Imperial College London

Semiconductor Lasers in Quantum Cryptography

Victor Lovic

2023

Department of Physics

Imperial College London

Submitted in part fulfilment of the requirements for the degree of

Doctor of Philosophy of Imperial College London

For my parents

María Bueno

Branko Lovic

Abstract

The unique properties of quantum mechanics, like entanglement and superposition, can be leveraged to carry out cryptographic tasks that cannot be achieved by classical means. For example, Quantum Key Distribution (QKD) enables two parties to communicate in a provably secure manner. Another application is Quantum Random Number Generation (QRNG), exploiting the inherent randomness in quantum mechanics to generate truly random numbers.

Semiconductor lasers are a key technology in both QKD and QRNG and greatly influence the performance and security of these systems. Semiconductor lasers are also an advanced technology, benefitting from decades of research and development from the field of classical fibre optic communications. This has resulted not only in low-cost, high-performance devices, but also an extensive associated literature.

While QKD and QRNG have similar laser requirements to classical fibre optic communications, and have thus significantly benefitted from the associated research and development, they also have unique requirements and use cases that have been insufficiently explored by the current literature. This thesis draws from the existing literature to study semiconductor lasers specifically in the context of quantum cryptography.

We introduce the essential methods for modelling semiconductor lasers and provide two specific applications of them. In the first, we model phase noise in a gain-switched laser diode,

crucial for security in quantum cryptography. And second, we study the so-called laser seeding attack in QKD. Throughout our work we complement our simulation results with experiments, and vice versa. This thesis contributes to the security and performance of QKD and QRNG, and provides tools and techniques for further study of semiconductor lasers in quantum cryptography.

This work is my own, except where otherwise stated and appropriately referenced.

Publications

Parts of this thesis have been published in the following articles and conferences.

Journal Articles

1. **V. Lovic**, D. G. Marangon, M. Lucamarini, Z. Yuan, and A. J. Shields, 'Characterizing Phase Noise in a Gain-Switched Laser Diode for Quantum Random-Number Generation', *Phys. Rev. Applied*, vol. 16, no. 5, p. 054012, Nov. 2021.

    - *Contributions:* I and D. G. Marangon contributed to the study conception and design. I carried out all experimental measurements and numerical simulations and wrote the manuscript. D. G. Marangon carried out the statistical tests of randomness and accompanying discussion (Sec. V). All authors read and approved the final manuscript.

2. T. K. Paraïso, R. I. Woodward, D. G. Marangon, **V. Lovic**, Z. Yuan, and A. J. Shields, 'Advanced Laser Technology for Quantum Communications (Tutorial Review)', *Adv Quantum Tech*, p. 2100062, Aug. 2021.

    - *Contributions:* All authors contributed to the study conception and design. I contributed to the Theory section (Sec. 2). The manuscript was written by all authors.

3. **V. Lovic**, D. G. Marangon, P. R. Smith, R. I. Woodward, and A. J. Shields, 'Quantified Effects of the Laser Seeding Attack in Quantum Key Distribution', *Phys. Rev. Applied*, Accepted for publication, 2023.

    - *Contributions:* I, D. G. Marangon, P. R. Smith and R. I. Woodward contributed to the study conception and design. I carried out all experimental measurements and numerical simulations and wrote the manuscript. All authors read and approved the final manuscript.

Conference Proceedings

1. **V. Lovic**, D. G. Marangon, M. Lucamarini, Z. Yuan, and A. J. Shields, "Quantifying Randomness in a Gain-Switched Laser Diode," in Conference on Lasers and Electro-Optics, Technical Digest Series (Optica Publishing Group, 2022), paper FTu4A.5.

Additional Publications

In addition, the following works were carried out during my PhD, but are beyond the scope of this thesis:

1. Y.S. Lo, R.I. Woodward, T. Roger, **V. Lovic**, T.K. Paraïso, I. De Marco, Z.L. Yuan, and A.J. Shields "Self-tuning transmitter for quantum key distribution using machine intelligence" *Phys. Rev. Applied*, vol. 18, no. 3, p. 034087, Sept. 2022.

2. D. G Marangon, P. R. Smith, **V. Lovic**, T. Roger, J. Dynes, M. Lucamarini, Z. Yuan and A. J. Shields "A fast and robust quantum random number generator with a self-contained

integrated photonic randomness core", Manuscript under review at Nature Electronics, 2023

3. (Conference Proceeding) Y. S. Lo, R. I. Woodward, T. Roger, **V. Lovic**, Z. L. Yuan, and A. J. Shields, "Self-tuning quantum key distribution transmitter based on a genetic algorithm," in Optical Fiber Communication Conference (OFC) 2022, S. Matsuo, D. Plant, J. Shan Wey, C. Fludger, R. Ryf, and D. Simeonidou, eds., Technical Digest Series (Optica Publishing Group, 2022), paper M3I.2.

4. (Conference Proceeding) T. K. Paraïso, T. Roger, D. G. Marangon, I. De Marco, M. Sanzaro, R. I. Woodward, J. F. Dynes, **V. Lovic**, Z. -. Yuan, and A. J. Shields, "Advanced Laser Modulation and Chip-Based Quantum Communications," in Quantum 2.0 Conference and Exhibition, Technical Digest Series (Optica Publishing Group, 2022), paper QTu3B.3.

5. (Conference Proceeding) Y. S. Lo, R. I. Woodward, T. Roger, **V. Lovic**, T. K. Paraiso, I. De Marco, Z. L. Yuan, A. J. Shields, "Towards a self-tuning quantum key distribution transmitter using a genetic algorithm," Proc. SPIE 12133, Quantum Technologies 2022, 121330D (31 May 2022)

Acknowledgements

I would like to thank Myungshik Kim for making me feel at home at Imperial and his research group. Thank you to Andrew Shields for hosting me in Toshiba's Cambridge Research Laboratory and the opportunity to pursue my PhD in a fantastic research environment.

Thank you to EPSRC for funding my PhD. Ultimately, I thank the British taxpayer for funding my entire university education, including some internships along the way. I am now myself a taxpayer in Britain, so I hope to literally repay the favour!

A special thank you to Davide Marangon for supervising my work and making me feel like a valued colleague. It was a pleasure working with you. A second special thanks to Raymond Smith, my lab mate. He saved me countless hours of struggle helping me out in the lab. I will remember the Security Lab at Toshiba with fondness.

Thank you to all my Toshiba friends and colleagues for making my time there so enjoyable and fulfilling.

On a personal note, I want to thank my joint-second-best friends, Stefan and Marko, who are also my brothers. It's so comforting to know that over whatever distance or time, I can always count on them.

A special thank you to my partner and first-best friend Anna. These past years we've gone through so much together: graduate degrees, global pandemic, first jobs, new city, creation and

then destruction of van, travelling, dog-sitting, and all the normal-living in between. And it was all so much better with you, thank you <3.

Lastly, I want to thank my parents, who this thesis is dedicated to. They would always say that my, and my brothers', education is the most important thing. And they lived up to it! Submitting this thesis is the last step in the education journey they set me on more than 20 years ago. Along the way I've always had their support and their love, for which I am ever grateful. Te quiero, Mamá! Love you, Dad! Thank you for everything.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Quantum cryptography (QC) is the first quantum technology to reach maturity and commercialisation [1], [2]. Already there are companies selling commercial products and a multitude of real-world demonstrations of the technology [3]–[7]. Part of the reason QC was able to advance so quickly is that it relies on the same technological foundations as classical fibre optic communications. Both technologies use semiconductor lasers (SLs) to send information encoded on photons down optical fibres over large distances which are detected at the receiver using photodiodes [8]–[10]. QC has therefore benefitted greatly from the decades of research and development in the field of classical fibre optic communications. Particularly relevant to this thesis are the great advances in SL technology, resulting in high-performance, low-cost devices, backed up by a vast literature on their characteristics and performance. The goal of this thesis is to make use of this existing literature on SLs, and usefully apply it in a QC context.

While QC uses much of the same technology as its classical counterpart, there are of course differences in how that technology is used. For example, quantum key distribution (QKD) encodes information on phase-randomised pulses with single-photon level intensities. Another example is quantum random number generation (QRNG), where phase noise in SLs is used as

a source of quantum randomness. These and other unique use cases of SLs have not been fully explored by the existing literature. But the same tools and techniques used to study SLs in classical communications can also be applied to study SLs is QC. In this thesis, we introduce the most relevant analytical and numerical tools to study SLs in QC. We then provide two concrete demonstrations, in Chapters 4 and 5, of using these tools to improve the performance and security of QKD and QRNG.

1.1 Thesis Overview

This thesis is structured as follows:

In this Introduction, we motivate the need for quantum cryptography: QKD provides secure communications even against quantum computers, while QRNGs provide the ultimate guarantee of randomness. We introduce the relevance of semiconductor lasers to these technologies.

In Chapter 2, we provide an in-depth introduction to QKD and QRNG, with an emphasis on their implementation security. We introduce the BB84 protocol, and essential concepts like privacy amplification and security proofs. Implementation security concerns are discussed, featuring potential quantum hacking attacks. We introduce QRNG and associated concepts such as min-entropy and randomness extraction. We emphasise the importance of characterising the physical QRNG hardware to provide stronger guarantees of randomness and security.

Chapter 3 introduces semiconductor laser physics, and the main analytical and numerical tools from the field of classical fibre optic communications which we use to study them. In particular, we introduce the laser rate equations and use them to study key effects like gain-switching, phase noise, and optical injection locking, relevant to quantum cryptography.

Chapters 4 and 5 present the main novel contributions of the thesis. Chapter 4 presents a method of quantifying phase noise in gain-switched SLs based on the laser rate equations. Phase randomisation is crucial to security in both QKD and QRNG. In particular, in QRNG we want to ensure that the output randomness originates from phase noise in the semiconductor laser, and not some other classical process like electronic noise. By quantifying the phase noise from a physical model of the device, we provide stronger guarantees that the device operates as intended, and that the output is genuinely quantum in origin. We back up our simulations with experimental measurements and discuss the relationship between phase noise and performance in QRNGs.

Chapter 5 studies the laser seeding attack (LSA) in QKD, in which an adversary injects light into a QKD transmitter to change the outgoing light in some way that is beneficial to her. In particular, a main effect of the LSA is to lock the phase of the QKD transmitter laser to the phase of an external laser controlled by the adversary. This can potentially give the adversary knowledge of, and even deterministic control over, the phase of the QKD transmitter laser, undermining the security of QKD. In our work, we experimentally quantify the effects of the LSA as a function of the injected optical power. This allows us to in turn quantify the amount of optical isolation required to mitigate the attack, improving the security of QKD. Further, we study the LSA using the laser rate equations by modelling it as a form of optical injection locking. This allows us to simulate other effects of the LSA, such as on the power output of the QKD transmitter laser, which can likewise have a detrimental effect on security.

1.2 Novel Contributions

This thesis studies semiconductor lasers in the context of quantum cryptography. The author has made the following novel contributions:

- Introduce the main theoretical, numerical and analytical tools from the field of classical fibre optic communications and demonstrate how they can be used in a quantum cryptography context.

- Model phase noise in a gain switched laser diode using laser rate equations with experimentally extracted parameters. Typically, phase noise is quantified by measuring the phase at the output of an asymmetric interferometer. Instead, we quantify the phase noise from a physical model of the semiconductor laser, based on the laser rate equations. This provides deeper insight into the underlying physical process, as well as stronger guarantees that the device works as intended within operational limits.

- Quantify the relationship between phase noise and QRNG performance as a function of experimentally-accessible parameters, such as the bias current. This allows us to determine operational limits within which the bias current, or other device parameters, should be set. Determining these operational limits from a physical model of the device, rather than measurements of the device output, again provides stronger guarantees of security.

- Quantify the performance of a partially-phase-randomised QRNG, as a function of the relative phase between both interferometer arms. Phase noise QRNGs are typically operated such that the phase fully randomises between pulses. Instead, we analyse the relationship between QRNG performance and phase noise when the phase is not fully random (i.e. not uniformly distributed). Under partial-phase-randomised conditions, the relative

phase of the interferometer arms becomes an important determinant of performance. We determine the phase noise and interferometer phase conditions which maximise QRNG performance per sample.

