitude lower for all scanning bandwidths. In the case of the ROGUE, we see that the minimal error is for a 21.16 nm bandwidth (0.34 $\mu\epsilon$, 4.5 times smaller than the SMF-28). The explanation for this is the same as for the noise level; since most of the signal comes from a narrower bandwidth region, a larger bandwidth does not necessarily yield a more accurate measurement. The higher performance of the noise characterization versus the accuracy characterization is due to the fact

that, for the latter, the fibers were not in an environment as controlled as for the former, leading to more environmental noise.

4.4.3 Spatial resolution in noise level

The data treatment for the noise level experiment was repeated while varying the gauge length. A smaller gauge length leads to a higher spatial resolution, but at the cost of the strain resolution. The influence of gauge length on RMS noise level is presented in Figure 4.9.

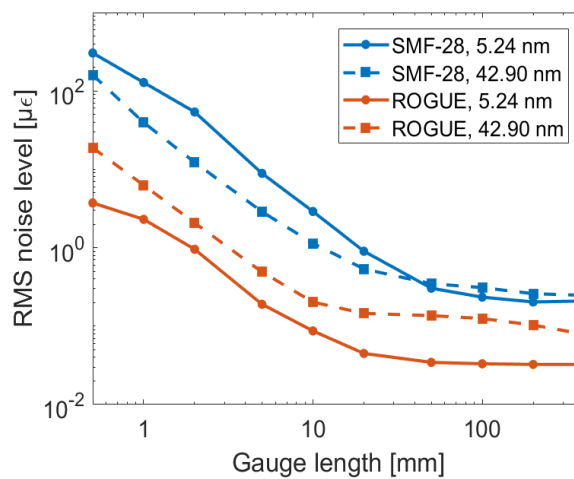


Figure 4.9: RMS noise level as a function of gauge length, for both unexposed fiber and ROGUE, when placed in an insulated box, averaged over 15 measurements, for bandwidths of 5.24 and 42.90 nm. The gauge length is varied from 0.5 mm to 200 mm. As can be seen, a ROGUE scanned with a 5.24 nm bandwidth requires a gauge length of only 2 mm to beat the noise level of SMF-28 with a 42.90 nm bandwidth and a 10 mm gauge length. A 30 dB enhanced ROGUE was used for these measurements.

From this figure, it can be easily seen that, for very short gauge length, the spectral and spatial resolution seem to be Fourier-transform-limited, and an increase in gauge length (spatial resolution) leads to a decrease in RMS noise level (spectral resolution). However, for very large gauge lengths, a plateau is met, and the added value of a larger gauge length is minimal. Furthermore, it is obvious that, regardless of the gauge length, the noise level is always much smaller with the ROGUE than with the unexposed SMF-28 fiber. Finally, a ROGUE can provide

a greater spatial resolution, while also using a smaller scanning bandwidth, at no cost to measurement resolution.

4.4.4 ROGUE gain and loss compensation

Finally, the influence of the strength of the ROGUE was evaluated. ROGUES of various strengths were written and an accuracy error measurement was performed. Only the 21.16 nm scanning bandwidth (the one that showed the smallest error) was used for this study. Figure 4.10 shows how the error is influenced by the ROGUE gain. For stronger gratings, the mean error decreases, until 25 dB gain when a plateau is reached. We suspect the accuracy to be limited by environmental fluctuations and vibrations, as the accuracy experiment could not be performed inside the insulated box as for the noise level measurements.

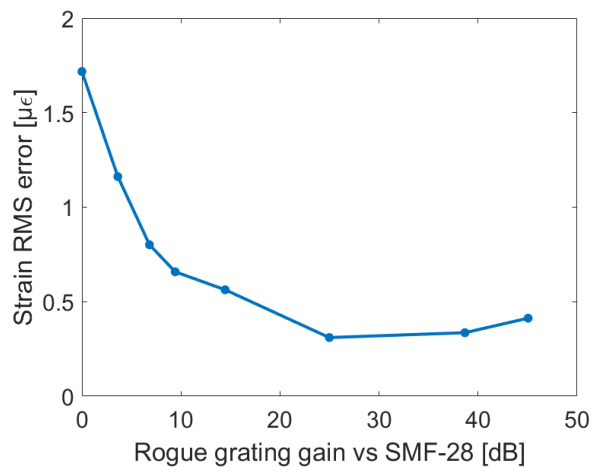


Figure 4.10 : Strain RMS error calculated over a 20 μm stretching and 80 mm of sensing fiber along the 1.15 m fiber length. (a) Spectral shift accuracy as a function of ROGUE gain (linear scale in y). The ROGUES were written using 21 mW of UV power, by varying the writing speed from 0.05 mm/s to 10 mm/s. The 0 dB gain value represents an unexposed SMF-28 fiber.

In order to characterize the ROGUE's ability to compensate for signal loss, the same experiment with the three strongest ROGUES was performed with induced optical loss from a variable optical attenuator placed before the ROGUE. Figure 4.11 presents these results as a function of induced loss in measurement signal. It can be observed that, as induced loss is increased before the ROGUE, the error increases progressively until a threshold is reached, when the accuracy of the

measurement decreases rapidly. When the loss is so high that the noise level is comparable to the ROGUE's maximum reflectivity, all information is lost in noise, and the algorithm can no longer recover the spectral shift accurately.

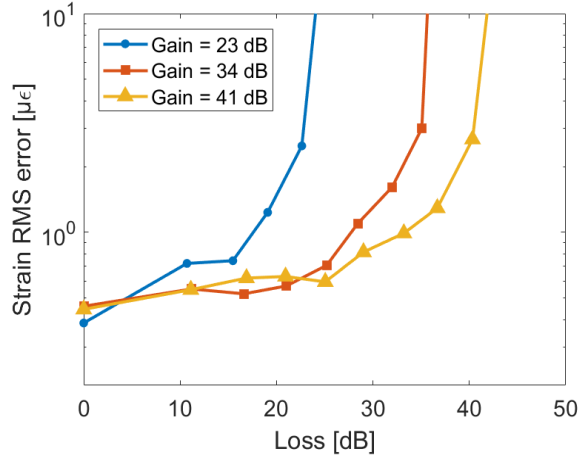


Figure 4.11: Spectral shift accuracy for three ROGUEs of different gains, as a function of optical loss induced *before* the ROGUE by an optical attenuator (logarithmic scale in y).

4.5 Discussion

Several techniques have been investigated in the literature to enhance the signal in a similar fashion as the ROGUE. For example, many authors describe sensing techniques using arrays of either identical [154] or random gratings [26]. However, these are not continuously distributed sensing techniques, and can only perform sensing where the gratings are inscribed in the fiber. These are satisfactory for applications where spatial resolution is not a concern, or when using other techniques such as optical time domain reflectometry (OTDR), but they have not been shown to achieve the 2 mm spatial resolution presented in this article. Other authors, such as Gifford *et al.* [74], used small-bandwidth FBGs separated by gaps, and reported similar accuracy with a 10 mK noise level using 12 mm gauge length and 5 nm scanning bandwidth. However, these gaps add blind-spots in the time-domain, thus limiting the spatial resolution. As the ROGUE retains a large bandwidth regardless of the grating's length, it does not have this limitation, allowing it such high spatial resolution.

Other techniques offering continuous scattering enhancement have been explored in the literature. We have previously shown a 20 dB increase in signal by UV exposure on the whole spectrum (demonstrated in C-band), but although simple, this technique requires a highly photosensitive fiber and relatively high UV exposure [149] compared to ROGUEs. Indeed, we tried implementing this technique to compare with the ROGUE inscription, but almost no improvement in backscatter was observed using this power and speed. Xu *et al.* [25] reported enhancement by the inscription of a random grating using ultrafast laser point by point inscription. However, this resulted in very high losses (~ 100 dB/m), making them impractical for more than very short range applications. Yan *et al.* [148], using a similar technique, demonstrated an increase of over 40 dB in backscatter, but observed the formation of nano-gratings in the core of the fiber, leading to transmission loss of 15 to 41 dB/m. More recently, Beisenova *et al.* [155] presented a technique to enhance the scatter by using nanoparticles doped inside the fiber, enhancing the backscatter by 36.5 dB, while suffering from losses of 25.5 dB/m. The common problem with those techniques is that, while significantly enhancing the scatter, this scatter is omni-directional. As such, only the very small proportion of light captured by the fiber's numerical aperture is backscattered to the detector, explaining the very high transmission losses. In comparison, our ROGUEs achieve transmission losses of only 0.15 dB/m, due to the directionality of the scatter enhancement.

Some techniques do show directional backscatter enhancement. Westbrook *et al.* [15, 156] presented an enhancement scheme based on the writing of superposed chirped FBGs, resulting in a 20 dB backscatter enhancement, with very low optical losses (0.4 dB/km). However, the superposition of those gratings limits the achievable spatial resolution to the spacing between each exposure (in their case, ~ 5 mm). The spatial resolution of our technique, being noise-driven and continuous, is only limited by the spot size (in our case, ~ 100 μ m). Using a smaller spot size (such as the 14 μ m demonstrated by Scholl *et al.* [157]) would potentially decrease even further that theoretical limit, and would increase the ROGUE bandwidth. Additionally, we demonstrate much higher backscatter enhancement. Indeed, to the best of our knowledge, this is the first time that a sensor showing more than 50 dB more backscatter than SMF-28 is reported. This increased signal can also be used to multiplex several ROGUEs, allowing sensing on all of them simultaneously, compensating for any additional losses from multiplexing. More importantly, this enhancement is

achieved without major increase in transmission loss, while simultaneously achieving an unprecedented $68 \text{ n\AA}$ (8 mK) noise level (with a 5.24 nm bandwidth and 10 mm gauge length).

Since a ROGUE is noise-generated, the alignment of the inscription system is non-critical and insensitive to vibrations, making the ROGUE a simple and affordable solution to amplify the backscattered signal critical to OFDR measurements. Relatively fast writing speeds of 1 or even 10 mm/s show sufficient increase in backscatter to noticeably enhance the accuracy of such sensors without requiring an enormous amount of UV power. The experimental setup described in this paper uses a Talbot interferometer configuration but could as easily use direct inscription of the ROGUE with the fiber directly behind the phase mask, or ultrafast laser exposure. Arguably, environmental fluctuations or equipment vibrations could even potentially increase the strength of the ROGUE by adding other sources of noise. Although the coating was removed prior to ROGUE inscription, making the sensors more brittle, different techniques could be implemented to ensure sensor robustness, such as recoating the fiber after the exposure, using a UV-transparent coating to remove the need to strip the coating, or even writing the ROGUE in the fiber drawing process, before it is coated.

In an ideal lab-controlled case where loss and parasitic reflections are minimized, a ROGUE is only useful for a gain of $\sim 25 \text{ dB}$ compared to bare SMF-28, as shown previously in Figure 4.10. Indeed, the strain RMS error reaches a plateau, and therefore remains the same for all stronger ROGUEs. However, in many sensing applications, these ideal conditions may not be available, as loss added from connectors or optical components can suppress the detector's dynamic range. A ROGUE increases the gain optically without losing any of the detector's dynamic range and without any sacrifice in scanning time. This increased signal can also be used to multiplex several ROGUEs, allowing sensing on all of them simultaneously.

The time it takes to make a measurement can be critical to many sensing applications, more so than sensitivity. Increasing the optical signal through a ROGUE can improve sensitivity, but it can also potentially reduce the measurement time for a constant sensitivity. For instance, as shown in Figure 4.8, for the same accuracy observed as standard SMF-28, the scanning bandwidth can be reduced by a factor of 8 for a ROGUE (from 42.9 nm to 5.24 nm). For our OBR, this reduces the 4.5 s scan time for SMF-28 down to 1.2 s (using the Fast Scanning option). Also, having more signal gain can allow the detector to operate at higher bandwidth, hence allowing faster wavelength sweep

speed until the maximum scan speed is reached (determined by the time-of-flight of light in the fiber). It should be noted that this enhancement is limited to the bandwidth of the ROGUE. The laser power and writing speed are not sufficient to generate uniform Rayleigh enhancement, and as such scanning outside the ROGUE does very little to enhance backscatter.

4.6 Conclusion

In conclusion, we have shown here that, simply by adding phase noise during FBG inscription we can write a ROGUE that generates an increase in backscatter of several orders of magnitude and whose large FWHM bandwidth (>7 nm) is independent of written length (for length >100 mm). This enhancement results in a SNR above 50 dB. This gain can be used to reduce noise in distributed sensing. For instance, we have shown that for a 10 mm gauge length, the noise level can be reduced by over an order of magnitude in noise and by 4.5 times in accuracy compared to standard SMF-28. We have also shown that such a high enhancement can be used to compensate system losses of up to 50 dB (25 dB one-way), which can significantly increase the robustness of such sensing equipment to losses and parasitic reflections. Finally, such gains could be used to significantly reduce the sensing time, as we have shown that to obtain similar performance to SMF-28, a ROGUE requires 8 times less bandwidth for the wavelength scan. Also, with increased gain, the tolerance to noise is higher, hence the detector bandwidth can be increased, allowing faster scan speeds. A ROGUE structure requires little exposure and is easy to write in-fiber, as it is noise-generated, making any environmental fluctuation irrelevant, if not advantageous. Therefore, it could potentially be easily implemented directly on a drawing tower.

4.7 Funding

Natural Sciences and Engineering Research Council (NSERC) Strategic Grant “Limoncello” and Fonds de Recherche du Québec – Nature et Technologies (FRQNT)

4.8 Acknowledgement

The authors would like to thank Jean-Sébastien Boisvert for fruitful discussions during the entire process, and Prof. Richard Labib for help developing the probabilistic model. We would also like to thank the NVIDIA GPU Grant Program.

CHAPTER 5 ARTICLE 2: NON FUNGIBLE GRATINGS AS PHYSICAL UNCLONABLE FUNCTIONS

Authors: Frédéric Monet, Anthony Roberge, Raman Kashyap

Submitted in: Journal of Selected Topics in Quantum Electronics, November 10, 2022

Physical Unclonable Functions (PUFs) are physical devices exploiting intrinsic randomness through the fabrication process that can be used for authentication and secure key generation. In this article, we describe a novel weak PUF architecture based on the inscription of random gratings in an optical fiber, which can be easily interrogated by a commercial instrument due to the enhanced backscatter. With PUF lengths of only 40 mm, we show that the false positive and false negative probabilities can reach below 10^{-27} . We also describe a temperature and strain compensation algorithm to mitigate environmental fluctuations. Furthermore, we describe an alternative technique which increases the number of bits used for digitizing the PUF's signature, thus significantly decreasing the false identification probabilities by almost two orders of magnitude.

5.1 Introduction

As new communications systems and technologies develop, there are ever-growing concerns about security and privacy. Indeed, in an increasingly digital world, the majority of our communications are made online, and are as such at risk of potential eavesdropping and hacking. Consequently, there is a real drive to develop novel techniques to authenticate a user's true identity in order to protect his confidential information from eavesdroppers and identity frauds. Many devices have been developed to address such challenges, for instance passwords [158], radio-frequency identification (RFID) [159] or biometric information [160]. While passwords are certainly the most commonly used authentication method today, they can be leaked, and are susceptible to human error (e.g. forgetting the password, choosing a weak, easily guessed password, etc.). RFID systems are based on either passive or active microchips, where a reader will scan an RFID tag to authenticate the identity of its carrier, or the attached item [159]. This type of identifier is heavily used in multiple industries, both to allow employees to authenticate their identity for access to facilities, as well as for identifying shipment of goods. However, they are vulnerable to external interference, and can be cloned, meaning that a third party can impersonate an authorized

user [161]. In more recent years, biometric information such as fingerprints and retinal scans are increasingly used as additional potential authentication methods [160]. While these are more complex to forge than RFIDs, they are still potentially clonable, and can be reverse-engineered from the databases' stored templates [162]. Furthermore, if biometric information is compromised, it is not easily revocable.

Physical Unclonable Functions (PUFs) are an alternative hardware-based system that has received considerable attention in recent years. PUFs are based on intrinsic noise and randomness inherent in their fabrication process, making each of them unique and impossible to reproduce, even when knowing the manufacturing process and desired output signal [107]. This makes them perfectly suited for authentication purposes, acting as a fingerprint ensuring the identity of its carrier [121]. Various types of PUFs have been demonstrated, such as electronics-based PUFs, like silicon PUFs [111] or static random access memory (SRAM) PUFs [116]. Optical PUFs were also proposed, based on optical and photonic techniques to probe intrinsically random systems. For instance, in the cold war, thin coatings of reflecting particles were sprayed on nuclear weapons [163]. Since these particles are randomly distributed on the surface, the interference pattern they generated when illuminated are unique and unpredictable, allowing them to be identified precisely. Many other optical PUF architecture were proposed over the years, for example relying on plasmonic nanoparticles [108], or laser speckle measurements [109]. Recently, optical fiber-based PUFs have shown potential for next-generation authentication applications, due to their low cost, relaxed requirements on optical alignment, and the fact that they are already integrated in the fiber optics networks. For example, Mesaritis et al. presented a PUF based on the speckle response of a multimode polymer optical fiber that could be interrogated from multiple angles and wavelengths [110], while Du et al. demonstrated a PUF architecture based on the intrinsic Rayleigh backscatter of an optical fiber [164], the latter being severely limited in usefulness due to the very weak signal.

Every PUF architecture is defined by an input challenge and its output response, in a process known as challenge-response pair (CRP) [121]. PUFs are categorized based on their CRP domain, which is the number of unique challenges the PUF can support while outputting a different unique response. A *weak* PUF has only one or a few CRPs, while a *strong* PUF has a CRP domain large enough that its entire measurement cannot be completed within a reasonable timeframe. *Weak*

PUFs are typically used for cryptographic key generation, which can then be used for authentication and encryption cryptographic protocols [112, 113, 116, 165]. *Strong* PUFs can realize the same applications, but can also be used for more advanced cryptographic protocols such as oblivious transfer and multi-party computation [121, 166, 167]. It is worth mentioning that the *weak* and *strong* characterizations are not measures of the PUF’s performance, but rather of its potential applications. A *weak* PUF is as intrinsically random and unclonable as a *strong* PUF, and both architectures can be used equally effectively for applications such as cryptographic key generation. However, since *strong* PUFs are not as susceptible to *cloning* and *replay* attacks as *weak* PUFs, *strong* PUFs can be directly used in authentication protocols, whereas *weak* PUFs are more suitable as parts of cryptographic protocols based on key generation, where the key does not have to leave the device [168]. Recently, we proposed a novel technique to increase the backscattered signal in optical fibers, by inscribing Random Optical Gratings by Ultraviolet or ultrafast laser Exposure (ROGUEs) [169]. We showed that such devices could increase the backscattered signal by up to 50 dB, significantly increasing the signal to noise ratio (SNR) in optical frequency domain reflectometry (OFDR) measurements. While these devices were developed for distributed sensing applications [170], the complex and intrinsically random frequency response of the ROGUEs makes them perfectly suitable to be used as *weak* PUFs.

5.2 Fabrication Methods

5.2.1 ROGUE Writing

In previous work, we demonstrated that ROGUEs could be fabricated by inducing noise in the fabrication process of a uniform fiber Bragg grating [169]. To achieve this, we added a pseudo-random noise signal to our state-of-the-art, meter-long FBG writing station, that was shown to achieve meter-long in-phase FBGs [130, 131]. This pseudo-random noise signal was added to prevent self-erasure of the grating, as well as to inscribe a random phase throughout the ROGUE’s length. However, the use of such a complex writing station is not necessary to write random gratings. Indeed, we demonstrate here that, by building a much simpler writing station, we can achieve similar results. The ROGUEs are written using a 213 nm UV laser, in a Talbot interferometer writing scheme. The central wavelength of the ROGUE reflection band can be tuned

by changing the angle of intersection of the two UV beams. The fiber is continuously pulled in front of the interference pattern at a constant speed of 20 mm/s by a stepper motor, which rotates an optical fiber bundle. This allows the writing of indefinite lengths of ROGUE, whereas our previous design was limited by the length of the linear stage. Instead of relying on an additional noise signal, the randomness here is provided by the inherent noise in the low-cost simple stepper motor that was used to pull the fiber. This noise is sufficient to prevent the grating's self-erasure while providing the random phase fluctuations necessary to fabricate the ROGUE's unique structure. The fiber is held in the focal spot of the laser by two fiber clamps (FiberVive™ from *PhotoNova Inc.*), which were specially designed to allow the fiber to slide only in the pulling direction. The continuous ROGUE writing setup is shown in Figure 5.1. As proof of concept, a 5 meter-long ROGUE was written in standard deuterium loaded SMF-28 telecommunications fiber.

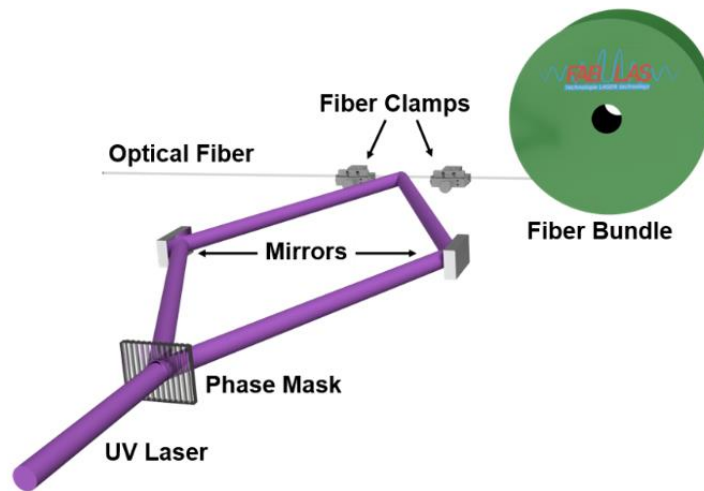


Figure 5.1 Continuous ROGUE writing setup

5.2.2 PUF Fabrication

The ROGUE's frequency spectrum is measured by OFDR, which relies on a tunable laser, which scans the fiber across a certain bandwidth. At every point along the fiber's length, part of the light is backscattered towards the interrogator, and measured by a photodetector. After the scan is completed, the spectrum of the entire fiber under test (FUT) is generated (similar to the spectrum shown in Figure 5.2(b)). An inverse Fourier transform is applied to the spectral data, which results in the reflectivity of the fiber in the spatial domain (see Figure 5.2(a)). By performing a windowed

Fourier transform on specific sections of the overall FUT, their associated spectra can be computed. The ROGUE's backscattered signal is significant enough to make it easily measurable by a commercially available optical backscatter reflectometer (e.g OBR4600, *Luna Inc.*) with a large signal to noise ratio (SNR). In the current case, using the OBR4600, the unexposed telecommunications fiber is approximately 4 dB above the instrument's noise level, while the ROGUE is approximately 24 dB above noise level. While the scan is performed using polarized light, the telecommunications fiber's birefringence is negligible, and therefore light polarization is not expected to affect the measurements. In our experiments, no particular attention was paid to polarization, which is indicative of the PUF's insensitivity to polarization.

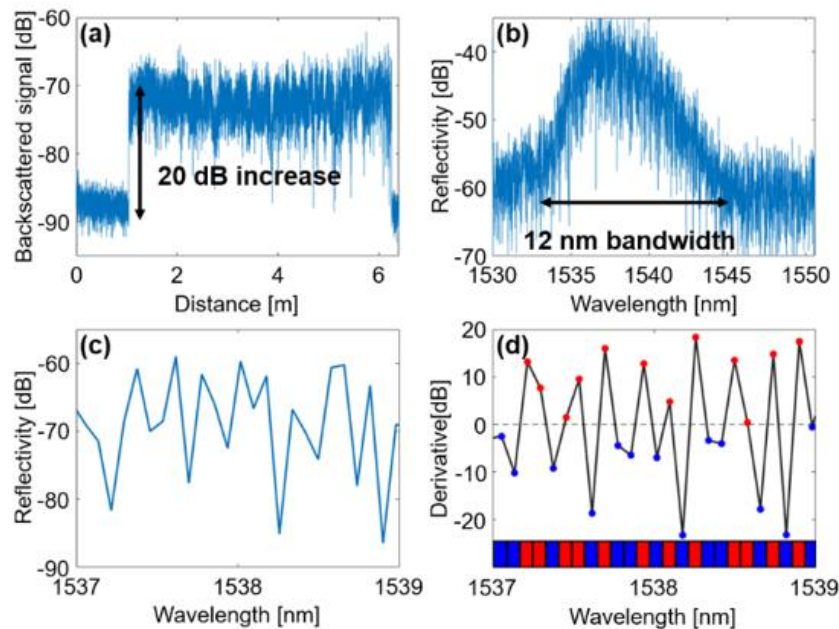


Figure 5.2 ROGUE backscatter signal both shown (a) in the spatial domain, where an improvement in backscattered signal of 20 dB above the unexposed fiber can be observed, and (b) in the spectral domain, where the random structure of the backscattered spectrum is shown, as well as its broad 12 nm full width at first zeros (FWFZ) bandwidth. The PUF generation algorithm is also displayed in (c-d), over a 2 nm bandwidth. From the initial spectrum (c), a discrete derivative is applied, resulting in the signal (d). Positive derivatives are attributed a “1” bit (red), and negative derivatives a “0” bit (blue). The resulting bit sequence is shown at the bottom of (d).

The 5-meter long ROGUE was thus subdivided into individual sections, each of which had its own spectral signature. A 10 mm fiber section, scanned over a 10 nm bandwidth with the interrogator,

returns a spectrum with 128 spectral components. This spectrum can be turned into a digital bit signature by computing the derivative of the spectrum, and attributing a 0 or a 1 depending on the sign of the derivative. This converts the spectrum into a unique 127-bit signature. This algorithm is schematized in Figure 5.2(c-d). The PUF was scanned at a speed of 200 nm/s, meaning the 10 nm bandwidth is acquired in 50 ms.

5.3 PUF Performance

5.3.1 Hamming Distance Distributions

In order to measure the PUFs' performance, two cases were considered. In the first (*intra* case), a single PUF was scanned over 100 successive measurements. Each measurement was separated by an approximately 15 second interval, for a total experimental measurement time of around 25 minutes. This demonstrates the robustness of the PUF's response to time and environmental fluctuations, as the PUFs were placed in an open-air environment with no special care taken to minimize bending or air currents. The extracted bit signature from the first measurement was compared to the subsequent 99 measurements, and the Hamming distances between the reference and measured signatures were computed. Ideally, to ensure correct authentication, the Hamming distance should be as small as possible, as it represents the number of bits that are incorrectly identified. In the second (*inter* case), the first PUF's signature is compared to 499 different PUFs, which were extracted from the 5-meter long inscribed ROGUE. Again, the Hamming distances between the first PUF and the other 499 were computed. If all PUFs are independently random bit signatures, the Hamming distance will be, on average, half the length of the bit sequence, since each bit has a 50% chance of being correct. To provide a basis for comparison, the same measurements were performed on standard SMF-28 telecommunications fiber (TF), whose signal depends solely on Rayleigh backscatter, instead of the inscribed random structure of the ROGUE. Figure 5.3(a-b) displays the resulting *intra* and *inter* distributions, both for the ROGUE PUFs (a), as well as for the TF PUFs (b).

While the *inter* distributions for both ROGUE and TF PUFs appear identical and are both centered near 64 bits, the *intra* distribution of the ROGUE PUFs is much closer to zero than that of its counterpart. This is not surprising, because the higher backscatter signal provided by the ROGUE

increases the SNR, making the measurement more repeatable, and thus each PUF more readily identifiable. While the two distributions for the ROGUE PUFs of Figure 5.3(a) are well apart and easily distinguishable, we can observe there is a significant overlap of the two histograms for the TF in Figure 5.3(b). This is problematic, as it means that it is possible that the correct PUF could be rejected, or alternatively that an intruder could be wrongly authenticated.

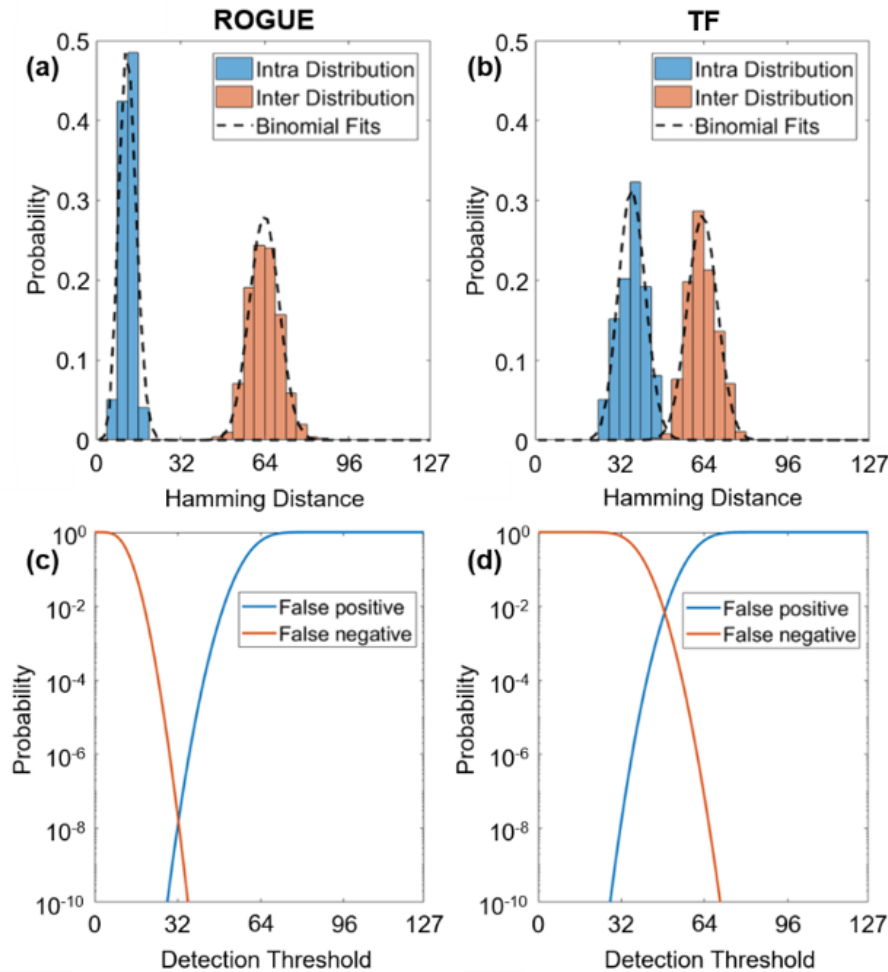


Figure 5.3 Hamming Distance distributions, for both (a) the ROGUE-inscribed PUFs and (b) the TF PUFs. In both cases, the *intra* distribution is shown in blue, while the *inter* distribution is in orange. Binomial distribution fits were applied to all the distributions, are displayed in dashed lines. The false positive and false negative probabilities are also displayed, depending on the detection threshold, for both (c) the ROGUE-inscribed PUFs and (d) the TF PUFs. False positive probabilities are in blue, while false negative probabilities are in orange.

5.3.2 False positive and negative probabilities

To quantify these probabilities, a theoretical fit was performed on the experimentally measured histograms. If each bit of the 127-bit signature of the PUF has a probability p of being incorrect, and that the probability of a given bit to be correct is independent of the probability of the others, then the Hamming distance H between two bit sequences is expected to follow a binomial distribution such that $H \sim B(n, p)$, with n the number of bits in the sequence [112]. The probability of measuring a certain Hamming distance k is given by the probability mass function

$$P(H = k) = \binom{n}{k} p^k (1-p)^{n-k}. \quad (5.1)$$

In the *inter* case, p is expected to be 0.5. As can be seen in Figure 5.3, the measured distribution of H has a good match with the theoretical binomial distribution $B(127, 0.5)$, shown by the dashed lines, in both cases of the ROGUE and TF. A binomial distribution fit was also performed in the *intra* case. This resulted in p values of respectively 0.091 and 0.286 for the ROGUE and TF PUFs.

To compute the probabilities of wrongly authenticating the incorrect user (false positive), or of wrongly rejecting the correct user (false negative), a Hamming distance authentication threshold k_{th} must be set. Therefore, if the measured Hamming distance is below the threshold, the user is authenticated, and if it is above the threshold, the user is rejected. From the fitted distributions, and depending on the threshold, the probabilities of false positive PFP and false negative PFN can be calculated using

$$P_{FP} = \sum_{k=0}^{k_{th}} P_{inter}(H = k), \quad (5.2a)$$

$$P_{FN} = \sum_{k=k_{th}+1}^n P_{intra}(H = k), \quad (5.2b)$$

where P_{inter} is the *inter* probability distribution and P_{intra} is the *intra* probability distribution. Figure 5.3(c-d) display those values, for both the ROGUE and the TF. Ideally, both values should be as low as possible, therefore it makes sense to look at the intersection of those two curves. For the ROGUE PUFs, this threshold would be at a Hamming distance of $k_{th} = 32$, which results in false positive and false negative rates of, respectively, 0.01 and 0.02 ppm (parts per million). For the TF,

this threshold obviously has to be higher, at 49, which results in probabilities of respectively 8,000 and 5,000 ppm, more than five orders of magnitude greater than that of the ROGUE PUFs. While a false positive probability of 0.01 ppm is very low, for certain high-stakes applications it may be insufficient. However, it is possible to choose a threshold that is lower than 32, which would further decrease the false positive probability, at the cost of raising the false negative probability. As an example, a threshold $k_{th} = 24$ could be picked, which would provide a false positive probability of less than 1 part per trillion (0.45 ppt). This would come at the cost of an increase to 171 ppm of the probability of false negative, meaning in some rare instances, the correct user could be wrongly rejected. However, this could be mitigated by allowing the user two or three attempts at authentication.

5.3.3 Temperature Dependence

The ROGUE's reflection spectra, like that of any fiber Bragg grating, will be dependent on environmental fluctuations. Indeed, applying a positive (negative) strain or temperature change on the ROGUE will shift its spectrum to the longer (shorter) wavelengths. This phenomenon is well known in literature and is the basis of OFDR sensing [171]. In our previous work, we demonstrated that the ROGUE could be used to accurately measure strain or temperature variations with high precision [169]. If this wavelength shift is not compensated, any temperature shift or bend in the fiber will completely change the PUF's signature, ruining the authentication process. Therefore, a temperature/strain compensation technique must be applied to measure and correct for this wavelength shift. To demonstrate this compensation technique, four 10-mm ROGUEs of different backscatter strengths were written in standard telecommunications fiber, by varying the speed used for writing. Then, a uniform strain was applied on the ROGUEs, to simulate different environmental conditions either due to temperature changes or axial strain of the fiber. An additional step of sensing is added to the PUF authentication algorithm to measure the wavelength shift and then compensate it. Since both strain and temperature changes have the same effect on the ROGUE's spectrum, the algorithm is unable to identify if it comes from strain or temperature change, but this information is irrelevant, so long as the algorithm is able to compensate it. This algorithm is described in detail in Supplementary Material (section 5.6). Considering the PUF's very short length (10 mm), we restricted this analysis to cases where either the strain or the

temperature changes are uniformly applied to it. This is very reasonable, as the PUF can be packaged to impose that restriction.

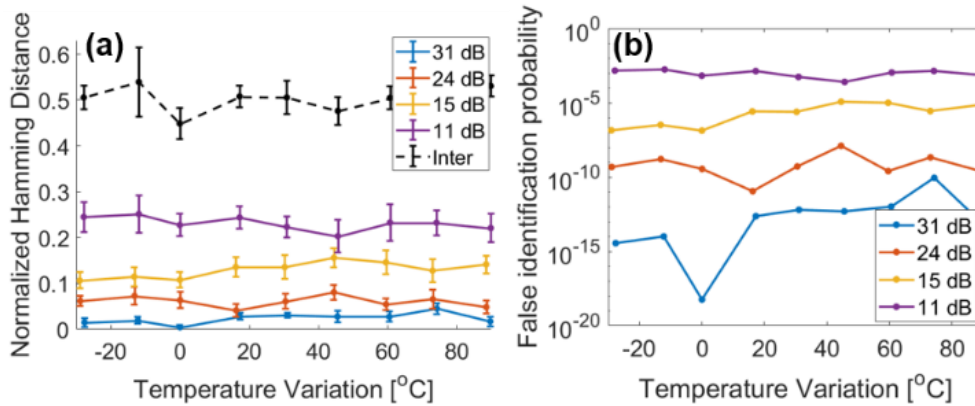


Figure 5.4 (a) Hamming distance for the *intra* case, for different ROGUE strengths, normalized by the bit signature's length, as a function of the temperature variation. The *inter* case is also shown in the dashed black line. The error bars correspond to one standard deviation. (b) False identification probabilities associated with the normalized Hamming distances.

The recovered Hamming distances after environmental fluctuations compensation is shown in Figure 5.4(a) for the different ROGUE strengths. For every data point, 10 measurements are made and compared to a single reference. The average Hamming distance is displayed in Figure 5.4(a), and the standard deviation is shown with the error bars. The Hamming distance here is normalized by the bit sequence's length, as part of the spectrum is lost due to its strain/temperature induced wavelength shift, thus slightly decreasing the bit sequence's length as the wavelength shift gets bigger. As can be observed, the algorithm can easily compensate for large temperature fluctuations with minimal degradation in its ability to correctly identify the PUF. The *inter* case shown in the black dashed line demonstrates that this additional post-processing step does not affect the algorithm's ability to reject the incorrect PUFs, as the normalized Hamming distance remains near 0.5 even after this post-processing step. The associated false identification probabilities are displayed in Figure 5.4(b), which are again mostly flat for all the environmental fluctuations investigated. It can be also noted that, unsurprisingly, the ROGUEs that exhibited higher backscatter strengths resulted in smaller Hamming distances, and therefore lower false identification probabilities, due to the enhanced SNR. The strain values (-25 grams to +75 grams

of tension) here are converted to temperature variations (-30 to +90 °C) as this is more representative of real life conditions.

5.3.4 Other interrogation parameters

Alternatively, the quality of the results can be further improved by tuning the interrogation parameters. For example, scanning across a larger bandwidth provides a spectrum with more spectral components, which increases the bit sequence length. As such, this increases the security of the generated PUF, and allows for more error correction capabilities. Similarly, the PUF's length can be increased to provide the same effect, where doubling the length would allow for twice as many bits. To observe the effect those parameters have on the PUF performance, measurements of both *intra* and *inter* distributions were realized with different interrogation parameters. In a similar fashion to the analysis described above, a binomial fit was performed to compute false positive and false negative probabilities. To provide a good basis of comparison, the authentication threshold k_{th} used for each of those measurements was the one where the false positive and false negative curves intersect. Due to the discrete character of the Hamming distance, P_{FP} and P_{FN} are not exactly equal, therefore the false identification probability is defined as

$$P_{FI} = \max(P_{FP}, P_{FN}). \quad (5.3)$$

Figure 5.5 displays this false identification probability, depending on the interrogation parameters used. Unsurprisingly, adding more bits to the bit sequence, either through a larger scanned bandwidth or through longer PUF lengths, results in decreased false identification probability, due to the larger separation between the *intra* or *inter* distributions. However, it can be seen that the effect of those parameters is not the same, namely the use of a longer PUF length has a much more dramatic effect on the false identification probability than the scanned bandwidth. This is because the ROGUE has a limited bandwidth, as shown in Figure 5.2(b), therefore using a wider scanned bandwidth dilutes the high SNR data within the ROGUE bandwidth with lower SNR data outside of it. This dilution of the SNR competes with the longer bit sequences originating from the wider scanned bandwidth, resulting in only small improvements in PUF performance. This could be avoided by writing a ROGUE with a larger bandwidth, which can be achieved by varying the writing laser's spot size. Indeed, as the ROGUE can be considered as a superposition of a multitude of individual gratings, of a length equal to that of its spot size, its overall bandwidth will localize

to that of the individual grating, as predicted by Shapira *et al.* [20], and as we observed experimentally [169]. As such, the spot size of the laser should be tuned to best fit the interrogation bandwidth used since, as can be seen, scanning beyond the ROGUE's bandwidth adds little to the PUF performance.

On the other hand, using a longer PUF increases the number of bits in the bit sequence without diluting the SNR, which results in much more dramatic decreases in false identification probability, as can be seen in Figure 5.5. Even while using the smallest 5.24 nm scanned bandwidth, the false probability is below 10^{-20} , and falls below 10^{-27} while using the broader 21.16 nm bandwidth.

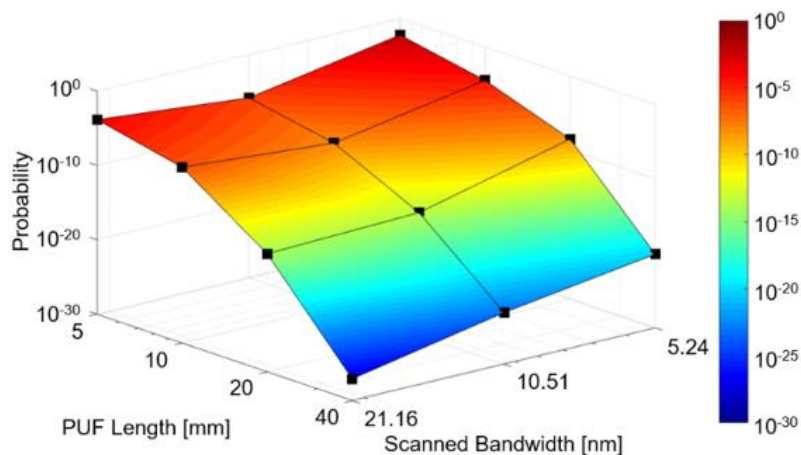


Figure 5.5 Probability of false identification for the ROGUE PUFs, for different PUF lengths and scanned bandwidth. The face color is interpolated from the experimental data points (black squares).

5.3.5 Alternative Digitization Algorithm

In the scheme developed so far, the 128 spectral components are digitized into a 127 bit sequence by using the sign of each of the 127 components of the discrete derivative to decide if a bit should be a 0 or a 1. This is akin to using the first bit (the sign bit) of a floating-point computer number format (e.g. the single 32-bit or double 64-bit formats) expressing the derivative. However, to achieve an even greater degree of security, one could consider using more bits than simply the sign bit of the derivative. Furthermore, this removes the need to perform the derivative, since the algorithm can directly use the measured data. This would turn the bit signature length n from

$(N-1)$ to $m \times N$, where N is the number of spectral components, and m is the number of bits used per floating-point number. However, depending on the signal, the bits used might change the probabilities p of the *intra* and *inter* distributions. Indeed, the bit used must be significant enough to be repeatable through multiple measurements (the *intra* case), while still being unpredictable from one PUF to the other (the *inter* case). Again, the enhanced SNR of the ROGUE allows here the use of a greater number of bits, since the measured values are less sensitive to external noise, and as such are more repeatable.

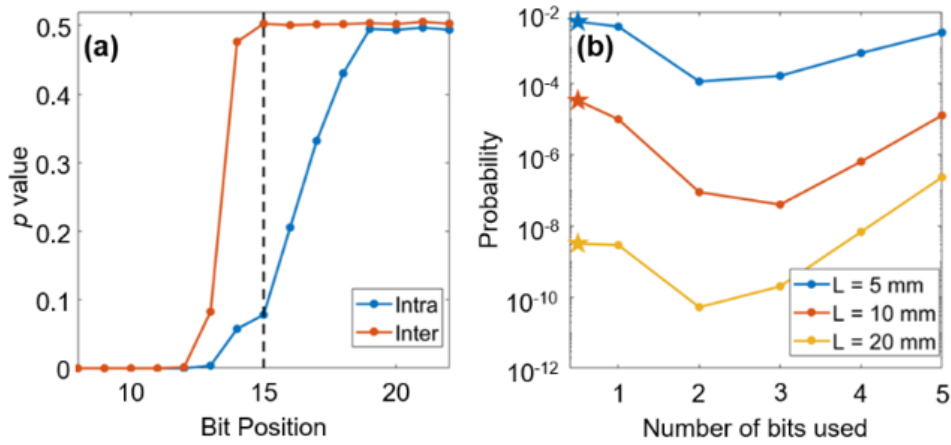


Figure 5.6 (a) Fitted binomial p values for both *intra* (blue) and *inter* (orange) distributions, for each of the bits of the 64-bit double representation, for $L = 20$ mm. Only bits 5 to 25 are shown, although the behaviour observed extends on both sides. The dashed line identifies the threshold at which the *inter* distribution reaches $p = 0.50 \pm 0.02$. (b) False identification probability P_{FI} depending on the digitization used, for the first three PUF lengths, with the 5.24 nm scanned bandwidth. The star marker is the probability computed using the derivative algorithm described earlier.

In order to make sure this is indeed the case, the p value was computed for each of the bits of the raw backscattered signal, when expressed in a double 64-bit floating-point computer format, as shown in Figure 5.6(a). Obviously, the first bits are identical for all the PUFs (*inter* case), since the backscatter is of a similar order of magnitude for all PUFs. However, as we move towards the least significant bits, it can be seen that the p value of the *inter* case increases, until the 15th bit where it reaches a value of approximately 0.5, which is the expected value for a randomly varying bit. This is indicated by the dashed line in Figure 5.6(a). At the same time, the p value of the *intra* case

remains small, meaning that, while those bits vary randomly between different PUFs, they can still be used to authenticate a single PUF.

To determine how many bits can be used in this fashion, the probability of false identification was computed for bit sequences using up to 5 bits per spectral component. The bits were taken sequentially after the threshold identified in Figure 5.6(a). Since this algorithm is highly dependent on the SNR, only the smallest 5.24 nm scanning bandwidth was used, to ensure that each spectral component profited from the ROGUE's enhancement. Figure 5.6(b) displays the evolution of the false identification probability, depending on the number of bits used in the algorithm. For ease of representation, only the three first PUF lengths were shown, although a similar behaviour was observed using the 40 mm PUF length. For comparison, the probability obtained by the derivative method is shown with the star marker. When using the first bit of this digitization scheme, the false identification probabilities are similar (and even slightly lower) than the ones obtained by using the derivative algorithm, due to the additional 128th bit that is kept. However, when expanding to 2 or 3 bits per spectral component, it can be observed that the false identification probability can decrease by almost 2 orders of magnitude for each of the investigated lengths.

5.4 Discussion

The PUFs described in this article combine high performance, small footprint, low-cost of fabrication and ease of implementation. Being fiber-based, they have the advantage of being easy to integrate in telecommunications networks. While in this current study, deuterium loading of the fiber was needed prior to the inscription to increase the fiber's photosensitivity, this is not necessary with photosensitive fibers, which generally contain higher concentration of germanium than standard telecommunications fiber [172]. To avoid the need to remove the protective acrylate coating, femtosecond laser writing through the coating could be implemented [16, 173, 174], as well as the use of UV-transparent coatings [15, 175]. Alternatively, the writing technique could be easily scaled to be used on the fiber drawing tower, so that the ROGUEs are written as the fiber is being pulled before the coating process. Indeed, this has been implemented using UV laser writing in a Talbot interferometer writing scheme similar to the one presented here [176, 177]. This would allow the UV inscription of the ROGUEs prior to the coating application, and would also help with

mass-production. Being noise-based, the ROGUEs necessitate no precise alignment nor perfect control over the fiber pulling speed.

Alternatively, highly scattering fibers [155, 178] could be used in a similar fashion as the PUFs we presented in this article, as well as other types of scattering enhanced optical fibers, such as through direct UV [149] or femtosecond laser [25, 148] exposure, without being restricted by the ROGUE's bandwidth. However, as the scattering in those fibers is non-directional, this would incur additional loss as light would also be scattered outside of the fiber. Even though the underlying principle is similar to the one proposed by Du *et al.* [164], the use of standard telecommunications fiber needed a custom interrogator designed to accommodate its minuscule Rayleigh scatter. In comparison, the ROGUE's enhanced backscatter makes it compatible with commercial interrogators, making this technology truly implementable for the first time. While in the current demonstration, the wavelength scan necessary to the PUF authentication is relatively slow (at 200 nm/s, a 21.16 nm scan takes approximately 100 ms), this is only limited by the current interrogator used. More recent OFDR interrogators can now perform OFDR measurements at rates above 250 Hz [179]. It should also be pointed out that the OFDR algorithm provides information on the spectrum in a distributed fashion along the length of the optical fiber over several meters with a resolution that can reach only a few mms. In practice, this means that, during the enrollment process, several PUFs could be scanned simultaneously, provided that they are either written in the same optical fiber or positioned sequentially on different fibers, before they are separated into independent PUFs. This could significantly speed up the enrollment process.

Throughout the years, there have been many different designs for optical PUF architectures. The simplest optical PUF architecture is based on laser speckle. While the interrogation system is very simple, requiring only a laser diode and a CCD camera, it is highly sensitive to interrogation parameters. For strong PUF applications, this is very good as it results in a wide CRP domain, however it means that each challenge is difficult to reliably reproduce. For instance, in Yeh *et al.* study [109], complex post-processing steps (a Gabor filter, Scale-Invariant Feature Transform and projection processes) had to be used to ensure reliable authentication in the presence of slightly different interrogation conditions. Even with all this computational complexity, only a few degrees of rotation or a few mm of displacement resulted in a significantly decreased accuracy.

Mesaritakis et al. [110] demonstrated the use of a multimode polymer optical fiber as PUF. Again, the speckle response of the PUF was measured, with different potential challenges being wavelength and angle of interrogation. The interrogation system they require is very similar, but again the response is very sensitive to perturbations. Indeed, they showed that by pushing on the side of the fiber with a piston, a displacement of only a few microns was sufficient to completely decorrelate the response. Again, this is fantastic to generate a large CRP domain, but is problematic when attempting to reproduce a challenge. In contrast, our system, being based on single-mode optical fibers, is not as dependent on interrogation parameters, as light will always be guided in the same optical mode. This makes the challenges much easier to reproduce.

Many designs of PUFs have been presented over the years, most of them relying on silicon devices such as SRAM, as they can easily be integrated in FPGAs and other integrated circuits. In a similar fashion, this PUF is written inside an optical fiber's core, which makes it easy to integrate into existing optical fiber communications network. Even though the current PUF only has a single CRP, there are many potential applications for such *weak* PUFs, most of them related to the generation of a private key from the PUF response. This private key, in conjunction with a fuzzy extractor, can then be used as a cryptographic key [114, 115], as a unique identifier [180], or for mutual authentication protocols, when combined with other modalities [181]. An additional advantage of PUF-based cryptographic keys, when compared with standard cryptographic protocols, is that the key is physically stored on the device, rather than digitally saved [113]. This enhances key storage security.

While it would be in theory possible to fabricate a copy of this ROGUE, for example by using a point-by-point fabrication technique [19], reverse-engineering the required recipe to achieve the exact same spectrum is far from trivial. Furthermore, experimentally obtaining the degree of precision required to perfectly enact this recipe is a daunting task which is nigh-impossible to achieve, even with a state-of-the-art fabrication station. However, even if a grating fabrication station could achieve the level of precision required to reproduce the ROGUEs presented in this manuscript, it is very easy to simply further increase the ROGUE length, which will increase the complexity of the spectral response, and thus make it even more challenging to copy.

While the current demonstration relies on an OFDR interrogator, it is not the only way to obtain the ROGUE's PUF signature. Indeed, at its core, all the information required is obtained by

measuring the spectral response of the ROGUE, which can be achieved using much simpler apparatus. While these other interrogation techniques may not be as sensitive as the OFDR system we used, this can be mitigated by using higher-scattering fibers. Indeed, the 20 dB enhancement in signal over the SMF28 level in the present ROGUEs is modest, compared to the >40 dB reported using femtosecond laser exposure [148] or nanoparticle-doped fibers [155], or even through ROGUE inscription, as we demonstrated that, in the appropriate writing conditions and with a highly photosensitive fiber, the enhancement could reach 50 dB [169]. Such highly enhanced fibers could then be interrogated using other techniques.

The alternate digitization algorithm described in section 5.3.5 makes use of the ROGUE's enhanced SNR to increase the number of bits extracted from each spectral component, and thus increases the complexity of the generated binary key. While, as shown in Figure 5.5, it may not be necessary to use this enhanced digitization scheme to achieve low false identification probabilities, depending on the interrogation and PUF fabrication schemes, this is an additional tool that can be used in the cases where the initial parameters cannot provide sufficiently high performance. Since the number of bits that can be extracted by using this algorithm is highly dependent on the SNR, it is expected that more bits could be thus extracted by using either a more sensitive interrogator or a higher scattering PUF. This would further increase the bit sequence length, and thus improve the PUF performance.

5.5 Conclusion

In conclusion, we demonstrate a novel *weak* PUF architecture, based on the inscription of Random Optical Gratings written by Ultraviolet or ultrafast laser Exposure (ROGUEs) in standard telecommunications fiber by a simple, low-cost fabrication station that could be easily implemented on the fiber drawing tower. The unique spectral signature of these ROGUEs can be measured by optical frequency domain reflectometry (OFDR), and is strong enough to be compatible with a commercial interrogator, making the commercial deployment of such a technology easy and much more attractive. We demonstrate that the ROGUEs exhibit impressive PUF performance, due to their enhanced random backscattered signal over a broad bandwidth. For the interrogations parameters used in the comparison, we show that the use of the ROGUE as PUFs results in an improvement of over 5 orders of magnitude in false identification probabilities when

compared with the unexposed fiber. Furthermore, we show that, depending on the interrogation parameters, this probability reaches values as low as 10^{-27} . Finally, we describe an alternative digitization scheme which allows the possibility of increasing the number of bits used in the digitization process, again profiting off the high backscatter enhancement offered by the ROGUE. This results in longer bit sequences, which provide additional security, decreasing the false identification probabilities by almost two orders of magnitude. While this enhancement may not be necessary for some of the parameters investigated in this article, it is an additional tool which can improve the security of this technique when needed.

Even though the current demonstration is based on ROGUEs written in single-mode fibers, this methodology could be easily implemented in multimode fibers, thus expanding the CRP domain by incorporating the interrogation angle in the challenge, which could pave the way for *strong* PUF applications. Finally, it should not escape the reader that these ROGUE PUFs are hardware equivalents of Non Fungible Tokens (NFTs) and hence should find applications in a variety of scenarios in which authentication is of paramount importance in determining authenticity and ownership.

5.6 Supplementary Material

5.6.1 Temperature and Strain Compensation Algorithm

To compensate for temperature or strain variations between the reference and subsequent measurements, additional compensation post-processing steps were implemented in the authentication algorithm to measure and then compensate for the resulting wavelength shift in the spectrum. The first step is to accurately measure the spectral shift due to those fluctuations. In order to do that, a standard OFDR sensing algorithm is applied, where the cross-correlation between the reference spectrum and its shifted version is computed, and the position of the maximum is then identified, to measure the spectral shift between the two measurements [73]. The cross correlation between the spectra $X(\lambda)$ and $Y(\lambda)$, as a function of the spectral shift Λ , is defined as

$$C_{x,y}(\Lambda) = \frac{\int \delta X(\lambda + \Lambda) \delta Y(\lambda) d\lambda}{\sqrt{\int (\delta X(\lambda))^2 d\lambda \int (\delta Y(\lambda))^2 d\lambda}}, \quad (5.4)$$

where $\delta X(\lambda) = X(\lambda) - \langle X(\lambda) \rangle$. A *sinc* interpolation technique is used to more accurately compute the position of the cross-correlation maximum, based on the use of padding zeros as described by Cui *et al.* [147] and implemented in our earlier work [169]. This technique can be implemented numerically, by simply adding zeros to the temporal signal, or physically, by performing the Fourier transform also on the unexposed regions of standard telecommunications fiber surrounding the ROGUE. Due to the significantly higher backscatter signal of the ROGUE, adding regions of unexposed fiber on both sides has a similar effect to numerically adding padding zeros, while also rendering the algorithm insensitive to changes in the temporal delay between the interrogator and the ROGUE. In the current demonstration, the Fourier transform is performed on a 40 mm section of fiber, which included the 10 mm ROGUE, with 10^5 additional padding zeros numerically added to further improve the *sinc* interpolation. The effect of this interpolation on the cross-correlation results is shown in Figure 5.7. While this interpolation results in a slight increase in the maximum cross-correlation values from Figure 5.7(b) to (f), the improvement in accuracy really comes from the enhanced resolution.

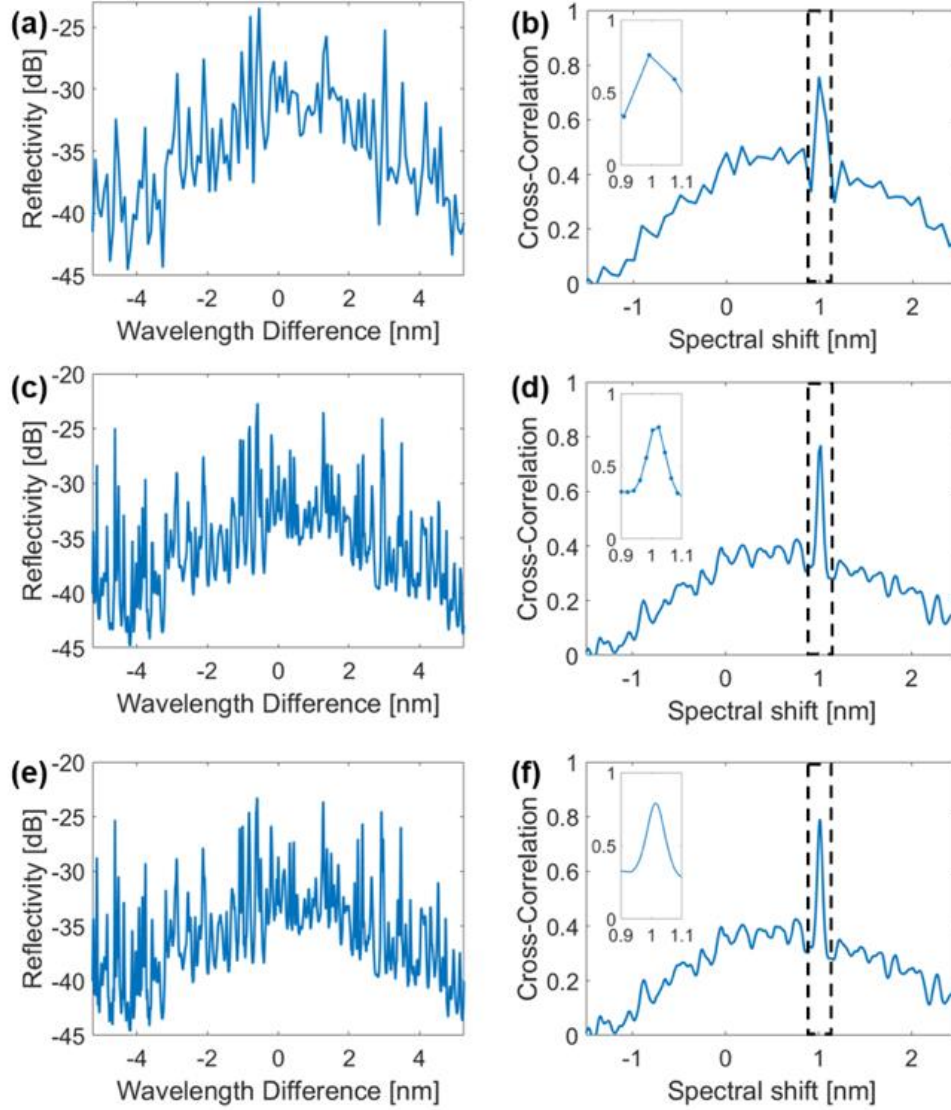


Figure 5.7 ROGUE Spectrum (a-c-e) and Cross-Correlation between reference and sample measurements (b-d-f) for different interpolation regimes. Subfigures (a-b) use only the raw data of the 10-mm ROGUE, (c-d) use the raw data using a 40-mm scanned window, including the 10-mm ROGUE and (e-f) use an additional 10^5 padding zeros added numerically. The inset in (b-d-f) displays the central peak, where the improvement in resolution can be better observed.

The measured spectral shift is then compensated for by shifting the spectrum by the same amount. Again, in order to improve the compensation accuracy, the interpolated spectrum is used instead of the raw spectrum to correct for shifts that are not an exact multiple of the raw spectral resolution. From this shifted interpolated spectrum, the values at the original 128 spectral components are then

extracted, and a numerical derivative is then performed on the extracted spectrum to obtain the digital bit signature. To avoid artificially decreasing the Hamming distances in the *inter* cases, this compensation technique is only applied when the cross-correlation is above a certain value (here, a threshold of 0.5 is applied).

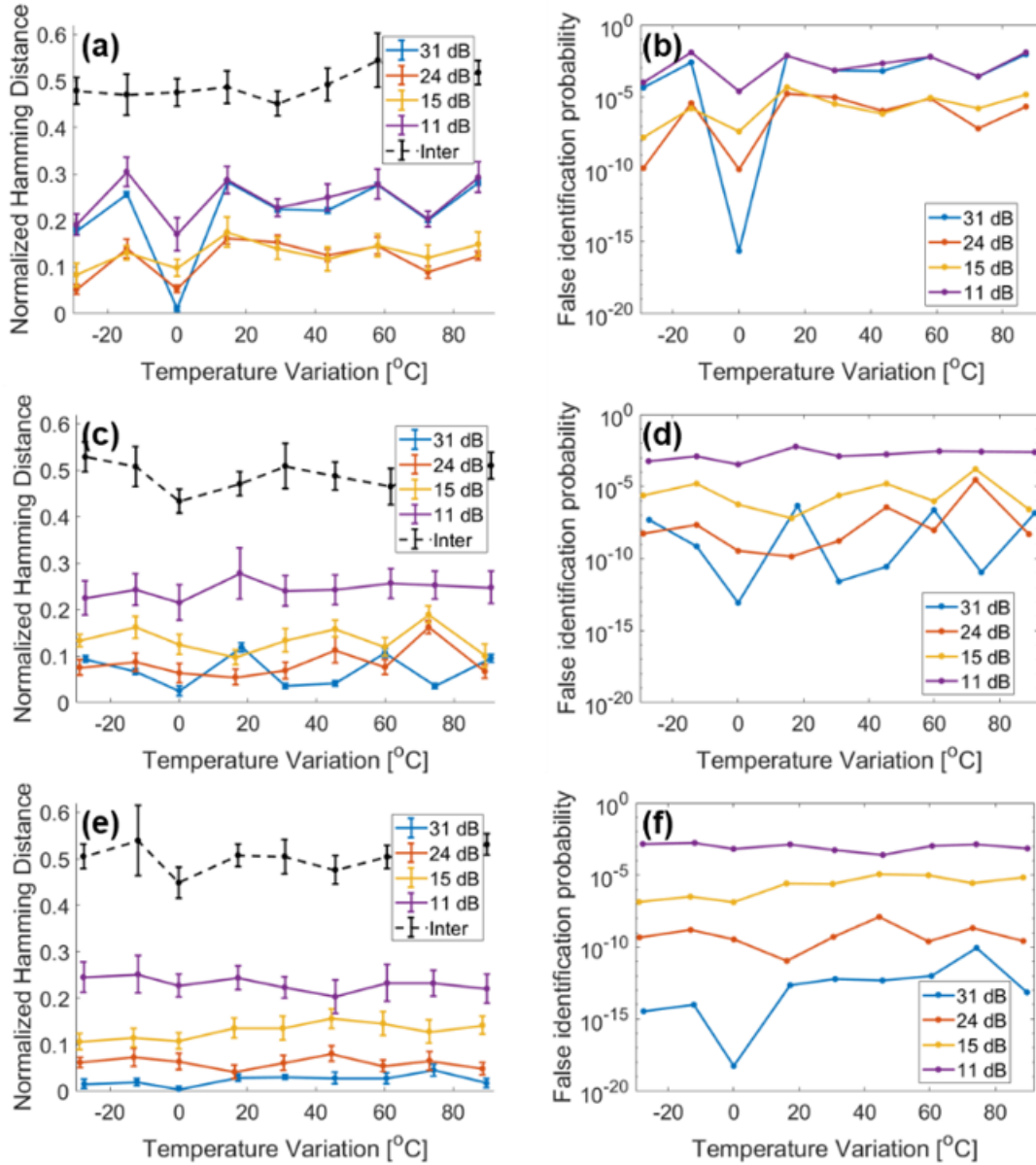


Figure 5.8 Normalized Hamming Distance (a-c-e) and associated false identification probabilities (b-d-f) for different interpolation regimes. Subfigures (a-b) use only the raw data of the 10-mm ROGUE, (c-d) use the raw data using a 40-mm scanned window, including the 10-mm ROGUE and (e-f) use an additional 10^5 padding zeros added numerically.

Figure 5.8 highlights the improvement this interpolation technique provides for the compensation technique on the Hamming distance computed as a function of the temperature variations. Indeed, when no interpolation is applied, the computed Hamming distances oscillate depending on how close the spectral shift is to a multiple of the raw spectral resolution. However, when the interpolation is applied, the Hamming distances are much flatter. As demonstrated in our earlier sensing article [169], while increasing the number of padding zeros used in the algorithm improves the ability to detect very small spectral shifts, it also increases the computing time. A compromise needs to be found between spectral resolution and computing demands. For the current application, 10^5 padding zeros were found to be sufficient for accurate compensation without being too demanding on computing capabilities, where the post-processing steps would take approximately 120 ms to compute on a standard laptop computer. This processing time scales with the number of padding zeros, with 10^6 zeros corresponding to 1.2 s.

It should also be pointed out that, for large temperature variations, part of the spectrum is no longer measured due to the wavelength shift. This could be mitigated by shifting the central wavelength of the interrogator by the appropriate amount after an initial scan used to sense the required wavelength shift. However, for the temperature/strain values investigated here, which are representative of most applications (-30C to +90C), this effect is minimal, where the total bit sequence length only decreases from 128 to 115 for the extreme values of the shifts investigated.

CHAPTER 6 ARTICLE 3: A SIMPLE HIGH-SPEED RANDOM NUMBER GENERATOR WITH MINIMAL POST-PROCESSING USING A RANDOM RAMAN FIBER LASER

Authors: Frédéric Monet, Jean-Sébastien Boisvert, Raman Kashyap

Published in: Scientific Reports 11(1), 1-8, June 23, 2021.

A simple novel method for random number generation is presented, based on a random Raman fiber laser. This laser is built in a half-open cavity scheme, closed on one side by a narrow-linewidth 100 mm fiber Bragg grating. The interaction between the randomly excited lasing modes of this laser, in addition to nonlinear effects such as modulation instability, allow the generation of random bits at rates of up to 540 Gbps with minimal post processing. Evaluation of the resulting bit streams' randomness by the NIST statistical test suite highlights the importance of evaluating the physical entropy content, as bit sequences generated by this random laser pass all the statistical tests with a significance level of 0.01, despite being generated at more than twice the theoretical entropy generation speed.

6.1 Introduction

Random number generation (RNG) has risen in interest for various applications such as Monte Carlo simulations and secure communications, where pseudo-random numbers generated by deterministic algorithms do not have the necessary non-reproducibility and non-periodicity of true physical random numbers [182]. To address this need, optical RNG based on physical phenomena have been investigated to generate random numbers at very high speeds. Chaotic semiconductor lasers are an interesting avenue, because their large bandwidth allows them to generate random numbers at extremely high bitrates [183]. Using external feedback to the cavity, RNG of hundreds of Gbps have been demonstrated using those lasers [93, 184, 185]. Furthermore, by combining multiple lasers and separating the measurements on multiple channels, RNG was demonstrated to achieve bit rates of up to 2.24 Tbps [99].

Random fiber lasers were also investigated in recent years, for their very simple design and unique properties. While they show great promise for applications such as in speckle-free imaging [44] and cancerous tissue diagnostics [43], they are particularly well suited for RNG, due to their

intrinsically unpredictable output. Using Brillouin random fiber lasers, RNG was demonstrated at tens of Mbps [92]. Another random fiber laser scheme using semiconductor optical amplifiers in a ring resonator achieved RNG at 1.6 Gbps [45]. However, this is still very far from the required bandwidths of high-speed secure communications and cannot compete with the high bitrates achieved by chaotic semiconductor lasers. Recent work involving ytterbium-doped random fiber lasers, relying on the Rayleigh scattering of a single mode fiber as feedback, have demonstrated bitrates of 200 Gbps [186]. This laser architecture was also used for temporal ghost imaging, demonstrating another possible application where random fiber lasers surpass the performance of conventional cavity-based fiber lasers [187].

A common technique used to enhance RNG speeds is to post-process the acquired data. The most typically used post-processing method is to truncate the least significant bits (LSBs) from the digitized signal [93, 99]. This technique requires the least amount of post-processing, can be realized in real-time, and has the additional benefit of multiplying the acquisition rate by the number of retained LSBs. Another common technique uses a delayed exclusive OR (XOR) operation on the bit streams to enhance randomness [94, 95, 103, 186]. Although simple, this technique requires additional steps which can compromise real-time implementation. Even more complex post-processing algorithms have also been investigated, for example relying on successive derivatives of the measured signal, which artificially increases the number of bits digitized by an analog to digital converter (ADC). Kanter *et al.* [96] showed that by computing the 15th derivative of the signal, their algorithm was able to recover 15 random bits per sample from a signal originally quantized by an 8-bit ADC. However, this complicated post-processing scheme cannot be achieved in real-time, limiting the possibility of its implementation. Furthermore, it is important to note that the use of XOR operations or numerical derivatives does not increase the physical entropy generated, which ultimately limits the attainable RNG rate. Indeed, the use of deterministic post-processing schemes can at best hide existing correlations in the dataset from statistical tests, but it cannot improve the bits' randomness [98].

An article recently published in *Science* by Kim *et al.* [103] demonstrated a different RNG technique based on the interference of multiple lasing modes, both longitudinal and transverse, in a chip-scale laser diode. Due to the interaction of all the lasing modes, a total bit rate of nearly 200 Tbps was achieved by spatially multiplexing 243 channels, each generating random numbers

at 820 Gbps. Each channel selected the 2 LSBs, sampling every 2.44 ps (corresponding to a 410 GSa/s sampling rate), and a self-delayed XOR operation was applied in post-processing to the acquired bits. However, it should be noted that the separation between the spatial channels (which ultimately determined the number of multiplexed channels) was selected based on statistical tests performed after the application of this XOR operation, and not on the entropy content evaluation, thus indicating the care needed to interpret the measured results.

In this work, we demonstrate a novel RNG technique that is also based on the interaction of lasing modes, but this time in a random laser. In our case, the modes are in the modeless cavity of a random Raman fiber laser, where a multitude of lasing modes will be randomly excited simultaneously. Furthermore, nonlinear effects such as modulation instability, increase the inherent randomness of this laser. This laser has a very simple architecture, which relies solely on a fiber Bragg grating (FBG) and some length of optical fiber, resulting in a half-open cavity scheme. No post-processing technique other than LSB selection was used, to avoid compromising the bits' true randomness, as well as to offer the possibility of real-time implementation. To the best of our knowledge, this is the first demonstration of RNG based on random Raman fiber lasers. It is also the highest reported bitrate for random laser based RNG, on par with current state of the art techniques such as chaotic semiconductor lasers. Furthermore, we show that, while a bit sequence generated at 1.28 Tbps can pass statistical tests such as autocorrelation and the National Institute of Standards and Technology (NIST) randomness test suite without any further deterministic post-processing steps, the theoretical entropy generated by this laser is limited to 540 Gbps. This highlights the importance of proper entropy content computation, especially for parallel RNG schemes where such tests are still heavily used to validate randomness [100, 103].

6.2 Random Raman fiber laser emission

The random Raman fiber laser is built in a very simple half-open cavity scheme comprising a highly reflective FBG and non-zero dispersion shifted optical fiber (see Methods). Figure 6.1 shows the output spectrum of the random laser at various pump powers. At lower pump powers, the laser exhibits a narrow linewidth of 320 pm at -10 dB. However, as the pump power increases, so does the linewidth, reaching 2.66 nm at 5.64 W pump power. This laser shows 49 dB ASE suppression at low powers and 35 dB suppression at this pump power. Increasing the pump power further results

in the generation of the second Raman Stokes, and as such decreases the output power at 1572 nm. Pumping near the fiber's ZDW gives rise to nonlinear phenomena such as modulation instability. Modulation instability will break the laser output into series of ultrashort, random pulses, which, when coupled to the large number of random lasing modes in the modeless cavity structure of this laser, will further promote the random number generation process. Further details on our observation of modulation instability can be found in Supplementary Material (section 6.10), as well as a comparison study between the fiber used in this experiment and a standard telecommunications fiber highlighting the importance of pumping near the ZDW.