- Quantify the effects on phase randomisation of the LSA as a function of the injected optical power. The level of optical power required for a successful attack is a crucial parameter for the security of QKD transmitters, and has not before been quantified. This allows us to in turn quantify the level of optical isolation required to mitigate the attack.

- Reproduce prior published experimental results about the LSA in simulation. We use a laser rate equation model to simulate the LSA as a form of optical injection locking. This allows us to reproduce existing experimental results in the literature, as well as generate new insight into the LSA based on a physical model of the attack.

- Using the rate equation model we quantify, in simulation, the effects of the LSA on the power output of a QKD transmitter under different current driving conditions. We then reproduce these simulation in experiment, demonstrating the accuracy and usefulness of rate equation simulations of the LSA.

1.3 Collaborative Research

The research presented in this thesis is a culmination of not only my individual efforts but also the contributions of various collaborators, whose inputs have been invaluable in shaping the work's final form. This section outlines the specific contributions of my colleagues and co-authors to the research and writing process that led to Chapters 3, 4 and 5.

Text from Section 2 of Ref. [11] served as a starting point for Chapter 3 of this thesis. All

text used in this way was initially drafted by me and edited collaboratively with co-authors. I edited and expanded on this text for inclusion in this thesis.

Text from Ref. [12] served as a starting point for Chapter 4 of this thesis. All text used in this way was initially drafted by me and edited collaboratively with co-authors, with the exception of Section V of the paper, which was initially drafted by Davide Marangon and feeds into Section 4.5 of this thesis. The study was devised in collaboration with co-author Davide Marangon. I carried out all experimental measurements and computational simulations. Davide Marangon carried out the statistical tests of randomness reported in Fig. 4.12 and advised on the interpretation and analysis of experimental and computational results.

Text from Ref. [13] served as a starting point for Chapter 5 of this thesis. All text used in this way was initially drafted by me and edited collaboratively with co-authors. The study was devised in collaboration with co-authors Davide Marangon, Raymond Smith and Robert Woodward. The measurement shown in Fig. 5.5 was devised in collaboration with Davide Marangon. Discussions with Raymond Smith led to the measurement and discussion around Fig. 5.6. Code written by Robert Woodward served as a starting point for the simulations carried out in Section 5.4. I carried out all measurements and computational simulations.

1.4 Note on terminology

In the literature the term "quantum cryptography" is often used to mean "quantum key distribution". In this thesis we use the term quantum cryptography more broadly, to refer to any application of quantum mechanics in a cryptographic task. In particular, both quantum key distribution *and* quantum random number generation fall under this term.

The term "quantum communications" is also used to refer to encrypted communications

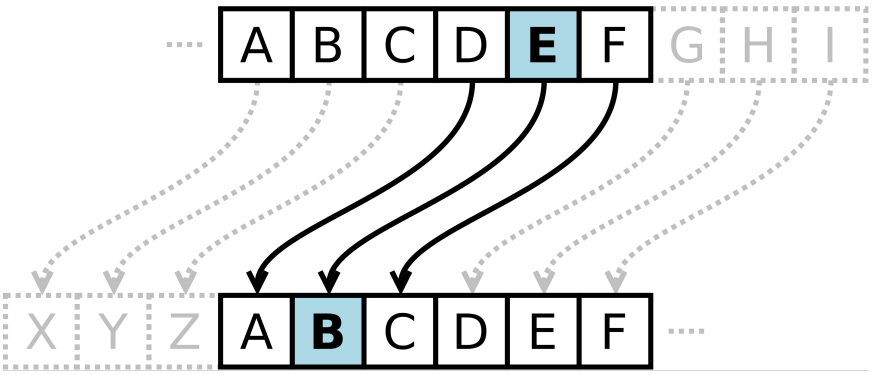

Figure 1.1: The Caesar cipher is one of the simplest encryption techniques. Two communicating parties agree on an integer number, the "key" k. To encrypt a message, each letter in the message is substituted by a letter k positions up the alphabet, and vice versa for decryption. This cipher is easily cracked using a brute force attack, or frequency analysis of the letters.

secured by quantum key distribution.

1.5 Classical Cryptography

To motivate the need for quantum cryptography, we first give an overview of classical cryptography. Parts of the content in this section and the next have been previously published in [14].

Cryptography has been used since ancient times to send and receive private messages. A famous example is the Caesar cipher, which works as follows: two people who want to exchange secret messages, we may refer to them as Alice and Bob, agree in private on a secret number which we call the 'key'. Before sending a message, Alice shifts each letter by a certain number of places up the alphabet, determined by the value of the key. For example, if the key was 1, and the message was "Hello", then Alice would first convert her message to "Ifmmp", since I is the next letter in the alphabet after H, f comes after e, and so on. Once Bob receives the message, he will shift each letter the same number of steps *down* the alphabet, from I to H, f to e, and so on, to recover the original message.

The Caesar cipher is a simple encryption technique, and is easily cracked. However, the underlying principle, i.e. two people using a shared private key to encrypt and decrypt their communications, is still used in modern encryption methods. This form of cryptography, in which the same key is used to encrypt and decrypt the secret message, is known as symmetric-key cryptography. The problem with symmetric-key cryptography is that in order to establish the secret key, the two communicating parties, Alice and Bob, have to meet in person or use a trusted courier, neither of which is a practical solution for securing the vast amount of information that is nowadays sent over the internet[1]. A solution to this "key distribution problem" was discovered in the 1970s, and is known as public-key cryptography. In public-key cryptography, the keys that are used to encrypt and decrypt the communications are different, but mathematically related. The key which is used to encrypt messages is made public, while the key used to decrypt messages is kept private. In this way Bob can send Alice his public key, which can be seen by anyone, for her to encrypt her messages with. She can then send her encrypted message to Bob and, crucially, only he will be able to decrypt it, since only he has the corresponding private key.

Since the keys are mathematically related, it is important that no eavesdropper is able to figure out the private key given the public key. The mathematical problem for doing this needs to be 'intractable', that is, very difficult and time-consuming. For example, the mathematical problem that guarantees the security of the widely used public-key RSA protocol is factoring: the process of finding the prime factors of a large number [15]. In RSA encryption, Alice can generate 3 large numbers that satisfy the following relationship:

$$(m^e)^d \equiv m \pmod{n} \tag{1.1}$$

[1]To ensure a high level of security, it is important to regularly change the secret key. For this reason Alice and Bob can't simply meet once and reuse the same key indefinitely.

where m is the message, and d is prime. The numbers (n, e) are the public key, and can be sent to Bob via an unsecured channel. The number d is kept private. Bob encrypts his message by creating the ciphertext as follows

$$c \equiv m^e \pmod{n}. \tag{1.2}$$

Alice can recover m from c by using her private key exponent d by computing

$$c^d \equiv (m^e)^d \equiv m \pmod{n} \tag{1.3}$$

The security of RSA rests on the fact that it is very difficult to find d, given n, e and m. It would take modern computers thousands of years to factor the public keys used in RSA encryption, which is why the communications are considered secure. If an eavesdropper were able to quickly factor large numbers, then they would be able to break RSA encryption since they could extract the private key from the public one. Although there are good reasons to think that factoring really is an intractable problem, there remains the possibility that a mathematical or technological breakthrough will allow us to quickly factor large numbers. Indeed, in 1994, the physicist Peter Shor showed that quantum computers will be able to quickly factor large numbers as well as other mathematical operations currently used in public-key cryptography [16], [17]. This means that, in a future with sufficiently advanced quantum computers, currently used public-key cryptography is at risk. And not only are our future communications at risk: quantum computers threaten our current communications too. Public keys, by definition, can be recorded and stored by anyone, along with the encrypted messages. In this way an eavesdropper could record encrypted private communications and corresponding public keys and wait for a sufficiently powerful quantum computer to become available. They could then

use the quantum computer to obtain the private key and decrypt the communications. This is known as 'retrospective decryption' and all public-key cryptography protocols are susceptible to this attack.

In light of the threat posed by quantum computers to currently used public-key cryptography methods, new public-key algorithms have been developed that rely on mathematical operations which are believed to be intractable even to quantum computers. These newer algorithms go by the name of "post-quantum cryptography" (PQC) and are a promising solution to the quantum computing threat. However, even with PQC, the possibility remains that mathematical problems that we once thought intractable, even for quantum computers, turn out not to be.

1.6 Quantum key distribution

Quantum key distribution (QKD) provides an alternative solution to the key distribution problem. Unlike public-key cryptography, it does not rely on the conjectured difficulty of carrying out certain mathematical operations. Rather, QKD is a fundamentally different approach, based on the principles of quantum mechanics [1], [18], [19].

1.6.1 The Intuition

QKD works by encoding information on single photons, which are transmitted through optical fibres like the ones used for conventional fibre optic communications. When storing information on photons, that information is referred to as *quantum information*, since photons are quantum objects. The security of QKD is guaranteed by two unique features of quantum information:

- Quantum information cannot be copied, due to the no-cloning theorem.

- Quantum information cannot be measured or observed without introducing some disturbance and changing it in some detectable way.

In this way, if Alice sends Bob a secret key using quantum information, they can be sure that, first, no one is able to copy the key, and second, no one is able to measure the key without them detecting some disturbance and aborting their communications. Crucially, quantum mechanics and these two properties of quantum information are fundamental theories in physics. This makes QKD resilient to any future advances in technology or mathematics since, unlike public-key cryptography, it does not make any assumptions about the intractability of certain mathematical operations, or about the technology available to potential eavesdroppers, like quantum computing.

Clearly, QKD offers a compelling solution to the key distribution problem, secure against any current or future technological or mathematical breakthroughs. The main challenges that QKD faces in becoming a widely adopted technology revolve around practicality. QKD relies of specialised hardware and electronics that must be integrated into our telecommunication infrastructure.

1.6.2 Practical Challenges in Quantum Key Distribution

The practical challenges faced by QKD can be divided in three parts: performance, cost and implementation security [20].

Performance

A central challenge in implementing QKD over long distances and at high communications rates is the 'transmission loss' in optical fibres: approximately nine out of ten photons are lost for every 50km of fibre they travel. In conventional communications this problem is easily solved: optical signals can be amplified at regular distance intervals using 'repeaters', allowing us, for example, to send signals from Europe to the American continent through underwater optical fibres. However, the process of amplifying an optical signal can be thought of as making extra copies of the photons to counteract the transmission losses. The no-cloning theorem states that quantum information cannot be copied, which makes it challenging to develop repeaters for quantum information. Although it is an active area of research, currently QKD cannot rely on quantum repeaters to send quantum information over long distances. This means that the range of QKD is limited and there is a trade-off between distance and the communication rate: the longer the distance between Alice and Bob, the fewer photons sent by Alice will reach Bob, slowing the communication rate.

Much of the research in QKD has been devoted to increasing the distance and communication rate. Over the past two decades, there has been great progress on both fronts: record distances for QKD have increased roughly tenfold from around 50km to current state-of-the-art demonstrations reaching distances over 500km in optical fibre [21], [22]. These improvements are due to advances in the QKD hardware as well as to the development of newer and more efficient theoretical protocols, like Twin-Field QKD [23]. For longer distances QKD needs to rely on repeaters [24]. We saw that quantum repeaters are not yet available, but by linking several QKD systems one after the other we can achieve a similar result. The drawback is that at every link, or node, the secret key is revealed. Therefore, we need to ensure that no eavesdropping

can occur at these nodes. Until quantum repeaters become available, trusted nodes will be the main, albeit imperfect, solution for long distance QKD.

Communication rate is another parameter where QKD falls short compared to classical communications. Current classical optical communications deliver speeds on the order of 100 Gbit/s, whereas QKD communications achieve rates in the range of Mbit/s. QKD is only used to distribute the secret keys used for encryption and not the private communications themselves, so the communication rate requirements for QKD are lower. However, increasing the communication rate of QKD is 'arguably the most pressing task in order to widen the applicable areas of QKD technology' [20].