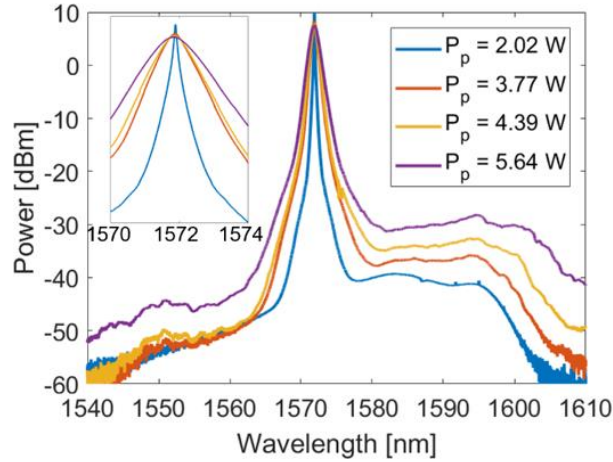


Figure 6.1 Output spectra of the random laser at various pump powers. The inset on the left shows the laser linewidth broadening.

To confirm that this laser is indeed operating in the random lasing regime, its output was connected to a 70 GHz photodiode, and the electrical signal was digitized by a 110 GHz, 10-bit analog-to-digital converter (ADC), real-time oscilloscope (Keysight UXR0702AP). This ADC sampled the signal at 256 GSa/s, and statistical analysis was performed on the resulting time-domain signal. Indeed, as demonstrated by Raposo *et al.* [53], and later experimentally confirmed for random Raman lasers by Li *et al.* [54], a random laser's output power is characterized by a Lévy-like distribution, an asymmetrical distribution with a heavy tail towards the higher powers. The α -stable Lévy probability density function (PDF) is most importantly characterized by the Lévy index α , where $\alpha = 2$ corresponds to a Gaussian distribution, and $0 < \alpha < 2$ corresponds to a Lévy-like distribution. As the pump power is increased, three different statistical regimes can be observed.

Below threshold, the output follows a Gaussian distribution, with $\alpha = 2$. However, near the threshold, the random laser's output changes towards a Lévy-like distribution, with a sharp decrease in the α parameter. This change in the statistical regime of the laser has even been suggested as a universal identifier of the lasing threshold in random lasers [55]. Finally, above threshold, a gradual return towards a Gaussian regime is observed. Figure 6.2(a) displays the evolution of both the α parameter and output power as the pump power is increased. As can be observed, a sharp transition from the Gaussian regime to the Lévy regime is identified near the lasing threshold, with a gradual return towards a Gaussian regime at higher pump powers, corresponding to the expected behaviour of a random laser. The α parameter was estimated using the regression method proposed by Koutrouvelis [188]. Histograms displaying the distributions governing the emitted powers for increasing pump powers can be found in Supplementary Material (see section 6.10), which highlight the transition from Gaussian to Lévy-like, and the return towards Gaussian distributions.

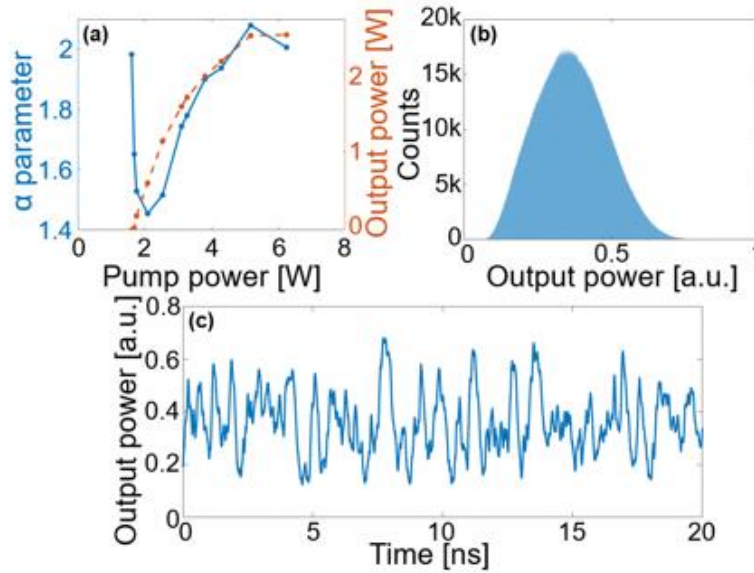


Figure 6.2 (a) Lévy α parameter fitted from experimental data (solid blue) and laser output power (dashed orange), as a function of input pump power. (b) Histogram of the output power at 5.6 W pump power, sampled over 10 million points. (c) Sample time sequence of the output power, at 5.6 W pump power.

6.3 Statistical randomness evaluation

To generate high quality random numbers, the distribution should be as symmetric as possible, so that the random bits are evenly distributed. In order to achieve this, a Gaussian distribution (such as the one obtained far above threshold) is preferred to the very asymmetrical Lévy-like distribution found near the threshold. As such, the pump power of 5.6 W, leading to both the highest output power and highest α value, was used to generate the random bit sequence. Figure 6.2(b) shows a histogram of the distribution of the output power in this regime. The distribution is very close to Gaussian, corresponding to a fitted α parameter of 2.0 ± 0.2 . Figure 6.2(c) displays a sample time sequence of the laser output over the first 20 ns, sampled at 256 GSa/s.

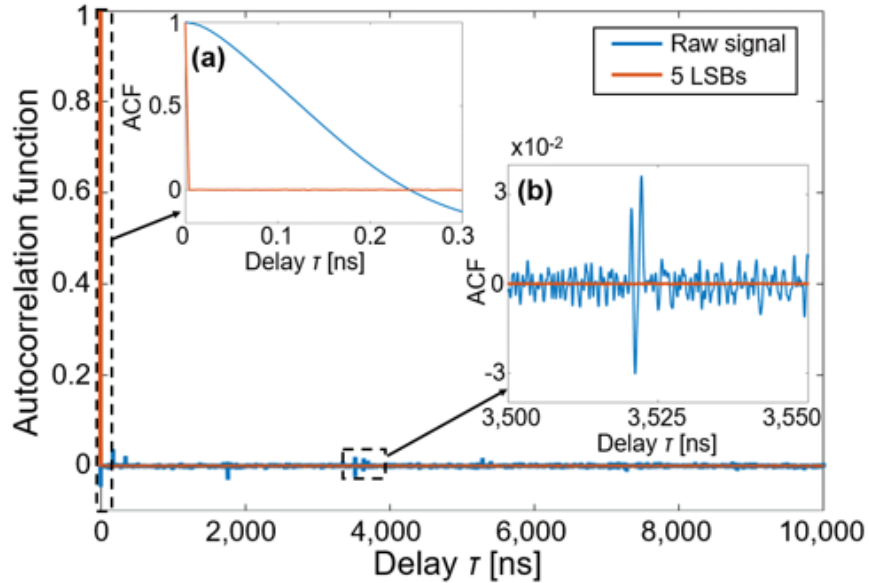


Figure 6.3 Autocorrelation of the first 10 μ s for the raw signal (blue) and the 5 LSBs. Inset (a) shows that no correlation exists between the truncated bits after the first delay of 4 ps (since the ACF drops to 0 instantly), while inset (b) shows that taking the 5 LSBs removes all further existing correlation.

Using this time sequence, the 5 LSBs were extracted from the original 10 bits of the raw signal. This results in a bit rate of 1.28 Tbps (5 bits $\times$ 256 GSa/s). In order to confirm the statistical randomness of the extracted bits, the autocorrelation function (ACF) of the signal was computed.

The ACF is defined as

$$ACF(\tau) = \frac{\langle (y(t) - \langle y(t) \rangle)(y(t+\tau) - \langle y(t) \rangle) \rangle}{\langle (y(t) - \langle y(t) \rangle)^2 (y(t+\tau) - \langle y(t) \rangle)^2 \rangle^{1/2}} \quad (6.1)$$

where $y(t)$ is the signal as a function of time and τ is the autocorrelation delay. Figure 6.3 displays the autocorrelation of both the raw signal and the extracted 5 LSBs. As can be seen, while some correlation exists in the raw signal, taking the LSBs completely removes this correlation within the first measured delay (4 ps). After the first delay, and for the remainder of the sampled data, ACF remains less than 6×10^{-3} , which is below the maximum value required for randomness of 1.3×10^{-2} experimentally observed by Takahashi *et al.* [94].

Figure 6.4 shows the statistics of a 160 Mb bit stream resulting from this data processing. As can be seen in Figure 6.4 (a), the bits are evenly distributed amongst the 5 LSBs and the bit map formed by the first 250,000 bits, reshaped in a 500×500 array, shows no significant pattern, as displayed in Figure 6.4 (b).

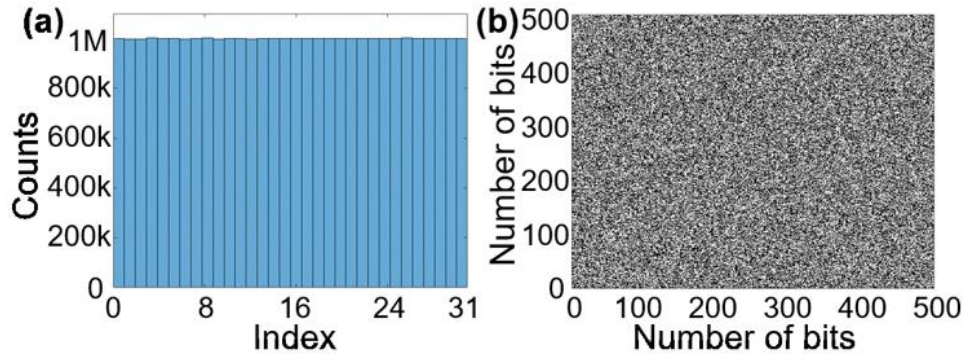


Figure 6.4 Representation of a 160 Mb bit stream. (a) Histogram displaying the distribution amongst the 5 LSBs. (b) Bit map with the first 500 x 500 random bits shown in a 2D array, where bits “0” are converted to black and bits “1” are converted to white.

The randomness of the data was then tested using the National Institute of Standards and Technology (NIST) Special Publication 800-22 test suite[134], the golden standard for RNG measurements. Each test was performed over 1,000 samples of 1 Mb per sample, with a significance level 0.01. All p-values exceed 0.0001, and the proportion of successes is at least 0.980, confirming the randomness of the bit sequence. These results are summarized in Table 6.1, where the indicated p-values and proportions are the smallest ones in the case of multiple tests.

Table 6.1 Results of the NIST SP 800-22 for the random bit sequence generated at 1.28 Tbps

Statistical test	p-value	Proportion
Frequency	0.419021	0.984
BlockFrequency	0.664168	0.991
CumulativeSums	0.070737	0.982
Runs	0.106877	0.989
LongestRun	0.140453	0.989
Rank	0.995777	0.990
FFT	0.008207	0.980
NonOverlappingTemplate	0.003224	0.980
OverlappingTemplate	0.637119	0.990
Universal	0.467322	0.989
ApproximateEntropy	0.385543	0.992
RandomExcursions	0.009604	0.983
RandomExcursionsVariant	0.021200	0.981
Serial	0.821937	0.991
LinearComplexity	0.347257	0.990

6.4 Physical entropy estimation

However, statistical evaluation of the randomness cannot distinguish between true random numbers and high-quality pseudo-random numbers, such as the ones generated by algorithms. In order to determine the highest physically possible RNG rate, the entropy content must be evaluated. We base these calculations on the recommendations made by Hart *et al.* for the evaluation of photonic RNG [98]. The maximum entropy of our system is given by

$$h_0 = \min(\tau^{-1}, 2BW)(N_\epsilon - D_{KL}(p(x)||u(x))) \quad (6.2)$$

where τ^{-1} is the sampling rate, BW is the limiting bandwidth, N_ϵ is the digitization, $p(x)$ is the probability density function (PDF) of the entropy source, $u(x)$ is the uniform distribution over the interval where $p(x)$ is non-zero and $D_{KL}(p(x)||u(x))$ is the Kullback-Leibler divergence from $u(x)$ to $p(x)$ [189]. Indeed, since the entropy source's PDF is typically not uniform, a correction factor must be applied to account for this and accurately calculate the maximum entropy.

The limiting bandwidth of our system can be determined by analysing the RF spectrum of the output of the laser. This was achieved by connecting the photodiode to a 50 GHz electrical spectrum analyser (Agilent PXA N9030A). Figure 6.5 presents the resulting spectra at different pump powers. As can be observed in the inset, at the lowest pump powers, several peaks can be observed

in the RF spectrum. These peaks originate from the beating of different modes that randomly start lasing. However, as the pump power is increased, more and more modes start lasing, resulting in an increase in the number of peaks that are observed. At sufficiently high pump power, nonlinear effects such as self-phase modulation and modulation instability start appearing, leading to a broadening of those peaks. This, coupled with the increasingly large number of lasing modes in the laser, results in a very flat spectrum at a pump power of 5.6 W. This flatness extends up to 29 GHz at -10 dB. Increasing the pump power further, as mentioned earlier, results in a decrease in output power due to the generation of the second Raman Stokes, and thus a decrease in spectrum flatness. As such, in order to maximize RNG speed, a pump power of 5.6 W should be used, to achieve maximum flatness. This corresponds with the state where the α value is closest to 2 (as shown in Figure 6.2), where the intensity distribution is the most symmetrical. The D_{KL} was calculated from the histogram obtained in Figure 6.2(b) to be 0.673 bit.

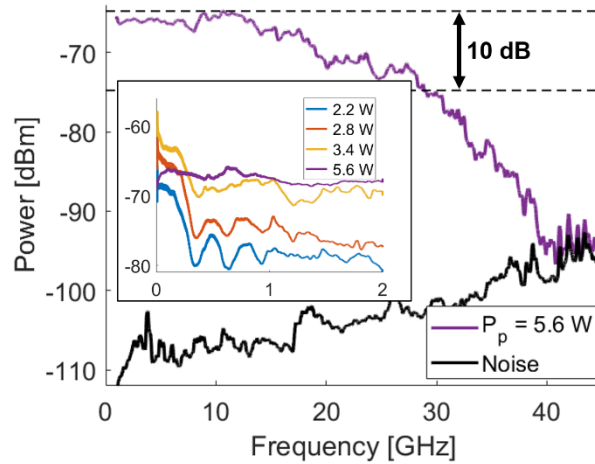


Figure 6.5 RF Spectra of the random laser over a 45 GHz span at a 5.6 W pump power. The inset shows the various peaks observed at lower pump powers, while as pump power is increased, the spectrum flatness is also improved.

Using the 29 GHz bandwidth, and with a digitization of 10 bits, this results in a physical entropy generation of 540 Gbps. This is far below the 1.28 Tbps random bit sequence that was extracted, and which passed all the NIST statistical tests. This demonstrates clearly that, as previously stated by Hart *et al.*[98], statistical testing is insufficient for RNG validation, as the results based on it exceed by more than two times the theoretical entropy content, and may have to be revisited to

establish a more rigorous test. A bit sequence generated by extracting 2 LSBs (resulting in a 512 Gbps RNG rate) was also tested for validation and passed all the NIST statistical tests.

In comparison with other state of the art RNG schemes, the experimental setup we demonstrate is much simpler, being based on a single fiber Bragg grating and some length of fiber, as it does not necessitate the fabrication of complex laser diode structures [103] or concealment of time-delay structure [46, 99, 190], due to the inherent randomness of the modes in our random laser. Furthermore, in agreement with Hart *et al.*'s recommendations [98], the only data post-processing used is least significant bits extraction to avoid tampering with the true randomness of the generated bits, and the RNG rate is based on entropy content evaluation, and not on statistical tests that, as we have demonstrated clearly, can be passed by bit sequences that exceed the generated entropy of our system. Indeed, while our bitrate of 540 Gbps may appear small in comparison to recent results such as the demonstration of nearly 200 Tbps by Kim *et al.* [103], it should be pointed out that their massive multiplexing technique relies on many spatial channels, which are determined by statistical testing performed after deterministic post-processing. This highlights the need for a new methodology for ascertaining the physical randomness content that is generated, especially in the case of multiplexing. Using a more conservative approach, based solely on single channel RNG (i.e. one laser, one detector), the RNG bitrate we have demonstrated is either higher or comparable with the other single channel systems in literature [45, 93, 186, 191, 192] and the bitrate of a single channel in the case of multiplexed channels [95, 99, 103]. With these considerations, multiplexing could potentially be implemented in the present configuration, either spectrally by using a more broadband reflector, which would allow the use of a larger portion of the Raman gain spectrum, and thus the use of multiple channels each measuring part of the spectrum, or spatially, by using for instance a multimode fiber instead of the single mode used in this experiment, which would result in a method of multiplexing equivalent to the one Kim *et al.* [103] demonstrated, but in an optical fiber rather than in a laser diode.

In conclusion, a novel, very simple RNG scheme is demonstrated based on the interaction of randomly excited lasing modes and modulation instability in the half-open cavity scheme of a random Raman fiber laser. An entropy generation of 540 Gbps was demonstrated, and a random bit sequence generated at 512 Gbps was obtained with minimal post-processing. This new technique for producing random numbers is very easy to implement and demonstrates the potential

of random fiber laser sources for RNG. The importance of calculating the physical entropy generation is also demonstrated, as statistical tests such as the NIST test suite are insufficient to confirm the randomness of a bit sequence. Indeed, we have shown here a bit sequence generated at 1.28 Tbps that passes all the statistical tests, even though the physical entropy generation of our current system is less than half this amount.

6.5 Methods

The random Raman fiber laser is built in a half-open cavity scheme which consists of a highly reflective fiber Bragg grating (HR FBG), and 6.66 km of non-zero dispersion-shifted (NZ-DS) single mode fiber (SMF-LS, Corning), as shown in Figure 6.6. The laser feedback is provided on one side by the HR FBG, and on the other side by the Rayleigh scattering of the 6.66 km long optical fiber, which also provides Raman gain. The laser was pumped by a 1480 nm CW laser. This results in a high efficiency random Raman fiber laser at 1572 nm. All output fibers were cleaved at an angle of 4° to avoid parasitic reflections.

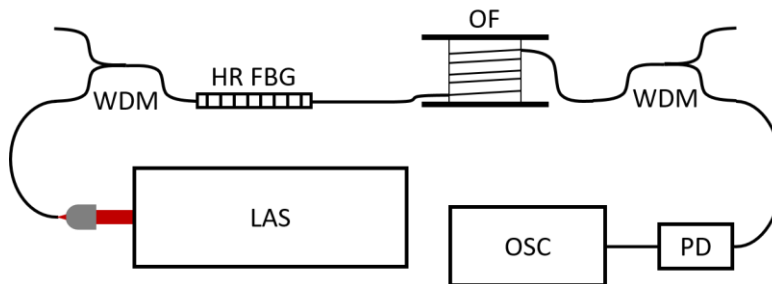


Figure 6.6 Schematic of the experimental setup, with LAS 1480 nm CW laser, WDM wavelength division multiplexer, HR-FBG highly reflective fiber Bragg grating, OF optical fiber bundle, PD photodiode and OSC oscilloscope.

The 100 mm FBG was written in standard, deuterium-loaded telecommunications fiber (SMF-28, Corning) using a Talbot interferometer writing scheme[130], with a reflectivity of 80%. The grating was written with a wavelength of 213 nm using the 5th harmonic of a 1064 nm solid-state laser (Xiton Photonics). The FBG wavelength was set to 1571.86 nm, near the zero-dispersion wavelength (ZDW) of the NZ-DS fiber, which is around 1560 nm. A cosine apodization profile was applied on the first and last 20 mm of the grating using a phase apodization technique[193] to mitigate the side-lobes amplitude, while maintaining a narrow bandwidth. The correction method

described by Loranger *et al.* [131] was used to compensate for refractive index variations along the fiber's length. This correction allowed an excellent control of the phase of the FBG, resulting in a 21.5 pm full width at first zeroes (FWFZ) bandwidth, as can be observed in Figure 6.7.

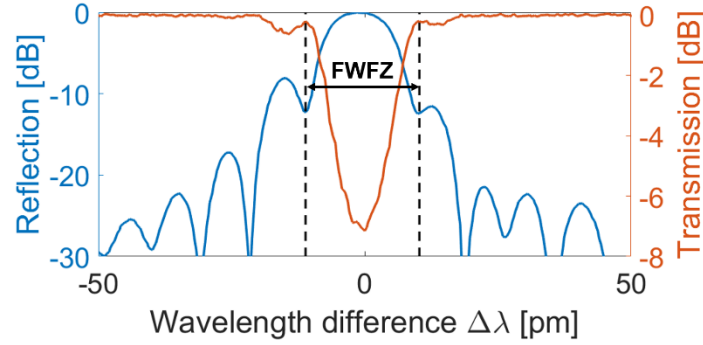


Figure 6.7 Reflexion (blue) and transmission (orange) spectrum of the FBG, showing the 21.5 pm full width at first zeroes (FWFZ) bandwidth, centered at 1571.86 nm.

6.6 Funding

Funding was from the Vanier Canada Graduate Scholarship program, Canadian Foundation for Innovation, the Strategic Grants program of the Natural Science and Engineering Research Council of Canada and Fonds de Recherche du Québec - Nature et Technologies

6.7 Acknowledgment

We thank the Poly-Grames research group for the use of their equipment, as well as the help of their technicians.

6.8 Disclosures.

The authors declare no conflicts of interest.

6.9 Author Contributions

F.M. wrote the main manuscript, fabricated the random laser and performed the measurements. J.S.B helped with the random laser Lévy statistics analysis. R.K. supervised the research and manuscript writing. All authors contributed to the application idea and reviewed the manuscript.

6.10 Supplementary Material

6.10.1 Random laser output power distributions at different pump powers

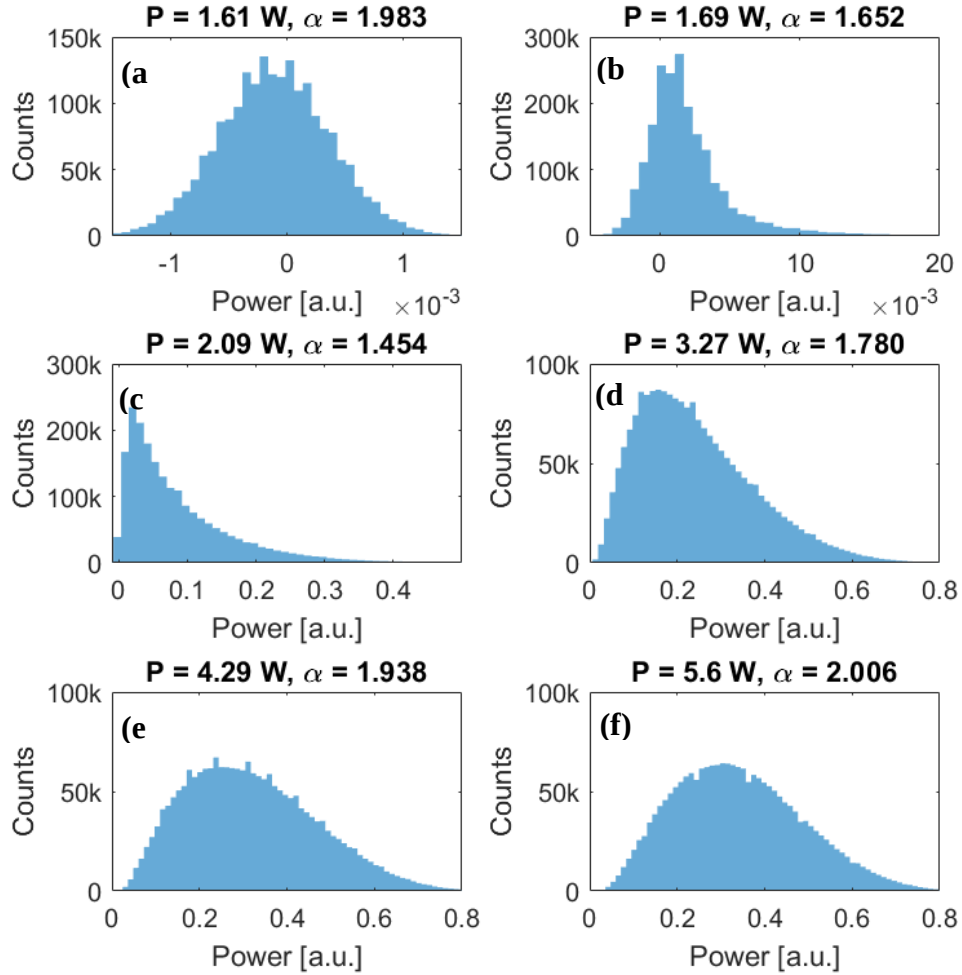


Figure 6.8 Histograms of the output power at increasing pump powers. As pump power increases, the distribution is shown to shift from Gaussian (a), to Lévy-like distributions (b-d), with a return to Gaussian (e-f).

As pump power increases, the probability density function (PDF) describing the output power statistics will change. Figure 6.8 displays histograms of the random laser output power at different pumps, and the associated Lévy exponent α . At low pump powers, the random laser's emission

will be in an initial Gaussian regime, with $\alpha \approx 2$, as shown in (a). The laser's output at that pump power is only amplified spontaneous emission, since we are below threshold. Near the threshold, the laser's statistics will shift to a Lévy-like distribution with $\alpha < 2$, characterised by an asymmetrical long tail towards the higher powers, seen in Figure 6.8(b-c). When pump power further increases, as displayed in Figure 6.8(d), the α exponent starts increasing again, as the PDF returns towards a Gaussian distribution. At high powers, the random laser's emission is almost perfectly Gaussian, as seen in Figure 6.8(e-f), where $\alpha \approx 2$ again.

6.10.2 Spectrum of NZ-DS and TF optical fibers

In order to demonstrate the importance of pumping near the fiber's zero-dispersion wavelength (ZDW), the non-zero dispersion shifted (NZ-DS) optical fiber (SMF-LS, Corning) used for the cavity was replaced by 6 km of standard telecommunications fiber (TF) (SMF-28, Corning). The same fiber Bragg grating (FBG) was used in both experiments. While the TF's ZDW is around 1300 nm, the NZ-DS fiber's is near 1560 nm, which is much closer to the 1572 nm lasing wavelength, dictated by the FBG used in the experiment. Figure 6.9 compares the spectrum of both lasers. As can be easily seen, in order to achieve the same linewidth broadening, a much higher pump power is necessary for the TF than for the NZ-DS fiber. This is not surprising, as the MI frequency is given by

$$\Omega_{MI} = \pm \sqrt{\frac{2\gamma P_0}{|\beta_2|}}, \quad (6.3)$$

where γ is the fiber's nonlinearity, P_0 is the lasing power and β_2 is the fiber's group velocity dispersion parameter. Since in the case of the NZ-DS fiber, the lasing wavelength is near the ZDW, the β_2 parameter is much smaller than for the TF. As such, the same MI frequency can be obtained at lower pump powers.

Using Equation (6.3), and the specifications of telecommunications fiber SMF28 ($\beta_2 = -25.3$ ps²/km, $\gamma = 0.78$ W/km), and an output power P_0 of 1 W, the theoretical modulation instability frequency is 2.52×10^{11} rad/s, which corresponds to a wavelength detuning of 0.33 nm at 1572 nm. This is in line with the observed side-lobes of Figure 6.9(b). For the SMF-LS fiber ($\beta_2 = -1.58$ ps²/km), the side-lobes are expected to appear near ± 1.3 nm. Due to the important broadening of the laser, those side-lobes are challenging to observe. However, at the lowest pump powers, a

symmetrical broadening can be observed at the calculated MI wavelengths, suggesting the presence of MI.

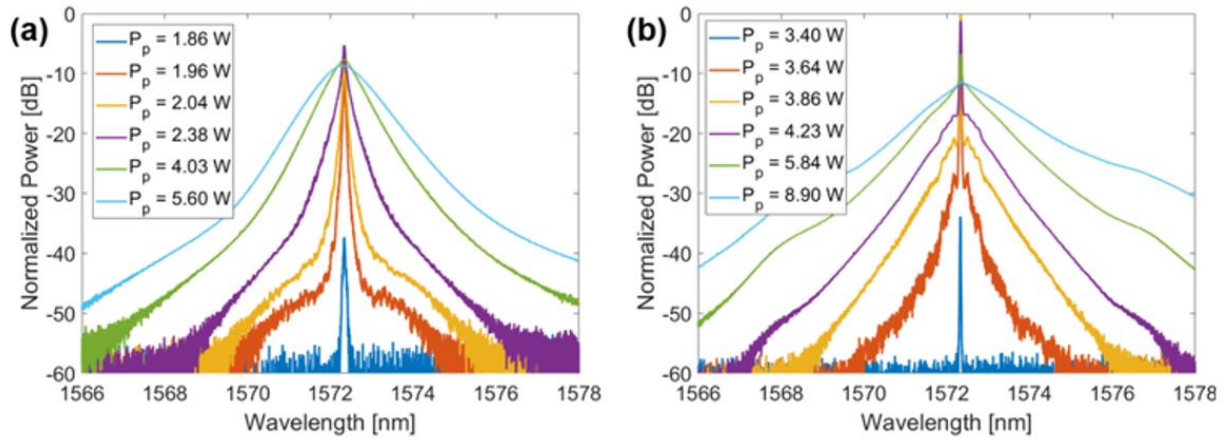


Figure 6.9 Comparison of the spectrum when using (a) NZ-DS optical fiber and (b) standard telecommunication fiber.

CHAPTER 7 ARTICLE 4: ON MULTIPLEXING IN PHYSICAL RANDOM NUMBER GENERATION, AND CONSERVED TOTAL ENTROPY CONTENT

Authors: Frédéric Monet, Raman Kashyap

Submitted in: Scientific Reports, November 3, 2022

In the current article, we use a random supercontinuum based on a random Raman distributed feedback laser to investigate the generation of random numbers by spectrally demultiplexing the broad supercontinuum spectrum in parallel channels. By tuning the spectral separation between two independent channels, we test the most typically used statistical tests' abilities to identify the required minimum spectral separation between channels, especially after the use of post-processing steps. Out of all the tests that were investigated, the cross-correlation across channels using the raw data appears to be the most robust. We also demonstrate that the use of post-processing steps, either least significant bits extraction or exclusive-OR operations, hinders the ability of these tests to detect the existing correlations. As such, performing these tests on post-processed data, often reported in literature, is insufficient to properly establish the independence of two parallel channels. We therefore present a methodology, which may be used to confirm the true randomness of parallel random number generation schemes. Finally, we demonstrate that, while tuning a single channel's bandwidth can modify its potential randomness output, it also affects the number of available channels, such that the total random number generation bitrate is conserved.

7.1 Introduction

Random number generation (RNG) is increasingly in demand for numerous applications, such as Monte Carlo simulations [75], machine learning algorithms [77] and secure communications [194]. While pseudo-random number generators based on algorithmic computations used to be sufficient for this purpose, certain applications requiring a very large amount of random numbers start revealing their limitations. As such, true random numbers generated by physical processes, as opposed to deterministic algorithms, have greatly risen in interest in recent years. Indeed, since they are based on true physical random systems, they do not suffer from the same reproducibility and periodicity issues that even the best pseudo-RNG systems exhibit. However, to ensure that the

numbers generated are truly random, it is important to properly identify the origin of the randomness and quantify its potential. RNG based on quantum processes offer absolute certainty over the true randomness of the system, as the randomness originates from inherent quantum probabilities. However, the bitrates that can be achieved by these systems is relatively low, typically in the Mbps to low Gbps speeds [91]. This is insufficient for the applications described earlier, which consume random bits at staggeringly high speeds. Therefore, new sources of randomness have been investigated to generate random bits at higher rates than what is currently achievable with quantum processes.

The current state of the art relies on the entropy generated by semiconductor lasers operating chaotically due to external feedback to the cavity. Owing to the large bandwidths of chaotic lasers, RNG rates of hundreds of Gbps have been demonstrated [93]. However, the source of randomness in these chaotic systems is not as obvious as in the case of quantum systems and, in the race to achieve the largest possible RNG rate, many shortcuts have been taken. One of the most prevalent ones in the literature is the use of complex post-processing steps to hide existing correlations in bit sequences that are not sufficiently random to pass statistical testing [94-97, 186]. A common post-processing step relies on the application of an exclusive-OR (XOR) operation between the original bit stream and a time-delayed version of it [94, 95, 186]. Even more complex post-processing operations, such as the use of successive numerical derivatives, offer the promise of generating more random bits per measurement than the original digitization used, which again should raise some concerns about the true randomness of the bit sequences thus generated [96, 97]. In 2017, Hart *et al.* issued some recommendations for the evaluation of the entropy content of physical RNG systems [98]. In their article, they recommend that researchers should rely solely on minimally post-processed data for the purpose of generating true RNG, and that any bit sequence that requires the use of complex post-processing to pass statistical tests should be viewed as nothing more than a high-quality pseudo-random bit sequence. Furthermore, they argue that the physical origin of the entropy should be investigated and theoretically computed, rather than solely relying on statistical testing.

It can be observed that, since the publication of this article, these recommendations are increasingly being followed by researchers in literature. However, in order to continue publishing record-breaking RNG rates, multiplexing in RNG is now being investigated, where multiple channels

simultaneously generate random bits in parallel [95, 99, 100, 103, 195]. This allows higher RNG rates by multiplying a single channel's output by the number of parallel channels. Furthermore, since each channel generates its own RNG throughput, this type of system is perfectly well suited for parallel computing applications, which are increasingly used as they are more efficient, but require independent RNG streams [196, 197]. One such way to achieve this is by using two or more chaotic laser sources and combining them in multiple ways to realize independent parallel channels using deterministic algorithms such as addition, subtraction or XOR operations for instance [95, 195]. Recently, by combining the waveforms of three chaotic semiconductor lasers, and multiplexing the RNG across seven distinct channels, RNG rates as high as 2.24 Tbps were reported in literature [99]. Alternatively, the output of a single laser source could be separated either spectrally [100-102], spatially [103] or by polarization [104] to generate random bits in parallel. Recently, Kim *et al.* reported an astounding 250 Tbps rate achieved by a single laser diode through the interaction of multiple lasing modes in a specially tailored cavity [103]. However, as Hart *et al.*'s recommendations applied for single channel RNG [98], at the moment there is no real consensus how to translate these for multiplexed RNG systems. It is the goal of this article to help provide insights how these recommendations might be formulated, by studying a novel RNG architecture and identifying the conditions ensuring independence between the multiplexed channels.

In our recent work, we demonstrated how a single channel narrow linewidth random Raman distributed feedback fiber laser could generate a theoretical entropy content of 540 Gbps [198]. We showed that, as illustrated by Hart *et al.* [98], the evaluation of this theoretical entropy content was critical, as a bit sequence generated at 1.28 Tbps (more than twice the theoretical entropy content) passed all the National Institute of Standards and Technology (NIST) statistical tests [88]. This highlighted the need for theoretical entropy content estimation for proper true RNG characterization. By performing minor modifications to the laser cavity architecture described in that article, the output characteristics can be significantly changed to result in the generation of a random Raman supercontinuum, induced by modulation instability and Raman self-frequency shift. Using this approach, we demonstrate how this laser can be used for multiplexed random generation by spectrally sampling multiple channels from this supercontinuum. In the current proof of concept, the spectral multiplexing is achieved using a pair of fiber Bragg gratings (FBGs),

instead of using a typical arrayed waveguide grating (AWG) for instance [102], which can provide a much higher number of spectral channels. However, our unconventional technique allows us to tune the spectral separation between the two channels to determine the minimum separation required ensuring they are indeed uncorrelated. Furthermore, we test some of the techniques found in literature to measure correlations between channels and demonstrate that caution should be exercised when performing these tests to ensure they truly measure what they are expected to, especially when using post-processed data.

7.2 Single-Channel Random Number Generation

7.2.1 Random Supercontinuum Generation

In our previous work, we fabricated a random Raman laser closed on one side with a 100 mm long phase-controlled apodized FBG, relying on Rayleigh backscatter on the other end to provide random feedback, while also providing Raman gain, thus achieving laser action [198]. We show here that, by replacing the FBG with the Fresnel reflection of a fiber end tip, lasing can also occur, with a significantly simpler cavity design. Furthermore, since the Fresnel reflection is broadband, lasing is no longer constrained to the FBG's wavelength, which fixed the lasing wavelength in our previous work. Indeed, as we show in Figure 7.1, while lasing is initially achieved at a wavelength of 1580 nm (which corresponds to the maximum of the Raman gain generated by the 1480 nm pump), a second peak is then generated at 1595 nm, and eventually becomes dominant. This two peak structure is typical of distributed feedback random lasers, and has been observed in multiple instances [57].

At higher pump powers, the spectrum starts broadening, and shifts towards the longer wavelengths. This is attributed to Raman intra-pulse scattering, which is due to the fact that the lasing wavelength is slightly above the zero dispersion wavelength (ZDW), placing this laser in the normal dispersion regime. Near the ZDW, nonlinear effects such as modulation instability (MI) can break the laser output into multiple ultrashort, random pulses, which will then experience Raman intra-pulse scattering, shifting them to longer wavelengths. In our previous work, MI side-lobes were observed near the lasing wavelength, however this is our first observation of self-frequency shift, which further confirms our previous observations. At even higher pump powers, the second Raman Stokes

line starts becoming apparent, and eventually becomes dominant. As the pump power increases, the self-frequency shift starts spanning the entire band between the first and second Raman Stokes peaks, covering a bandwidth of 77 nm. This bandwidth is only limited by the available pump power and would extend further in the longer wavelengths at higher pump powers. This type of behavior has been observed in other random laser architectures [199, 200], although generally with much more complex setups requiring one or more FBGs, and typically with at least two different types of fiber, whereas our setup relies simply on the Fresnel reflection of the fiber tip, and one bundle of optical fiber.

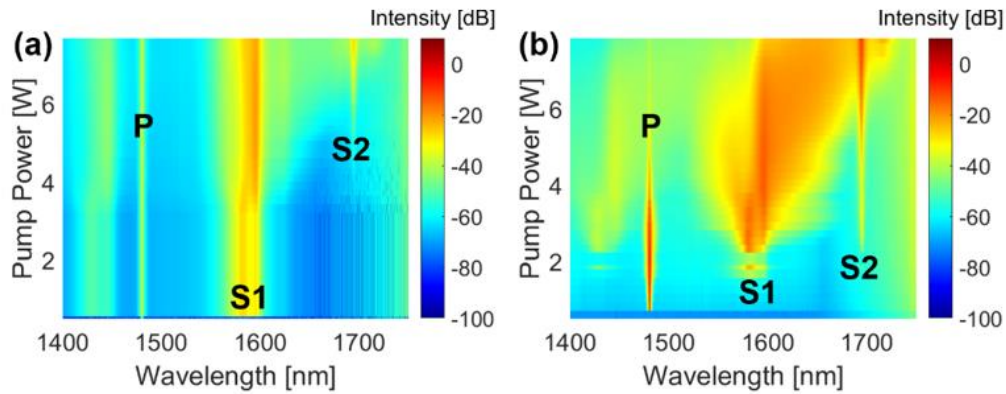


Figure 7.1 Output spectra of the random laser, both in (a) backward direction and (b) forward direction. At high pump power, the random supercontinuum can be observed. The pump (P), first Stokes (S1) and second Stokes (S2) lines are identified on both spectra.

7.2.2 Single-Channel Random Number Generation

Before attempting multiplexed RNG operation, the ability of a single channel to generate random bits was investigated and quantified. From the supercontinuum output, a single 0.39 nm channel was isolated using an apodized 9-mm long FBG (see Methods for more details). Figure 7.2(a) displays the resulting channel's output spectrum, where the isolation with respect to the supercontinuum can be observed, with an extinction ratio of 27 dB.

In order to use this channel to generate random bits, the output of the channel was first converted to the electrical domain by a high-speed 70 GHz photodiode, and the electrical signal thus generated was digitized by an 8-bit 12 GHz ADC, sampled at 40 GSa/s. From this digital signal, the 3 least significant bits (LSBs) were extracted, resulting in a random bit sequence generated at

120 Gbps. The bit sequence was then analyzed by the National Institute of Standards and Technology (NIST) statistical testing suite [88], using 1,000 samples of 1 Mb each. The results are presented in Table 7.1 below. As can be seen, the bit sequence passes all of the statistical tests at the $p < 0.01$ significance level, since all tests have at least 0.980 success rate, and the lowest p-value is above 0.0001.

Table 7.1 Results of the NIST SP 800-22 for the random bit sequence generated at 120 Gbps

Statistical test	p-value	Proportion
Frequency	0.011383	0.991
BlockFrequency	0.753844	0.991
CumulativeSums	0.204439	0.992
Runs	0.155499	0.985
LongestRun	0.753844	0.987
Rank	0.792508	0.993
FFT	0.054314	0.995
NonOverlappingTemplate	0.011144	0.981
OverlappingTemplate	0.316052	0.992
Universal	0.030197	0.987
ApproximateEntropy	0.031428	0.989
RandomExcursions	0.003797	0.984
RandomExcursionsVariant	0.002406	0.981
Serial	0.110734	0.987
LinearComplexity	0.844641	0.992

7.2.3 Physical Entropy Evaluation

In order to properly quantify the randomness of an RNG scheme, it is important to evaluate the physical entropy generated by such a system. Indeed, as noted by Hart *et al.* [98], randomness evaluation through statistical tests, such as is customary in RNG literature, is not sufficient to properly ascertain the physical randomness of one RNG scheme. Indeed, they demonstrated that multiple RNG schemes in literature claim an RNG bitrate larger than the underlying physical entropy generated by the systems they used, making them pseudo-random numbers at best. We also arrived at similar conclusions in our previous work [198].

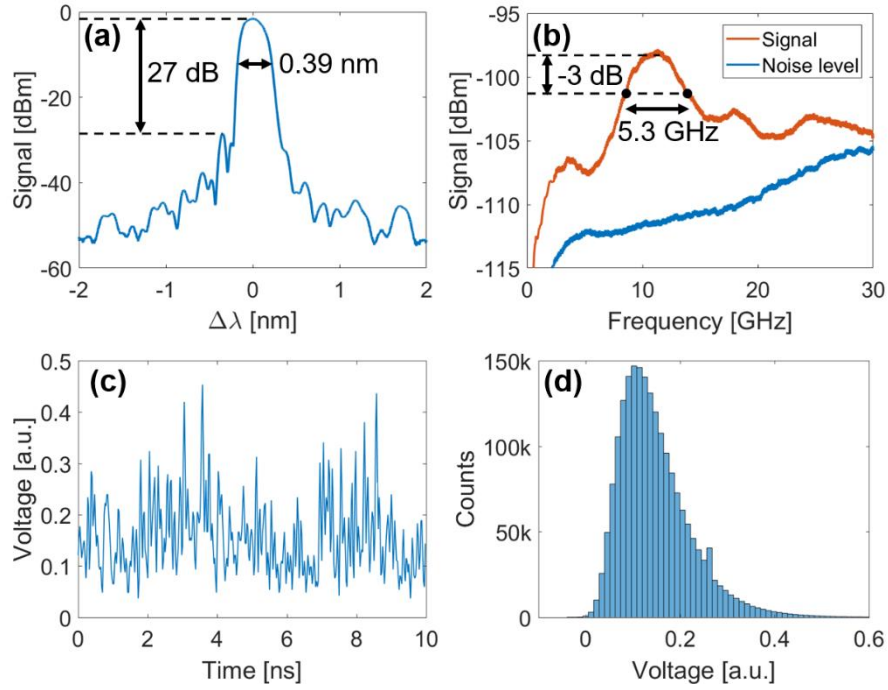


Figure 7.2 (a) Single-channel's optical spectrum, displaying the narrow -10 dB bandwidth of 0.39 nm. (b) RF spectrum of the single channel, displaying a 5.3 GHz bandwidth at -3 dB. (c) Sample time sequence, measured at 40 GSa/s. (d) Histogram of the channel output, sampled over 2 million points.

The maximum entropy of a given system is given by

$$h_0 = \min(\tau^{-1}, 2\Delta f)(N_\epsilon - D_{KL}(p(x) || u(x))) \quad (7.1)$$

where τ^{-1} is the sampling rate, Δf is the limiting bandwidth, N_ϵ is the number of bits used in the digitization, $p(x)$ is the probability density function (PDF) of the entropy source, $u(x)$ is the PDF of the uniform distribution over the same interval as $p(x)$ and D_{KL} is the Kullback-Leibler divergence from $u(x)$ to $p(x)$, in bits [189]. Indeed, the ideal distribution for RNG purposes is a uniform distribution, so that each number has an equal probability of being generated. However, since physical entropy sources rarely follow a uniform distribution, the correction factor D_{KL} must be applied to the maximum theoretical entropy due to the divergence between the ideal uniform distribution and the actual entropy source's distribution.

In order to characterize the theoretical physical entropy generated by such a channel, its output was analyzed by an electrical signal analyzer (*Agilent PXA N9030A*) which can measure up to 50 GHz.

The electrical spectrum associated to the isolated channel is shown in Figure 7.2(b). The electrical bandwidth, which limits the channel's physical entropy, was defined at the -3 dB bandwidth, and was measured at 5.3 GHz. A sample time sequence of the channel's output, sampled at 40 GSa/s, is displayed in Figure 7.2(c), while a histogram of the signal's distribution is shown in Figure 7.2(d). From this histogram, the Kullback-Leibler divergence can be computed at 1.38 bit. Using Equation (7.1), the theoretical entropy content can thus be estimated to be 70 Gbps. Rather unsurprisingly, the computed theoretical entropy content is smaller than the one that was experimentally demonstrated. This highlights again the insufficiency of the NIST statistical tests to distinguish between true random numbers and high-quality pseudo-random bits. For the rest of this manuscript, we will consider that this laser has the potential for 70 Gbps random bit generation, even though the sample generated at 120 Gbps passed all tests.

7.3 Parallel RNG

The previous section demonstrated our ability to generate random bits in a single-channel scheme by isolating a narrow spectral channel from the generated supercontinuum. However, to take full advantage of the broad supercontinuum bandwidth, multiple channels could be used to generate random bits in parallel. A naive computation of the number of potential spectral channels would be to divide the supercontinuum's 77 nm bandwidth by the channel's 0.4 nm bandwidth, resulting in a total of 192 parallel channels. From the 70 Gbps single-channel demonstrated in the previous section, this would result in a total potential bitrate up to 13.44 Tbps. If the entropy content had not been evaluated, using the 120 Gbps rate that was validated with the NIST statistical tests, this would push the bitrate even higher, at 23.04 Tbps, although these would theoretically only be high-quality pseudo-random bits. However, one key assumption made here is that the signals generated by two separate spectral channels are independent. To maximize this independence, we used apodized FBGs to eliminate the side-lobes that could contribute to crosstalk across the channels. However, it is not obvious that the channels are completely uncorrelated since they originate from the same laser, even though they come from different parts of the spectrum. To investigate this further, two identical apodized FBGs were used to generate two parallel channels. Since the two FBGs are identical and centered at the same wavelength, the two channels are expected to be perfectly correlated. Then, by applying strain to one of the FBGs, its central wavelength can be

shifted by up to 15 nm (corresponding to a 1% strain). This allows the observation of how the wavelength separation between the two channels influences the correlations between the channels.

In literature, two tests are mainly used to quantify these correlations across parallel channels: cross-correlations and mutual information. Both these tests will be performed on the extracted sequences, and the impact of post-processing will be quantified. One key advantage of our technique is that it allows the use of a reference, which corresponds to the case where the two FBGs are unstrained. Performing these tests on this reference allows us to ensure that the post-processing steps have no effect on the validity of the tests. Indeed, if the post-processing steps decrease the minimum required spectral separation, but also decrease the ability of the test to identify the existing correlations when the channels are expected to be correlated, then these post-processing steps actually reduce the ability of the statistical test to perform as intended.

7.3.1 Cross-correlations across channels

The first statistical test that was applied to the extracted data was the computation of the cross-correlation across the two channels, as a function of their spectral separation. To correct for the delay caused by any mismatch between the two channels' propagation length, the cross-correlation was computed between the two channels, and the delay τ_m associated with the maximum of this cross-correlation function was thus identified as the mismatch between the two channels' lengths. The cross-correlation between the two intensities X and Y is given by

$$C_{X,Y}(\tau) = \frac{\int \delta X(t + \tau) \delta Y(t) dt}{\sqrt{\int (\delta X(t))^2 dt \int (\delta Y(t))^2 dt}}, \quad (7.2)$$

where $\delta X(t) = X(t) - \langle X(t) \rangle$. These results are illustrated in Figure 7.3(a). As can be observed, when the two FBGs' central wavelengths are matched, a correlation of almost 1 is measured (0.90), which confirms that the signals are the same on both channels. As the spectral separation increases due to the applied strain, the correlation continually decreases. It remains above 0.5 (-3 dB) up to a channel separation of 2 nm, and the signals remain correlated until a spectral separation of 8 nm. This has a dramatic effect on the total achievable RNG rate, as this limits the number of potential parallel channels to only 11, rather than the 192 obtained by our initial naïve computation.

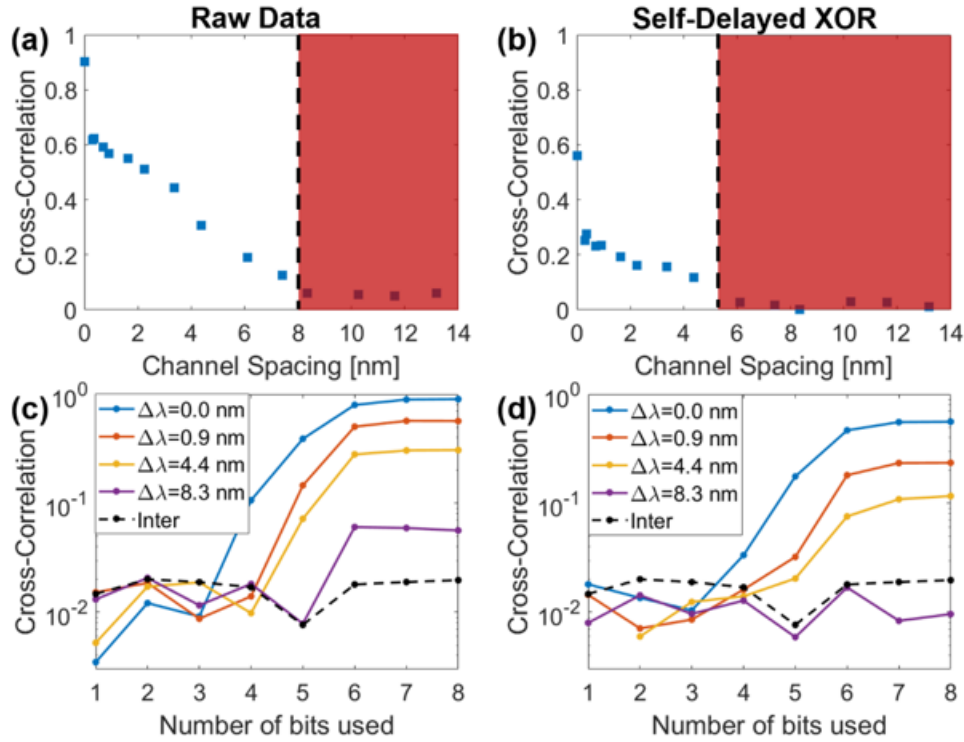


Figure 7.3 Cross-correlation values using (a) the raw data and (b) the same data after applying a self-delayed XOR operation, as a function of the channels' spectral spacing. The region highlighted in red corresponds to spectral separations considered uncorrelated. The cross-correlation is also computed after extraction of a number of LSBs, using (c) the raw data and (d) the same data after applying a self-delayed XOR operation. The *inter* values (dashed line) displays the cross-correlation measured between two separate measurements as comparison.

This approach is significantly different from what is typically observed in literature. While certain authors do present the cross-correlation computations based on the raw data [100, 201], it is far from the norm. Indeed, when this analysis is performed, most authors rather perform it on post-processed data [102], usually after extracting the random bits [99, 101], sometimes followed by further post-processing steps such as XOR operations [103, 195, 202]. To compare the results, the same process was applied with the current data. For example, a typically used post-processing step is the self-delayed XOR operation. Even though Hart *et al.* argued against the use of such post-processing techniques [98], they are still used in recent publications, both in single-channel [191, 203] and multiplexed RNG schemes [99, 100, 103, 104]. To quantify the impact of the self-delayed XOR operation, we digitized the raw data using 8-bit representation (the digitization used by the

real-time oscilloscope used in these experiments). An XOR operation was then applied between the resulting bit sequence and a version of itself delayed by 1.6 ns. After performing this additional post-processing step, an important decrease in correlations can be observed (see Figure 7.3(b)). Indeed, as the spectral separation is increased, no correlation can be observed past 5 nm. While it may be tempting to claim that the use of the self-delayed XOR increased the number of potential multiplexed channels due to this reduction in the required spectral spacing, it should be noted that it also decreased the correlations when there was no spectral separation between the channels. Indeed, the correlation between the two signals in this case dropped from 0.90 to 0.56. The fact that it had such a drastic effect even with no spectral separation rather implies this operation reduced the ability of the cross-correlation test to accurately detect the existing correlations.

Another approach typically used in literature is to first extract LSBs before characterizing channel independence. To reproduce this data processing, a varying number of LSB was extracted from the digitized raw data and the cross-correlation between the two channels was computed after LSBs extraction. These results are presented in Figure 7.3(c). Indeed, as can be observed, extracting the LSBs before computing the cross-correlation greatly decreases the correlations between the channels, and it appears that when 3 LSBs or less are extracted, the correlations across channels are similar to those obtained from two separate measurements (the *inter* case displayed with the dashed line). This would seem to indicate that LSBs extraction improves the independence across channels. However, here again, the proposed methodology allows the computations of this correlation when there is no spectral separation between the two channels, which is not typically measured in literature. This leads to the observation that the correlations also disappear when a small enough number of LSBs is selected, even when the two channels are expected to be perfectly correlated. This would seem to imply that no spectral separation is required to ensure that the channels are completely uncorrelated, which obviously does not make sense. Our measurements show that, while the correlations measured after LSBs extraction are indeed lower, they cannot be relied upon to quantify the channels' independence. Instead, the full raw data should be used to compute the correlations across channels, in a similar fashion to what we have shown in Figure 7.3(a). Similarly, when looking at the effect of the self-delayed XOR after LSB extraction in Figure 7.3(d), it can be observed that the correlations converge to that of the *inter* case even faster than without this post-processing operation. Again, one could use this as evidence that the self-delayed

XOR, combined with the LSBs extraction, enhances the channels' independence, but based on the above arguments, we showed that both these techniques only decrease the effectiveness of the cross-correlation test.

7.3.2 Mutual Information between channels

The second statistical test that was realized was the computation of the mutual information between the channels. Mutual information between two bit-streams X and Y is defined as

$$I(X;Y) = \sum_{y \in Y} \sum_{x \in X} P_{(X,Y)}(x,y) \log_2 \left(\frac{P_{(X,Y)}(x,y)}{P_X(x)P_Y(y)} \right), \quad (7.3)$$

where $P_X(x)$ is the probability that $X = x$, $P_Y(y)$ is the probability that $Y = y$ and $P_{(X,Y)}(x,y)$ is the probability that $(X,Y) = (x,y)$. The base-2 logarithm is chosen here to express the mutual information in bits. The computation of the mutual information across channels is another statistical test used in literature [101, 103], because from it one can infer whether the bits generated in one channel contain information on the bits in the other channel. Obviously, for RNG purposes, this mutual information should be as close to zero as possible.

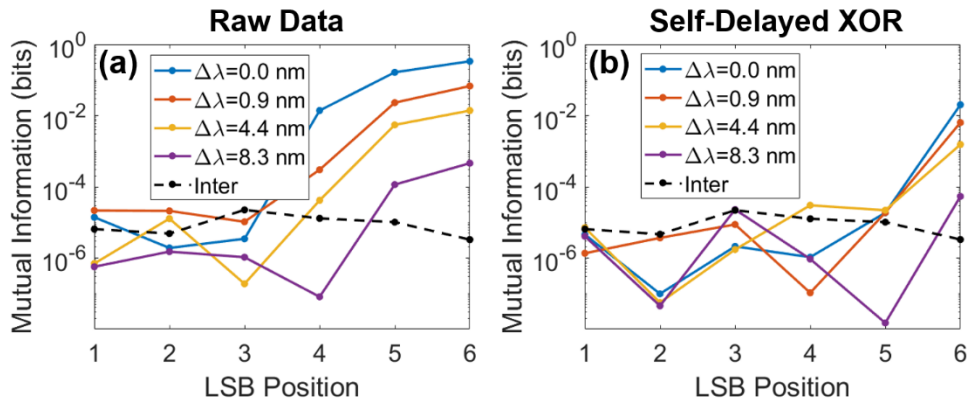


Figure 7.4 Mutual information between the two channels, as a function of the LSB position, where 1 is the least significant bit and 8 the most significant one, for various spectral separations. The mutual information is computed from (a) the digitized raw data and (b) after performing a self-delayed XOR operation. In both cases, the sequence was digitized using 8 bits, and consisted of 10^5 samples. The sequence length is inversely proportional to the mutual information limit of detection, observed in the *inter* case as 10^{-5} .

Here, the mutual information was computed for each bit position, for various spectral separations. The mutual information is only computed for the 6 LSBs, because the first two do not contain enough information due to their uneven distribution of ones and zeros (for more details, see Supplementary Information in section 7.11). As can be observed in Figure 7.4(a), the mutual information between the two channels for the most significant bits tested (LSB Position 6) is very high, and quickly decreases as the bits become less significant, until the last 3 LSBs, where the mutual information is of the same order of magnitude ($\sim 10^{-5}$) as the one obtained from two different measurements (here again named the *inter* measurement with the dashed line).

This behavior is more or less exactly the same than the one that was observed with the cross-correlation measurements. Here too, when the spectral separation is zero, even though the mutual information is much higher for the more significant bits, it also rapidly decreases and becomes undistinguishable from the *inter* case for the last 3 LSBs, which would again seem to indicate that no spectral separation is required to achieve independent multiplexed channels, as long as 3 LSBs or less are kept. For completeness, the same data treatment was realized after an additional self-delayed XOR operation was applied on the generated bits, where again the mutual information decreases much faster for all plotted spectral separations, as shown in Figure 7.4(b). What this demonstrates is that the mutual information computation is as vulnerable as the cross-correlation measurements to LSB extraction and therefore cannot be considered a robust method of ensuring independence across channels. However, looking at the mutual information of each bit individually (instead of only looking at the least significant ones), as depicted in Figure 7.4, appears to be somewhat more robust, as the mutual information is much higher for the more significant bits (e.g. LSB 6 in Figure 7.4). However, again, the use of the self-delayed XOR greatly decreases the mutual information content, even when there is no spectral separation. Therefore, it still appears that the cross-correlation computation using solely the raw data is the most robust technique to ensure independence across channels.

7.3.3 Channel widths and conserved total entropy

From the analysis of the previous sections, it appears that, in order to ensure proper decorrelation between neighboring channels, the 0.4 nm channels must be spectrally separated by a minimum of 8 nm. Considering this, it is tempting to wonder whether the use of channels broader than the

0.4 nm demonstrated so far might help with the total achievable RNG rate. Indeed, it makes intuitive sense that a broader spectral channel might have the potential for higher single-channel RNG, and the current channel width is much narrower than the minimal channel spacing. Indeed, as can be observed in Table 7.2, when varying the channel's bandwidth from 0.4 nm to 1.7 nm, a broadening of its electrical spectrum can be observed, which will result in increased RNG potential, as per Equation (7.1). However, in order to make sure that the use of a broader channel's bandwidth indeed results in a greater total RNG rate, the analysis performed in section 7.3.1 must be repeated for these new channel widths. These results are displayed in Figure 7.5. As can be observed, while using a broader channel spectral width increases the potential for single-channel RNG generation, it also increases the minimum spectral separation between channels, which will decrease the number of potential channels that can be extracted from the supercontinuum. As such, the total RNG rate remains constant at around 760 Gbps, as can be observed from the data in Table 7.2, where an increase in single-channel RNG rate is accompanied by a decrease in the number of achievable channels. This is perhaps unsurprising, as the total RNG rate should be limited by the entropy generated by the laser, regardless of the number of channels it is separated into. However, in practice, single-channel RNG rates are limited by the speed of the electronics, and it can therefore be helpful to use several parallel channels generating bits at more reasonable rates. On the other hand, an increasing number of parallel channels increases complexity and costs. Therefore, depending on the entropy source that is used, proper optimization must thus be performed to perform RNG across the optimal number of channels based on these limitations.

Table 7.2 RNG Potential of different channel's optical bandwidth $\delta\lambda$

Optical Bandwidth $\delta\lambda$	Electrical Bandwidth Δf	Single-channel RNG Potential	Number of potential channels	Total RNG Potential
0.4 nm	5.3 GHz	70 Gbps	11	772 Gbps
0.9 nm	6.4 GHz	85 Gbps	9	763 Gbps
1.7 nm	8.2 GHz	109 Gbps	7	760 Gbps

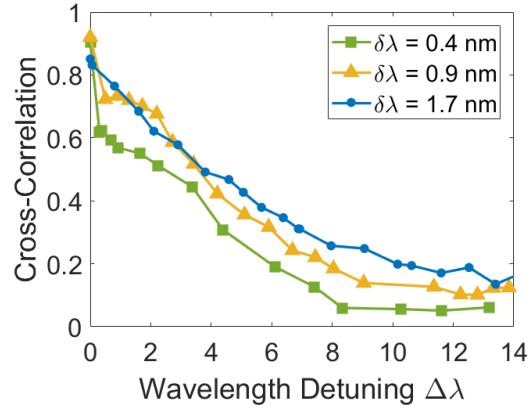


Figure 7.5 Cross-correlation values as a function of wavelength detuning, for different channel spectral widths.

7.4 Discussion

Novel methods to generate high-speed physical RNG systems are increasingly popular in literature. However, in the race to report the highest RNG rate, one must exercise extreme caution that the process is indeed based on true physical randomness, and that the bits generated are not simply high-quality pseudo-random ones. Other researchers have formulated recommendations in that regard, for example cautioning against post-processing steps that can only hide existing correlations at best. However, there exist no such recommendations when generating random bits in parallel using multiplexed channels, which is becoming an increasingly popular subject of research. In this work, using a very simple random Raman laser architecture, we generated a 77 nm random supercontinuum that allowed us to investigate parallel RNG using spectrally multiplexed channels. Furthermore, this technique allowed us to look at which tests can be used to ensure independence between the channels. We demonstrated that both cross-correlation and mutual information computations after LSBs extraction are insufficient to ensure that the channels are truly uncorrelated, as they both indicate that the tested channels are uncorrelated even when there is no spectral separation between them. From an initial assumption of 192 random channels in the supercontinuum, we showed that using the cross-correlation tests reduced the true randomness to only 11, demonstrating the pitfalls of a naïve approach. We also demonstrated that the use of an exclusive OR (XOR) operation on the extracted bits further decreased the calculated correlations. Rather than improving the randomness of the extracted bits, this post-processing step reduced the

ability of the two investigated statistical tests to properly quantify the existing correlations. From our tests, simply computing the cross-correlations using the raw data appears to be the most robust method to determine the minimum spectral separation. It is our opinion that, as more and more researchers investigate the potential of parallel RNG using multiplexed channels, more advanced statistical tests should be developed to ensure there are no correlations across the channels. We believe the methodology presented in this article can be used in conjunction with these tests to ensure they properly measure what they intend. Finally, while this technique was demonstrated in the case of spectral multiplexing, we believe it can be translated easily to RNG techniques relying on spatial multiplexing with minimal changes.

7.5 Methods

The random Raman supercontinuum relies on a half-open random laser cavity architecture. The feedback of the cavity is provided on one end by the 4% Fresnel reflection at the tip of the fiber, which is cleaved at a 0 degree angle, and on the other side by the random Rayleigh backscatter of 6.66 km of non-zero dispersion-shifted (NZ-DS) single mode fiber (SMF-LS, Corning), while the gain is provided by stimulated Raman scattering. All fiber outputs are cleaved at a 4 degree-angle to prevent parasitic reflections. The NZ-DS fiber has a zero-dispersion wavelength (ZDW) near 1560 nm. This ZDW closely coincides with the first Raman Stokes peak (1580 nm) of the CW pump laser at 1480 nm that is injected into the fiber. The RF spectra of this laser was measured by a 50 GHz electrical spectrum analyzer, while the optical spectra (both backward and forward) were measured by connecting the output to an optical spectrum analyzer with a 0.01 nm resolution. The random laser cavity is displayed in Figure 7.6(a).

To simulate the multiplexing operation, the forward output of this laser was separated into two channels by a 50:50 coupler. Two identical 9 mm FBG were written with a cosine apodization profile by UV laser inscription, in a Talbot interferometer scheme, using a commercial semi-automatic FBG writing station (*BraggATuneTM*, *PhotoNova Inc*). This resulted in two identical channels with a 0.39 nm bandwidth centered at 1630 nm. This wavelength was selected as it is far beyond the Raman gain bandwidth, to ensure that the reflected channels do not affect the lasing operation. This was validated by monitoring the optical spectrum and laser output power before and after including this channel separator, showing no significant change. By applying strain on

one of the FBGs, the spectral spacing between the two channels could then be tuned to investigate the effects of this spacing on the correlation across the two channels. The two outputs were then connected to two 70 GHz photodiodes, and digitized by a 12 GHz, 8 bit analog-to-digital converter (ADC), real-time oscilloscope. The spectral separation between the two channels was monitored by an optical spectrum analyzer connected to the reverse output of the optical coupler separating the two channels, to measure the central wavelength of both channels simultaneously (Port 5 of Figure 7.6(b)). Figure 7.6(b) displays the experimental setup used to demultiplex the two channels.

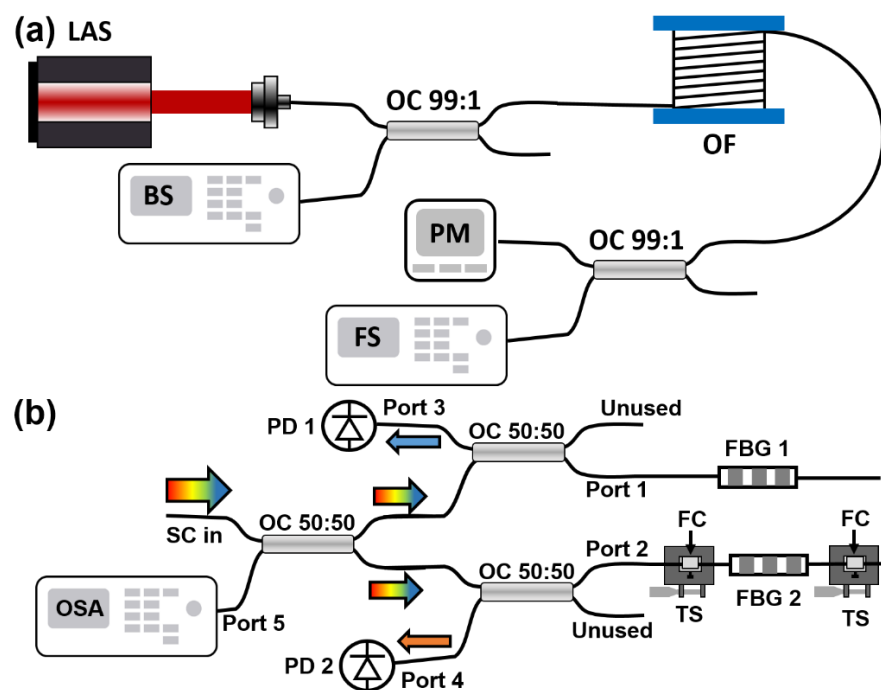


Figure 7.6 (a) Experimental setup for the random laser, with LAS the pump laser, OC the optical coupler, OF the optical fiber bundle, PM the power meter used to measure the output power, BS and FS, respectively measure the backward and forward spectra of the laser. (b) Experimental setup for the parallel channel demultiplexer. The supercontinuum SC is split in two channels by a 50:50 optical coupler OC, and each channel's central wavelength is defined by its own FBG (Ports 1 and 2). The optical signal of each channel is converted to an electrical signal by a pair of high-speed photodiodes PD (Port 3 and 4). The spectral separation between the channels can be tuned by applying strain on one FBG, using the translation stages TS, where on top of each one a fiber clamp FC (*FiberViceTM*, *PhotoNova Inc*) holds the fiber. An optical spectrum analyzer OSA monitors the spectral separation between the two channels (Port 5).

7.6 Funding

Funding was from the Vanier Canada Graduate Scholarship program, Canadian Foundation for Innovation, the Strategic Grants program of the Natural Science and Engineering Research Council of Canada and Fonds de Recherche du Québec - Nature et Technologies

7.7 Acknowledgment

We thank the Poly-Grames research group for the use of their equipment, as well as the help of their technicians.

7.8 Disclosures.

The authors declare no conflicts of interest.

7.9 Data Availability

All data used in this manuscript can be made available upon reasonable request to the authors.

7.10 Author Contributions

F.M. wrote the main manuscript, fabricated the random laser and performed the measurements. R.K. supervised the research and manuscript writing. All authors contributed to the application idea and reviewed the manuscript.

7.11 Supplementary Material

7.11.1 Mutual Information for all 8 bits

In the experimental data, due to the digitization process of the real-time oscilloscope used, the probabilities of each bit of being either a “0” or a “1” was uneven, depending on the position of that bit. The probability of each bit being a “1” is illustrated in Figure 7.7, in orange, as a function of its position. The most significant bit (LSB position 8) is almost always a 0 ($P_X(x=1) = 10^{-4}$), and thus contain very little information, while the 5 least significant bits (LSB positions 1 through 5) have an approximatively 50% chance of being either a 1 or a 0. This is due to the fact that the binning used by the oscilloscope is not perfectly centered with the probability density function (PDF) of the random signal, as well as the due to the slight asymmetry of the PDF. As such, the most significant bits will have an uneven distribution of “0”s and “1”s. This is not a problem for the RNG process demonstrated here, which only utilizes the 3 LSBs, but affects negatively the mutual information computation for these most significant bits, since it has $P_X(x)$ in the denominator. The result of the mutual information computation is shown in Figure 7.7 in blue and compared with the probability $P_X(x=1)$ of X being a 1.

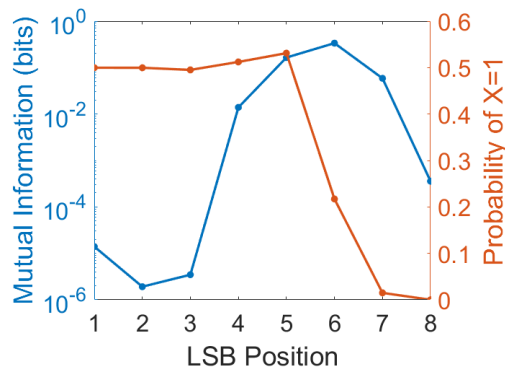


Figure 7.7 Mutual information for all LSB positions (blue), compared to that bit’s probability of being equal to 1 (orange), in the case where there was no spectral separation between the two channels. LSB position 1 is the least significant bit, and 8 is the most significant bit.

For demonstration purposes, this is schematized in Figure 7.8 with a Gaussian distribution with a 4 bit digitization, where the distribution and its associated binning is shown in Figure 7.8(a), and the resulting probabilities $P_X(x=1)$ for each LSB Position in displayed in Figure 7.8(b). Again, it

can be observed that the least significant bits have a probability $P_X(x)$ around 50%, whereas the most significant ones diverge from an even distribution.

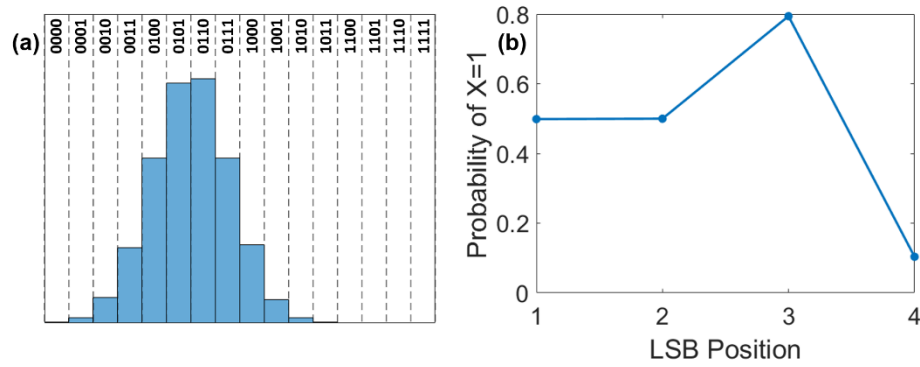


Figure 7.8 (a) Histogram of a Gaussian distribution, binned using 4 bits. (b) Probability of all bits being equal to 1, depending on the LSB position.