Cost

QKD secured communications require specialised hardware and will undoubtedly cost more to develop than the PQC alternative. As QKD moves out of the lab and towards commercialisation and real-world use, cost-effectiveness is becoming an increasing focus of QKD research efforts. Two results are particularly promising: first, it has been demonstrated that QKD can be performed on the same optical fibres and at the same time as high-traffic classical communications [25]. QKD signals are so faint that there is no negative consequence for other users of these fibres. In this way QKD can make use of existing optical fibre networks, removing much of the need for expensive new optical fibre connections. Second, QKD components are being integrated onto semiconductor chips similar to the ones used in computers and mobile phones [26], [27]. By leveraging advances in semiconductor device manufacturing, QKD chips can be mass-produced at low cost and with extremely small footprints. Chip-based QKD will lower costs and allow for easier integration with conventional computers and communication systems.

Implementation Security

The theories which prove the security of QKD-based communications inevitably must make certain assumptions about the physical devices used to implement QKD. Such devices are often assumed to be ideal, but may in practice display imperfections which could undermine the overall security of the system. The security implications of this gap between theoretical proofs, and physical implementations of QKD, is referred to as *implementation security*. Given that QKD makes claim to the highest levels of security for encrypted communications, it is important that implementation security issues are studied and addressed[2].

During the last two decades of QKD research there has been a two-sided effort to bridge this gap between theory and practice: on the one hand QKD security proofs and protocols have advanced, making fewer and more realistic assumptions [28]–[30]; on the other, physical QKD systems have moved closer to theoretical requirements by implementing countermeasures to known security vulnerabilities [13], [31].

1.7 Quantum Random Number Generation

The second quantum technology we study in this thesis is quantum random number generation (QRNG) [32], [33]. Again here, quantum mechanics can be leveraged to provide capabilities beyond what is possible using only classical means. QRNG is a closely related technology to QKD: QKD is used to distribute random keys securely. A crucial assumption is therefore that the random keys being distributed are in fact genuinely random. If they are not, then this undermines the security of any communications encrypted with those keys. QRNG is a method

[2]Implementation security is not just an issue for quantum cryptography, but also for classical cryptography. Many security breaches in modern cryptographic systems are due to faulty implementations of otherwise secure cryptographic protocols.

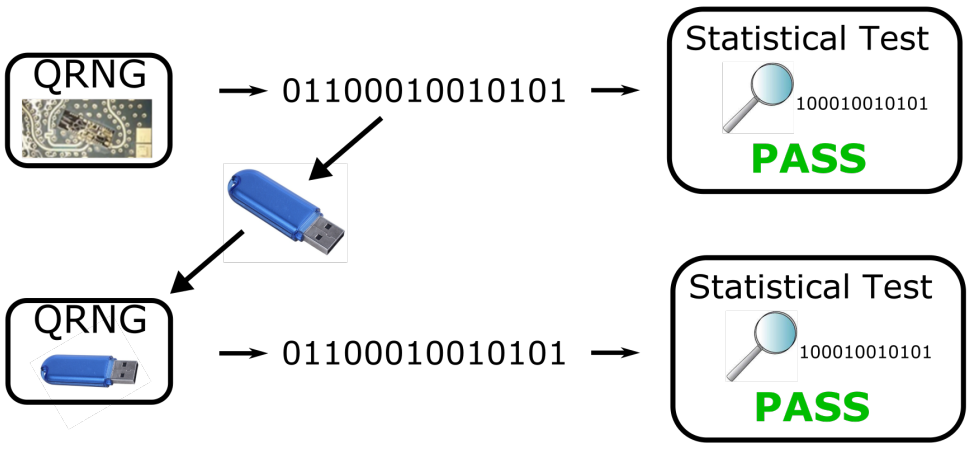

Figure 1.2: The memory stick attack illustrates that whether or not a number is random is not a property of the number itself. If a random number is loaded onto a memory stick and reused, then it ceases to be random. Statistical tests of randomness can therefore only determine whether a number is *not* random, since a memory stick RNG will pass any test.

for generating random keys from fundamentally unpredictable quantum processes, and can provide greater guarantees of randomness than comparable classical RNGs. To motivate the need for QRNG, we therefore start with an overview of classical random number generation.

1.7.1 The Memory-Stick Attack

Random numbers are an essential resource for many applications including Monte Carlo simulations, cryptography, and gambling. For each application, the requirements on the random numbers are different. We can differentiate between two properties of random numbers: their statistical randomness, and their unpredictability. Applications such as Monte Carlo simulations only require that the numbers be statistically random. That is, we only require that the numbers not contain any recognisable patters or regularities. For cryptographic applications, however, it is also essential that the numbers be unpredictable. That is, nobody should be able to predict the next number in a sequence of random numbers.

To illustrate this distinction, consider the so-called "memory stick attack" of random num-

ber generation [34]. In this attack, an eavesdropper Eve generates a large quantity of random numbers from a genuine random number generator, and stores them on a memory stick. She then packages the memory stick to make it look like a genuine random number generator, and sells the device to Alice who uses it to generate the random keys needed to encrypt her communications. However, instead of generating random numbers, the device simply outputs the sequence of numbers stored on the memory stick, which Eve has full knowledge of. Crucially, the output of Alice's device will "look" completely random, since it was originally generated from a genuine random number generator. The only way Alice can realise that her device is not actually generating random numbers is by looking inside and verifying for herself that the numbers come from a memory stick. We can say that the output of the device is statistically random, since it doesn't contain any patterns or regularities. However, it is clearly not unpredictable, since Eve can predict every number coming out of the device.

The memory stick attack illustrates that whether a number is random or not is not a property of the number itself, but rather of how that number was generated. The only way for Alice to verify that her device is producing genuine random numbers is for her to open it up and see for herself. It is not sufficient to just check the output for signs of non-randomness.

For certain applications, like Monte Carlo simulations, statistical randomness is all that is required. It does not matter for the purposes of a computer simulation whether anybody can predict the random numbers. However, for cryptographic applications, or lotteries and gambling, unpredictability is crucial.

1.7.2 Pseudo vs True Random Number Generators

Random numbers can be generated by one of two methods. The first method is to measure some random physical process, like thermal noise in electronic components, or atmospheric noise from a radio receiver. This method is known as "true random number generation" (TRNG) or "hardware random number generation" (HRNG). The second method, known as "pseudo random number generation" (PRNG) instead relies on mathematical algorithms to produce a sequence of seemingly random numbers, starting from a smaller "seed" random number. As the name suggests, the output of a PRNG is not truly random because it is completely determined by the mathematical algorithm and the seed used to initialise it[3]. We can say that the numbers generated from a PRNG have high statistical randomness, but lower unpredictability.

Although it may seem that TRNGs are strictly better than PRNGs, PRNGs have several unique advantages that make them very suitable for certain applications. They can generate random numbers at very high speeds, are limited only by the computing power available, and they can generate statistically random sequences of numbers in a reproducible manner: if a PRNG is initialised with the same seed number, it's output will always be the same. This is useful for example to ensure that numerical simulations can be reproduced.

Ultimately, the output of a PRNG is only as random as the seed used to initialise it. For this reason, TRNGs are preferable for applications where unpredictability is the main concern. TRNGs measure inherently random physical processes, making their output very unpredictable.

[3]It is conventional to quote von Neumann when first introducing PRNGs: "Anyone who attempts to generate random numbers by deterministic means is, of course, living in a state of sin."

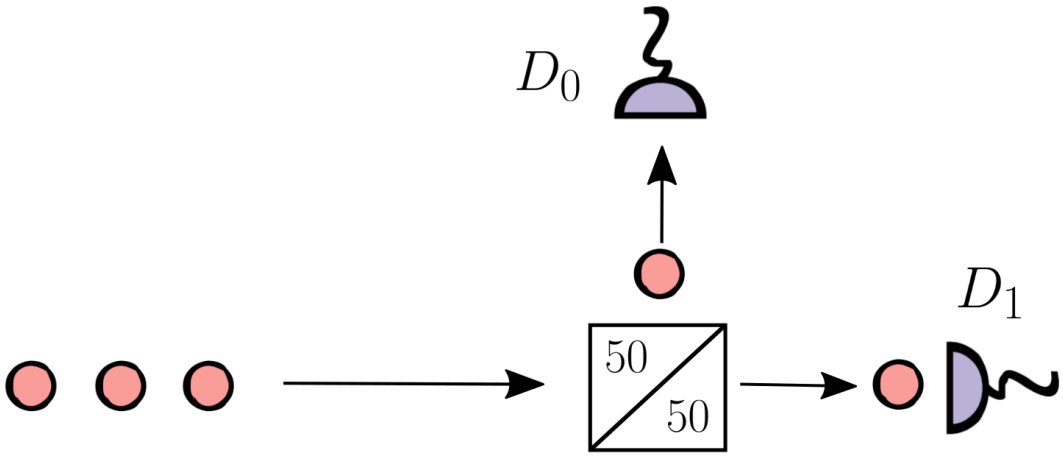

Figure 1.3: One of the conceptually simplest QRNGs consists of a symmetric beam splitter, a single photon source, and two single photon detectors. At the output of the beam splitter, the single photons are in an equal superposition of states corresponding to having been reflected or transmitter. Measuring this superposition will yield one state or the other with 50% probability and can therefore be used to generate unbiased random bits. The measurement is inherently quantum in nature, and there is no amount of information which could let any observer, or eavesdropper, predict the outcome of each measurement before it happens.

1.7.3 Quantum Random Number Generators

QRNGs are a subset of TRNGs. Like TRNGs, QRNGs generate random numbers by measuring an unpredictable physical process. QRNGs are unique in that they measure unpredictable *quantum* processes. For example, a simple QRNG could consist of a source of single photons directed at a 50:50 beam splitter [35], [36]. After the beam splitter, the photons will be in an equal superposition of positions: half of the wavefunction will exit each of the beam splitter outputs, call them output 0 and output 1. By placing photodetectors at each output, we can measure the position of the photon. If the photon is detected at output 0, the QRNG can output a 0, and likewise for output 1.

The scheme we just described might be thought of as essentially equivalent to a coin-flipping machine. Much like flipping a coin, there is a 50:50 probability of obtaining a 0 (heads) or 1 (tails). But in the coin flip, the 50:50 probabilities arise not from any fundamental properties of coins, but rather from a lack of knowledge. Given sufficient information about the initial

position and velocity of a coin we can, in principle, predict which side it will land on. The fact that we assign a 50% probability to each outcome is simply because of a lack of information. In contrast, in the case of photons arriving at a beam splitter, there is no amount of information we could use to predict which output the photon will exit. The event is fundamentally unpredictable, as described by quantum mechanics.

1.7.4 Practical Challenges in QRNG

A central question that QRNGs must answer is: how do we know that the output of a QRNG genuinely originates from a quantum process? A QRNG consists of many components apart from the source of quantum randomness: there are electronics, optical components and external sources of randomness such as ambient temperature. The output of a QRNG will be affected by all of these components, such that the original signal obtained by measuring a quantum process can be diluted into a mixture of classical and quantum noise at the output. If QRNGs want to claim true quantum randomness, the quantum noise must be quantified and isolated from the classical noise.

For example, it could be the case that the reflection to transmission ratio of a beam splitter depends on the temperature of the device. If such a beam splitter were used in a QRNG such as the one described above and in Fig. 1.3, then the output of the QRNG would be a mixture of the quantum process (the 50:50 percent chance of being transmitted or reflected) and classical noise (the effects of temperature on the reflection-transmission ratio). Under the most stringent of security analyses, the user of a QRNG must assume that any source of classical noise is known to, and even controlled by, a malicious eavesdropper. For this reason, in order to claim true randomness of quantum origin, a QRNG must quantify and distil the quantum noise from the

quantum-classical mixture, such that no amount of knowledge of or influence over the classical noise will give an eavesdropper information about the output numbers.

1.8 Semiconductor Lasers

Semiconductor lasers are key components of both QKD and QRNG systems. QKD uses semiconductor lasers as a source of photons by attenuating the laser output to the single-photon level. In QRNG, although not all implementations use lasers, most modern high-performing QRNGs are optical and have semiconductor lasers as a key component.

However, semiconductors have many other applications, notably in the field of fibre-optic communications. They have therefore benefitted from decades of research into their characteristics and performance, which has resulted in low-cost, high-performance devices. Semiconductor lasers are small, energy efficient, cheap, and can be modulated at GHz rates. All of this has enabled $>$100 GBit/s fibre-optic communications, and the fast internet speeds many of us enjoy.