CHAPTER 8 ADDITIONAL RESULTS

This chapter describes additional results that were realized during the course of this PhD, but that were not published in the articles presented in the previous chapters. The first section describes how the ROGUE was used for shape reconstruction of a minimally invasive surgical robot. This work was realized during an internship in the laboratory of Prof. Iulian Iordachita, at Johns Hopkins University (JHU) in Baltimore, and is a direct application of the work described in the first article. The second section covers additional investigations of the ROGUE's unique properties, as an ideal tool to study light localization and random lasing. Finally, the last section covers high-quality FBGs and fiber lasers. While the main results presented in this thesis relate to random gratings and random lasers, understanding how to fabricate high-quality FBGs was another important part of this PhD. Indeed, manufacturing the worst (most random) gratings requires knowledge of how to make the best ones first. Furthermore, this work allowed the expansion of the already state-of-the-art capabilities of our FBG fabrication station. While not strictly related to the subject of secure communications, these results are direct applications of the techniques developed in the search for improved communications security.

8.1 Shape reconstruction of a Continuum Dexterous Manipulator

During the internship at JHU, the ROGUE sensors developed and presented in the first article were used to increase the accuracy of shape reconstruction of surgical robots. The JHU research team led by Prof. Iulian Iordachita achieved shape reconstruction based on quasi-distributed sensing, using discrete FBG sensors. My assignment was to investigate how the enhanced signal and improved accuracy of the OFDR distributed sensing using ROGUEs would improve the shape reconstruction. This led to a peer-reviewed conference proceeding [170] that I co-first authored with Shahriar Sefati, a PhD student at JHU, and that I presented at the International Conference on Robotics and Automation, one of the biggest and most important conference in robotics. In this research, we compared the accuracy in the shape reconstruction of a Continuum Dexterous Manipulator (CDM), using two fiber triplets, one made of typical FBGs using quasi-distributed sensing, and one made of ROGUEs using OFDR sensing. Mr. Sefati and the JHU team fabricated the CDM and FBG fiber triplet, and developed the software to operate the CDM, while I integrated

the ROGUE fiber triplet with the CDM, performed the experiments of CDM bending and realized the shape reconstruction and data treatment.

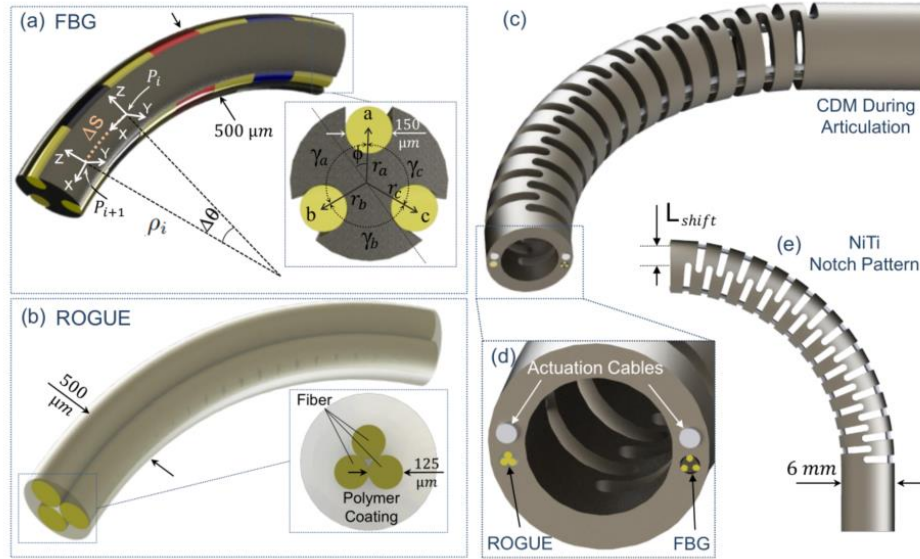


Figure 8.1 (a) The FBG fiber triplet, where each fiber is glued in a groove engraved in a nitinol wire, and contains three FBGs. (b) The ROGUE fiber triplet, where the fibers are extruded in a polymer coating. (c) The CDM during articulation and (d) its tip, showing the actuation cables pulling the CDM, and the FBG and ROGUE triplets. (e) The nitinol notch pattern in the CDM design. Taken from [170].

Figure 8.1 displays the CDM used in these experiments, as well as the two fiber triplets used for this comparison study. The CDM was developed for minimally invasive orthopedic surgery, and is constructed in nitinol, a highly flexible nickel and titanium alloy, which was also used for the FBG triplet. The notch pattern in the CDM allow its flexibility when pulled by the actuation cables. The length of the flexible part of the CDM is 35 mm, and it has an outside diameter of 6 mm, as shown in Figure 8.1(e). Inside the CDM wall, four channels allow passing of the actuation cables and the fiber sensors. Pulling in one of the actuation cable results in the CDM bending, as can be observed in Figure 8.2. Various experiments were performed to characterize the accuracy of both fiber sensors, first in free environment, where the CDM will bend in the C-shape shown in Figure 8.2(a), and when interacting with obstacles placed at different positions over the CDM's flexible length. The interaction with obstacles will result in more complex shapes that should be harder to

reconstruct with the limited spatial resolution of the FBG quasi-distributed technique (three FBGs spaced by 10 mm), while the 0.65 mm spatial resolution of the completely distributed sensing OFDR technique should allow it to better resolve these shapes. Finally, an additional S-shape was forced upon the CDM, as shown in Figure 8.2(b), to test the limitations of both sensing techniques. Testing the interaction with obstacles and complex shapes is important, because it is more representative of real work environment when the CDM is performing surgery inside a human patient, where it is bound to encounter obstacles like bones or organs.

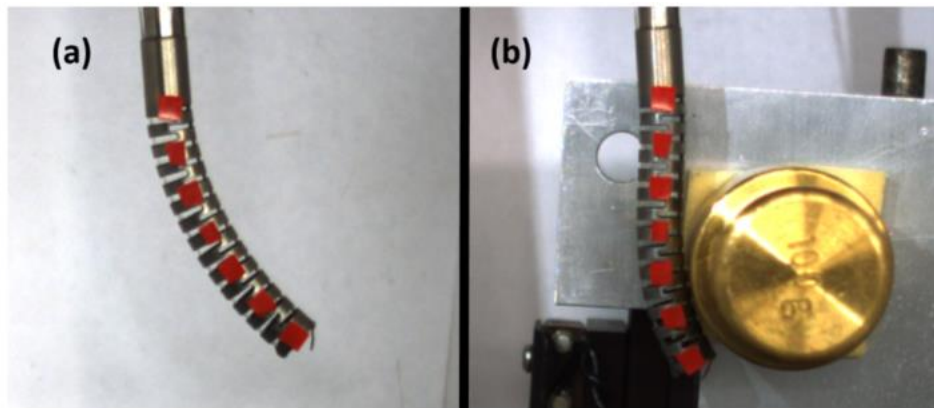


Figure 8.2 Pictures of the CDM bending experiments, taken (a) in free environment and (b) when interacting with an obstacle. The red markers are used with a pair of stereo cameras to provide a ground truth for the shape reconstruction. Taken from [170].

After conducting these experiments, the triplet's shape was reconstructed based on the strain measured along the sensor's length, and compared with the position of red markers placed on top of the CDM (see Figure 8.2), whose positions were obtained by a pair of stereo cameras. This provided a ground truth to which the reconstructions were compared. Over this series of experiments, the mean tip position error for the ROGUE (FBG) triplet was found to be 0.32 (0.83) mm when the experiments were performed in free environment, 0.41 (0.80) mm when interacting with obstacles, and 0.45 (2.27) mm for the forced S-bend. Overall, for the free bending and obstacles experiments, an improvement of a factor of 2 has been observed on the tip position accuracy when using the distributed OFDR technique over the quasi-distributed FBG sensing technique. However, it really shines when more complex shapes are introduced such as the S-bend, where the limited spatial resolution of the FBG triplet is insufficient to ensure proper shape reconstruction. Moreover, the maximum tip position error measured across all these experiments

remained sub-millimeter (typically an acceptable upper bound for minimally invasive surgery) for the ROGUE triplet, while it reached 3.40 mm for the FBG triplet. These results demonstrate the potential of the ROGUE used in conjunction with the OFDR distributed sensing technique as an alternative for more accurate shape reconstruction than the typically used FBG quasi-distributed sensing technique.

8.2 ROGUE-based localization and random lasers

The unique properties of the ROGUE make it also a very interesting device to study other effects such as localization. Indeed, as was shown in Figure 4.5, the ROGUE's bandwidth reaches an asymptotic value after a certain length, unlike a conventional FBG, whose bandwidth is inversely proportional to the grating's length. This phenomenon is due to the localization of light, in a way similar to the demonstration by Shapira *et al.* that the reflection bandwidth of a large number of randomly spaced uniform FBGs would converge towards the bandwidth of a single FBG [20].

The similarities between the ROGUE and Shapira's experiments is further supported by the conclusion of the statistical model described in section 4.3. Indeed, it demonstrated that the ROGUE can be also modeled as an array of randomly-spaced uniform FBGs. Furthermore, the model predicted an average μ FBG length of 72.5 μm , which is quite close to the experimental 100 μm spot size used for inscription (the spot size here is defined as $1/e^2$). The discrepancy between these two values comes most likely from the fact that the model used uniform gratings, while the experimental spot size has a Gaussian shape, resulting in apodization of the experimentally inscribed μ FBGs. Obviously, this model makes relatively naïve assumptions, resulting in an imperfect representation of the ROGUE. In reality, the ROGUE does not consist of uniform FBGs separated by large gaps with no index modulation, but is rather a continuum of overlapping, low-reflective gratings. This makes the ROGUE even more complex than the arrangement described by Shapira *et al.* [20]. Nonetheless, the similarities between the two are striking, and demonstrate that the ROGUE should be also an ideal subject for studying localization effects. Therefore, one would expect that, past a certain localization length, the ROGUE's bandwidth would converge to be that of a single FBG formed by the inscription spot size. Indeed, this is what was observed experimentally in Figure 8.3(a).

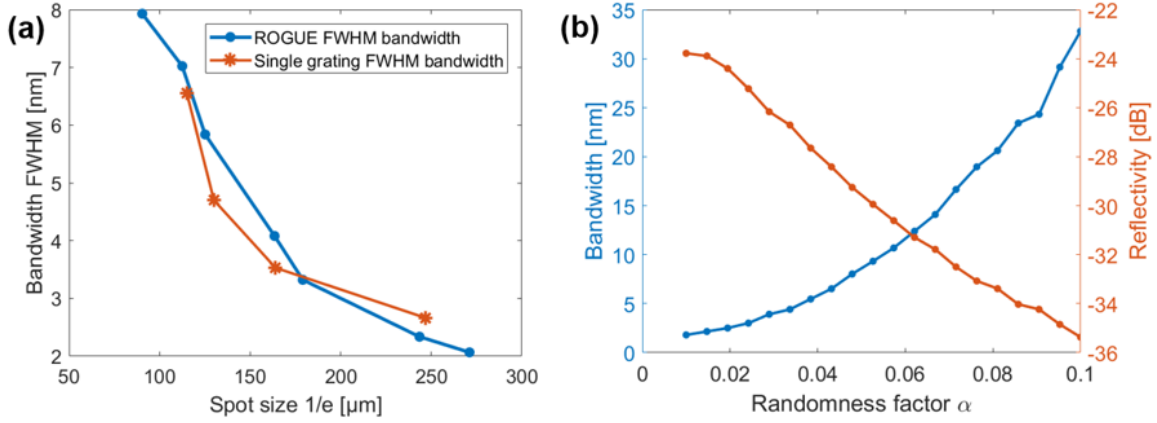


Figure 8.3 (a) ROGUE full-width at half-maximum (FWHM) bandwidth for different inscription's spot sizes (blue), compared with the FWHM of a single grating written with the same spot size (orange). (b) Simulated ROGUE bandwidth (blue) and reflectivity (orange) as a function of the randomness factor α .

This localization of bandwidth can be also linked to Arash Mafi's work [21] discussed in section 2.1.3 of the literature review. Indeed, he described a model for random gratings, where the phase difference between two planes is equal to $\pi + \theta\pi$, where θ is computed from a randomness factor α , multiplied by a number picked from a uniform random distribution ranging from -1 to 1. A grating with a randomness factor $\alpha = 0$ would be a standard uniform grating, whose bandwidth decreases inversely proportionally to its length (for weak κL gratings), while a randomness factor $\alpha = 1$ would describe a grating where the phase between each grating plane could take any value between 0 and 2π , and would have an infinite bandwidth. For values between 0 and 1, the bandwidth would converge to a value that depends on α . The randomness factor would define the reflectivity of the random grating, such that the integral is conserved. A simulation based on Mafi's methodology was developed, and the results highlighting this conclusion are shown in Figure 8.3(b). Therefore, a compromise must be obtained between the randomness of the grating (and thus the ROGUE bandwidth) and the required signal to noise ratio (SNR), which can be obtained by tuning the inscription laser's spot size.

These localization effects were in fact the subject of a conference presentation during the course of this PhD, where localization observed simultaneously in terms of the bandwidth were reported, that localized to a fixed value, as well as in the transmission, which quickly converged to an

exponential decay, as expected in the presence of localization [204]. These effects are demonstrated in Figure 8.4. Indeed, it is striking to observe that the bandwidth converges to a fixed value (here, about 5.5 nm) at exactly the same ROGUE length than that at which the transmission converges to an exponential decay (here showed in reflection). This value is found here to be ~ 50 mm, which is similar to the localization lengths reported in other random grating arrangements (also 50 mm for Gagné *et al.*'s continuous random grating [23], 60 mm for Lizárraga's random grating array [22]).

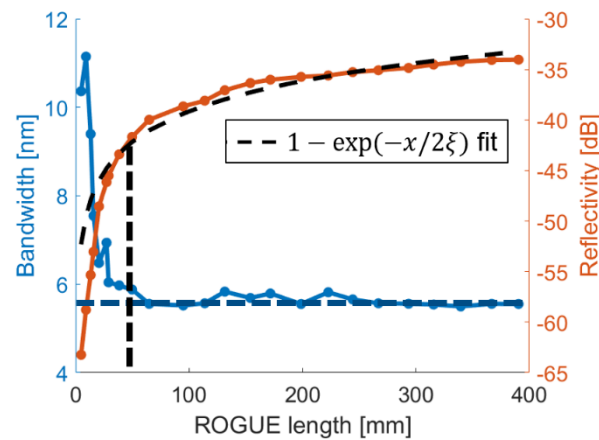


Figure 8.4 Localization effects observed in the ROGUE. The reflectivity (orange) starts following the fit in the dashed black line (which is the equivalent of an exponential decay of the transmission) for the same ROGUE length at which the bandwidth (blue) localizes to that of the single grating.

If localization effects can be observed in the ROGUE, then random lasing could also occur. This was tested by using a modified version of the experimental setup of Chapter 6, where an additional 3 meter-long ROGUE was placed at the end of a 3 km standard telecommunications (SMF-28) fiber bundle. The FBG closing the cavity on the other side was written at a Bragg wavelength of 1569 nm, while the ROGUE was centered at 1577 nm (the ROGUE's transmission bandwidth is shown in Figure 8.5(c)). The first experiment was realized without using the ROGUE. By simply pumping the cavity in a similar fashion to that demonstrated in Chapter 6, random lasing began for a pump power of 5 W (see Figure 8.5(a), blue). When adding the ROGUE, the threshold was reduced by a factor of 3 to approximately 1.6 W (see Figure 8.5(a), orange). However, the lasing wavelength (1569 nm) was at the very edge of the ROGUE's bandwidth (the first blue curve in Figure 8.5(c)). By applying strain to the FBG, its wavelength (and thus that of the laser) can be

shifted towards longer wavelengths. By tuning the FBG's wavelength to 1577 nm (the center of the ROGUE's bandwidth), the random lasing threshold can be further reduced by another factor of 2, to 0.8 W (see Figure 8.5(a), green). One can notice that, as the threshold decreases, the slope efficiency also decreases. This is due to the higher quality (Q) factor of the cavity caused by the increased scatter of the ROGUE.

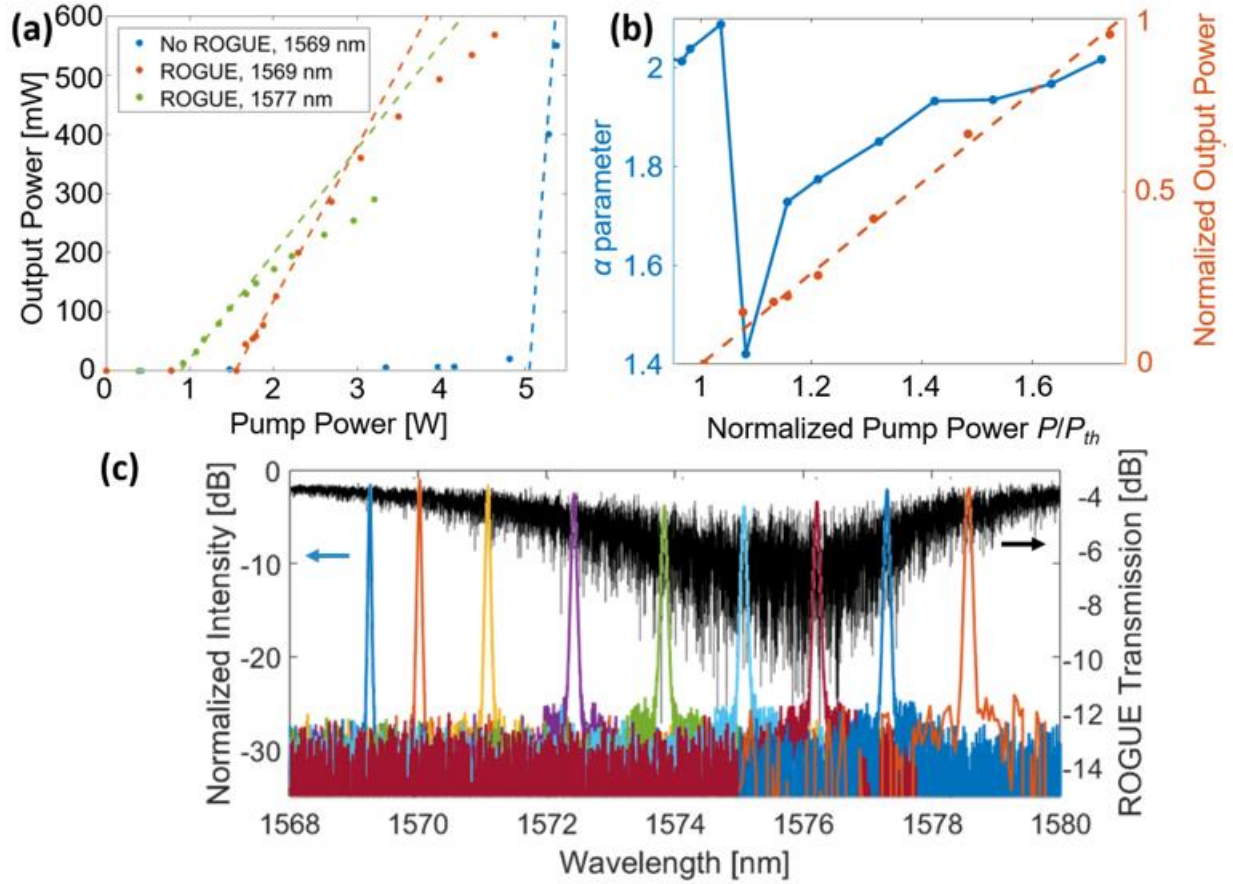


Figure 8.5 (a) Output of the laser as a function of pump power, both with and without the ROGUE, using a 3 km length of standard telecommunications fiber as a cavity. (b) Lévy α parameter with the ROGUE confirming the laser is truly operating in a random regime. Here P_{th} is defined by the intersection of the linear fit, rather than by the α parameter. (c) Spectrum of the ROGUE's transmission (black) and of the laser while applying different values of strain to the FBG, highlighting the laser's tunability across the ROGUE's broad bandwidth.

In order to verify that the laser indeed operated in the random regime, and not based on a reflection at a fixed point within the ROGUE, the emission statistics of this laser were measured, and a Lévy

α -stable fit was performed on the data to quantify the α parameter at different pump powers. As can be seen on Figure 8.5(b), the α parameter acts exactly as expected for a random laser, with $\alpha = 2$ below threshold, corresponding to Gaussian ASE emission, with a sharp decrease in α at the threshold, followed by a gradual return towards $\alpha = 2$ above threshold. This confirms this laser indeed operates in the random lasing regime. Finally, as mentioned earlier, the lasing wavelength of this laser can be tuned within the ROGUE's broad bandwidth by applying strain to the FBG. This is demonstrated in Figure 8.5(c), where different lasing spectra are displayed under the ROGUE's bandwidth, each corresponding to a certain strain applied to the FBG.

These experiments demonstrate that the ROGUE, while being perfectly well suited for distributed sensing and PUF applications, can be also used to study localization and random lasing effects. Indeed, localization effects are observed within the ROGUE for lengths of only 50 mm, and a 3 meter-long ROGUE can reduce the threshold of a 3 km long random distributed feedback Raman laser by a factor of 6, while enabling the possibility of tuning within its broad bandwidth.

8.3 Fabrication of high-quality FBGs and lasers

While most of the results presented in this thesis rely on randomness, both in fiber Bragg gratings and lasers, the reader should not be left with the impression that all the results obtained during this PhD are based on noise. Indeed, a significant portion of this PhD has been spent working on improving the FBG fabrication process that was developed by previous students of the Fabulas laboratory [41, 130, 131]. The following sections cover the two main contributions of this PhD towards the improvement and realization of high-quality FBGs, namely the optimization of the apodization, and the fabrication of high-quality, single-frequency distributed feedback lasers (DFBs) written in thulium (Tm) doped fiber.

8.3.1 Optimization of the FBG Apodization

Apodization, as mentioned in section 2.1.1 of the literature review, is an important parameter in FBG fabrication, as its proper control allows elimination of reflection side-lobes. This is very important in many FBG applications, such as filters for optical wavelength division multiplexing (WDM), since side-lobes will result in reflection outside the desired band, thus limiting WDM density [205]. This is also critical for sensors, for example in quasi-distributed sensing schemes,

since the presence of side-lobes implies that the spectral separation between each sensor needs to be greater to ensure there is no overlap between the spectra of two sensors. A greater spectral separation between two sensors thus results in the need for a larger wavelength tunable range, resulting in lower measurement speed [206]. In our fabrication station, apodization is achieved by applying a high frequency, periodic voltage on the piezoelectric element on which the inscription phase mask is mounted. The apodization voltage applied on the piezoelectric element induces a rapid phase change on the interference pattern resulting from the overlapping UV beams on the fiber. Applying a peak-to-peak apodization voltage $V_{2\pi}$ corresponding to a 2π phase change resulting in complete apodization of the grating, while no voltage results in an unapodized grating. To obtain certain apodization profiles, such as a Gaussian apodization for instance, the amplitude of this apodization voltage can be changed accordingly over the grating's length. It had been assumed by the previous users of this fabrication station that the apodization varied linearly with the applied voltage. While imperfect apodization had been observed, it had been theorized that this was the result of mechanical vibrations of the piezoelectric element [17]. However, as described by Cheng and Chrostowski it is incorrect to assume a linear dependence between the periodic phase function's amplitude and the apodization. Indeed, for a uniform FBG to which a periodic phase function $\phi(z)$ is applied, the effective refractive index Δn along the length z of the grating can be written as

$$\Delta n(z) = \Delta n \times \text{Re} \left\{ \exp \left(\frac{2\pi iz}{\Lambda_g} \right) \times \exp(i\phi(z)) \right\}, \quad (8.1)$$

where Λ_g is the period of the uniform grating and i is the imaginary number. The term $\exp(i\phi(z))$ can be expanded into Fourier series such that equation (8.1) can be rewritten

$$\Delta n(z) = \Delta n \sum F_m \text{Re} \left\{ \exp \left(i \left(\frac{2\pi z}{\Lambda_g} + \frac{2\pi m z}{\Lambda_\phi} \right) \right) \right\}, \quad (8.2)$$

where F_m is the m^{th} Fourier coefficient and Λ_ϕ is the period of the phase function. This results in multiple resonances on each side of the central Bragg resonance given by the initial grating's period Λ_g . The spacing between the resonances is given by

$$\Delta\lambda = \lambda_B \left(\frac{2n_g\Lambda_\phi}{\lambda_B} + 1 \right)^{-1}, \quad (8.3)$$

where λ_B is the original Bragg wavelength of the uniform grating and n_g is the group index of the waveguide. In our current case, since $\Delta\phi$ is very small, these additional resonances will be far outside the spectral region of interest. For example, using a typical writing speed of 50 $\mu\text{m/s}$, and an apodization frequency of 20 Hz, results in a phase function period of 2.5 μm . For a central wavelength of 1550 nm, this results in a spacing $\Delta\lambda$ of 273 nm. Even if the effect of these additional resonances can be neglected, the strength of the central Bragg resonance is dependent on the 0th Fourier term F_0 of the periodic phase function. F_0 can be derived by

$$F_0 = \frac{1}{\Lambda_\phi} \int_0^{\Lambda_\phi} \exp(i\phi(z)) dz. \quad (8.4)$$

On the fabrication station used during this thesis, the periodic phase function used for apodization is typically either a triangle or sawtooth wave. In both these cases, the relationship of F_0 and A (the amplitude of the phase function) follows a sinc function

$$F_0 = \frac{\sin(A)}{A}. \quad (8.5)$$

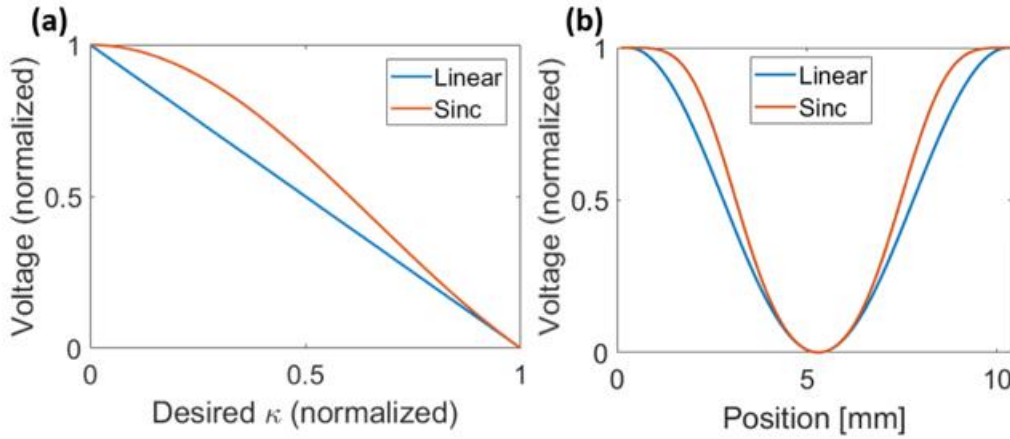


Figure 8.6 (a) Required apodization voltage to achieve a certain grating strength κ , depending on the assumption of a linear or *sinc* relationship. (b) Resulting applied voltage to achieve a cosine apodization for a 10 mm grating, depending on a linear or *sinc* relationship.

Therefore, the voltage amplitude that must be applied to the piezoelectric element can be found by taking the inverse *sinc* function of the desired apodization profile. Figure 8.6 displays how the effects of this correction on the applied voltage both in (a) a linear case, and (b) a cosine apodization profile. The effect of this correction on the quality of the apodization can be observed in Figure

8.7(a), where an improvement from an apodization of 19 dB to 25 dB can be observed when using a *sinc* relationship instead of the linear relationship that was initially assumed. This is in line with the simulated spectra of Figure 8.7(b). While the experimentally obtained apodization is slightly lower than the simulation, due to other sources of noise, the effect of the *sinc* correction on the apodization quality is comparable.

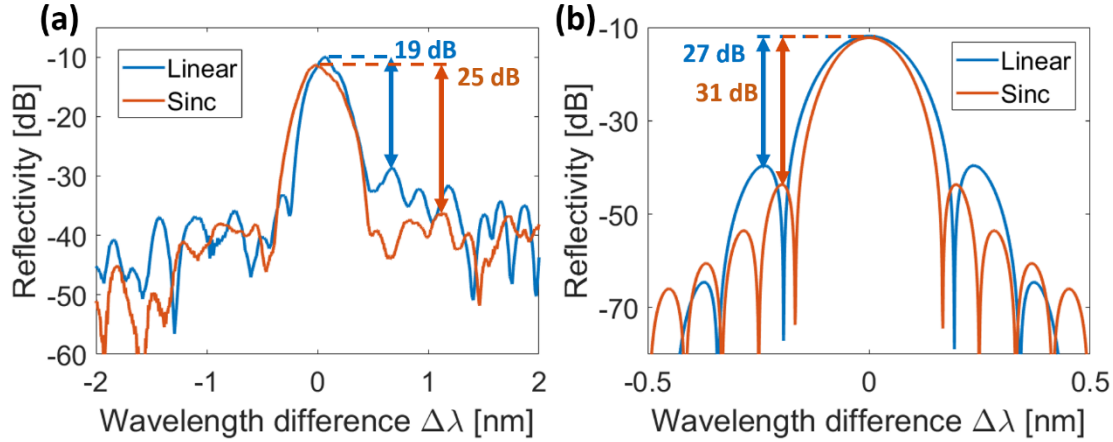


Figure 8.7 Comparison of the apodization quality when assuming the apodization voltage and the coupling strength κ_{ac} have a linear relationship (blue) and a *sinc* relationship (orange), both for (a) experimentally measured data and (b) simulated spectra. All gratings are 10 mm long with a cosine apodization, written at a central wavelength of 1558 nm.

8.3.2 Fabrication of DFB lasers in Tm-doped fiber

The enhanced capabilities of our FBG manufacturing station were used to fabricate state-of-the-art distributed feedback (DFB) lasers in thulium-doped fiber. Thulium has a very broad emission cross-section that covers wavelengths from 1.6 μm to 2.2 μm , and as such has been used to develop laser sources in the 2 μm band [207]. In a collaboration project with MPB Communications, we were tasked with the development of a single-frequency, single-polarization fiber laser at a wavelength of 1.73 μm capable of outputting at least 1 mW of output power. Developing a laser source in Tm-doped fiber at this wavelength is much more challenging than at 2 μm , since the tail of the absorption cross-section extends up to 1.9 μm . Therefore, the ground-state absorption of thulium is still high at 1.73 μm and competes with the gain, which is also lower at this wavelength than at its peak of 1.85 μm [208]. I worked on this project with Yannick Cuerno, a Masters student

in our laboratory, where I manufactured the DFBs and FBGs, and he tested and characterized them. A journal article presenting these results is currently in preparation.

As proof of concept, the grating was written at a wavelength of $1.74\ \mu\text{m}$, but with minimal adjustments the grating could be just as easily inscribed at the required wavelength of $1.73\ \mu\text{m}$. The DFB laser was fabricated in a polarization-maintaining (PM) fiber, where a large birefringence induced in the fiber core ensures that the polarization is maintained throughout the propagation. This birefringence results in different effective refractive indices along the two axes of the fiber, and as such the DFB's central wavelength is not the same for the two polarizations. For the PM fiber used in this application, its birefringence induces a $0.4\ \text{nm}$ separation between the polarizations.

Table 8.1 Writing parameters used for the DFB

Parameter	Value
DFB Length	100 mm
Coupling coefficient	$64\ \text{m}^{-1}$
Phase shift amplitude	π
Phase shift position	55 mm
Apodization Proportion	0.4
Apodization Type	Cosine

After optimization of the grating's length, strength and apodization, the writing parameters that were picked are presented in Table 8.1, while the variation of the phase and apodization as a function of the DFB's length is shown in Figure 8.8(a). Here, the apodization proportion refers to the proportion of the DFB where the chosen apodization type (here cosine) is applied. In the current case, this means that a cosine apodization is applied on the first and last 20 mm of the DFB. This apodization profile was chosen to ensure the side-lobes are sufficiently suppressed to prevent them from lasing, but that the DFB's coupling coefficient is strong enough to achieve lasing of the central mode. The DFB's reflection and transmission spectra were simulated from the above parameter, using the transfer matrix method. The results are displayed in Figure 8.8(b).

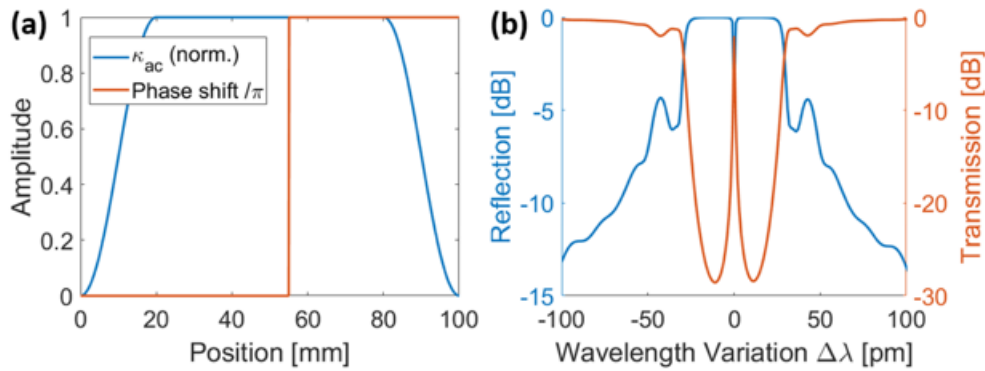


Figure 8.8 (a) The DFB apodization displayed as the normalized coupling coefficient κ as a function of length, as well as the π phase shift located at 55 mm. (b) Reflection and transmission spectra of the simulated DFB.

To ensure single-polarization operation, an additional uniform FBG was written in standard telecommunications fiber matched to the fast-axis mode of this DFB (the wavelength corresponding to the polarization with the highest effective refractive index). A fusion splice then connected this FBG to the DFB, to ensure that the fast-axis mode was reflected to the DFB, thus forming a Fabry-Perot cavity, without affecting the slow-axis mode. This additional feedback to the fast-axis polarization significantly affects its lasing threshold. The spacing between the DFB and the second FBG determines whether the fast-axis mode is in resonance with a Fabry-Perot cavity mode, in which case the fast-axis can lase, or if it is in anti-resonance, in which case the slow-axis will lase. As such, it ensured that when the DFB started lasing, it could remain in a single-polarization state to very high pump powers. Figure 8.9 displays the experimental cavity design.

The cavity was pumped with a 1575 nm CW fiber laser provided by MPB Communications that could deliver up to 1.3 W of power. The threshold of our DFB laser was found to be 220 mW, with a slope efficiency of 0.86%. By using a pump power of 450 mW, up to 1.4 mW of output power could be obtained in single-polarization, single-frequency operation. This accomplishes all the requirements set by our collaborator MPB Communications. Up to 3 mW of output power was achievable at higher pump power, however a second lasing mode could be observed corresponding to the slow-axis polarization. The DFB laser's single-frequency operation is shown in Figure 8.10, obtained by an optical spectrum analyzer (Figure 8.10(a)) and a scanning Fabry-Perot interferometer (Figure 8.10(b)). The first spectrum measurement ensures that there is only a single

polarization mode lasing, while the second measurement provides a higher resolution measurement of the lasing mode's linewidth (here, 8MHz). The Fabry-Perot's higher resolution also ensures that there is only a single lasing mode, and not two narrowly spaced modes that could not be resolved by the optical spectrum analyzer.

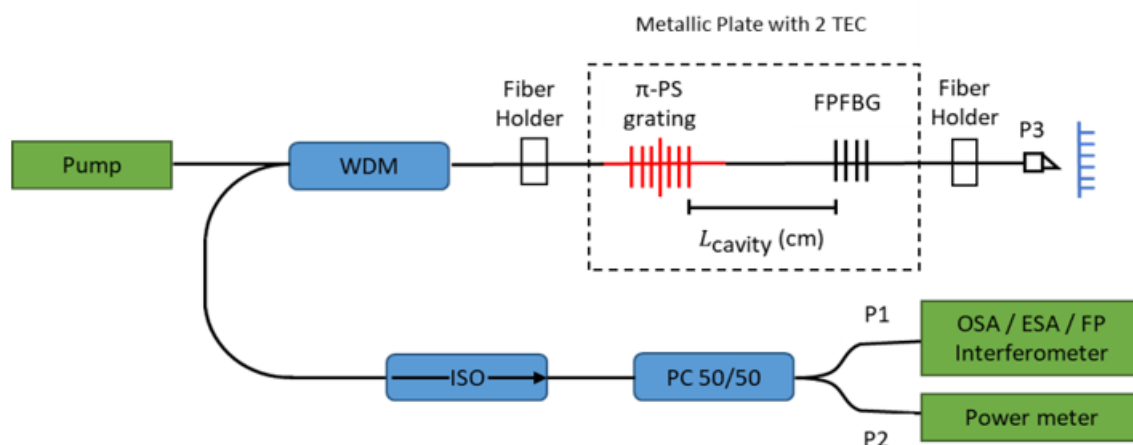


Figure 8.9 Cavity design for the single-frequency, single-polarization fiber laser, where the pump goes through the Wavelength Division Multiplexer (WDM) coupler and pumps the π phase shifted (π -PS) grating. The active Tm-doped fiber is highlighted in red. In the forward direction, the Fabry-Perot FBG (FPFBG) written in telecommunications fiber reflects the fast-axis mode towards the laser. The fiber is held by two fiber holders, and placed on a metallic plate whose temperature is controlled by two thermoelectric coolers (TEC), to ensure uniform temperature across the entire cavity. The reverse output of the laser is filtered by the WDM coupler, and is split in two ports by a power coupler (PC), where output P2 is used to monitor the output power, while output P1 is used to characterize the optical/electrical spectrum with an optical/electrical spectrum analyzer (O/ESA), or to ensure it is operating in a single mode with the scanning Fabry-Perot (FP) interferometer. An isolator before the PC ensures that no backreflection destabilises the laser, while forward output P3 is cleaved at an angle for the same reason. Taken with permission from [209].

The laser's single-polarization stability was tested by tuning the metallic plate's temperature using the two thermoelectric coolers on which the fiber was placed (see Figure 8.9). With a pump power of 330 mW, the laser remained stable in the fast-axis polarization over a tuning range of more than 6 °C. Similarly, strain was applied to the fiber by moving one of the fiber holders. Using again

330 mW of pump power, the laser remained in the fast-axis polarization with up to $130 \mu\epsilon$ of strain applied to the fiber. The single-polarization stability is of course dependent on the distance between the π -shifted grating and the FBG, as the longer the distance separating them, the larger the accumulated phase difference will be. For that reason, the separation was kept as short as possible, to 3.2 cm. This distance could be reduced in further designs.

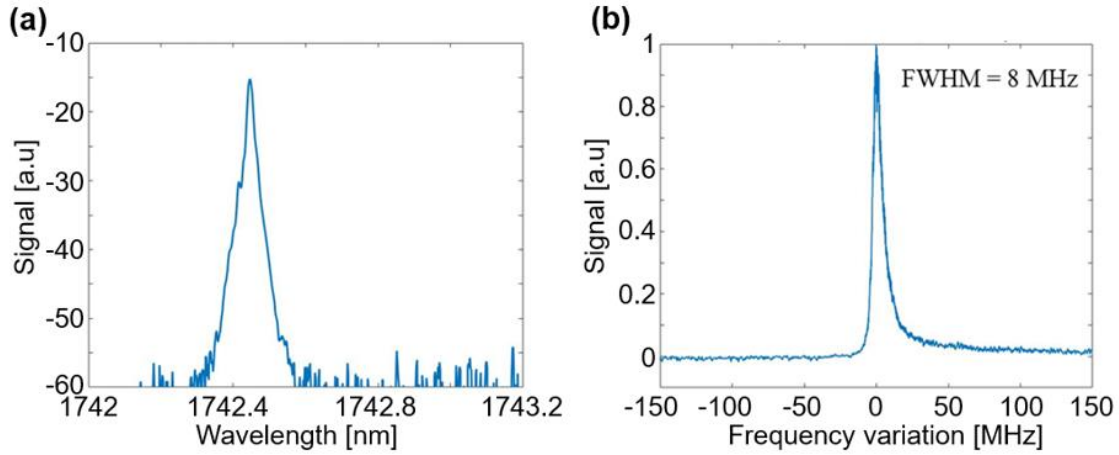


Figure 8.10 DFB output spectra, when operating at a pump power of 361 mW, using (a) an optical spectrum analyzer and (b) a scanning Fabry-Perot interferometer. The mode's full width at half-maximum (FWHM) of 8 MHz can be observed in (b). Adapted with permission from [209].

CHAPTER 9 GENERAL DISCUSSION

This chapter discusses the main results of the articles presented in the previous chapters, and their relationship with the objectives identified at the beginning of this thesis. It will be separated into two parts. The first section will review each objective, and discuss how they were accomplished by the results described in the previous chapters. The second section will provide some additional discussion regarding the overall achievements presented in the thesis.

9.1 Review of the objectives

9.1.1 Fabrication of a novel, noise-based random grating

The first objective of this thesis was to fabricate novel, noise-based random gratings for secure communications applications. This objective was addressed in Chapter 4 by the demonstration of how ROGUEs could be fabricated by adding noise to a standard FBG fabrication station. However, before discussing the results presented in this chapter, one might wonder why there is even a need for novel random gratings in the first place. Indeed, as was shown in section 2.1.3, random gratings have been demonstrated in the past. In our group several years ago, Mathieu Gagné (a PhD student at the time) demonstrated that randomly spaced phase errors occurring during the fabrication process of a continuous FBG resulted in the inscription of a random grating. He further demonstrated how this grating could be used for random lasing [23]. Other researchers also achieved random grating inscription by introducing pre-programmed phase errors in a uniform FBG recipe [22, 25]. However, for secure communications applications, random gratings have an additional constraint. No one, not even the manufacturer, should be able to reproduce any of these gratings. Due to the discrete nature of the phase errors in the schemes above, a potential attacker could reproduce such gratings if he knew or reverse-engineered the required recipe.

On the other hand, the ROGUE presented in Chapter 4 has a continuously varying random phase, making experimental reproduction of this grating much more challenging, if not impossible. To successfully clone a ROGUE, the attacker would need to reproduce exactly the randomly varying phase profile used in the fabrication process, along with all the additional experimental noise. This randomness is however somewhat limited by the inscribing UV laser's spot size, which provides a certain degree of coherence within the random grating, as multiple fringes are inscribed at the same

time. This makes them potentially easier to reproduce than a completely random grating. However, this coherence is only within the length of the spot size ($\sim 100\ \mu\text{m}$), orders of magnitude smaller than the PUFs' lengths used in Chapter 5, which were tens of millimeters long. Additionally, the phase interaction between the multitude of individual μFBGs that make the ROGUE results in very complex features whose spectral resolution are limited by the interrogator's spectral resolution rather than the individual feature size. Finally, this coherence can be tuned by reducing the spot size, as mentioned in section 8.2. At the limit, a point-by-point technique could completely remove that coherence by writing the ROGUE one fringe at a time, using either a UV [210] or infrared [19, 211] ultrafast laser inscription technique. This is somewhat similar to the work described in Xu *et al.* [25], although one would want to ensure that the phase variations are random and not recorded, rather than being pre-programmed for PUF applications.

However, a certain degree of coherence is not necessarily a bad thing. While writing the random grating a single fringe at a time would reduce its coherence, and at the same time increase its bandwidth, it would also lower its reflectivity, as demonstrated by Arash Mafi with his conserved area theorem [21]. This results in a decreased SNR, making the random grating measurements more susceptible to noise. Keeping reflectivity constant would thus require increasing the inscription laser's power, which leads to increased losses. Indeed, the random gratings described in Xu *et al.*'s work had very high losses ($\sim 100\ \text{dB/m}$) for this reason [25].

Since both the distributed sensing application described in Chapter 4 and the PUF application described in Chapter 5 scan the ROGUE's reflectivity over a relatively narrow bandwidth, the spot size cannot be decreased too much. Indeed, if the ROGUE's bandwidth became larger than the scanned region, part of the enhancement in signal is no longer measured by the instrument, and is therefore wasted. The scanning bandwidth can be increased, however this also increases the scanning time, and the complexity of the required interrogator. In our experiments, we chose to keep an inscription spot size of approximately $100\ \mu\text{m}$, resulting in a bandwidth of around $8\ \text{nm}$, a compromise between the two most widely used scanning bandwidths of $5\ \text{nm}$ and $10\ \text{nm}$. This also resulted in a very small coherence length, while the SNR was sufficiently large to achieve high quality measurements.

The demonstration of ROGUE fabrication described in Chapter 4 was not sufficient to achieve Objective 1. Indeed, while the ROGUE demonstrated had all the required qualities, they were

fabricated using a 4 M\$ state-of-the-art FBG writing station limited to 1-meter long grating lengths, which is obviously not sustainable for commercial applications. To successfully achieve the first objective, these random gratings should be written continuously using a much lower cost system that could be scaled up for commercial purposes. Thus, another ROGUE fabrication station was designed for this, and presented in Chapter 5. Instead of using a one-meter long high-accuracy translation stage, the fiber is being pulled continuously in front of the intersecting UV beams by a rotating fiber optic bundle. Furthermore, the low-cost stepper motor used to rotate the bundle is not only significantly cheaper than an air-bearing stage, but also provides the noise necessary to inscribe the ROGUE. There is therefore no need for an additional source of randomness to drive the piezoelectric element, which was also removed for simplicity. Such a writing station could be directly implemented in the middle of the fiber drawing process if necessary, to write the ROGUEs as the fiber is being pulled. This fabrication technique is therefore low cost, and can be easily scaled up. This demonstration thus allows the completion of Objective 1.

The different types of random gratings discussed in this section are enumerated in Table 9.1, and their properties are compared. The random grating arrays refer to both Shapira *et al.* and Lizárraga *et al.*'s work on localization and random lasing using an array of identical uniform FBGs [20, 22], while the uniform grating with phase error corresponds to Mathieu Gagné's work on random lasing [23]. Two different point-by-point techniques are identified in this Table. The first technique refers to Xu *et al.*'s random grating, where each grating plane is randomly spaced from the previous one [25], resulting in enhanced reflectivity across the entire spectrum. While in their demonstration, the grating planes' position were recorded, this does not have to be the case, and would provide more security for PUF applications as it would make the random grating more challenging to reproduce. This could be achieved for example by replacing the UV laser in the continuous ROGUE writing scheme developed in Chapter 5 by an ultrafast infrared laser, and is the modality considered here. The second point-by-point technique identified in Table 9.1 relies on the point-by-point FBG writing technique that was recently developed in our group [19], which allows precise control over the exact spacing between every grating plane. This technique can allow the inscription of arbitrarily complex grating profiles, and can thus be used to write random gratings with a specified randomness to target a specific bandwidth, based on Mafi's work [21]. This was experimentally demonstrated recently by our group, and the random gratings thus realized were

used for shape sensing [212], using the same OFDR sensing technique described in Chapter 4 for strain and temperature sensing.

Table 9.1 Comparison of the different random gratings properties

Type of random grating	Bandwidth	SNR	Fabrication station	Length limitation	Reproducibility	Losses
Random grating array [20, 22]	Given by the FBG, easy to tune	Very high	Relatively simple	Unlimited	Relatively easy to reproduce	Low
Uniform FBG with phase errors [23]	Small, difficult to tune	Very high	Relatively complex	Unlimited	Possible, but challenging to reproduce	Low
Randomly spaced point-by-point grating [25]	Entire spectrum	Low	Relatively simple	10 cm, but could be unlimited	Very difficult to reproduce	High
Pre-programmed point-by-point grating [19]	Easily tunable	Very high	Very complex	1 meter	Could be reproduced with the recipe, but very difficult to reverse-engineer	Low
ROGUE (this work)	Given by the spot size, easy to tune	High	Very simple	Unlimited	Very difficult to reproduce	Low

As can be seen from Table 9.1, the ROGUE inscription technique presented in this thesis is the simplest one, but also one of the most challenging ones to reproduce, as it is completely based on noise. While not a concern for applications like sensing, for security applications such as PUFs, it is the most important property. The randomly-spaced point-by-point inscription technique [25] offers a similar challenge for reproducibility, however it requires a more complex fabrication station, and the broadband enhancement results in very high losses to achieve an SNR comparable to that of the ROGUE. The pre-programmed point-by-point inscription [19] is also a strong contender, as it can be easily tuned to achieve high SNR with low losses, but this technique is significantly more complex, and follows a recipe that could potentially be leaked or reproduced, which is a potential security concern. Indeed, for PUF applications, nobody, not even the manufacturer, should be able to reproduce the PUF.

9.1.2 Secure communications using random gratings

The second objective of this thesis was to demonstrate how these random gratings could be used to enhance the security of existing public-key cryptosystems. This objective was achieved by the demonstration that the ROGUE could be used as a very effective PUF, using its random spectrum as a unique signature. The performance and repeatability of the ROGUE PUF has been demonstrated at length in Chapter 5, using multiple parameters such as PUF length and interrogation bandwidths. This section will discuss how such PUFs could be implemented in secure communications.

Typically, *weak* PUFs such as the ones demonstrated in Chapter 5 are used for secret key generation, in lieu of digitally stored secret keys. The advantage of using a physical device to do so is that the key generated does not have to be stored in non-volatile memory, making it less susceptible to hacking. In such a configuration, the PUF is scanned whenever the secret key is required and stored in volatile memory while in use, to then be flushed from memory after use. Secret keys require absolute repeatability. If only a single bit of the key were to be incorrect, the communication would become gibberish. This would then require the PUF to be able to consistently achieve a Hamming distance of 0. To compensate the small amount of noise that is inherent to real-world measurements, *weak* PUFs can be combined with fuzzy extractors, as mentioned in section 2.6.2. However, the Hamming distance should still be as close to possible to 0, to ensure that the fuzzy extractor can reliably extract the secret key every time. Depending on the fuzzy extractor algorithm used, the sensitivity to noise will differ. Figure 5.8 shows how the Hamming distance varies as a function of the ROGUE strength, where a stronger ROGUE results in decreased Hamming distance. Therefore, the required ROGUE strength can be assessed depending on the sensitivity of the chosen fuzzy extractor.

Table 9.2 identifies the few fiber-based PUF architectures that have been reported in literature, and compares their properties. The multimode polymer optical fiber described by Mesaritis *et al.* [110] could be viewed as the fiber-based equivalent of Pappu's first description of the PUF [107], using various wavelengths and interrogation angles to issue different challenges. Its large challenge-response pair (CRP) domain means it could be used effectively as a *strong* PUF. However, as they demonstrated in their article, it is very sensitive to small changes in the curvature

of the fiber, which decreases the robustness, and makes each challenge difficult to reproduce. Furthermore, its response is based on the speckle image obtained after propagation, which is measured in free-space. This therefore negates some of the main advantages of the fiber, i.e. its compatibility with existing telecommunications systems, and the ability to measure it remotely. The Rayleigh scatter-based architecture presented by Du *et al.* is an interesting proof of principle [164], as it can be integrated into communications channels easily, and requires no modification of the already present optical fiber. However, this type of PUF is only associated with a limited number of CRPs (scanning a certain wavelength range), making it a *weak* PUF. Additionally, the very weak SNR makes its application difficult, especially across long distances. In contrast, the ROGUE provides a very large enhancement in signal, which can easily compensate the losses originating from long distance fiber propagation, or in-line passive optical components required for signal processing. The only drawback is the slight increase in complexity of the PUF, as it requires prior inscription of the ROGUE in the fiber. However, the writing setup is simple and, being noise-driven, does not require expensive components. As mentioned earlier, this step could easily be implemented during the fiber drawing process. Like the Rayleigh-scatter based PUF, the ROGUE PUF is also a *weak* PUF.

Table 9.2 Comparison of the different fiber-based PUF architectures

PUF Type	CRP Domain	Robustness	Ease of Fabrication	SNR	Remote interrogation
Rayleigh scatter [164]	Small	High	Pristine standard optical fiber	Very weak	Yes, limited by the low signal.
Multimode polymer optical fiber [110]	Large	Low, very sensitive to environment	Relatively easy to fabricate	Moderate	No
ROGUE (this work)	Small	Very high	Requires ROGUE inscription	High	Yes

It should be pointed out that, while the PUFs presented in Chapter 5 are based on enhanced scatter due to the inscription of ROGUEs inside the fiber core, there are numerous other techniques that could be used to achieve a similar effect. Indeed, while this idea had never been investigated for PUFs, fibers with enhanced scattering have been developed for many other applications, most importantly for distributed sensing applications to improve the SNR. Among these techniques, the

most promising are UV irradiation [149], femtosecond laser micromachining [148] or nanoparticle doping [155]. As such, the results presented in this thesis could be easily translated to these types of fiber to take advantage of their enhanced scatter. However, these fibers typically induce high losses, as the scattering is in all directions, resulting in most of the light being scattered out of the fiber core. In contrast, the ROGUE provides directional backscattering, minimizing the loss of optical power. Since the PUFs presented have a very short length, this loss may not be as critical as in some distributed sensing applications. However, in the case where longer PUFs are required, or if multiple PUFs are placed in the same fiber, these losses can quickly add up and become detrimental.

User authentication is another important application of PUFs, and addresses the vulnerability of existing cryptosystems to man-in-the-middle attacks. Authentication is typically achieved with *strong* PUFs with a large CRP domain, and each challenge is only used once to prevent repeat attacks, where an attacker could reproduce the PUF's response to a known challenge. However, *weak* PUFs could also be used for authentication, since their signature provides a unique identifier. This can, however, be achieved only if the replication of the PUF is prohibitively complex. The security of this type of protocol would not be absolute, as a motivated attacker could attempt replication of the PUF, which would allow him to impersonate other users if he were successful in his attempt. However, this would represent a significant barrier to entry, as random grating replication is incredibly difficult to achieve even with state-of-the-art FBG fabrication stations such as the ones used during this thesis. The possibility of PUF replication (however tiny and technologically challenging) could be too large for certain high-stakes applications, which would be better suited to the absolute security provided by systems such as quantum key distribution [124]. However, it could be sufficient for most other applications, especially when combined with other modalities and security protocols.

An interesting parallel can be made between the security of cryptosystems and the replication of the PUFs. Cryptosystems rely on the fact that it is very computationally expensive for an eavesdropper to reverse-engineer the secret keys used to encrypt the data, but very easy for the intended receiver to decrypt the message. Similarly, it is very easy to fabricate and measure the random grating's signature, but it is very difficult to reproduce it. In cryptosystems, the difficulty is computational, and relies on the difficulty standard computers have to realize certain operations,

such as factoring large numbers. The complexity of this task scales with increasing number of digits of the secret keys. However, these algorithms are susceptible to new algorithms and computers that could realize these operations much faster (e.g. quantum computers). Similarly, the difficulty in cloning the random grating's signature is technological, and relies on the state-of-the-art FBG manufacturing stations inability to reproduce perfectly a given random recipe. The complexity of this task scales with the random grating's length in this case, as well as with the interrogator's resolution, which results in more complex spectral signature.

This section, in conjunction with Chapter 5, described the various potential applications of the ROGUE in improving the security of existing cryptosystems. The ROGUE PUF presents low Hamming distances, and can be interrogated across long distances, while being able to easily compensate for losses. It could therefore find applications within secure communications protocols, either through secure key generation or authentication. This thus addresses the second Objective of this thesis.

9.1.3 Demonstrate the robustness to changing environmental conditions

Stability to environmental changes is also critical, and the third Objective of this thesis was to demonstrate the ROGUE stability to changing environmental conditions. Even though the ROGUE PUF could be packaged properly to minimize temperature and strain fluctuations, some amount of change is inevitable. Therefore, it is important to properly characterize the PUFs resilience to environmental fluctuations. As optical fibers are sensitive to both temperature and strain variations, a small temperature change would shift the reflection spectrum, affecting the PUF signature considerably. This issue was addressed in two parts. First, the environmental fluctuations had to be monitored, which implied the use of a sensing technique. Second, a compensation algorithm had to be developed to recover the original PUF signature, based on the measured fluctuations.

Since the PUF is written in optical fiber, the various fiber-based sensing techniques described in section 2.4 were considered. Indeed, while it could have been possible to use different modalities to achieve sensing, such as packaging the ROGUE with a thermocouple to monitor temperature, it made more sense to use the same medium for both PUF and environmental fluctuations measurement. Additionally, since optical fibers are sensitive to both strain and temperature

changes, both these metrics need to be measured. This is the case for most fiber-based sensing techniques (apart from Raman scattering), but is not true of other sensors, such as thermocouples.

Within fiber-based sensing techniques, quasi-distributed sensing could have been an option, by writing an additional FBG on top of the ROGUE at a different wavelength, and using this additional FBG for sensing while the ROGUE was used as a PUF. However, this would increase complexity, as FBG sensing would require an additional interrogator to probe this other wavelength. Furthermore, distributed approaches offer more flexibility. Indeed, in an application scenario where one would want to expand the CRP domain, a longer ROGUE could be subdivided into individual PUFs, in a similar fashion to what has been demonstrated in Chapter 5. For example, a meter-long ROGUE could be subdivided into 100 individual 10 mm PUFs, resulting in 100 unique challenges. In that case, quasi-distributed sensing would require the inscription of 100 unique FBGs on top of each 10 mm PUF. In the case where 10 mm PUFs do not offer a sufficiently large amount of bits, the meter-long ROGUE could be subdivided into fifty 20 mm PUFs instead. Quasi-distributed sensing does not have this flexibility, and is restrained by the existing FBGs inscribed in the fiber. Brillouin-based distributed sensing methods, as well as the Rayleigh scattering-based ϕ -OTDR, were also considered, but are very limited in spatial resolution. In the case where multiple PUFs are inscribed in the same fiber, the sensing technique's spatial resolution should be ideally at least as high as the PUF's length. On the other hand, as was demonstrated in Figure 4.9, OFDR sensing allows spatial resolutions of only a few millimeters, which is smaller than even the smallest PUFs considered in this thesis. It also requires no additional FBG inscription, like what would be required for quasi-distributed sensing. Furthermore, it makes much more sense to use the same interrogator and interrogation technique for both PUF measurement and temperature/strain sensing. Therefore, the ROGUE can be used simultaneously as a PUF and as a sensor compensating the environmental fluctuations. The sensing capabilities of the ROGUE were described in Chapter 4.

While this addresses the need for sensing environmental fluctuations, this is only the first half of the problem. A compensation algorithm also needed to be implemented to recover the original PUF signature from the altered response that was measured. This algorithm (described in the Supplementary Material of the article presented in Chapter 5) is based on the same principles as OFDR sensing. Indeed, to recover the initial PUF signature, all that is required is to shift the spectrum back to its original position. However, the PUF signature could be accurately recovered

only when the environmentally induced spectral shift was a multiple of the spectral resolution, which is quite limited when using a narrow gauge length (82 pm for a 10 mm spatial resolution, corresponding to a variation of $\sim 10^\circ\text{C}$). Therefore, the interpolation technique that was described in section 4.2.3 of this thesis was also used to artificially increase this spectral resolution. This resulted in stable PUF operation from -30°C to $+90^\circ\text{C}$, as shown in Figure 5.8, and thus addressed the third Objective.

It should be pointed out that the temperature/strain variations investigated here are completely uniform along the ROGUE's length. Obviously, a non-uniform variation would be more complex to compensate. There are two potential solutions to address this issue. The first, easiest solution, is the use of proper packaging. Placing the optical fiber on a metallic plate should ensure a uniform temperature over its length, especially considering the relatively short length of only a few centimeters. If that would prove insufficient, another potential solution could be to use a sensing gauge length smaller than that of the ROGUE's length, to individually compensate each subsection within the PUF, in case there is a temperature or strain gradient over the ROGUE's length. However, that would complicate data processing and would increase computation time.

On the other hand, programmable non-uniform temperature or strain variations could be used to dynamically change the phase relationships within the ROGUE, resulting in a reconfigurable PUF. Since the CRP domain of reconfigurable PUFs can evolve through time, they are more robust against many security attacks. Their expanded CRP also makes them better candidates for authentication purposes [213]. In the current case, this could be achieved for example by a set of a programmable heating elements placed in parallel under the ROGUE, to dynamically tune its spectral properties.

9.1.4 Development of novel entropy sources for RNG using random lasers

The fourth Objective of this thesis was to develop novel entropy sources for RNG. While state-of-the-art physical RNG relies on chaotic lasers, achieving RNG rates of many Tbps, it could be argued that chaos, while being extraordinarily sensitive to the initial conditions, is purely deterministic. Therefore, there might be ways to replicate the chaotic output of the laser by placing it in the same starting conditions, so that a potential attacker could have access to the bits used for encryption. In fact, this is precisely how chaotic communications work, where two identical chaotic

lasers are placed in identical states, and the chaotic waveform of the emitter laser is used to hide a message that can only be decrypted by the receiver laser, which can remove the identical chaotic waveform [127]. Alternatively, if an attacker was able to reverse engineer the laser's configuration and its initial conditions, he could simulate the laser's output and predict the next bit sequences that the laser would output beforehand, rendering the encryption useless. Random lasers, on the other hand, are intrinsically random, and therefore their output cannot be so easily replicated, either by reproducing the laser or by simulating it. Additionally, the fixed cavity of chaotic lasers, and in fact of all conventional lasers, induces a time-delay signature that can be observed by analyzing the laser's output, which is very detrimental for most chaotic lasers' applications, including RNG, as it is a pattern that could potentially be exploited. On the other hand, random lasers do not exhibit this time-delay signature, since they do not rely on a fixed cavity. This makes them perfectly suited for applications such as RNG, as they do not require the use of additional complex steps to hide this signature from their output [46, 190].

While some random lasers have been investigated for RNG, these first demonstrations are limited to low bitrates insufficient for high-speed communications. Random lasers based on the Brillouin scattering are limited to the Brillouin bandwidth of the optical fiber used, which is in the order of 10 MHz [92]. In comparison, the Raman scattering in optical fibers has a much broader bandwidth of many THz, and therefore has the potential for much higher RNG rates. While RNG using random lasers had been investigated using Brillouin lasers [92], semiconductor amplifiers [45] or ytterbium-doped fiber lasers [186], to the best of our knowledge random Raman lasers had never been used for RNG, which we believed was an important oversight, due to the massive Raman bandwidth. Furthermore, such lasers are very easy to fabricate, requiring only a pump laser and a bundle of a few kilometers of optical fibers, as demonstrated by Turitsyn *et al.* [57]. Using a Raman random distributed feedback laser appeared thus the ideal way to address the fourth Objective of this thesis.

In Chapter 6, the approach for building this laser was described, and is based on a half-open cavity, with an FBG on one side and an optical fiber bundle on the other. A potential attacker wanting to experimentally reproduce this laser would have to fabricate an identical laser with the exact same properties. While the FBG used to close the cavity on one side could be relatively easy to clone with the appropriate facilities, reproducing the other side of the cavity is a much greater challenge.

Indeed, the random feedback on the other side of the cavity comes from the intrinsic Rayleigh scattering of the 6.66 km fiber bundle. This Rayleigh scattering originates from defects, impurities and small changes in refractive index in the fiber. To fabricate a fiber bundle identical to the one used, one would have to first reverse-engineer the exact properties (defects, refractive index profile, etc.) of the optical fiber all along its length, at a sub-micrometer scale. In itself, this is an extraordinarily challenging task, which can be prevented very simply by using optical isolators after the output of the laser, thus ensuring no attacker could measure the optical properties of the fiber.

Even if an attacker could somehow have access to this information, one would have to fabricate another 6.66 km length of optical fiber with the exact same properties, which would be a nigh-impossible task. Indeed, these non-uniformities are inherent to the fiber drawing process, and if a manufacturer could have sufficient control over them to draw a fiber with a pre-designed Rayleigh scattering profile, they would choose to eliminate these non-uniformities, as they are one of the main limitations of the propagation of light in optical fibers. Therefore, the intrinsic randomly distributed Rayleigh scattering that fiber optic manufacturers work so hard to mitigate is exactly what allows this laser to lase, and what makes it impossible to reproduce. This is very reminiscent of the PUF concept explored in the previous sections, where the inherent randomness and imperfections of the manufacturing process ensured the PUFs unclonability.

Similarly, if a potential attacker wanted to simulate the random laser operation, he would also need to have access to the fiber's characteristics. Putting this concern aside, to properly simulate the laser's output, an attacker would then need to input the precise starting conditions of the laser, followed by the simulation of the lasing operation of a 6.66 km long random cavity, again using sub-micrometer spatial resolution. Furthermore, the entropy originates not only from the localized lasing modes of the laser, but also from the modulation instability (MI) nonlinear effect that takes place in this laser. This effect occurs because of small, unpredictable perturbations, making proper simulation of the output of this laser impossible. Therefore, this laser's output cannot be reproduced by a potential attacker, either physically or by simulation, thus ensuring that the random numbers generated by this laser can safely be used for secure communications.

Table 9.3 Comparison of the different RNG schemes discussed in this thesis

RNG Source	Bitrate	Robustness	Packaging	Reproducibility
Chaotic semiconductor laser [93, 183]	100s of Gbps	Requires proper positioning of the self-injection mirror	Can be relatively small	Chaos can be potentially reproduced or simulated
Quantum optics [91]	Few Gbps	Very sensitive to electrical and thermal noise	Can be small and with cheap components	Absolute randomness coming from quantum states or quantum noise
Brillouin random laser [60]	Tens of Mbps	Robust, requires no alignment	Bulky (requires many kms of optical fiber)	Almost impossible to reproduce (experimentally or by simulation)
Raman random laser (this work)	100s of Gbps	Robust, requires no alignment	Bulky (requires many kms of optical fiber)	Almost impossible to reproduce (experimentally or by simulation)

Different RNG sources are compared in Table 9.3. For secure communications protocols, the most important parameter is the reproducibility. Indeed, if a potential attacker can experimentally reproduce or simulate the laser's output, the secrecy of the communications is at risk. As mentioned above, this is potentially problematic for chaotic semiconductor sources. Quantum RNG systems offer the most secure source of randomness, as it comes from the intrinsic randomness of quantum states. While the first demonstrations based on single-photon sources required expensive equipment, recent prototypes based on the measurement of vacuum fluctuations can be made with off-the-shelf components [91]. However, these are very sensitive to other sources of noise, and the bitrate they can produce is orders of magnitude slower than what can be achieved with chaotic semiconductors. In contrast, the random laser sources discussed here are very difficult to reproduce or simulate, making them great sources of randomness for secure communication applications. While the Brillouin random laser had a very low bitrate in comparison with the other RNG sources, this is not the case with the Raman random laser described in this work, which has an RNG rate comparable with chaotic semiconductor sources. The only drawback of this kind of laser is that they are relatively bulky, since they require long lengths of optical fiber. However, this bulkiness could be potentially reduced by the use of random gratings. Indeed, as was demonstrated in section 8.2, using a ROGUE of only a few meters drastically decreased the lasing threshold of the random distributed

feedback laser. Therefore, the ROGUE could also be used to reduce the cavity length, thus addressing the only major drawback of this kind of RNG scheme.

The demonstration of multiplexed RNG with the Raman random laser completed the fourth Objective. Indeed, while generation of random bits at rates comparable to that of chaotic semiconductor lasers was achieved in Chapter 6, the random supercontinuum achieved in Chapter 7 further increased the applicability of this novel technology by expanding the throughput of random bits, and allowed parallel RNG. Therefore, a single entropy source could provide the random numbers necessary for encryption of multiple communications channels, which is much more efficient than having one RNG source per channel. Additionally, while the focus of this PhD thesis was on secure communications, it should be mentioned that generating random bits across multiple channels is also beneficial to other fields. For example, random bits are heavily used in Monte Carlo simulations, and parallel processing is increasingly used to accelerate computations [101]. Machine learning and artificial intelligence algorithms also use a massive quantity of random numbers, and their output is directly related to the quality of these random bits [77]. There is thus a need for RNG sources that can produce random bits independently in parallel, which could be filled by this RNG architecture.

9.1.5 Investigation of the limits of the RNG schemes developed

The fifth and final Objective of this thesis was to investigate the limits of the RNG in the schemes developed throughout the fourth Objective. This was achieved in two parts. First, the random lasers' potential for true RNG was evaluated. Proper characterization of the RNG potential is important, because even if an attacker cannot reproduce the laser's output (either physically or by simulation), if there are existing patterns in bit sequences, a potential attacker could identify and exploit them. While there are many advanced statistical test suites that have been designed to test a bit sequence's randomness [89, 214, 215], there are no of statistical tests that can ascertain for sure that the bit sequences are truly random. Due to the nature of the statistical tests, they can only provide at best an upper bound on the probability that the bits are not truly random. Therefore, the physical entropy generated by the randomness source was used to evaluate its RNG potential. This provides a theoretical reason to explain the RNG potential of the physical source, rather than running statistical tests that can be gamed by using complex post-processing techniques hiding the

existing correlations [95-97, 186]. The laser demonstrated in Chapter 6 had a theoretical entropy generation of 540 Gbps, while the supercontinuum laser source developed in Chapter 7 further expanded this entropy rate to ~760 Gbps. To the best of our knowledge, this is the highest RNG rate produced by a random laser source.

The second part of Objective 5 was achieved by investigating the conditions governing the independence of multiplexed RNG channels. Multiplexing of parallel RNG channels is a relatively novel concept, and there are no agreed upon guidelines in literature to ensure proper independence between channels. In fact, there appeared to be almost as many ways of processing the data and testing it as the number of publications in multiplexed RNG [95, 99-101, 103]. This highlights the importance of Objective 5: if there is no well-established methodology defining the best practices for evaluating the parallel bits' independence, each researcher will attempt to develop his own way of testing the data, with no guarantees that the test truly measures what he intends to.

In the case of the current work, the most important parameter is the spectral spacing between two parallel channels. Indeed, while one could make the assumption that two spectrally separated channels would be uncorrelated, since they both originate from the same laser, there could be some remaining correlations. A protocol to determine the minimum required separation thus needed to be established. Various protocols found in literature were tested, as well as their ability to identify correlations based on various post-processing steps. Based on the results of Chapter 7, the most robust test to ensure channel independence appeared to be the use of a simple cross-correlation measurement using the raw, untreated data. In this work, this allowed the use of a spectral separation of 8 nm, resulting in a total of 11 potential channels extracted from the supercontinuum.

As an alternative way of testing the limits of this RNG scheme, the FBGs defining the channels' bandwidth were changed, to test whether a broader channel bandwidth would result in improved RNG rate. Intuitively, it would make sense that a broader channel bandwidth would result in greater single-channel entropy, and it is indeed what was found. However, while a larger channel bandwidth increased the ability of this specific channel to generate random bits, it also increased the required spacing for two neighbouring channels to remain independent, such that the total RNG rate remained constant. This makes sense, since the total RNG rate should be given by the amount of entropy generated by the source (in our case, the random laser), not by the number of channels

this entropy is separated into. This is the same reasoning for why the various post-processing steps found in literature should not have an impact on the achievable RNG rates of a given source.

These various tests and investigations thus allowed the completion of the fifth Objective. Whether in the single-channel or multiplexed channels schemes, the main limitation in all cases is the entropy generated by the source. While the NIST testing suite and other statistical tests can help provide an estimate of the achievable bitrate, as shown in the previous chapters, they cannot distinguish between true randomness and high-quality pseudo-random bits. Therefore, proper entropy estimation must be performed. We also demonstrated that the various post-processing steps investigated are ineffective at increasing the number of achievable parallel channels, just as they cannot increase the randomness of extracted bits in single-channel schemes.

9.2 Overall discussion

The main goal of this thesis was the development of novel tools to improve the security of cryptosystems. The two main vulnerabilities of cryptosystems investigated in this thesis relate to the process of generation of the secret keys, and the authentication of the different users. The first proposed alternative for secret key generation relied on a physical device, the ROGUE-based PUFs, which could be used as the basis for generating the secret keys. This prevents the need to digitally store the keys, reducing the risks of hacking or leakage. While the additional complexity is probably not well suited for all web users, the improved security may be beneficial to entities trading with highly sensitive information, such as government agencies. Additionally, the secure key storage provided by these PUFs could be interesting for entities such as certificate authorities (CAs), since the security of millions of users' information is compromised if their private key was exposed. An alternative for secret key generation is the use of a physical random number generation scheme, to replace the pseudo-random number generation algorithms that are currently typically used. In this thesis, this RNG scheme takes the form of a random distributed feedback Raman fiber laser, whose intrinsic randomness is further enhanced by modulation instability. The random bits generated by this laser could thus be used as secret keys in existing cryptosystems. This scheme ensures there are no correlations between the generated bits, and that the random bits generated cannot be predicted or simulated by a potential attacker. However, as described in the section above, the entropy content must be properly evaluated, to ensure that the RNG content is not

sampled above the entropy limit of the source, which could induce unwanted correlations between the bits that could be exploited by an attacker.