Quantum cryptography, both QKD and QRNG, shares many of the same technical requirements for semiconductor lasers as classical fibre-optic communications: high bandwidth, low linewidth, emission frequencies that minimise loss in silica fibres, etc. Quantum cryptography therefore benefits greatly from the advanced development of this technology.

However, quantum cryptography also has some unique requirements, which is does *not* share with classical communications. For example, for certain applications, quantum cryptography uses phase randomised signals, requires pulses of light with low chirp for better visibility interference, among others. There are also unique implementation security issues related to semiconductor lasers in quantum cryptography. There exists a whole class of 'attacks' on

quantum cryptography systems which target the laser.

The rest of this thesis will use the knowledge, tools and techniques from the field of classical fibre optic communications, and apply them to the study of semiconductor lasers in quantum cryptography systems.

1.9 Summary

We have motivated and briefly introduced the main topics of this thesis, namely, quantum key distribution, quantum random number generation and semiconductor lasers.

In the next two chapters we will give a more technical and rigorous description of these technologies before presenting the main results of the thesis.

Chapter 2

Implementation Security of Quantum Cryptography

In this chapter we provide an introduction to quantum cryptography, both QKD and QRNG, with an emphasis on *implementation security*.

Implementation security refers to security vulnerabilities that arise due to imperfections in the physical implementation of a quantum cryptography system, as opposed to issues with the underlying theoretical protocol [37]. These imperfections can come from components like lasers, detectors, optics, and electronics, which do not perform exactly as assumed in the theoretical security proofs. Implementation issues can lead to side channels that leak information to an eavesdropper [38]–[41].

In this thesis, we focus specifically on laser-related issues in quantum cryptography transmitters, such as the laser seeding attack in Chapter 5. By modelling and characterising the laser behaviour through laser rate equations, we aim to provide a better understanding of these lasers and how to minimise associated security risks. With a more rigorous treatment of lasers and other components, we can close the gap between the theory and practice of quantum cryp-

tography, leading to more secure real-world implementations.

2.1 Implementation Security of QKD

As QKD has moved closer to commercialisation, implementation security has taken on a greater importance. During the last two decades of QKD research, there has been a two-sided effort to bridge this gap between theory and practice. On the one hand, QKD security proofs and protocols have advanced, making fewer and more realistic assumptions. On the other hand, physical QKD systems have moved closer to theoretical requirements by implementing countermeasures to known security vulnerabilities. In this section, we will explore the current state of implementation security in QKD and discuss some of the challenges and opportunities for further research in this area.

2.1.1 Introduction to QKD

QKD is best explained by example. In the following section we describe the first and still most widely used QKD protocol: BB84[1].

BB84

Alice prepares photons in one of four states $|H\rangle$, $|V\rangle$, $|D\rangle$, $|A\rangle$, choosing randomly, and sends them to Bob. In the original implementation of BB84, these states corresponded to horizontal, vertical, diagonal and anti-diagonal polarisation states respectively. However, modern implementations of QKD use other degrees of freedom to encode information [43]–[45]. Nonetheless,

[1]Named after Charles Bennett and Gilles Brassard who developed the protocol in 1984 [42]

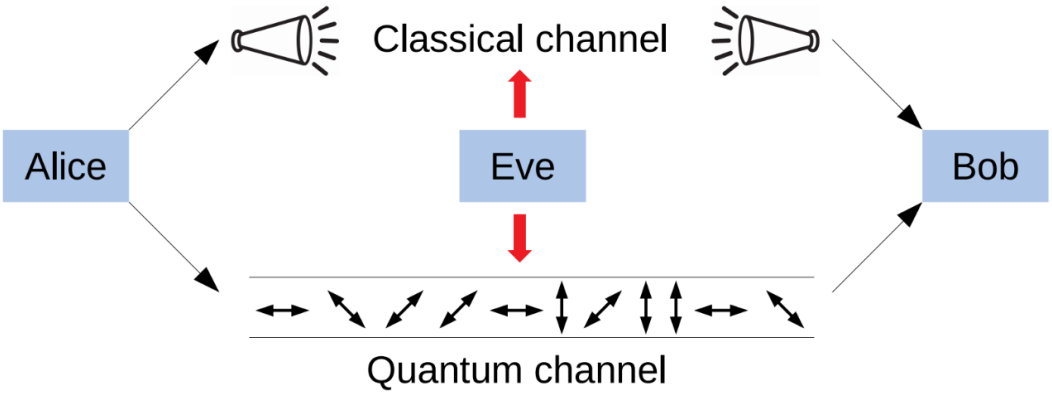

Figure 2.1: Alice sends Bob polarised single photons in on of four states at random. After the quantum states have been received, she tells Bob via an authenticated public channel which basis she used for each photon. No assumptions are made about Eve, who can listen in to the classical communications, and can intercept and measure any of the quantum states. If she does so, errors will be introduced into the shared secret key, which can be detected and the communications aborted.

describing BB84 in terms of polarisation is pedagogically useful. The four states are related by:

$$|D\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle + |V\rangle\right) \tag{2.1}$$

$$|A\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle - |V\rangle\right) \tag{2.2}$$

and therefore the states form two orthogonal bases, $\{|H\rangle, |V\rangle\}$ and $\{|D\rangle, |A\rangle\}$, in a 2-dimensional Hilbert space. We assign the bit value 0 to both $|H\rangle$ and $|D\rangle$ and the value 1 to $|V\rangle$ and $|A\rangle$. Bob then measures the photons he receives in one of the two bases $\{|H\rangle, |V\rangle\}$ or $\{|D\rangle, |A\rangle\}$, choosing the basis randomly. After receiving all the qubits, Bob can use a classical channel to tell Alice which basis he used to measure each photon and Alice can tell Bob on which occasions he (by chance) measured in the correct basis. On these occasions Alice and Bob will agree on the state of the qubit and so they share a common bit sequence which can be used as a secret key.

Mutually Unbiased Bases

To give some intuition of the security of this protocol consider the case where an eavesdropper, conventionally called Eve, intercepts the photons sent by Alice in an attempt to obtain information about the secret key. First, note that the bases used by Alice and Bob are mutually unbiased. Two bases $\{|a_m\rangle\}$ and $\{|b_n\rangle\}$ are said to be mutually unbiased if

$$|\langle a_m \mid b_n\rangle|^2 = \frac{1}{d} \tag{2.3}$$

for any values of n and m and where d is the number of vectors in each basis, called the dimension [46].

This means that for a system prepared in a state belonging to one of the bases, the outcome of a measurement with respect to the other basis will be random. Note that the bases we defined above in Eqs. 2.1 and 2.2 are mutually unbiased. We can see that the basis states obey the condition 2.3, for example:

$$|\langle H \mid A\rangle|^2 = \left|\frac{1}{\sqrt{2}}(\langle H \mid H\rangle - \langle H \mid V\rangle)\right|^2 = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}, \tag{2.4}$$

and similarly for the other states, where in this case $d = 2$. So the bases $\{|H\rangle, |V\rangle\}$ and $\{|D\rangle, |A\rangle\}$ are mutually unbiased. In this way if Eve measures a photon in the wrong basis she will not gain any information and instead will introduce a disturbance by projecting the photon onto the basis she measured in.

Of course, she may get lucky and measure in the correct basis. On average, she will choose the correct basis 50% of the time, and so if she measured all of the signals between Alice and Bob, she would obtain 50% of the information of their shared key. However, when she measures

in the wrong basis, she will collapse the superposition into the wrong state 50% of the time, for an overall error rate of 25%. By monitoring the quantum bit error rate (QBER), Alice and Bob can chose to abort their communications if they detect an error rate above some threshold.

However, still Eve could measure only some of the signals between Alice and Bob, so as to only increase the QBER up to this threshold. To counter this Alice and Bob can implement privacy amplification, which we explain in 2.1.2.

No-Cloning Theorem

A second property of quantum information that is crucial to security is that quantum information cannot be copied [47], [48]. That is, given a quantum state, it is impossible to create a new independent and identical quantum state. If this were not the case then instead of directly measuring the quantum signals between Alice and Bob, Eve could create copies of them. With enough copies, Eve could accurately reconstruct the original quantum state via quantum state tomography, and obtain full knowledge of the secret communications [49]. Box 1 provides a simple proof of the no-cloning theorem.

Box 1: No-Cloning Theorem

Proving the no-cloning theorem is straightforward. Following Ref. [50]: suppose we have a quantum copying machine, which takes an unknown quantum state $|\psi\rangle$ and an arbitrary 'blank' state $|b\rangle$ onto which the unknown state will be copied. The initial state of the copying machine is therefore

$$|\psi\rangle \otimes |b\rangle \tag{2.5}$$

Some unitary operation U then, ideally, implements the procedure:

$$|\psi\rangle \otimes |b\rangle \xrightarrow{U} U(|\psi\rangle \otimes |b\rangle) = |\psi\rangle \otimes |\psi\rangle \tag{2.6}$$

Now, suppose that this copying procedure works for two different quantum states $|\psi\rangle$ and $|\phi\rangle$. Then

$$\begin{aligned} U(|\psi\rangle \otimes |s\rangle) &= |\psi\rangle \otimes |\psi\rangle \\ U(|\varphi\rangle \otimes |s\rangle) &= |\varphi\rangle \otimes |\varphi\rangle \end{aligned} \tag{2.7}$$

Taking the inner product of both equations gives

$$\langle\psi \mid \varphi\rangle = (\langle\psi \mid \varphi\rangle)^2 \tag{2.8}$$

But $x = x^2$ has only two solutions, $x = 0$ and $x = 1$, so either $|\psi\rangle = |\varphi\rangle$ or $|\psi\rangle$ and $|\varphi\rangle$ are orthogonal. Thus a cloning device can only clone states which are orthogonal to each other, and therefore a general quantum cloning device is impossible [50].

2.1.2 Theoretical security

Proving the security of QKD is far from trivial, and has been an active area of research since the inception of this technology. There are two key complicating factors. First, theoretical QKD protocols are implemented using imperfect hardware: imperfect lasers, imperfect detectors, etc. A security proof must take into account all of these imperfections. Second, in QKD, the presence of an eavesdropper is detected by monitoring the error rate in Alice and Bob's shared key. However, there are many other sources of errors other than eavesdropping, such as noise in the quantum channel. A security proof must guarantee the security of the communications,

even when Alice and Bob cannot tell whether their error rate is due to an eavesdropper, or simply random noise.

Privacy Amplification

A main challenge in *proving* the security of QKD is the inability of Alice and Bob to differentiate between errors due to interference by Eve and errors simply due to noise in the channel. In fact Alice and Bob should assume that *all* errors are due to Eve since in theory, without making assumptions about the technology available to her, she could replace a noisy channel with a perfectly noiseless one. So, in practice, the secret key shared by Alice and Bob will contain errors which they must assume are due to interference by Eve. Using (classical) error correction [51] they can remove the errors. At this stage, however, Eve may still have information about the key, that she could have obtained by measuring the qubits in transit to Bob. To reduce Eve's information, Alice and Bob can use *privacy amplification* [52] to reduce Eve's information about the key to an arbitrarily small amount, at the expense of shortening the length the shared key. Box 2 provides two simple examples of error correction and privacy amplification methods. Fig. 2.2 provides a visual summary of the overall process to convert the initial sifted key, which Eve has some information of, to a shorter, but secret key which Eve has no information of.

Box 2: Error Correction & Privacy Amplification

Simple Error Correction

A simple example error correction: Alice announces the parity of pairs of bits, then Bob announces whether his corresponding bits agree. They both discard the bit pairs that don't [1, p. 151].

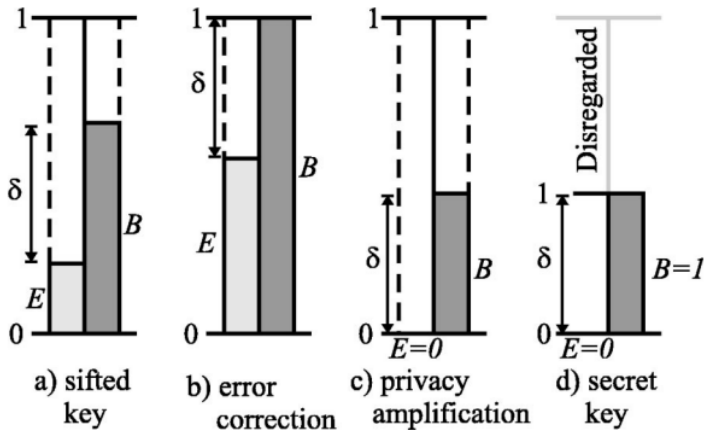

Figure 2.2: Once the quantum states have been received, and the preparation bases revealed, Bob does not have full knowledge of Alice's key due to errors during the transmission. These can be corrected with error correction, giving Bob full knowledge of Alice's key, and importantly also increasing Eve's knowledge of the key. Privacy amplification is used to reduce the length of the key in such a way that Eve's information approaches zero, while Alice and Bob retain a shared secret, but shortened, key. Reproduced from Ref. [1].