Authentication could be also addressed by the ROGUE-based PUF described in this thesis. In this case, each user would use a single PUF as a unique identifier, which could be scanned remotely by other users wishing to verify the receiver's identity. In this case, the security of this communication relies on the difficulty of cloning a specific ROGUE, which is a major technological challenge rather than a computational one. In such a protocol, the secret keys used for encryption could then be refreshed in real time, using an RNG scheme such as the random laser presented in this thesis. This would thus combine the two modalities explored in this thesis.

Other more complex authentication protocols could be developed based on the tools developed during this thesis. Recently, a provably secure protocol for privacy-preserving mutual authentication was proposed, using an SRAM *weak* PUF in conjunction with a true random number generator [181]. Combining the *weak* PUF with the RNG system is akin to turning the *weak* PUF into a *strong* PUF, meaning that the *weak* PUF signatures are not publicly available, only the combined signature of the *weak* PUF with the RNG output. This allows secure authentication in the same way as the *strong* PUF-based authentication systems described in section 2.6.2. Since the PUF is no longer publicly available in this protocol, a potential attacker is no longer able to breach the security by replicating the PUF (even though this task is very difficult, it is not impossible per say). While this protocol was proposed using a silicon-based PUF, a similar arrangement could be achieved by combining the ROGUE PUFs with the random laser's RNG. Since both these techniques are fiber-based, they could potentially even be integrated together without requiring conversion to the electrical domain. This could even allow them to be then integrated into all-optical computers [216].

CHAPTER 10 CONCLUSION AND RECOMMENDATIONS

In our interconnected world, there is a need for developing novel techniques ensuring the security of communications over unsecure channels. While protocols such as quantum key distribution systems offer absolute security, they currently cannot be scaled to the requirements of modern-day telecommunications. An alternative approach is thus to investigate novel techniques and devices to enhance the security of already existing cryptographic protocols. Random numbers are at the core of these protocols, as they are used for generation of secret keys and encryption of data. The uniqueness and confidentiality of these secret keys is critical to the security of these protocols, and they therefore require large quantities of *true* random numbers that are impossible to predict or emulate. For that purpose, fiber components were developed during the course of this thesis. These fiber devices successfully addressed the objectives identified at the beginning of this thesis, and also resulted in the filing of a US patent [217] describing their use for secure communications. In addition, the generation of the components required to achieve these objectives led to the study of two additional applications in the field of high-resolution distributed sensing and random lasing. The first led to a now granted US patent [218], while the other led to the development of a novel high-speed random number generation (RNG) scheme that allowed the study of the limitations of entropy in RNG systems. While at the outset these topics seem unrelated, they are central to the goal of this thesis, and resulted in the two main axes of research that guided this thesis.

In the first one, randomness in fiber-based photonics was used to fabricate physical devices, in the form of random gratings. These random gratings were then implemented as an additional physical layer of security to enhance the security of existing secure communications systems. In the second research axis, randomness was implemented through random lasers, whose unique properties make them particularly well suited for certain applications such as random number generation. The random numbers thus generated can then be used to replace the pseudo-random numbers typically used in these communication schemes. This ensures no existing pattern can be exploited by a potential attacker.

The first two articles are directly related with the first research axis. The first article described how the addition of noise to a continuous FBG writing process resulted in the inscription of a random grating, which was dubbed Random Optical Grating by Ultraviolet or ultrafast laser Exposure

(ROGUE). This ROGUE demonstrated enhanced backscattering (up to 50 dB more than unexposed optical fiber) and low insertion losses, due to its directional feedback. Indeed, most optical fiber scattering enhancement techniques induce large losses, since their scattering is omnidirectional, and only a small percentage of the scattered light is captured by the fiber's numerical aperture and backscattered to the detector. In this article, the ROGUE's potential for distributed sensing was also investigated, where its high signal to noise ratio allowed it to accurately measure very small temperature variations with an impressive spatial resolution.

In the second article, a simplified version of the ROGUE inscription setup was presented, which allowed continuous writing of ROGUES for unlimited lengths at relatively high speeds (20 mm/s). This article also discussed how the ROGUES could be used for secure communications, as the ROGUE behaved as a high-quality Physical Unclonable Function (PUF). This PUF could then find application in many secure communications protocols, for instance for secure key generation or authentication. While most PUF architectures are based on silicon devices, this fiber-based PUF has the advantage of being compatible with existing telecommunications networks, and to be easily interrogated from a long distance. Indeed, its high signal to noise ratio makes it able to compensate the losses of long propagation distances and passive optical components. Finally, the distributed sensing algorithms presented in the first article were integrated to the PUF measurement algorithm, enabling compensation of environmental fluctuations. This ensures the robustness of the ROGUE PUF in real-world applications, where such fluctuations are inevitable.

The second research axis was addressed by the last two articles. In the third article, a random distributed feedback Raman fiber laser architecture was presented, based on a narrow, highly-reflective fiber Bragg grating which defined the lasing wavelength, as well as a 6.66 km bundle of optical fiber, which provided both the Rayleigh scattering and the Raman gain necessary for random lasing. Other nonlinear effects such as self-phase modulation and modulation instability further promoted the randomness of this laser's operation. Random numbers were extracted from the laser output, and an entropy content of 540 Gbps was demonstrated. This places it on par with the state-of-the-art physical random number generation (RNG) schemes, while having all the advantages of random lasers, such as robustness, low cost and ease of fabrication.

The fourth article introduced a minor tweak in the random laser cavity that had a huge impact on its operation. Indeed, the fiber Bragg grating was replaced by the broadband Fresnel reflection of

a cleaved fiber facet. This promoted the generation of a supercontinuum spanning 77 nm, due to the interaction of modulation instability and Raman self-frequency shift. This supercontinuum allowed the investigation of multiplexed RNG across multiple parallel spectral channels. A novel methodology was developed to help identify the conditions ensuring independence of the parallel channels. This methodology ensures the random numbers generated in the different channels are truly uncorrelated, and is highly relevant as there are currently no well-established guidelines for multiplexed RNG. Furthermore, spectral channels of different widths were investigated, to quantify the effect the channel separation had on the total RNG potential. This demonstrated that the total achievable bitrate is constant and limited by the entropy of the laser source used, regardless of the way the different parallel channels are separated.

The ROGUE, which was developed at the beginning of this PhD, is at the core of the work described in this thesis. Its enhanced scatter and low losses make it an ideal device for the various applications considered here, as the increased signal to noise ratio results in higher quality measurements, and the ability to easily compensate optical losses. Alternatively, this enhanced signal could allow the use of less sensitive interrogators, which would be more affordable and accessible to a wider range of applications. Furthermore, the ROGUE's low cost and ease of fabrication means it could be easily mass produced, for example by integrating ROGUE writing in the fiber drawing process, before the fiber's coating is applied. This would allow easy fabrication of kilometers of ROGUEs, which would democratize its adoption and could lead to other applications unforeseen by the author. They also represent a great platform to study complex and interesting phenomena such as light localization, which could lead them to be applied in various other fields, both practical and fundamental.

Random distributed feedback Raman fiber lasers also occupy a central part of this thesis. While already a known technology, their potential for random number generation was never investigated, which is an important oversight. Indeed, random Raman lasers have the potential to generate random bits at rates comparable to the state-of-the-art chaotic semiconductor lasers, due to the large Raman gain bandwidth, without the chaotic lasers' characteristic time-delay signature that researchers work so hard to conceal. Furthermore, their very complex cavity makes them impossible to clone properly, either experimentally or by simulation, which further ensures the security provided by the random numbers they generate. Finally, they have an incredible synergy

with the random gratings described in the first research axis, where the ROGUE's enhanced and directional scatter can be used to reduce the required length of these random lasers. This would reduce the bulkiness of the distributed feedback lasers, which is one of their main limitations for commercialisation.

The main goal of this thesis was to demonstrate how randomness in fiber-based photonics could help improve the security of the existing cryptosystems used for secure communications. This was achieved by targeting the main weaknesses of these systems, namely the secret keys at the core of these protocols, and their vulnerability to man-in-the-middle attacks. Various potential solutions were proposed during this thesis, based on random gratings and random lasers. However, it should not escape the reader that secure communications is only one of the potential applications for the devices developed during this PhD. Indeed, the ROGUE's unique properties make it perfectly well suited for various other unrelated applications, some of which were investigated in this thesis, like distributed sensing and shape reconstruction of minimally invasive surgical instruments. However, the ROGUE is a very novel tool, and like most developed tools in their infancy, its best application may not have been identified yet. Indeed, in its beginning, it was said that the laser was a solution looking for a problem! In a similar fashion, while the emphasis was placed here on the applications for secure communications, the random bits generated by the random Raman laser schemes presented in this thesis could find application in various other fields, such as Monte Carlo simulations or machine learning, artificial intelligence and data-driven algorithms. In a more general view, the random lasers developed in this thesis could also find use in unexpected applications such as modeling light scatter in bio samples. Indeed, random lasing is a relatively new concept, and researchers are only beginning to scratch the surface of all the potential capabilities that their unconventional, modeless structure offers.

I began this thesis by the legend of the original marathon, as an illustration of how old the concept of telecommunications is. It is only fitting that I would end this thesis by going back over this example. Indeed, completing a PhD is often compared to running a marathon. Since I ran my first marathon during the course of this PhD, I feel I am well qualified to comment on this comparison. Although the slowest walker would certainly finish his marathon years before the most productive PhD student, I feel like the comparison is not without merits. In both cases, regardless of the contender's shape at the starting line, making it to the end is more a testament of strength of will

and determination than it is of physical or intellectual prowess. But, more importantly, the real hard work is not achieved on race (or defense) day, but rather in the months and years leading up to it, even though most of that work is often unnoticed. Finally, this big achievement is never the success of a single person, and would not be possible without the help and support of those around. I would like to take this opportunity to thank again all those who contributed to help me complete this PhD, and to thank you, the reader, for making it to the end of this thesis.

REFERENCES

- [1] Z. Ghassemlooy, L. N. Alves, S. Zvanovec, and M.-A. Khalighi, *Visible light communications: theory and applications*. CRC press, 2017.
- [2] J. F. Carrington, "The talking drums of Africa," *Scientific American*, vol. 225, no. 6, pp. 90-95, 1971.
- [3] M. Sabina, M. Daniela, and D. GABRIELA, "Marathon, between history and tradition," *Ovidius University Annals, Series Physical Education and Sport/Science, Movement and Health*, vol. 18, no. 2 S1, pp. 319-325, 2018.
- [4] T. Morkel and J. Eloff, "Encryption techniques: a timeline approach," *Information and Computer Security Architecture (ICSA) Research Group, University of Pretoria*, vol. 2, 2004.
- [5] D. B. Keck, "Optical fiber spans 30 years," *Lightwave*, vol. 17, no. 8, p. 78, 2000.
- [6] W. A. Gambling, "The rise and rise of optical fibers," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 6, no. 6, pp. 1084-1093, 2000.
- [7] J. Ballato and P. Dragic, "Glass: the carrier of light-a brief history of optical fiber," *International Journal of Applied Glass Science*, vol. 7, no. 4, pp. 413-422, 2016.
- [8] D. Naylor *et al.*, "The cost of the "s" in https," in *Proceedings of the 10th ACM International on Conference on emerging Networking Experiments and Technologies*, 2014, pp. 133-140.
- [9] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120-126, 1978.
- [10] É. Trottier, "Le crack du Keno pourra empocher son gain," *La Presse*, no. Mercredi 27 avril 1994, p. A3. [Online]. Available: <https://numerique.banq.qc.ca/patrimoine/details/52327/2177701>
- [11] A. Snyder. "A Keno System That Works?" Las Vegas Advisor. <https://www.lasvegasadvisor.com/gambling-with-an-edge/a-keno-system-that-works/> (accessed 2022).
- [12] J. Stone, "Interactions of hydrogen and deuterium with silica optical fibers: A review," *Journal of Lightwave Technology*, vol. 5, no. 5, pp. 712-733, 1987.
- [13] J. Zhao, Y. Zhao, Y. Peng, R.-q. Lv, and Q. Zhao, "Review of femtosecond laser direct writing fiber-optic structures based on refractive index modification and their applications," *Optics & Laser Technology*, vol. 146, p. 107473, 2022.
- [14] F. Hindle *et al.*, "Inscription of long-period gratings in pure silica and germano-silicate fiber cores by femtosecond laser irradiation," *IEEE Photonics Technology Letters*, vol. 16, no. 8, pp. 1861-1863, 2004.
- [15] P. S. Westbrook *et al.*, "Continuous multicore optical fiber grating arrays for distributed sensing applications," *Journal of Lightwave Technology*, vol. 35, no. 6, pp. 1248-1252, 2017.
- [16] J. Habel, T. Boilard, J.-S. Frenière, F. Trépanier, and M. Bernier, "Femtosecond FBG written through the coating for sensing applications," *Sensors*, vol. 17, no. 11, p. 2519, 2017.

- [17] S. Loranger, "Discovery and Correction of Spatial Non-Uniformity in Optical Fibers: Towards the Fabrication of Perfect Ultra-Long Fiber Bragg Gratings for Applications in Non-Linear Optics," École Polytechnique de Montréal, 2018.
- [18] A. Roberge, "Fabrication of fiber Bragg gratings using femtosecond laser direct-writing techniques," M.Sc., Polytechnique Montreal, Montreal, Canada, 2022.
- [19] A. Roberge, S. Loranger, J.-S. Boisvert, F. Monet, and R. Kashyap, "Femtosecond laser direct-writing of high quality first-order Bragg gratings with arbitrary complex apodization by phase modulation," *Optics Express*, vol. 30, no. 17, pp. 30405-30419, 2022.
- [20] O. Shapira and B. Fischer, "Localization of light in a random-grating array in a single-mode fiber," *JOSA B*, vol. 22, no. 12, pp. 2542-2552, 2005.
- [21] A. Mafi, "Anderson localization in a partially random Bragg grating and a conserved area theorem," *Optics Letters*, vol. 40, no. 15, pp. 3603-3606, 2015.
- [22] N. Lizárraga, N. Puente, E. Chaikina, T. Leskova, and E. Méndez, "Single-mode Er-doped fiber random laser with distributed Bragg grating feedback," *Optics Express*, vol. 17, no. 2, pp. 395-404, 2009.
- [23] M. Gagné and R. Kashyap, "Demonstration of a 3 mW threshold Er-doped random fiber laser based on a unique fiber Bragg grating," *Optics Express*, vol. 17, no. 21, pp. 19067-19074, 2009.
- [24] M. Gagne and R. Kashyap, "Random fiber Bragg grating Raman fiber laser," *Optics Letters*, vol. 39, no. 9, pp. 2755-8, May 1 2014, doi: 10.1364/OL.39.002755.
- [25] Y. Xu, P. Lu, S. Gao, D. Xiang, S. Mihailov, and X. Bao, "Optical fiber random grating-based multiparameter sensor," *Optics Letters*, vol. 40, no. 23, pp. 5514-5517, 2015.
- [26] J. Liu, P. Lu, S. J. Mihailov, M. Wang, and J. Yao, "Real-time random grating sensor array for quasi-distributed sensing based on wavelength-to-time mapping and time-division multiplexing," *Optics Letters*, vol. 44, no. 2, pp. 379-382, 2019.
- [27] P. W. Anderson, "Absence of diffusion in certain random lattices," *Physical Review*, vol. 109, no. 5, p. 1492, 1958.
- [28] R. Myers, N. Mukherjee, and S. R. Brueck, "Large second-order nonlinearity in poled fused silica," *Optics Letters*, vol. 16, no. 22, pp. 1732-1734, 1991.
- [29] R. W. Boyd, *Nonlinear Optics*. Academic press, 2020.
- [30] E. Woodbury and W. Nag, "First demonstration of stimulated Raman scattering," *Proc. IRE*, vol. 50, no. 6, p. 2347, 1962.
- [31] G. P. Agrawal, *Nonlinear Fiber Optics*. New York: Academic Press, 1995.
- [32] M. F. S. Ferreira, "Optical Amplifiers | Raman, Brillouin and Parametric Amplifiers," in *Encyclopedia of Modern Optics*, R. D. Guenther Ed. Oxford: Elsevier, 2005, pp. 297-308.
- [33] R. Stolen and E. Ippen, "Raman gain in glass optical waveguides," *Applied Physics Letters*, vol. 22, no. 6, pp. 276-278, 1973.

- [34] J. M. Dudley, G. Genty, and S. Coen, "Supercontinuum generation in photonic crystal fiber," *Reviews of Modern Physics*, vol. 78, no. 4, pp. 1135-1184, 2006, doi: 10.1103/RevModPhys.78.1135.
- [35] N. Nishizawa and T. Goto, "Widely wavelength-tunable ultrashort pulse generation using polarization maintaining optical fibers," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 7, no. 4, pp. 518-524, 2001.
- [36] C. L. Hagen, J. W. Walewski, and S. T. Sanders, "Generation of a continuum extending to the midinfrared by pumping ZBLAN fiber with an ultrafast 1550-nm source," *IEEE Photonics Technology Letters*, vol. 18, no. 1, pp. 91-93, 2005.
- [37] Y. Gong, P. Shum, D. Tang, C. Lu, and X. Guo, "660GHz soliton source based on modulation instability in a short cavity," *Optics Express*, vol. 11, no. 20, pp. 2480-2485, 2003.
- [38] H. Kogelnik and C. V. Shank, "Coupled-wave theory of distributed feedback lasers," *Journal of Applied Physics*, vol. 43, no. 5, pp. 2327-2335, 1972.
- [39] M. Sejka, P. Varming, J. Hübner, and M. Kristensen, "Distributed feedback Er³⁺-doped fibre laser," *Electronics Letters*, vol. 31, no. 17, pp. 1445-1446, 1995.
- [40] S. Agger, J. H. Povlsen, and P. Varming, "Single-frequency thulium-doped distributed-feedback fiber laser," *Optics Letters*, vol. 29, no. 13, pp. 1503-1505, 2004.
- [41] S. Loranger, A. Tehranchi, H. Winful, and R. Kashyap, "Realization and optimization of phase-shifted distributed feedback fiber Bragg grating Raman lasers," *Optica*, vol. 5, no. 3, 2018, doi: 10.1364/optica.5.000295.
- [42] K. S. Abedin, P. S. Westbrook, J. W. Nicholson, J. Porque, T. Kremp, and X. Liu, "Single-frequency Brillouin distributed feedback fiber laser," *Optics Letters*, vol. 37, no. 4, pp. 605-607, 2012.
- [43] R. C. Polson and Z. V. Vardeny, "Random lasing in human tissues," *Applied Physics Letters*, vol. 85, no. 7, pp. 1289-1291, 2004.
- [44] B. Redding, M. A. Choma, and H. Cao, "Speckle-free laser imaging using random laser illumination," *Nature Photonics*, vol. 6, no. 6, pp. 355-359, 2012.
- [45] Y. Xu, P. Lu, S. Mihailov, and X. Bao, "Real-time physical random bit generation at Gbps based on random fiber lasers," *Optics Letters*, vol. 42, no. 23, pp. 4796-4799, 2017.
- [46] Y. Xu, M. Zhang, L. Zhang, P. Lu, S. Mihailov, and X. Bao, "Time-delay signature suppression in a chaotic semiconductor laser by fiber random grating induced random distributed feedback," *Optics Letters*, vol. 42, no. 20, pp. 4107-4110, 2017.
- [47] M. Berry and S. Klein, "Transparent mirrors: rays, waves and localization," *European Journal of Physics*, vol. 18, no. 3, p. 222, 1997.
- [48] T. Schwartz, G. Bartal, S. Fishman, and M. Segev, "Transport and Anderson localization in disordered two-dimensional photonic lattices," *Nature*, vol. 446, no. 7131, pp. 52-55, 2007.
- [49] S. Karbasi, K. W. Koch, and A. Mafi, "Image transport quality can be improved in disordered waveguides," *Optics Communications*, vol. 311, pp. 72-76, 2013.
- [50] V. Letokhov, "Generation of light by a scattering medium with negative resonance absorption," *Sov. Phys. JETP*, vol. 26, pp. 835-840, 1968.

- [51] N. M. Lawandy, R. Balachandran, A. Gomes, and E. Sauvain, "Laser action in strongly scattering media," *Nature*, vol. 368, no. 6470, p. 436, 1994.
- [52] C. B. d. Araújo, A. S. Gomes, and E. P. Raposo, "Lévy statistics and the glassy behavior of light in random fiber lasers," *Applied Sciences*, vol. 7, no. 7, p. 644, 2017.
- [53] E. Raposo and A. Gomes, "Analytical solution for the Lévy-like steady-state distribution of intensities in random lasers," *Physical Review A*, vol. 91, no. 4, p. 043827, 2015.
- [54] J. Li *et al.*, "Lévy spectral intensity statistics in a Raman random fiber laser," *Optics Letters*, vol. 44, no. 11, pp. 2799-2802, 2019.
- [55] R. Uppu and S. Mujumdar, "Lévy exponents as universal identifiers of threshold and criticality in random lasers," *Physical Review A*, vol. 90, no. 2, p. 025801, 2014.
- [56] C. J. de Matos, S. M. L. de, A. M. Brito-Silva, M. A. Martinez Gamez, A. S. Gomes, and C. B. de Araujo, "Random fiber laser," *Physical Review Letters*, vol. 99, no. 15, p. 153903, Oct 12 2007, doi: 10.1103/PhysRevLett.99.153903.
- [57] S. K. Turitsyn *et al.*, "Random distributed feedback fibre laser," *Nature Photonics*, vol. 4, no. 4, pp. 231-235, 2010, doi: 10.1038/nphoton.2010.4.
- [58] L. Wang, X. Dong, P. P. Shum, and H. Su, "Tunable erbium-doped fiber laser based on random distributed feedback," *IEEE Photonics Journal*, vol. 6, no. 5, pp. 1-5, 2014.
- [59] X. Du, H. Zhang, X. Wang, and P. Zhou, "Tunable random distributed feedback fiber laser operating at 1 μm ," *Applied Optics*, vol. 54, no. 4, pp. 908-911, 2015.
- [60] D. Xiang, P. Lu, Y. Xu, S. Gao, L. Chen, and X. Bao, "Truly random bit generation based on a novel random Brillouin fiber laser," *Optics Letters*, vol. 40, no. 22, pp. 5415-5418, 2015.
- [61] V. Balaswamy, S. Ramachandran, and V. Supradeepa, "High-power, cascaded random Raman fiber laser with near complete conversion over wide wavelength and power tuning," *Optics Express*, vol. 27, no. 7, pp. 9725-9732, 2019.
- [62] J. Dong *et al.*, "High order cascaded Raman random fiber laser with high spectral purity," *Optics Express*, vol. 26, no. 5, pp. 5275-5280, 2018.
- [63] R. Kashyap, "Principles of Optical Fiber Grating Sensors," in *Fiber Bragg Gratings (Second Edition)*. Boston: Academic Press, 2010, ch. 10, pp. 441-502.
- [64] X. Zhang, Z. Wu, and B. Zhang, "Strain dependence of fiber Bragg grating sensors at low temperature," *Optical Engineering*, vol. 45, no. 5, pp. 054401-054401-4, 2006.
- [65] C. Trono, F. Baldini, M. Brenci, F. Chiavaioli, and M. Mugnaini, "Flow cell for strain-and temperature-compensated refractive index measurements by means of cascaded optical fibre long period and Bragg gratings," *Measurement Science and Technology*, vol. 22, no. 7, p. 075204, 2011.
- [66] Y. Wang, J. Gong, B. Dong, D. Y. Wang, T. J. Shillig, and A. Wang, "A large serial time-division multiplexed fiber Bragg grating sensor network," *Journal of Lightwave Technology*, vol. 30, no. 17, pp. 2751-2756, 2012.
- [67] A. Rogers, "Distributed optical-fibre sensors," *Journal of Physics D: Applied Physics*, vol. 19, no. 12, p. 2237, 1986.

- [68] T. Kurashima, T. Horiguchi, and M. Tateda, "Distributed-temperature sensing using stimulated Brillouin scattering in optical silica fibers," *Optics Letters*, vol. 15, no. 18, pp. 1038-1040, 1990.
- [69] Y. Dong, L. Chen, and X. Bao, "Time-division multiplexing-based BOTDA over 100km sensing length," *Optics Letters*, vol. 36, no. 2, pp. 277-279, 2011.
- [70] Y. London, Y. Antman, R. Cohen, N. Kimelfeld, N. Levanon, and A. Zadok, "High-resolution long-range distributed Brillouin analysis using dual-layer phase and amplitude coding," *Optics Express*, vol. 22, no. 22, pp. 27144-27158, 2014.
- [71] S. Personick, "Photon probe—An optical-fiber time-domain reflectometer," *The Bell System Technical Journal*, vol. 56, no. 3, pp. 355-366, 1977.
- [72] A. Masoudi and T. P. Newson, "High spatial resolution distributed optical fiber dynamic strain sensor with enhanced frequency and strain resolution," *Optics Letters*, vol. 42, no. 2, pp. 290-293, 2017.
- [73] M. Froggatt and J. Moore, "High-spatial-resolution distributed strain measurement in optical fiber with rayleigh scatter," *Applied Optics*, vol. 37, no. 10, pp. 1735-40, Apr 1 1998. [Online]. Available: <https://www.ncbi.nlm.nih.gov/pubmed/18273081>.
- [74] D. K. Gifford, M. E. Froggatt, and S. T. Kreger, "High precision, high sensitivity distributed displacement and temperature measurements using OFDR-based phase tracking," in *21st International Conference on Optical Fiber Sensors*, 2011, vol. 7753: International Society for Optics and Photonics, p. 77533I.
- [75] V. Du Preez, M. Johnson, A. Leist, and K. Hawick, "Performance and quality of random number generators," in *International Conference on Foundations of Computer Science (FCS'11)*, 2011: CSREA, pp. 16-21.
- [76] J. Lockhart, K. Al Rawashdeh, and C. Purdy, "Verification of random number generators for embedded machine learning," in *NAECON 2018-IEEE National Aerospace and Electronics Conference*, 2018: IEEE, pp. 411-416.
- [77] S. Takeuchi, M. Hasegawa, K. Kanno, A. Uchida, N. Chauvet, and M. Naruse, "Dynamic channel selection in wireless communications via a multi-armed bandit algorithm using laser chaos time series," *Scientific Reports*, vol. 10, no. 1, pp. 1-7, 2020.
- [78] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656-715, 1949.
- [79] C. Nist, "The digital signature standard," *Communications of the ACM*, vol. 35, no. 7, pp. 36-40, 1992.
- [80] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644-654, 1976.
- [81] B. Song and C. J. Mitchell, "RFID authentication protocol for low-cost tags," in *Proceedings of the first ACM conference on Wireless network security*, 2008, pp. 140-147.
- [82] M. Zhang and Y. Fang, "Security analysis and enhancements of 3GPP authentication and key agreement protocol," *IEEE Transactions on wireless communications*, vol. 4, no. 2, pp. 734-742, 2005.

- [83] A. M. Ferrenberg, D. Landau, and Y. J. Wong, "Monte carlo simulations: Hidden errors from ‘‘good’’ random number generators," *Physical Review Letters*, vol. 69, no. 23, p. 3382, 1992.
- [84] B. Hayes, "The Science of Computing: The Wheel of Fortune," *American Scientist*, vol. 81, no. 2, pp. 114-118, 1993.
- [85] S. K. Park and K. W. Miller, "Random number generators: good ones are hard to find," *Communications of the ACM*, vol. 31, no. 10, pp. 1192-1201, 1988.
- [86] B. F. Green Jr, J. K. Smith, and L. Klem, "Empirical tests of an additive random number generator," *Journal of the ACM (JACM)*, vol. 6, no. 4, pp. 527-537, 1959.
- [87] D. Knuth, "The art of computer programming, 2 (Seminumerical Algorithms)," 1981.
- [88] E. Barker and Q. Dang, "NIST special publication 800–57 part 3: Application-specific key management guidance," *NIST Special Publication*, vol. 800, p. 57, 2015.
- [89] G. Marsaglia, "DIEHARD: a battery of tests of randomness," <http://stat.fsu.edu/geo>, 1996.
- [90] W. Thomson, "ERNIE—A mathematical and statistical analysis," *Journal of the Royal Statistical Society: Series A (General)*, vol. 122, no. 3, pp. 301-324, 1959.
- [91] Z. Zheng, Y. Zhang, W. Huang, S. Yu, and H. Guo, "6 Gbps real-time optical quantum random number generator based on vacuum fluctuation," *Review of Scientific Instruments*, vol. 90, no. 4, p. 043105, 2019.
- [92] S. Gao, L. Zhang, Y. Xu, L. Chen, and X. Bao, "High-speed random bit generation via brillouin random fiber laser with non-uniform fibers," *IEEE Photonics Technology Letters*, vol. 29, no. 16, pp. 1352-1355, 2017.
- [93] L. Zhang *et al.*, "640-Gbit/s fast physical random number generation using a broadband chaotic semiconductor laser," *Scientific Reports*, vol. 7, p. 45900, 2017.
- [94] R. Takahashi *et al.*, "Fast physical random bit generation with photonic integrated circuits with different external cavity lengths for chaos generation," *Optics Express*, vol. 22, no. 10, pp. 11727-11740, 2014.
- [95] R. Sakuraba, K. Iwakawa, K. Kanno, and A. Uchida, "Tb/s physical random bit generation with bandwidth-enhanced chaos in three-cascaded semiconductor lasers," *Optics Express*, vol. 23, no. 2, pp. 1470-1490, 2015.
- [96] I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, "An optical ultrafast random bit generator," *Nature Photonics*, vol. 4, no. 1, p. 58, 2010.
- [97] T. Butler *et al.*, "Optical ultrafast random number generation at 1 Tb/s using a turbulent semiconductor ring cavity laser," *Optics Letters*, vol. 41, no. 2, pp. 388-391, 2016.
- [98] J. D. Hart, Y. Terashima, A. Uchida, G. B. Baumgartner, T. E. Murphy, and R. Roy, "Recommendations and illustrations for the evaluation of photonic random number generators," *APL Photonics*, vol. 2, no. 9, p. 090901, 2017.
- [99] S. Xiang, B. Wang, Y. Wang, Y. Han, A. Wen, and Y. Hao, "2.24-Tb/s Physical Random Bit Generation With Minimal Post-Processing Based on Chaotic Semiconductor Lasers Network," *Journal of Lightwave Technology*, vol. 37, no. 16, pp. 3987-3993, 2019.

- [100] P. Li *et al.*, "Parallel optical random bit generator," *Optics Letters*, vol. 44, no. 10, pp. 2446-2449, 2019.
- [101] X. Li, A. B. Cohen, T. E. Murphy, and R. Roy, "Scalable parallel physical random number generator based on a superluminescent LED," *Optics Letters*, vol. 36, no. 6, pp. 1020-1022, 2011.
- [102] G. Cao, L. Zhang, X. Huang, W. Hu, and X. Yang, "16.8 Tb/s true random number generator based on amplified spontaneous emission," *IEEE Photonics Technology Letters*, vol. 33, no. 14, pp. 699-702, 2021.
- [103] K. Kim *et al.*, "Massively parallel ultrafast random bit generation with a chip-scale laser," *Science*, vol. 371, no. 6532, pp. 948-952, 2021.
- [104] X. Tang *et al.*, "Multi-channel physical random bits generation using a vertical-cavity surface-emitting laser under chaotic optical injection," *IEEE Access*, vol. 6, pp. 3565-3572, 2018.
- [105] CERT. "Advisory CA-2001-04 Unauthentic "Microsoft Corporation" Certificates." Software Engineering Institute Carnegie Mellon. <https://web.archive.org/web/20131102170603/http://www.cert.org/advisories/CA-2001-04.html> (accessed 2023).
- [106] J. A. Berkowsky and T. Hayajneh, "Security issues with certificate authorities," in *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*, 2017: IEEE, pp. 449-455.
- [107] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," *Science*, vol. 297, no. 5589, pp. 2026-2030, 2002.
- [108] A. F. Smith, P. Patton, and S. E. Skrabalak, "Plasmonic nanoparticles as a physically unclonable function for responsive anti-counterfeit nanofingerprints," *Advanced Functional Materials*, vol. 26, no. 9, pp. 1315-1321, 2016.
- [109] C.-H. Yeh, P.-Y. Sung, C.-H. Kuo, and R.-N. Yeh, "Robust laser speckle recognition system for authenticity identification," *Optics Express*, vol. 20, no. 22, pp. 24382-24393, 2012.
- [110] C. Mesaritakis *et al.*, "Physical unclonable function based on a multi-mode optical waveguide," *Scientific Reports*, vol. 8, no. 1, pp. 1-12, 2018.
- [111] B. Gassend, D. Clarke, M. Van Dijk, and S. Devadas, "Silicon physical random functions," in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, 2002, pp. 148-160.
- [112] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *2007 44th ACM/IEEE Design Automation Conference*, 2007: IEEE, pp. 9-14.
- [113] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1126-1141, 2014.
- [114] Y. Gao, Y. Su, W. Yang, S. Chen, S. Nepal, and D. C. Ranasinghe, "Building secure SRAM PUF key generators on resource constrained devices," in *2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 2019: IEEE, pp. 912-917.

- [115] A. R. Korenda, F. Afghah, B. Cambou, and C. Philabaum, "A proof of concept SRAM-based physically unclonable function (PUF) key generation mechanism for IoT devices," in *2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, 2019: IEEE, pp. 1-8.
- [116] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," in *International workshop on cryptographic hardware and embedded systems*, 2007: Springer, pp. 63-80.
- [117] K. Xiao, M. T. Rahman, D. Forte, Y. Huang, M. Su, and M. Tehranipoor, "Bit selection algorithm suitable for high-volume production of SRAM-PUF," in *2014 IEEE international symposium on hardware-oriented security and trust (HOST)*, 2014: IEEE, pp. 101-106.
- [118] M.-D. Yu and S. Devadas, "Secure and robust error correction for physical unclonable functions," *IEEE Design & Test of Computers*, vol. 27, no. 1, pp. 48-65, 2010.
- [119] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *International conference on the theory and applications of cryptographic techniques*, 2004: Springer, pp. 523-540.
- [120] A. Van Herrewege *et al.*, "Reverse fuzzy extractors: Enabling lightweight mutual authentication for PUF-enabled RFIDs," in *Financial Cryptography and Data Security: 16th International Conference, FC 2012, Kralendijk, Bonaire, February 27-March 2, 2012, Revised Selected Papers 16*, 2012: Springer, pp. 374-389.
- [121] Y. Gao, S. F. Al-Sarawi, and D. Abbott, "Physical unclonable functions," *Nature Electronics*, vol. 3, no. 2, pp. 81-91, 2020.
- [122] M. Bhargava and K. Mai, "An efficient reliable PUF-based cryptographic key generator in 65nm CMOS," in *2014 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2014: IEEE, pp. 1-6.
- [123] W. Che, F. Saqib, and J. Plusquellic, "PUF-based authentication," in *2015 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, 2015: IEEE, pp. 337-344.
- [124] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, no. P1, pp. 7-11, 2014.
- [125] A. Dixon, Z. Yuan, J. Dynes, A. Sharpe, and A. Shields, "Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate," *Optics Express*, vol. 16, no. 23, pp. 18790-18797, 2008.
- [126] B. Korzh *et al.*, "Provably secure and practical quantum key distribution over 307 km of optical fibre," *Nature Photonics*, vol. 9, no. 3, p. 163, 2015.
- [127] K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz, "Synchronization of Lorenz-based chaotic circuits with applications to communications," *IEEE Transactions on circuits and systems II: Analog and digital signal processing*, vol. 40, no. 10, pp. 626-633, 1993.
- [128] P. Colet and R. Roy, "Digital communication with synchronized chaotic lasers," *Optics Letters*, vol. 19, no. 24, pp. 2056-2058, 1994.
- [129] A. Argyris *et al.*, "Chaos-based communications at high bit rates using commercial fibre-optic links," *Nature*, vol. 438, no. 7066, pp. 343-6, Nov 17 2005, doi: 10.1038/nature04275.

- [130] M. Gagné, S. Loranger, J. Lapointe, and R. Kashyap, "Fabrication of high quality, ultra-long fiber Bragg gratings: up to 2 million periods in phase," *Optics Express*, vol. 22, no. 1, pp. 387-398, 2014/01/13 2014, doi: 10.1364/OE.22.000387.
- [131] S. Loranger, V. Lambin-Iezzi, and R. Kashyap, "Reproducible ultra-long FBGs in phase corrected non-uniform fibers," *Optica*, vol. 4, no. 9, 2017, doi: 10.1364/optica.4.001143.
- [132] P. Paradis, M. Briand, M. Otis, M. Levesque, A.-C. Jacob-Poulin, and B. Labranche, "Documentation for the Fabulas station, INO 105181DS RFI N/A," Institut National d'Optique, Québec, Canada, 2012.
- [133] M. Gagné and R. Kashyap, "New nanosecond Q-switched Nd: VO4 laser fifth harmonic for fast hydrogen-free fiber Bragg gratings fabrication," *Optics Communications*, vol. 283, no. 24, pp. 5028-5032, 2010.
- [134] A. Rukhin *et al.*, "National Institute of Standards and Technology, Special Publication 800-22, Revision 1a (2010)," *PD1 PD2 DFB1 DFB2 SOA1 SOA2 M PW*.
- [135] M. Farries and A. Rogers, "Distributed sensing using stimulated Raman interaction in a monomode optical fibre," in *2nd International Conference on Optical Fiber Sensors: OFS'84*, 1984, vol. 514: International Society for Optics and Photonics, pp. 121-133.
- [136] W. Eickhoff and R. Ulrich, "Optical frequency domain reflectometry in single-mode fiber," *Applied Physics Letters*, vol. 39, no. 9, pp. 693-695, 1981.
- [137] M. A. Soto *et al.*, "Raman-based distributed temperature sensor with 1 m spatial resolution over 26 km SMF using low-repetition-rate cyclic pulse coding," *Optics Letters*, vol. 36, no. 13, pp. 2557-2559, 2011.
- [138] M. A. Soto, J. A. Ramírez, and L. Thévenaz, "Optimizing Image Denoising for Long-Range Brillouin Distributed Fiber Sensing," *Journal of Lightwave Technology*, vol. 36, no. 4, pp. 1168-1177, 2018.
- [139] Luna. "Optical Backscatter Reflectometer 4600 - User Guide." http://lunainc.com/wp-content/uploads/2014/05/OBR-4600-UG6_SW3.10.1.pdf (accessed 2019).
- [140] J. Song, W. Li, P. Lu, Y. Xu, L. Chen, and X. Bao, "Long-range high spatial resolution distributed temperature and strain sensing based on optical frequency-domain reflectometry," *IEEE Photonics Journal*, vol. 6, no. 3, pp. 1-8, 2014.
- [141] F. Parent *et al.*, "Enhancement of accuracy in shape sensing of surgical needles using optical frequency domain reflectometry in optical fibers," *Biomedical Optics Express*, vol. 8, no. 4, pp. 2210-2221, Apr 01 2017, doi: 10.1364/BOE.8.002210.
- [142] K. J. Peters *et al.*, "High-accuracy fiber-optic shape sensing," presented at the Sensor Systems and Networks: Phenomena, Technology, and Applications for NDE and Health Monitoring 2007, 2007.
- [143] J. M. López-Higuera, L. R. Cobo, A. Q. Incera, and A. Cobo, "Fiber optic sensors in structural health monitoring," *Journal of Lightwave Technology*, vol. 29, no. 4, pp. 587-608, 2011.
- [144] T. Chen, Q. Wang, B. Zhang, R. Chen, and K. P. Chen, "Distributed flow sensing using optical hot-wire grid," *Optics Express*, vol. 20, no. 8, pp. 8240-8249, 2012.

- [145] S. T. Kreger, A. K. Sang, D. K. Gifford, and M. E. Froggatt, "Distributed strain and temperature sensing in plastic optical fiber using Rayleigh scatter," in *Fiber Optic Sensors and Applications VI*, 2009, vol. 7316: International Society for Optics and Photonics, p. 73160A.
- [146] S. Rizzolo *et al.*, "Radiation response of OFDR distributed sensors based on microstructured pure silica optical fibers," in *Radiation and Its Effects on Components and Systems (RADECS), 2015 15th European Conference on*, 2015: IEEE, pp. 1-3.
- [147] J. Cui, S. Zhao, D. Yang, and Z. Ding, "Investigation of the interpolation method to improve the distributed strain measurement accuracy in optical frequency domain reflectometry systems," *Applied Optics*, vol. 57, no. 6, pp. 1424-1431, Feb 20 2018, doi: 10.1364/AO.57.001424.
- [148] A. Yan *et al.*, "Distributed Optical Fiber Sensors with Ultrafast Laser Enhanced Rayleigh Backscattering Profiles for Real-Time Monitoring of Solid Oxide Fuel Cell Operations," *Scientific Reports*, vol. 7, no. 1, p. 9360, Aug 24 2017, doi: 10.1038/s41598-017-09934-3.
- [149] S. Loranger, M. Gagne, V. Lambin-Iezzi, and R. Kashyap, "Rayleigh scatter based order of magnitude increase in distributed temperature and strain sensing by simple UV exposure of optical fibre," *Scientific Reports*, vol. 5, p. 11177, Jun 16 2015, doi: 10.1038/srep11177.
- [150] L. Thévenaz, S. Chin, J. Sancho, and S. Sales, "Novel technique for distributed fibre sensing based on faint long gratings (FLOGs)," in *23rd International Conference on Optical Fibre Sensors*, 2014, vol. 9157: International Society for Optics and Photonics, p. 91576W.
- [151] J. F. C. Kingman, *Poisson Processes*. Clarendon Press, 1992.
- [152] S. M. Ross, *Stochastic Processes, 2ND ED*. Wiley India Pvt. Limited, 2008.
- [153] R. Kashyap, *Fiber Bragg Gratings*. Academic press, 2009.
- [154] W. Bai, H. Yu, D. Jiang, and M. Yang, "All fiber grating (AFG): a new platform for fiber optic sensing technologies," in *24th International Conference on Optical Fibre Sensors*, 2015, vol. 9634: International Society for Optics and Photonics, p. 96342A.
- [155] A. Beisenova *et al.*, "Multi-fiber distributed thermal profiling of minimally invasive thermal ablation with scattering-level multiplexing in MgO-doped fibers," *Biomedical Optics Express*, vol. 10, no. 3, pp. 1282-1296, 2019.
- [156] P. S. Westbrook *et al.*, "Kilometer length, low loss enhanced back scattering fiber for distributed sensing," in *2017 25th Optical Fiber Sensors Conference (OFS)*, 2017: IEEE, pp. 1-5.
- [157] S. L. Scholl *et al.*, "Thermal approach to classifying sequentially written fiber Bragg gratings," *Optics Letters*, vol. 44, no. 3, pp. 703-706, 2019.
- [158] R. Morris and K. Thompson, "Password security: A case history," *Communications of the ACM*, vol. 22, no. 11, pp. 594-597, 1979.
- [159] A. Juels, "RFID security and privacy: A research survey," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 381-394, 2006.
- [160] D. Bhattacharyya, R. Ranjan, F. Alisherov, and M. Choi, "Biometric authentication: A review," *International Journal of u-and e-Service, Science and Technology*, vol. 2, no. 3, pp. 13-28, 2009.
- [161] Y.-J. Tu, W. Zhou, and S. Piramuthu, "Critical risk considerations in auto-ID security: Barcode vs. RFID," *Decision Support Systems*, vol. 142, p. 113471, 2021.

- [162] A. Ross, J. Shah, and A. K. Jain, "From template to image: Reconstructing fingerprints from minutiae points," *IEEE Transactions on pattern analysis and machine intelligence*, vol. 29, no. 4, pp. 544-560, 2007.
- [163] S. N. Graybeal and P. B. McFate, "Getting out of the STARTing block," *Scientific American*, vol. 261, no. 6, pp. 61-67, 1989.
- [164] Y. Du, S. Jothibas, Y. Zhuang, C. Zhu, and J. Huang, "Unclonable optical fiber identification based on Rayleigh backscattering signatures," *Journal of Lightwave Technology*, vol. 35, no. 21, pp. 4634-4640, 2017.
- [165] A. Maiti and P. Schaumont, "Improved ring oscillator PUF: An FPGA-friendly secure primitive," *Journal of Cryptology*, vol. 24, no. 2, pp. 375-397, 2011.
- [166] U. Rührmair and M. van Dijk, "On the practical use of physical unclonable functions in oblivious transfer and bit commitment protocols," *Journal of Cryptographic Engineering*, vol. 3, no. 1, pp. 17-28, 2013.
- [167] C. Brzuska, M. Fischlin, H. Schröder, and S. Katzenbeisser, "Physically uncloneable functions in the universal composition framework," in *Annual Cryptology Conference*, 2011: Springer, pp. 51-70.
- [168] A. Vijayakumar and S. Kundu, "A novel modeling attack resistant PUF design based on non-linear voltage transfer characteristics," in *2015 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2015: IEEE, pp. 653-658.
- [169] F. Monet, S. Loranger, V. Lambin-Iezzi, A. Drouin, S. Kadoury, and R. Kashyap, "The ROGUE: a novel, noise-generated random grating," *Optics Express*, vol. 27, no. 10, pp. 13895-13909, 2019/05/13 2019, doi: 10.1364/OE.27.013895.
- [170] F. Monet *et al.*, "High-resolution optical fiber shape sensing of continuum robots: A comparative study," in *2020 IEEE International Conference on Robotics and Automation (ICRA)*, 2020: IEEE, pp. 8877-8883.
- [171] M. Froggatt, R. J. Seeley, and D. K. Gifford, "High Resolution Interferometric Optical Frequency Domain Reflectometry (OFDR) Beyond The Laser Coherence Length," United States of America Patent US007515276B2 Patent Appl. 11/779,527, 2009.
- [172] K. Hill, B. Malo, F. Bilodeau, and D. Johnson, "Photosensitivity in optical fibers," *Annual Review of Materials Science*, vol. 23, no. 1, pp. 125-157, 1993.
- [173] A. Martinez, I. Y. Khrushchev, and I. Bennion, "Direct inscription of Bragg gratings in coated fibers by an infrared femtosecond laser," *Optics Letters*, vol. 31, no. 11, pp. 1603-1605, 2006.
- [174] S. Mihailov, D. Grobncic, and C. Smelser, "Efficient grating writing through fibre coating with femtosecond IR radiation and phase mask," *Electronics Letters*, vol. 43, no. 8, pp. 442-443, 2007.
- [175] L. Chao, L. Reekie, and M. Ibsen, "Grating writing through fibre coating at 244 and 248 nm," *Electronics Letters*, vol. 35, no. 11, pp. 924-926, 1999.
- [176] C. Askins, M. Putnam, G. Williams, and E. Friebele, "Stepped-wavelength optical-fiber Bragg grating arrays fabricated in line on a draw tower," *Optics Letters*, vol. 19, no. 2, pp. 147-149, 1994.

- [177] M. W. Rothhardt, C. Chojetzki, and H. R. Mueller, "High-mechanical-strength single-pulse draw tower gratings," in *Photonics North 2004: Photonic Applications in Telecommunications, Sensors, Software, and Lasers*, 2004, vol. 5579: International Society for Optics and Photonics, pp. 127-135.
- [178] V. Fuertes *et al.*, "Engineering nanoparticle features to tune Rayleigh scattering in nanoparticles-doped optical fibers," *Scientific reports*, vol. 11, no. 1, pp. 1-12, 2021.
- [179] Luna. "Luna ODiSI 6000 Data Sheet." <https://lunainc.com/sites/default/files/assets/files/data-sheet/Luna%20ODiSI%206000%20Data%20Sheet.pdf> (accessed 2022).
- [180] J. G. Merchan, S. S. Kumar, P. T. Tuyls, and G. J. Schrijen, "Identification of devices using physically unclonable functions," ed: Google Patents, 2011.
- [181] A. Aysu, E. Gulcan, D. Moriyama, P. Schaumont, and M. Yung, "End-to-end design of a PUF-based privacy preserving authentication protocol," in *Cryptographic Hardware and Embedded Systems--CHES 2015: 17th International Workshop, Saint-Malo, France, September 13-16, 2015, Proceedings 17*, 2015: Springer, pp. 556-576.
- [182] M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," *Reviews of Modern Physics*, vol. 89, no. 1, p. 015004, 2017.
- [183] A. Uchida *et al.*, "Fast physical random bit generation with chaotic semiconductor lasers," *Nature Photonics*, vol. 2, no. 12, pp. 728-732, 2008.
- [184] N. Oliver, M. C. Soriano, D. W. Sukow, and I. Fischer, "Fast random bit generation using a chaotic laser: approaching the information theoretic limit," *IEEE Journal of Quantum Electronics*, vol. 49, no. 11, pp. 910-918, 2013.
- [185] Y. Akizawa *et al.*, "Fast Random Number Generation With Bandwidth-Enhanced Chaotic Semiconductor Lasers at 8×50 Gb/s," *IEEE Photonics Technology Letters*, vol. 24, no. 12, pp. 1042-1044, 2012.
- [186] H. Wu *et al.*, "Ultra-high speed random bit generation based on Rayleigh feedback assisted ytterbium-doped random fiber laser," *Science China Technological Sciences*, pp. 1-7, 2021.
- [187] H. Wu, B. Han, Z. Wang, G. Genty, G. Feng, and H. Liang, "Temporal ghost imaging with random fiber lasers," *Optics Express*, vol. 28, no. 7, pp. 9957-9964, 2020.
- [188] I. A. Koutrouvelis, "Regression-type estimation of the parameters of stable laws," *Journal of the American statistical association*, vol. 75, no. 372, pp. 918-928, 1980.
- [189] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. John Wiley & Sons, 1999.
- [190] S.-S. Li, X.-Z. Li, and S.-C. Chan, "Chaotic time-delay signature suppression with bandwidth broadening by fiber propagation," *Optics Letters*, vol. 43, no. 19, pp. 4751-4754, 2018.
- [191] W. Tian, L. Zhang, J. Ding, S. Shao, X. Fu, and L. Yang, "Ultrafast physical random bit generation from a chaotic oscillator with a silicon modulator," *Optics Letters*, vol. 43, no. 19, pp. 4839-4842, 2018.
- [192] P. Li *et al.*, "Ultrafast fully photonic random bit generator," *Journal of Lightwave Technology*, vol. 36, no. 12, pp. 2531-2540, 2018.

- [193] M. Cole, W. Loh, R. Laming, M. Zervas, and S. Barcelos, "Moving fibre/phase mask-scanning beam technique for enhanced flexibility in producing fibre gratings with uniform phase mask," *Electronics Letters*, vol. 31, no. 17, pp. 1488-1490, 1995.
- [194] K. Lee, S.-Y. Lee, C. Seo, and K. Yim, "TRNG (True Random Number Generator) method using visible spectrum for secure communication on 5G network," *IEEE Access*, vol. 6, pp. 12838-12847, 2018.
- [195] X. Tang *et al.*, "Tbits/s physical random bit generation based on mutually coupled semiconductor laser chaotic entropy source," *Optics Express*, vol. 23, no. 26, pp. 33130-33141, 2015.
- [196] M. Mascagni and A. Srinivasan, "Algorithm 806: SPRNG: A scalable library for pseudorandom number generation," *ACM Transactions on Mathematical Software (TOMS)*, vol. 26, no. 3, pp. 436-461, 2000.
- [197] J. Ackermann, U. Tangen, B. Bödekker, J. Breyer, E. Stoll, and J. McCaskill, "Parallel random number generator for inexpensive configurable hardware cells," *Computer Physics Communications*, vol. 140, no. 3, pp. 293-302, 2001.
- [198] F. Monet, J.-S. Boisvert, and R. Kashyap, "A simple high-speed random number generator with minimal post-processing using a random Raman fiber laser," *Scientific Reports*, vol. 11, no. 1, pp. 1-8, 2021.
- [199] R. Ma *et al.*, "Backward supercontinuum generation excited by random lasing," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 24, no. 3, pp. 1-5, 2017.
- [200] L. Abrardi, S. Martín-López, A. Carrasco-Sanz, P. Corredera, M. L. Hernanz, and M. González-Herráez, "Optimized all-fiber supercontinuum source at 1.3 μm generated in a stepwise dispersion-decreasing-fiber arrangement," *Journal of Lightwave Technology*, vol. 25, no. 8, pp. 2098-2102, 2007.
- [201] Q. Zhang, C. Zhou, J. Meng, F. Guo, and H. Chang, "Parallel quantum random number generation based on spontaneous emission of alkaline earth," *Applied Physics Express*, vol. 13, no. 1, p. 012015, 2019.
- [202] X. Tang *et al.*, "Generation of multi-channel high-speed physical random numbers originated from two chaotic signals of mutually coupled semiconductor lasers," *Laser Physics Letters*, vol. 12, no. 1, p. 015003, 2014.
- [203] Z. Ge, Y. Xiao, T. Hao, W. Li, and M. Li, "Tb/s Fast Random Bit Generation Based on a Broadband Random Optoelectronic Oscillator," *IEEE Photonics Technology Letters*, vol. 33, no. 22, pp. 1223-1226, 2021.
- [204] F. Monet, S. Loranger, and R. Kashyap, "Strong localization in weakly scattering medium," in *2019 Conference on Lasers and Electro-Optics / Europe*, Munich, Germany, 2019: Optica and IEEE.
- [205] O. Ozoliņš and Ģ. Ivanovs, "Realization of Optimal FBG Band-Pass Filters for High Speed HDWDM," *Elektronika ir Elektrotechnika*, vol. 92, no. 4, pp. 41-44, 2009.
- [206] F. Chaoui, O. Aghzout, M. Chakkour, and M. El Yakhoulfi, "Apodization optimization of FBG strain sensor for quasi-distributed sensing measurement applications," *Active and Passive Electronic Components*, vol. 2016, 2016.

- [207] C. W. Rudy, M. J. Digonnet, and R. L. Byer, "Advances in 2- μ m Tm-doped mode-locked fiber lasers," *Optical Fiber Technology*, vol. 20, no. 6, pp. 642-649, 2014.
- [208] M. J. Digonnet, *Rare-earth-doped fiber lasers and amplifiers, revised and expanded*. CRC press, 2001.
- [209] Y. Cuerno, "Towards Space Grade Lasers for Sr87 Atomic Clock Applications: Fabrication and Characterization of a Distributed-Feedback Thulium Polarization Maintaining Fiber Laser with a Novel Single Polarization Single Frequency Design," Master's, Polytechnique Montreal, Montreal, Canada, 2022.
- [210] M. Dubov, I. Bennion, D. N. Nikogosyan, P. Bolger, and A. Zayats, "Point-by-point inscription of 250 nm period structure in bulk fused silica by tightly focused femtosecond UV pulses," *Journal of Optics A: Pure and Applied Optics*, vol. 10, no. 2, p. 025305, 2008.
- [211] A. Martinez, M. Dubov, I. Khrushchev, and I. Bennion, "Direct writing of fibre Bragg gratings by femtosecond laser," *Electronics Letters*, vol. 40, no. 19, pp. 1170-1172, 2004.
- [212] J. Francoeur *et al.*, "Optical frequency domain reflectometry shape sensing using an extruded optical fiber triplet for intra-arterial guidance," *Optics Express*, vol. 31, no. 1, pp. 396-410, 2023.
- [213] S. Sutar, A. Raha, and V. Raghunathan, "D-PUF: An intrinsically reconfigurable DRAM PUF for device authentication in embedded systems," in *Proceedings of the International Conference on Compilers, Architectures and Synthesis for Embedded Systems*, 2016, pp. 1-10.
- [214] R. G. Brown, D. Eddelbuettel, and D. Bauer, "Dieharder," *Duke University Physics Department Durham, NC*, pp. 27708-0305, 2018.
- [215] P. L'ecuyer and R. Simard, "TestU01: AC library for empirical testing of random number generators," *ACM Transactions on Mathematical Software (TOMS)*, vol. 33, no. 4, pp. 1-40, 2007.
- [216] A. A. Sawchuk and T. C. Strand, "Digital optical computing," *Proceedings of the IEEE*, vol. 72, no. 7, pp. 758-779, 1984.
- [217] F. Monet and R. Kashyap, "Tangible Un-Fungible Tokens: TUFTs, or Optically Encoded NFTs," U.S. Patent Appl. 63/357,657 - AXE-0090, 2022.
- [218] R. Kashyap, S. Loranger, F. Monet, S. Kadoury, and P. Lorre, "Method and system for fabricating an optical fiber device for shape sensing," U.S. Patent Number 11,249,248, 2022.

APPENDIX A LIST OF PUBLICATIONS AND AWARDS

PUBLICATIONS

Published Peer-Reviewed Journal Articles

J. Thomas, T. Mayneng, Y. Ledemi, A. Roberge, F. Monet, D. Seletskiy, Y. Messadèq and R. Kashyap (2023). Enhancing the optical performance of oxyfluoride glass ceramics by optimizing the oxide:fluoride ratio and crystallinity for optical refrigeration, *Journal of Non-Crystalline Solids*, 10173.

J. Francoeur, **F. Monet**, A. Roberge, P. Lorre, S. Kadoury, R. Kashyap and C. Wright (2023). Optical Frequency Domain Reflectometry Shape Sensing Using an Extruded Optical Fiber Triplet for Intra-Arterial Guidance, *Optics Express*, 31(1), 396-410.

A. Svecic, J. Francoeur, G. Soulez, **F. Monet**, R. Kashyap and S. Kadoury (2022). Shape and Flow Sensing in Arterial Image Guidance from UV Exposed Optical Fibers based on Spatio-temporal Networks, *IEEE Transactions on Biomedical Engineering*.

A. Roberge, S. Loranger, J.S. Boisvert, **F. Monet**, and R. Kashyap (2022). Femtosecond laser direct-writing of high quality first-order Bragg gratings with arbitrary complex apodization by phase modulation. *Optics Express*, 30(17), 30405-30419.

F. Monet, J.S. Boisvert and R. Kashyap (2021). A simple high-speed random number generator with minimal post-processing using a random Raman fiber laser. *Scientific Reports*, 11(1), 1-8.

F. Monet, S. Loranger, V. Lambin-Iezzi, A. Drouin, S. Kadoury, R. Kashyap (2019). The ROGUE: A novel, noise-driven random grating, *Optics Express*, 27(10), 13895-13909.

F. Parent, M. Gérard, **F. Monet**, S. Loranger, G. Soulez, R. Kashyap and S. Kadoury (2018). Intra-arterial Image Guidance with Optical Frequency Domain Reflectometry Shape Sensing. *IEEE Transactions on Medical Imaging*, 38(2), 482-492.

N. Rousset, **F. Monet** and T. Gervais (2017). Simulation-assisted design of microfluidic sample traps for optimal trapping and culture of tissues and spheroids, *Scientific Reports*, 7(1), 245.

M. Astolfi, B. Péant, M. A. Lateef, N. Rousset, J. Kendall-Dupont, E. Carmona, **F. Monet**, F. Saad, D. Provencher, A.-M. Mes-Masson and T. Gervais (2016), Micro-dissected tumor tissues on chip: an ex vivo method for drug testing and personalized therapy, *Lab on a Chip*, 16(2), 312-325.

Submitted Peer-Reviewed Journal Articles

F. Monet, A. Roberge and R. Kashyap. Non Fungible Gratings as Physical Unclonable Functions, *IEEE Journal of Selected Topics in Quantum Electronics* (accepted on March 19, 2023).

J. Thomas, T. Meyneng, A. Terhanchi, N. Grégoire, **F. Monet**, D. Seletskiy, Y. Messadeq and R. Kashyap. First demonstration of laser cooling in a novel all oxide GAYY silica glass, *Scientific Reports* (accepted on March 17, 2023).

F. Monet and R. Kashyap. On Multiplexing in physical Random Number Generation, and conserved total entropy content, *Scientific Reports* (submitted: November 2022).

Published Peer-Reviewed Conference Articles (* identifies the presenter, [†] identifies authors with equal contribution)

A. Svecic*, G. Soulez, **F. Monet**, R. Kashyap and S. Kadoury (September 2021). Multimodal Sensing Guidewire for C-Arm Navigation with Random UV Enhanced Optical Sensors Using Spatio-Temporal Networks. In *International Conference on Medical Image Computing and Computer-Assisted Intervention* (pp. 249-258). Springer, Cham.

F. Monet^{*,†}, S. Sefati[†], ... and R. Kashyap. (May 2020). High-resolution optical fiber shape sensing of continuum robots: A comparative study. In *2020 IEEE International Conference on Robotics and Automation (ICRA)* (pp. 8877-8883). IEEE.

Conference Invited Presentations (as presenter)

F. Monet, J.S. Boisvert and R. Kashyap (May 2020). Ultrafast random Raman soliton random bit generator, In *Photonics North 2020*. IEEE.

Conference Contributed Presentations (as presenter)

F. Monet, A. Roberge and R. Kashyap (August 2022). Random Grating-based Physical Unclonable Functions, In *Latin America Optics and Photonics Conference 2022*. Optica.

F. Monet and R. Kashyap (July 2022). Random Raman Supercontinuum fiber laser. In Nonlinear Photonics, *Advanced Photonics Congress 2022*. Optica.

F. Monet, A. Roberge and R. Kashyap (July 2022). Physical Unclonable Functions based on random gratings. In Bragg Gratings, Photosensitivity and Poling in Glass Waveguides, *Advanced Photonics Congress 2022*. Optica.

F. Monet, A. Roberge and R. Kashyap (July 2022). Random Grating-based Physical Unclonable Functions. In *International Conference on Optical and Optoelectronic Properties of Materials and Applications 2022*.

F. Monet, J.S. Boisvert and R. Kashyap (July 2020). Ultrafast random Raman solitons for real-time Tbps random number generation. In *Advanced Photonics Congress 2020*. Optica.

F. Monet, V. Lambin-Iezzi, J.S. Boisvert, B. Maubois and R. Kashyap (March 2020). ROGUE-based, random distributed feedback lasers. In Fiber Lasers XVII: Technology and Systems (Vol. 11260, p. 112601J), *Photonics West 2020*. SPIE.

F. Monet, S. Loranger, R. Kashyap. (June 2019). Strong localization in weakly scattering medium. *2019 Conference on Lasers and Electro-Optics / Europe*. Optica and IEEE.

F. Monet, S. Loranger, V. Lambin-Iezzi, S. Kadoury, R. Kashyap. (February 2019). The ROGUE: Order of magnitude increase in the resolution of temperature and strain sensing. SPIE Photonics West OPTO. *Photonics West 2019*. SPIE.

Conference Poster Presentations (as presenter)

F. Monet, P. Lorre, J.S. Boisvert, V. Lambin-Iezzi and R. Kashyap (August 2019). Towards a better understanding of the ROGUE. In Seventh European Workshop on Optical Fibre Sensors (Vol. 11199, pp. 513-516). SPIE.

Patents

F. Monet and R. Kashyap. Tangible Un-Fungible Tokens : TUFTs , or Optically Encoded NFTs, DIV-964, provisional patent filed in 2022.

R. Kashyap, S. Loranger, **F. Monet** and S. Kadoury (2022). Method and system for fabricating an optical fiber device for shape sensing, U.S. Patent No 11,249,248.

AWARDS

Best Student Paper Award, BGPP 2022

SPIE Optics and Photonics Education Scholarship, 2019

FRQNT Doctoral Scholarship, 2019

Canada Vanier Graduate Scholarship, 2019

NSERC Alexander-Graham-Bell Doctoral Scholarship (declined), 2019

Médaille du lieutenant-gouverneur pour la jeunesse (bronze), 2019

Bourse d'excellence en recherche de la Fondation J. A. Desève, 2019

Bourse d'excellence Hydro-Québec, 2018

Student grant for the International School on Light Sciences and Technologies, 2018

Mitacs Globalink Research Scholarship, 2018

Bourse RBC Banque Royale, 2018

Graduate Studies Admission Scholarship, 2018

NSERC Master's Scholarship, 2017

FRQNT Master's Scholarship, 2017

APPENDIX B MATHEMATICAL DEVELOPMENTS

B.1 Fiber Bragg gratings equations

The refractive index of an FBG as a function of position is defined as

$$n(z) = n_0 + \overline{\Delta n}(z) \left(1 + v(z) \cos \left(\frac{2\pi z}{\Lambda} + \phi(z) \right) \right) \quad (\text{B.1})$$

The impact of this refractive index modulation on the waves propagating in the optical waveguide can be understood by first considering the wave equation

$$\nabla^2 E = \mu_0 \varepsilon_0 \frac{\partial^2 E}{\partial t^2} + \mu_0 \frac{\partial^2 P}{\partial t^2} \quad (\text{B.2})$$

For simplification, let us consider that the wave is propagating along the z axis, such that

$$\nabla^2 E = \frac{\partial^2 E}{\partial z^2} \quad (\text{B.3})$$

We can describe the relationship between P and E from the polarization equation, by considering the effect of the FBG inscription as a perturbation of the permittivity $\Delta\varepsilon$, such that

$$P = \varepsilon_0 (\varepsilon_r - 1 + \Delta\varepsilon(z)) E \quad (\text{B.4})$$

where P is the polarization vector, ε_0 is the vacuum permittivity, ε_r is the relative permittivity of the medium and E_μ is the electric field of the propagating wave. Since the permittivity of a material is equal to the square of its refractive index, we therefore have

$$\varepsilon_r + \Delta\varepsilon(z) = n(z)^2 \quad (\text{B.5})$$

By inserting Equation (B.1), and considering an index modulation $\overline{\Delta n}$ much smaller than n_0 (such as is the case typically for FBGs), we can deduce from Equation (B.5) that

$$\Delta\varepsilon(z) = 2n_0 \overline{\Delta n}(z) \left(1 + \frac{v(z)}{2} e^{i\left(\frac{2\pi z}{\Lambda} + \phi(z)\right)} + cc \right) \quad (\text{B.6})$$

where Λ is the index modulation period and cc is the complex conjugate.

We can also insert Equations (B.4) in Equation (B.2), such that the wave equation now is

$$\frac{\partial^2 E}{\partial z^2} = \mu_0 \varepsilon_0 \varepsilon_r \frac{\partial^2 E}{\partial t^2} + \mu_0 \varepsilon_0 \Delta\varepsilon(z) \frac{\partial^2 E}{\partial t^2} \quad (\text{B.7})$$

We can express the electrical field as the sum of two contributions, one forward propagating field A_v and one backward propagating field B_μ , resulting in

$$E = \frac{1}{2} (A_v(z) \xi_v e^{i(\omega t - \beta_v z)} + B_\mu(z) \xi_\mu e^{i(\omega t + \beta_\mu z)}) \quad (\text{B.8})$$

where ξ_v and ξ_μ are the transverse electric field overlap integral with the waveguide and β_v and β_μ are the propagation constants. The negative sign in the first exponent indicates the forward propagation of the A_v mode, while the positive sign of the B_μ mode indicates backward propagation. In the case of an FBG written in a single-mode fiber, $\beta_v = \beta_\mu = \beta$ and $\xi_v = \xi_\mu = \xi$. The second derivative with respect to time of Equation (B.7) is easy to compute, and results simply in

$$\frac{\partial^2 E}{\partial t^2} = -\omega^2 E \quad (\text{B.9})$$

The second derivative with respect to z is more challenging. However by using the slowly varying envelope approximation, the second derivative of A_v and B_μ can be ignored as they will be much smaller than the other terms, meaning that

$$\frac{\partial^2 E}{\partial z^2} \approx \frac{1}{2} \left(-i\beta \frac{\partial A}{\partial z} \xi e^{i(\omega t - \beta z)} + i\beta \frac{\partial B}{\partial z} \xi e^{i(\omega t + \beta z)} \right) - \beta^2 E \quad (\text{B.10})$$

Knowing that $\beta^2 = \omega^2 \mu_0 \varepsilon_0 \varepsilon_r$, the last term of Equation (B.10) cancels out the first term of the right-hand side of Equation (B.7), which can thus be rewritten

$$\frac{1}{2} \left(-i\beta \frac{\partial A}{\partial z} \xi e^{i(\omega t - \beta z)} + i\beta \frac{\partial B}{\partial z} \xi e^{i(\omega t + \beta z)} \right) = -\omega^2 \mu_0 \varepsilon_0 \Delta \varepsilon(z) E(z) \quad (\text{B.11})$$

Since both $\Delta \varepsilon(z)$ and $E(z)$ have two terms, this equation is quite complex. However, using arguments of orthogonality between modes and conservation of momentum, the two coupled equations describing the rate of variation of A and B can be extracted, and are the following

$$\frac{\partial A}{\partial z} = -i\kappa_{dc} - i\kappa_{ac}^* B e^{i(\Delta \beta z - \phi(z))} \quad (\text{B.12a})$$

$$\frac{\partial B}{\partial z} = i\kappa_{dc} + i\kappa_{ac} A e^{-i(\Delta \beta z - \phi(z))} \quad (\text{B.12b})$$

where

$$\kappa_{dc} = n_0 \omega \varepsilon_0 \overline{\Delta n} \xi \xi^* = \frac{4\pi n_{eff} \overline{\Delta n} \eta}{\lambda} \quad (\text{B.13a})$$

$$\kappa_{ac} = \frac{n_0 \omega \varepsilon_0 \overline{\Delta n} v \xi \xi^*}{2} = \frac{2\pi n_{eff} \overline{\Delta n} v \eta}{\lambda} \quad (\text{B.13b})$$

$$\Delta\beta = 2\beta - \frac{2\pi}{\Lambda}. \quad (\text{B.13c})$$

where η is the overlap integral of the optical power with the core cross-section. The value of κ_{ac} is related to the value of the refractive index modulation, and will define the strength of the grating, while κ_{dc} is related to the average refractive index modulation. $\Delta\beta$ is the phase matching between the forward and backward waves. The phase matching will be optimal when $\Delta\beta = 0$, which defines the Bragg wavelength

$$\lambda_B = 2n_{eff}\Lambda. \quad (\text{B.14})$$

where n_{eff} is the guided mode's effective refractive index. After performing the following substitution

$$R = Ae^{-\frac{i}{2}(\Delta\beta z - \phi(z))} \quad (\text{B.15a})$$

$$S = Be^{\frac{i}{2}(\Delta\beta z - \phi(z))} \quad (\text{B.15b})$$

We can obtain from Equations (B.12) the following coupled equations

$$\frac{\partial R}{\partial z} + i(\kappa_{dc} + \frac{1}{2}(\Delta\beta - \frac{d\phi(z)}{dz}))R = -i\kappa_{ac}^*S \quad (\text{B.16a})$$

$$\frac{\partial S}{\partial z} - i(\kappa_{dc} + \frac{1}{2}(\Delta\beta - \frac{d\phi(z)}{dz}))S = i\kappa_{ac}R \quad (\text{B.16b})$$

This set of equation allows to solve the reflection and transmission values of a given FBG, based on the various parameters such as the refractive index change $\overline{\Delta n}$, the visibilty v and the phase ϕ , all of which can vary along the length of the FBG. It is important to observe that, in these equations, the derivative of the phase $d\phi(z)/dz$ has the same effect as the phase matching $\Delta\beta$. Therefore, if the phase variation is non-zero, coupling can occur at a different wavelength than the Bragg wavelength. This is the case for example for *chirped* gratings, who reflect light at different wavelengths along their length. For instance, achieving a linear chirp would require a quadratic phase $\phi(z)$, so that its derivative is linear. This would result in a grating where the coupled wavelength would increase (or decrease, depending on the sign of the derivative) as a function of length.

The most simple FBG, the uniform FBG, is defined by a constant amplitude modulation and a constant phase, such that $\overline{\Delta n}$, v and ϕ are all constants (which means that $d\phi(z)/dz = 0$). For this

specific FBG, the coupled Equations (B.16) can be solved analytically. After applying the boundary conditions $R(0) = 1$ (we fix the initial incident amplitude to a value of 1) and $S(L) = 0$ (there is no reflected field at the end of the grating, as there is nothing beyond to generate it), we obtain that the amplitude reflection coefficient is

$$\rho = \frac{S(0)}{R(0)} = -\frac{\kappa_{ac} \sinh(\alpha L)}{\delta \sinh(\alpha L) - i \alpha \cosh(\alpha L)} \quad (\text{B.17})$$

where

$$\delta = \kappa_{dc} + \frac{1}{2} \left(\Delta\beta - \frac{d\phi(z)}{dz} \right) \quad (\text{B.18a})$$

$$\alpha = \sqrt{|\kappa_{ac}|^2 - \delta^2}. \quad (\text{B.18b})$$

It should be noted that ρ is the amplitude reflection coefficient associated with the electrical field. The power reflection coefficient (what is usually measured) is $|\rho|^2$. At its peak, the reflectivity of a uniform FBG is

$$|\rho|^2 = \tanh^2(\kappa_{ac} L) \quad (\text{B.19})$$

And its full width at first zeroes (FWFZ) is given by

$$\Delta\lambda = \frac{\lambda_B^2}{\pi n_{eff} L} \sqrt{(\kappa_{ac} L)^2 + \pi^2} \quad (\text{B.20})$$