Simple Privacy Amplification

A simple example of privacy amplification: Alice and Bob replace their shared key with the XOR value of randomly chosen bit pairs. In this way if Eve knows the bit value of only one bit in a pair, she will have no information about the XOR value. And even if she knows the value of both bits with some probability $0.5 < p < 1$, her knowledge of the XOR value will be: $p^2 + (1-p)^2$ which is less than p [1, p. 151].

A security proof of QKD then needs to answer: "Up to what QBER can Alice and Bob apply error correction and privacy amplification to their classical bits?" [1, p. 185]. Shor and Preskill [53], building on the work of Mayers [54] and Lo and Chau [55], proved the security of the BB84 protocol showing that Alice and Bob are able to distil a secret key as long as the QBER is below 11%.

It is important to stress that the above-mentioned proofs still make important and unrealis-

tic assumptions about QKD, namely that the hardware is ideal. Of course in practice nothing is ideal, and much of the research into QKD has been aimed at "closing the gap" [38, p. 1307] between idealised security proofs and practical experimental implementations. Progress has been made on both fronts: newer protocols and security proofs make less experimentally demanding assumptions [28], [29], [56]–[58] and implementation vulnerabilities are being identified and addressed.

2.1.3 Implementation security

Implementation security can be considered the study of "side-channels". These are flaws in the implementation of a cryptographic protocol (classical or quantum), which leak information to an eavesdropper. A famous example is the first experimental demonstration of quantum key distribution [59]: Bennett et al. used a Pockels cell (to control the polarisation of photons) that made an audible "click" whenever it changed settings, from which an eavesdropper could figure out the secret key[2]. A more serious example is the so-called photon-number-splitting (PNS) attack [61], [62]: the BB84 protocol uses single photons for secure key distribution, yet reliable and high-performance single photon sources are not yet available. For this reason most QKD implementations use laser pulses which are attenuated to below the single-photon level. Laser light is a good approximation to a coherent state, which follows a Poisson number distribution. Most pulses then contain either zero or one photons, but sometimes two or more. This opens the possibility for Eve to intercept and measure one of the photons in a multi-photon pulse, leaving the rest intact, obtaining information about the key without introducing errors. The PNS attack has been addressed by newer protocols and security proofs [56], [57], so in that

[2] "This lead Charles Bennett to notice that the QKD system was only secure against an eavesdropper who happened to be deaf." [60]

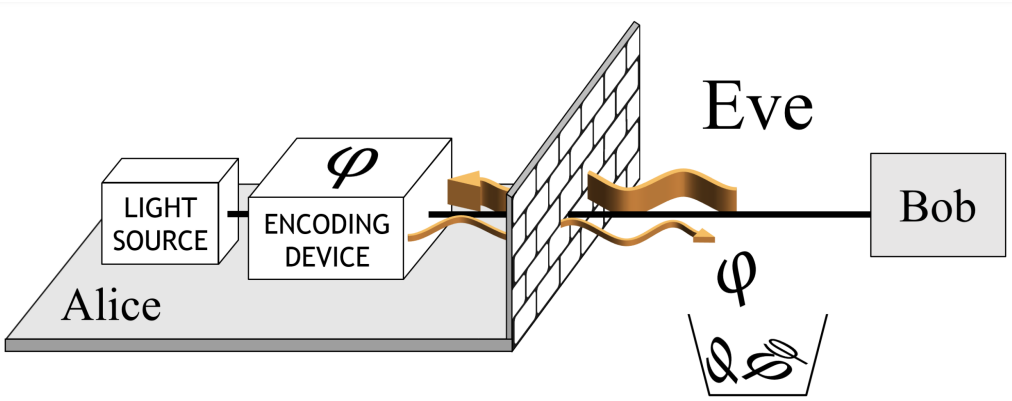

Figure 2.3: Eve injects light into the transmitter (Alice) and measures the back reflected light to gain information about the settings of the encoding device. Reproduced from Ref. [63].

sense it is no longer an issue in implementation security.

However, there are other side-channels which have not, or cannot, be incorporated into security proofs. In these cases it is necessary to implement a countermeasure. As an example, in the so-called Trojan horse attack (THA) Eve injects light into Alice's transmitter and measures the back-reflected light to gain information about the settings of the encoding device (see Figure 2.3). Possible countermeasures include using optical isolation to prevent light entering the transmitter, or installing a "watchdog" detector to monitor the incoming light and aborting the protocol if a THA is detected. However, it is hard to claim these countermeasures completely remove any possible information leakage to Eve. For example optical isolators only have a finite attenuation and both optical isolators and detectors are wavelength dependent, opening the possibility for Eve to launch her attack using a different wavelength. But for a countermeasure to be successful, completely removing a side-channel is not necessary. We saw that privacy amplification gives us a way to reduce Eve's information (at the cost of shortening Alice an Bob's shared key). As long as the amount of information leakage is below some threshold (in a similar way to how in BB84 the QBER must remain below 11%), we can use privacy amplification to reduce Eve's information. The question then becomes how much privacy amplification is

needed.

In the ideal case we are able to put strict bounds on the information leakage. In ref. [63] Lucamarini et al. put an upper bound on the amount of light Eve can inject into a QKD transmitter by considering the "laser induced damage threshold" of optical fibre. Optical fibres can only carry so much power (per unit area) before becoming damaged, so this limits the amount of light Eve can inject into a transmitter when performing a THA. This in turn limits the maximum information leakage and allows us to estimate the worst-case level of privacy amplification needed to guarantee security.

For other attacks on QKD systems, bounding the information leakage is more problematic. Consider the so-called laser damage attack [64]: shining very bright light on optical isolators can permanently reduce their attenuation. This could lead Alice and Bob to underestimate the amount of information Eve is able to gain through a THA. It is unclear how to quantify the effects of laser damage on optical attenuators. Attacks from the domain of classical cryptography also have to be considered. In all, there remain many implementation security issues and closing these side channels requires substantial future efforts [20]. Table 2.1 gives a summary of the most prominent side-channels and attacks in QKD.

Device Independence

An appealing solution to implementation security issues is so-called device-independent QKD [75], [76]. This refers to protocols for which the security of the communications does not depend on any assumptions about the physical implementation. This means that device independent QKD systems can operate securely as "black-box" devices and their security can be fully guaranteed just by observing the output of the black-box. An end user need not know about, or trust, any of the internal workings of the device for the communications to be secure. Clearly

Table 2.1: A list of prominent side-channels and attacks in QKD.

Security issue / attack	**Description**
Photon-number-splitting attack [61], [62]	When using weak coherent states to communicate, some laser pulses will contain more than one photon.
Trojan horse [65], [66]	Eve injects light into the transmitter and measures the back reflected light to gain information about the encoding device settings.
Detector blinding [67]	By using bright light Eve can in some cases manipulate the behaviour of photon detectors.
Efficiency mismatch [68]	Eve can determine which of two detectors clicked when the two detectors have different efficiencies.
Laser seeding [69], [70]	Eve injects light into the transmitter to modify properties of the outgoing light, e.g. the phase [69] or intensity [70].
Time-shift [71]	When two detectors take different times to respond to incoming light, Eve can determine which detector clicked.
Laser damage [64], [72]	Very bright light can damage optical components which can give an advantage to Eve. E.g. the attenuation of optical isolators can be permanently reduced.
Detector backflash [73], [74]	Avalanche photodiodes commonly used in QKD will sometimes emit photons after a detection event. These can travel back out of the receiver and be detected by Eve.

this is the perfect solution for secure communications. However, device-independent protocols are experimentally challenging and have poor key generation rates, making them impractical.

An interesting compromise between fully device-independent security and practicality is measurement-device-independent (MDI) QKD [77], [78]. In MDI QKD, both Alice and Bob become transmitters and send light pulses to a mid-point receiver, conventionally called Charlie.

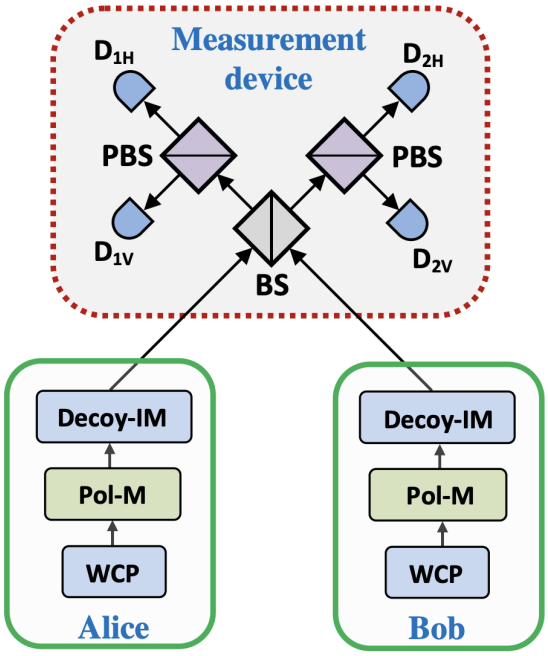

Figure 2.4: In MDI QKD, Alice and Bob send quantum states to an intermediate untrusted node (Charlie), where they interfere. After detection, Charlie can determine and announces whether the states were the same or different. Based on this information, and using error correction and privacy amplification, Alice and Bob can agree on a shared secret key. Reproduced from Ref. [77].

The idea is that Charlie can interfere the light coming from Alice and Bob at a beam splitter from which he can measure the correlation between the bit values, rather than the bit values themselves. He then publicly announces the measured correlations so that Alice and Bob can deduce what the other sent and arrive at a shared key. Crucially, Charlie can be completely untrusted and for this reason the mid-point receiver is sometimes called Eve to bring attention to the fact that the protocol is secure even if an eavesdropper is the receiver.

MDI QKD is a promising solution to a wide class of implementation security vulnerabilities. Many attacks on QKD systems focus on the receiver which is considered to be more vulnerable than the transmitter. Intuitively this makes sense: transmitters prepare quantum states locally by a trusted user and can be optically isolated; measurement devices are by definition meant to receive light from the outside, which might have therefore been prepared by Eve. MDI QKD

sidesteps any potential vulnerability of the measurement device so the focus of implementation security can shift to the (intuitively safer) transmitter.

2.1.4 Randomness

An obvious, yet essential, assumption in security proofs of QKD is that Alice and Bob really do choose the states and bases to send/measure in randomly. Any non-randomness can be exploited by an eavesdropper and undermine the security of the communications. Given that QKD offers the possibility of unconditional security, it is essential that the random number generators used in QKD are cryptographically sound and secure. QRNGs provide the strongest guarantees of true randomness, and are therefore a natural match for QKD.

2.2 Implementation Security of QRNG

2.2.1 Introduction to QRNG

QRNGs generate random numbers by measuring fundamentally unpredictable quantum events. There are many types of QRNG, based on measuring different types of quantum process [79]–[83]. In Chap. 1 we presented a simple QRNG based on measuring whether a single photon was reflected or transmitted at a beam splitter. Another classic implementation of a QRNG consists in measuring the timing of radioactive decay from a radioactive substance [84].

This thesis focuses on so-called phase noise QRNGs, where the quantum process being measured is phase noise in lasers [85]–[94]. Phase noise QRNGs are simple yet high-performance devices, and are therefore one of the most popular implementations of QRNG. In the following we briefly describe this particular type of QRNG before presenting the theoretical concepts

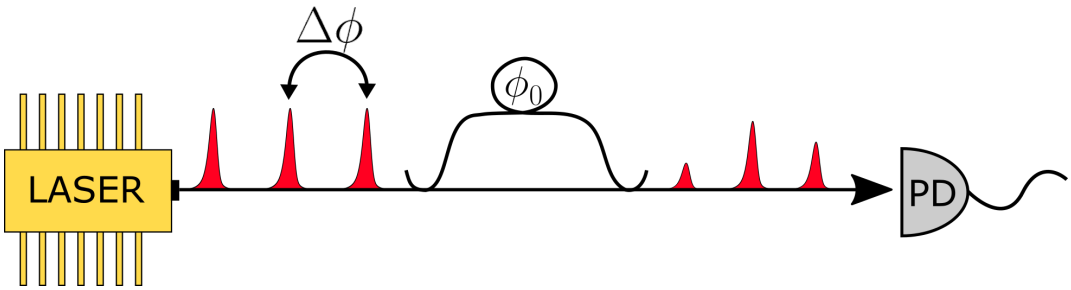

Figure 2.5: A gain switched laser can produce pulses of phase randomised light. The phase cannot be measured directly, but using an asymmetric interferometer successive pulses can interfere converting the phase difference between pulses into random intensities at the interferometer output. The phase difference between pulses is due to spontaneous emission in the laser cavity, which is a quantum effect.

required in general for quantifying and extracting random numbers from a QRNG.

Phase Noise QRNGs

Laser phase noise is a consequence of spontaneous emission [95]. Each spontaneously emitted photon has a random phase that is added to the total electromagnetic field in the laser cavity, leading to random phase fluctuations. These fluctuations can be measured using an asymmetric interferometer to interfere the laser output with a delayed version of itself, as in Fig. 2.5. During this time delay, spontaneous emission events in the laser cavity randomise the phase, leading to the interference of light with a random phase difference at the interferometer output. This converts the random phase into a random intensity, which can be measured and digitised to generate random numbers. The intensity at the output of the asymmetric interferometer is given by

$$I_{\text{out}} = \frac{I_{\text{in}}}{2}\left[1 + \cos\left(\Delta\phi + \phi_0\right)\right], \tag{2.9}$$

where I_{in} is the input intensity, $\Delta\phi$ is the random phase difference between delayed and non-delayed light due to spontaneous emission, and ϕ_0 is the relative phase between both interferometer arms due to the difference in their length. The light intensity is converted into current by

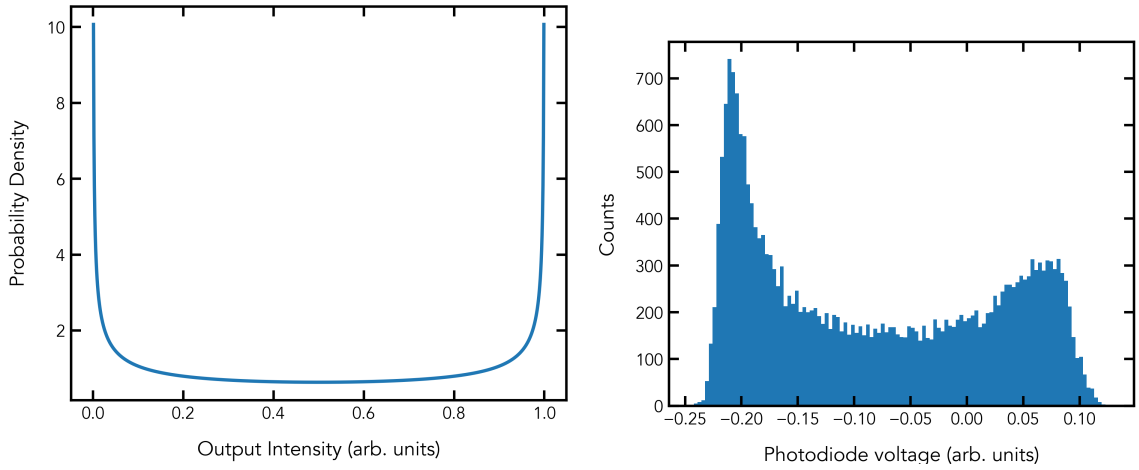

Figure 2.6: The intensity at the interferometer output follows an arcsine distribution (left) in theory. In practice, due to various sources of noise, the measured distribution is flatter and asymmetric (right).

a photodiode (PD) and then digitised using an analogue-to-digital converter (ADC) to generate random numbers.

When $\Delta\phi$ is uniformly distributed, the output intensity I_{out} follows an arcsine distribution, as depicted in Fig. 2.6. This "double peak" distribution can then be digitised using an analogue-to-digital converter (ADC) to generate random numbers. For example, a 3-bit ADC will output a 3-bit number for each measurement, depending on where on the distribution the output intensity was measured.

The output of the ADC will, however, be very biased given the non-uniformity of the underlying distribution. The bit values associated with the lowest- and highest-power measurement, corresponding to the two peaks in the distribution, will occur much more often than the intermediate values. So, although the output of the ADC is a 3-bit number per measurement, the amount of randomness being produced by the QRNG is below 3 bits per measurement.

Clearly then it is necessary to quantify the amount of randomness which is actually being produced, and post-process the biased output bits to achieve a uniform distribution

Entropy

Entropy, in the realm of information theory, is a measure of the unpredictability of a random variable. One of the most fundamental entropy measures is the Shannon entropy. The Shannon entropy quantifies the average unpredictability associated with a random event. A 50:50 coin flip has a large Shannon entropy, since the outcome is maximally unpredictable. A biased coin, say 60% heads 40% tails, has less Shannon entropy, because the outcome is less unpredictable: it is more likely to land on heads. For a discrete random variable X with probability mass function $p(x)$, Shannon entropy, denoted by $H(X)$, is defined as:

$$H(X) = -\sum_{x \in X} p(x) \log_2 p(x) \tag{2.10}$$

On the other hand, the amount of randomness produced by a QRNG is quantified by the *min-entropy*. Unlike Shannon entropy, which provides an average measure of unpredictability over all outcomes, the min-entropy depends only on the most-likely outcome. Specifically, the min-entropy (in bits) of a random variable X is the largest value m having the property that each observation of X provides at least m bits of information. This value is determined by the most likely outcome, since this is the outcome which provides the least amount of information. The min-entropy of X is, therefore, the greatest lower bound for the information content of potential observations of X. It is formally defined as:

$$H_{\min}(X) = -\log_2 \left(P(x)_{\max}\right) \tag{2.11}$$

where $P(x)_{\max}$ the probability of the most likely outcome of the source.

In Chap. 1, we observed that the output of a QRNG comprises a blend of quantum and

classical noise. This is evident in Fig. 2.6, which depicts a real measurement of the distribution of intensities from the interferometer of a phase noise QRNG. Although this measured distribution showcases the "double peak" characteristic of the ideal distribution seen in Fig. 2.6, the actual distribution is broader and flatter owing to various noise sources like laser intensity noise, electronic noise, etc.

At a superficial level, a broader and flatter distribution might appear beneficial, since the probability of the most likely outcome has decreased, and the min-entropy correspondingly increased. However, this increase in min-entropy can be attributed to classical noise sources: phase changes in the interferometer, laser intensity noise, etc. The joint quantum-classical distribution is a convolution of the quantum arcsine distribution, and the arbitrary distribution of the classical noise, which produces a flatter distribution. For quantum random number generation, we must assume that such classical sources of noise are entirely known, or even controlled, by an eavesdropper. To factor in this classical interference along with the quantum randomness, one can utilise the *conditional* min-entropy.

The measured probability distribution in Fig. 2.6 can then be thought of as a joint distribution P_{AE}, where part A of the system is under control of the legitimate user, and part E is under control of the eavesdropper. The conditional min-entropy of A given E, denoted $H_{\min}(A \mid E)$, is defined by:

$$2^{-H_{\min}(A|E)} = \sum_a P_A(a) 2^{-H_{\min}(A|E=e)} \tag{2.12}$$

where

$$H_{\min}(A \mid E = e) = -\log_2 \left[\max_a P_{A|E=e}(a \mid e) \right] \tag{2.13}$$

and quantifies the probability of guessing the outcome of measurements on A given the outcome of measurements on E. In this case, E could be the classical noise known by the eaves-

dropper.

Post-processing

Once the conditional min-entropy has been estimated, we can reduce the size of the generated string to remove any information an Eavesdropper might have, using *randomness extraction*. The goal of a randomness extractor is to convert raw quantum randomness into a uniform and independent sequence of random bits. Despite the intrinsic randomness of quantum processes, the raw data produced by QRNG systems can exhibit biases and correlations due to imperfections in the physical setup or measurement apparatus. In order to achieve the highest degree of randomness and security for cryptographic applications, it is crucial to eliminate such biases and correlations through effective randomness extraction techniques.

The primary objective of randomness extraction is to distil a near-uniform random sequence from the non-uniform input, while preserving the entropy of the source. This process involves the use of algorithms or functions that are designed to remove any discernible patterns or structure in the input data, ensuring the output is as close to uniform randomness as possible.

A simple example of a randomness extractor is the von Neumann extractor. It works by processing adjacent bits in pairs from a raw bit sequence and outputs a single bit for each pair, depending on the input pair values. The extractor follows these rules:

- If the input pair is '01', output '0'
- If the input pair is '10', output '1'
- If the input pair is '00' or '11', discard the pair and output nothing

This method effectively eliminates biases in the input sequence by only considering pairs with different bit values. However, the von Neumann extractor has some notable limitations:

- Dependency on input correlations: The performance of the von Neumann extractor is highly dependent on the input sequence's correlations. If the input data exhibits strong temporal correlations, the output sequence may still contain residual biases.

- Inefficiency: The von Neumann extractor can be highly inefficient, especially when the input sequence has significant biases.

In contrast, more advanced techniques can address these limitations and offer improved performance for quantum randomness extraction. For example, Toeplitz hashing relies on the construction of a Toeplitz matrix, a special kind of matrix with constant diagonals, using the input source as a seed. The extracted random bits are generated by computing the matrix-vector product between the Toeplitz matrix and a vector derived from the input source. Toeplitz hashing is computationally efficient and preserves a significant portion of the input entropy, making it an attractive option for QRNG applications.

Randomness tests

We can test whether the output "looks" random by applying statistical tests of randomness to the generated string. It is important to stress, however, that randomness tests can only tell us whether a string is *not* random. This is illustrated by the "memory stick attack" which was described in Chap. 1. Nonetheless, randomness tests are in important part of ensuring the quality of the generated random numbers.

Randomness tests aim to evaluate the statistical properties of the output sequence, ensuring that it adheres to the expected characteristics of a truly random sequence. Randomness tests are essential in identifying any biases, correlations, or patterns that may remain after applying the randomness extraction techniques.

Several popular test suites have been developed for evaluating the randomness of generated sequences. Some of the most widely used test suites include:

- NIST Statistical Test Suite: Developed by the National Institute of Standards and Technology (NIST), this test suite consists of 15 different tests that analyse various statistical properties, such as frequency, runs, longest runs of ones, and spectral tests.
- TestU01: Developed by Pierre L'Ecuyer and Richard Simard, TestU01 is a comprehensive library of C functions that offers a wide range of tests, including both classical tests and more specialised tests that target specific weaknesses in random number generators.

2.2.2 Trust and Device Independence

In the realm of quantum random number generation (QRNG), the issue of trust remains a critical concern. Trust refers to the reliance placed on the devices and components involved in the QRNG process, including the lasers, detectors, and electronics, to function as expected. A noteworthy example of a trust-related vulnerability is the memory stick attack, wherein an entire device is compromised.

A potential adversary, Eve, could exploit this trust by controlling or manipulating one or more components in a manner that the output appears random. To address this, researchers have sought to develop methods that minimise the need for trust in QRNG systems. This has led to the exploration of device-independent quantum random number generation (DI-QRNG).

Device Independence and Semi Device Independence

The concept of device independence, inspired by quantum key distribution (QKD) protocols, aims to eliminate the need for trust in any device or component. However, despite its theo-

retical appeal, DI-QRNG remains largely impractical due to the significant technological and experimental challenges involved in its implementation.

A more feasible alternative is semi device-independent QRNG (SDI-QRNG), which shares similarities with semi device-independent QKD. SDI-QRNG entails trusting certain components while allowing others to be completely untrusted. This approach enables the design of systems in which the most vulnerable components are untrusted, thereby enhancing security.

The Role of Trust in QRNG

While the need for trust in QRNG systems cannot be entirely eliminated, it is important to note that this is not necessarily an insurmountable issue. We can increase trust in cryptographic devices by thoroughly characterising and monitoring their components. By gaining an in-depth understanding of the underlying physics and verifying the device's conformance to expected behaviour through experimental tests, confidence in the system can be bolstered.

One of the primary contributions of this thesis is the detailed study of a critical component in QRNG and QKD systems: the semiconductor laser. By investigating the behaviour and properties of semiconductor lasers, potential security vulnerabilities can be identified, and appropriate countermeasures can be implemented.

In conclusion, the issue of trust in QRNG systems remains a significant challenge. While device independence is an appealing solution, practical limitations render it largely unattainable. As an alternative, semi device-independent approaches can help strike a balance between trust and security. Ultimately, trust in QRNG systems can be established through rigorous characterisation and monitoring of components, with the semiconductor laser serving as a prime example of a component that can be thoroughly examined to enhance the security and reliability of QRNG systems.

2.3 Summary

In this chapter we introduced both QKD and QRNG, with en emphasis on implementation security. At the heart of implementation security, for both technologies, is the issue of trust: how much we trust our devices to work as our theories assume they do. This thesis makes a contribution to implementation security by studying a key component for both technologies, namely the semiconductor laser.

By studying semiconductor lasers and operating them according to a strong physical understanding of their characteristics, we can increase our trust that these devices work as we intend and according to theoretical requirements.

In the following chapter we introduce the main theory and techniques for the study of semiconductor lasers. In particular we introduce the laser rate equations and use them to simulate various properties of semiconductor lasers, such as phase noise, gain-switching and optical injection locking.

Chapter 3

Semiconductor Lasers in Quantum Cryptography

Some of the contents of this chapter are based on Ref. [11].

Semiconductor lasers serve as the primary means of generating photons in Quantum Key Distribution (QKD) and optical Quantum Random Number Generation (QRNG) systems. Although single-photon sources represent the ideal choice for QKD applications, their technological maturity remains limited. As a result, researchers have adopted semiconductor lasers, whose light can be attenuated to achieve the desired single-photon level emission. The attenuated output of a semiconductor lasers can be described as a weak coherent pulse (WCP), which follows a Poisson distribution in the number of photons per pulse. The probability distribution of a Poisson distribution has one parameter, in this case the mean photon number, and is given by:

$$f(k;\mu) = \Pr(X = k) = \frac{\mu^k e^{-\mu}}{k!} \tag{3.1}$$

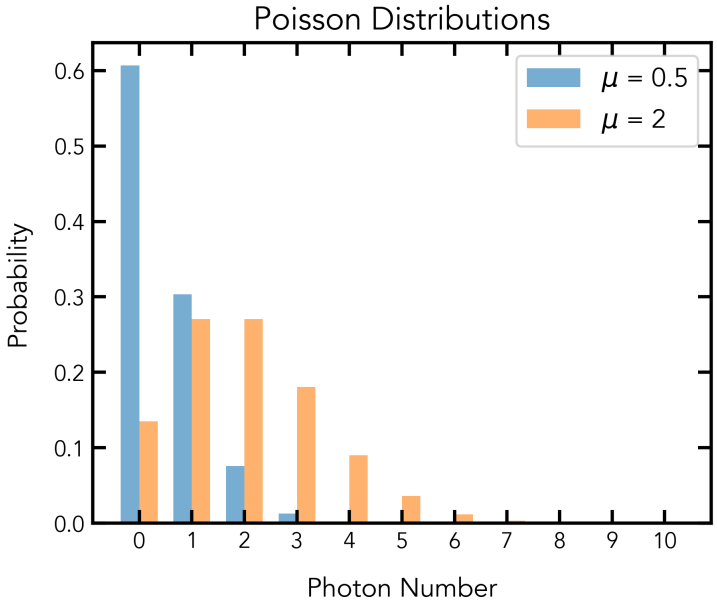

Figure 3.1: Attenuated laser pulses follow a Poisson distribution in the number of photons per pulse. By setting the mean photon number less than 1, multi-photon emission can be greatly suppressed.

By adjusting the mean photon number per pulse to a sufficiently low value, one can significantly reduce the probability of multi-photon emission events, as shown in Fig. 3.1. For example, if we select $\mu = 0.5$, then $P(X > 1) = 9\%$ while for a larger $\mu = 2$ then the probability of multi-photon emission is much higher at $P(X > 1) = 60\%$.

It is worth noting that this adjustment also increases the likelihood of zero-photon emission, but this trade-off is generally acceptable within the context of QKD and QRNG systems.

3.1 Semiconductor Laser Basics

Semiconductor lasers are compact, efficient sources of coherent light widely used in optical communications, sensing, and many other applications. Semiconductor lasers leverage the unique electronic band structure of semiconductor materials to achieve lasing through electrical injection.

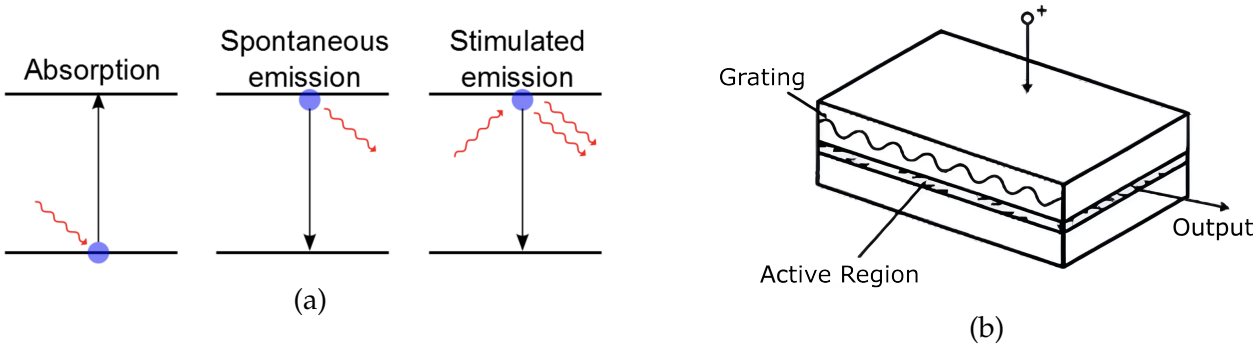

Figure 3.2: (a) Photons with energy above the bandgap can be absorbed, lifting an electron to an excited state. Excited states can either decay spontaneously, or via stimulated emission. Stimulated emission produces a photon with identical energy, direction and polarisation as the photon that triggered it. (b) Schematic of a DFB laser, consisting of a p-n junction where a Bragg grating has been etched into the semiconductor gain medium. The Bragg grating favours one longitudinal mode depending on the grating frequency, enabling stable single mode operation.

The key to lasing action is achieving population inversion, meaning there are more electrons occupying excited states than ground states. In semiconductors, electrons can be excited from the valence band to the conduction band by absorbing photons with energy exceeding the bandgap (absoption in Fig. 3.2a). This leaves behind vacant states known as holes in the valence band. Stimulated emission occurs when an incident photon triggers recombination of an electron-hole pair, resulting in the emission of another photon with identical properties (stimulated emission in Fig. 3.2a). When stimulated emission exceeds absorption, light amplification is achieved. Excited states can also spontaneously decay (spontaneous emission in Fig. 3.2a), emitting a photon in a random direction and with a random phase, introducing noise to the laser output.

To obtain population inversion, charge carriers (electrons and holes) are injected into the semiconductor using a forward bias. In the simplest case, a cavity is formed just by the Fresnel reflections at the cavity ends. The allowed longitudinal modes depend on the cavity length L:

$$m\lambda = 2nL \tag{3.2}$$

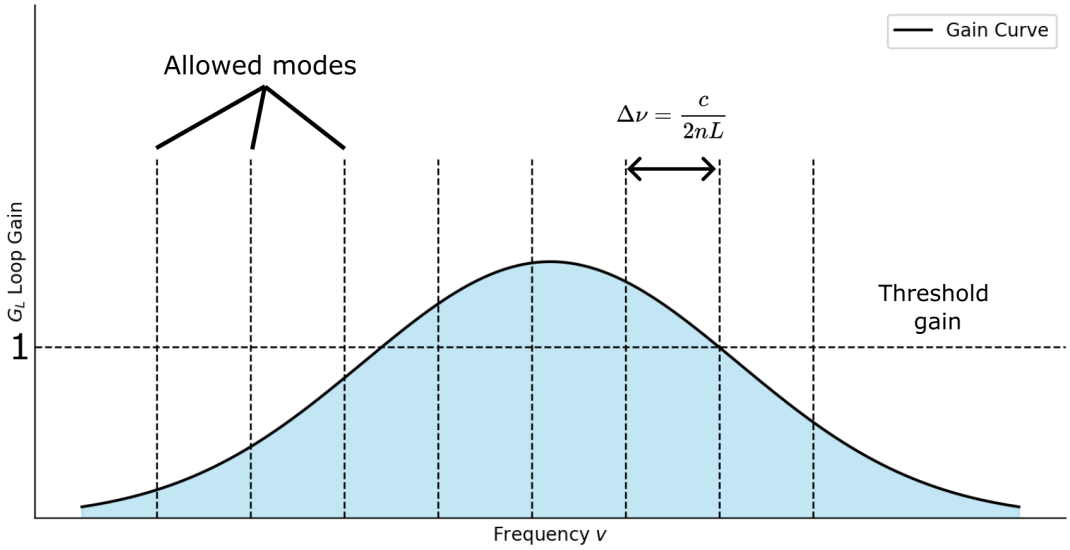

Figure 3.3: The allowed lasing modes correspond to wavelengths which produce standing waves in the laser cavity, according to Eq. 3.2. Lasing is achieved when the loop gain overcomes the loop cavity losses.

where m is an integer mode number, λ is the wavelength, and n is the effective refractive index.

In Fabry-Pérot lasers, lasing begins when the modal gain exceeds losses for a particular mode. However, as current increases, other modes may reach threshold leading to multimode operation and mode hopping.

Distributed feedback (DFB) lasers address this limitation by incorporating a periodic variation of the refractive index along the laser cavity length, forming an internal Bragg grating (see Fig. 3.2b). The grating acts as a wavelength-selective mirror, reflecting light at the Bragg wavelength back into the cavity while transmitting other wavelengths. This increases the cavity losses for all modes except the Bragg wavelength. As a result, the selected mode reaches threshold first, enabling stable single-mode operation over a wider range of injection currents and temperatures. The lasing wavelength can be tuned by changing the temperature to alter the refractive index of the lasing medium, thereby changing the optical cavity length and the

allowed lasing modes.

Semiconductor Laser Technology

Semiconductor laser technology has seen significant advancements since its inception, driven by the growing demand for high-performance, miniaturised, and cost-effective light sources in various fields. The core of this technology lies in the precise engineering of semiconductor materials, predominantly gallium arsenide (GaAs) and indium phosphide (InP), which allow for the production of lasers with specific wavelengths suitable for different applications.

In the manufacturing process, layers of different semiconductor materials are deposited on an initial substrate to create a p-n junction. Techniques include molecular beam epitaxy (MBE) and chemical vapour deposition (CVD). The epitaxial growth process is central to the manufacturing of semiconductor lasers and their design and performance. Over the years, semiconductor lasers have evolved from simple edge-emitting structures to more complex designs like Vertical-Cavity Surface-Emitting Lasers (VCSELs), Quantum Cascade Lasers (QCLs) and DFB lasers.

The versatility of semiconductor laser technology is exemplified by its wide range of applications. From the high-speed data transmission in fibre optic networks to precision material processing in manufacturing, from medical diagnostics and surgery to consumer electronics like barcode scanners and optical drives, semiconductor lasers have become indispensable tools in modern technology.

3.2 Modelling Semiconductor Lasers

Semiconductor lasers find applications in a wide range of fields due to, among other things, their low-cost, high-performance and power-efficiency. The field of fibre optic communications in particular has pushed this technology forward through decades of research into their characteristics and performance resulting in not only low-cost, high-performance devices, but also a large academic literature studying their properties and behaviour [8]–[10], [96], [97]. We can leverage this research to investigate the performance of SLs in the context of quantum cryptography. Quantum cryptography shares many of the same considerations and requirements regarding the characteristics of SLs, e.g. high modulation bandwidths, high efficiency, etc. However, quantum cryptography has unique requirements which can nonetheless be investigated using the standard analytical and numerical tools developed for the study of SLs. Of particular interest to this report are the unique implementation security requirements of quantum cryptography. This section introduces the standard method for modelling SL dynamics, namely the laser rate equations. In later sections we apply the laser rate equations to model various aspects of SLs of particular relevant to quantum cryptography.

3.2.1 Laser Rate Equations

The behaviour of semiconductor lasers can be understood and predicted by using a set of mathematical relationships known as the rate equations. These equations provide a framework for describing the time evolution of the carrier density and the photon density within the active region of the semiconductor laser. By solving these equations, using appropriate approximations, one can determine crucial laser parameters such as threshold current, output power, modulation response, and wavelength characteristics.

These equations enable researchers and engineers to investigate the complex interplay between the carrier and photon dynamics and their influence on the performance of the laser. The rate equations can be solved analytically under specific simplifying assumptions, or numerically using various computational techniques, providing valuable insights into the behaviour of semiconductor lasers and their optimisation for various applications.

The rate equations are a set of three coupled differential equations that describe the rates of change of the three relevant quantities in laser dynamics: carrier density (N), photon density (S) and phase (ϕ). They are given by [98]–[100]:

$$\frac{dN(t)}{dt} = \underbrace{\frac{I(t)}{qV}}_{\text{electrical injection}} - \underbrace{\frac{N(t)}{\tau_n}}_{\text{spontaneous emission}} - \underbrace{g\frac{N(t)-N_0}{1+\epsilon S(t)}S(t)}_{\text{stimulated emission}} + F_N(t) \tag{3.3}$$

$$\frac{dS(t)}{dt} = \underbrace{\Gamma g\frac{N(t)-N_0}{1+\epsilon S(t)}S(t)}_{\text{stimulated emission}} - \underbrace{\frac{S(t)}{\tau_p}}_{\text{cavity losses}} + \underbrace{\frac{\Gamma\beta N(t)}{\tau_n}}_{\text{spontaneous emission}} + F_S(t) \tag{3.4}$$

$$\frac{d\phi(t)}{dt} = \underbrace{\frac{\alpha}{2}\left[\Gamma g(N(t)-N_0) - \frac{1}{\tau_p}\right]}_{\text{carrier density-phase coupling}} + F_\phi(t) \tag{3.5}$$

where $I(t)$ is the applied current, q is the electron charge and V is the active layer volume. The first term in Eq. 3.3 therefore represents the number of carriers (electrons and holes with charge $-e$ and $+e$ respectively) being injected into the lasing medium per unit volume. τ_n is the carrier lifetime, and represents the average amount of time it takes for a carrier to decay due to spontaneous emission. For each carrier lost to spontaneous emission, a photon is gained, which is reflected in the term $\Gamma\beta N(t)/\tau_n$ in Eq. 3.4. Spontaneously emitted photons are emitted in random directions, so only a fraction β are emitted into the lasing mode. Γ is the mode confinement factor, which accounts for the fact that only a fraction Γ of the photons are confined to the active layer.

g is the differential gain coefficient. The overall gain, call it $G(N)$, is a function of the carrier density. It is empirically observed that the gain varies almost linearly with the carrier density, and so a linear approximation is made:

$$G(N) = g(N - N_0) \tag{3.6}$$

where g is the differential gain, and N_0 is the carrier density at transparency, that is, when the gain is zero and $G(N_0) = 0$.

The term $-g\frac{N(t)-N_0}{1+\epsilon S(t)}S(t)$ in Eq. 3.3 therefore represents the decrease in carrier density due to stimulated emission. The denominator $1 + \epsilon S(t)$ introduces the effect of "gain compression" where the laser gain is reduced at higher laser intensities, due to various effects such as spectral and spacial hole burning. ϵ is referred to as the gain compression factor.

τ_p is the photon lifetime and, like the carrier lifetime, represents the average amount of time a photon lives in the laser cavity before exiting the cavity, or otherwise being absorbed.

In the phase rate equation, Eq. 3.5, the so-called linewidth-enhancement factor α (also known as the Henry factor), is crucial. It captures the unique coupling between carrier density and phase in semiconductor lasers. The refractive index of the semiconductor lasing medium depends on the carrier density. The refractive index in turn affects the optical path length of the laser cavity, leading to this coupling between carrier density and phase.

The terms $F_{N,S,\phi}$ are so-called Langevin noise terms that account for the effects of sponta-

neous emission noise. They are given by [98]:

$$F_S(t) = \sqrt{\frac{2\Gamma\beta N(t)S(t)}{\tau_n \Delta t}} \cdot x_S \tag{3.7}$$

$$F_\phi(t) = \sqrt{\frac{\Gamma\beta N(t)}{2\tau_n S(t)\Delta t}} \cdot x_\phi \tag{3.8}$$

$$F_Z(t) = \sqrt{\frac{2N(t)}{\tau_n \Delta t}} \cdot x_Z \tag{3.9}$$

$$F_N(t) = F_Z(t) - F_S(t) \tag{3.10}$$

where $F_Z(t)$ is a noise term, uncorrelated to $F_S(t)$ and $F_\phi(t)$, used to define the carrier density noise term $F_N(t)$. Δt is the integration time step and x_S, x_ϕ and x_Z are three independent standard normal random variables. Often the rate equations are used without noise terms, when the effects of noise are not of interest. In this case the rate equations can be solved using standard numerical integration tools. However, when the noise terms are included, the rate equations become stochastic differential equations and must be solved using stochastic numerical integration methods, the simplest of which is the Euler-Maruyama method [101].

Note that the above rate equations, and the parameters introduced are just one possible representation of the rate equations. Depending on the approximations and the laser dynamics which one wants to capture, other forms of the rate equations can be used. For example, Eqs. 3.3 - 3.4 make several assumptions, including:

- Single mode operation: the model assume only a single longitudinal mode and does not account for mode competition or other multi-mode dynamics. This assumption can be justified in the case of DFB lasers, which offer stable single mode operation.

- Temperature dependence and constant parameters: the rate equation parameters can be

affected by temperature, or other factors which can vary over time. We use a TEC controller to keep the temperature constant during experiments.

- Non-radiative recombination: we assume all carrier decay produces a spontaneously emitted photon, neglecting non-radiative recombination mechanisms like Auger recombination. Other recombination mechanisms can be accounted for by adding additional terms to the rate equations. For example, the Auger recombination would be proportional to the carrier density cubed, with some coefficient.

- Gain compression and linear gain: the model accounts for gain compression (via the $1/(1+\epsilon S)$ term) and assumes a linear dependence of the gain as a function of carrier number (via the g parameter). The effects of gain compression can also be captured using the form $(1-\epsilon S)$, or $1/(1+\epsilon S)^{1/2}$[98].

The power output of the laser is related to the photon density by:

$$P(t) = \frac{V\eta h\nu}{2\Gamma\tau_p} S(t) \tag{3.11}$$

where η is the differential quantum efficiency. η quantifies the number of photons produced per carrier injected in the laser cavity, and therefore determines the slope of the P-I curve. h is Planck's constant and ν is the laser frequency.

The rate equation parameters are intrinsic properties of each laser and will vary from laser to laser. There are various experimental methods that can be used to obtain estimates for them, one of which we introduce in Chapter 4 [100], [102]–[104]. Table 3.1 gives a summary with typical values for the rate equation parameters. By numerically solving the rate equations, the laser output power $P(t)$ and phase $\phi(t)$ can be obtained as a function of time for any given

Table 3.1: Typical rate equation parameters (after Refs. [99], [100]).

Parameters	Values	Description
τ_n (ns)	0.74	Carrier lifetime
τ_p (ps)	0.74	Photon lifetime
g ($\times 10^{-6}$ cm^{3}s^{-1})	1.27	Differential gain coefficient
ε ($\times 10^{-17}$ cm^3)	1.18	Gain compression factor
N_0 ($\times 10^{18}$ cm^{-3})	0.85	Carrier density at transparency
β ($\times 10^{-5}$)	0.50	Spontaneous emission factor
α	2.7	Linewidth enhancement factor
η	0.20	Differential quantum efficiency
V ($\times 10^{-11}$ cm^3)	1.72	Active layer volume
Γ	0.27	Mode confinement factor
κ ($\times 10^{11}$ Hz)	1.13	OIL coupling term

current input function $I(t)$. We start, in the following section, by analysing the steady-state laser characteristics. In later sections we introduce and study gain-switching, a common method of laser pulse generation in quantum cryptography.

3.3 CW Characteristics

We can analyse the rate equations in their steady-state conditions, setting all derivatives to zero.

We can make several simplifying assumptions to derive the expected linear dependence of the power above threshold. We first assume that spontaneous emission has a negligible effect on the laser carrier density and output power above threshold. Second, we neglect the effects of gain-compression. The resulting equation for the photon density is:

$$\Gamma g(N - N_0) = \frac{1}{\tau_p} \tag{3.12}$$

The laser threshold current is characterised as the current at which the steady-state laser

gain G equals the losses. However, this is also true for currents *above* threshold:

$$G(I > I_{\text{th}}) = G(I_{\text{th}}) \tag{3.13}$$

If the gain exceeded the losses even above threshold (in steady state conditions), then the laser photon density and output would continue increasing, which is not compatible with a steady-state. Because the gain increases monotonically with the carrier density, this also implies that the above-threshold carrier density is *clamped* at its threshold value:

$$N(I > I_{\text{th}}) = N_{\text{th}} \tag{3.14}$$

Above threshold, Eq. 3.12 is therefore:

$$\Gamma g(N_{\text{th}} - N_0) = \frac{1}{\tau_p} \tag{3.15}$$

Combing this with Eq. 3.3, we obtain:

$$\frac{I}{eV} - \frac{1}{\Gamma\tau_p}S - \frac{N_{\text{th}}}{\tau_n} = 0 \tag{3.16}$$

Recognising that at threshold, stimulated emission is still a small contribution to the laser output, and so the steady-state threshold current is:

$$I_{\text{th}} = \frac{eVN_{\text{th}}}{\tau_n} \tag{3.17}$$

Multiplying Eq. 3.15 by eV therefore gives:

$$I - \frac{eV}{\Gamma\tau_p}S - I_{\text{th}} = 0 \tag{3.18}$$

Finally, substituting for power, and rearranging:

$$P = \frac{\eta h\nu}{2e}(I - I_{\text{th}}) \tag{3.19}$$

Of course, near threshold, spontaneous emission is significant contribution to the laser output. Ref. [102] provide the following expression which accounts for spontaneous emission:

$$(\frac{2e}{\eta h\nu}P)^2 - (I - I_{\text{th}} - I_s)\frac{2e}{\eta h\nu}P - I_s I \approx 0 \tag{3.20}$$

where $I_s = \beta eV/(\Gamma g\tau_n\tau_p)$ captures the effects of spontaneous emission. Without this term we recover the linear dependence in Eq. 3.19.

3.4 Gain-Switching

There are two main methods used to generate laser pulses in QKD and QRNG: pulse carving and gain-switching. Pulse carving is a technique used to generate a train of pulses from a continuous wave (CW) laser by modulating the intensity of the output laser beam, using an external high-speed intensity modulator. Pulse carving can produce pulses at GHz frequencies, and with desirable laser light properties: because a CW laser is used, the output light is stable and with minimal chirp. However, pulse carving has disadvantages. Most obvious is the added cost and complexity of adding an intensity modulator at the output of the laser. Additionally,

since the laser pulses were carved out of coherent CW laser light, all the pulses are in phase (up to the coherence length of the laser). This is actually a disadvantage in quantum cryptography, since many applications require using phase randomised pulses that do not share any phase relationship. To achieve this phase randomisation with pulse carving, it is therefore necessary to also add a phase modulator after the intensity modulator to change the phase of each pulse by a random amount, again adding cost and complexity.

Gain-switching is an alternative method of generating pulses of light. The principle of operation is simple: instead of driving the SL with a constant current, the laser is driven with an alternating current above and below the lasing threshold. Between pulses, the laser is driven below threshold, such that no light is emitted. Periodically, the driving current is increased above the lasing threshold to produce a pulse of light. Gain-switching can be thought of as turning the laser on and off, very rapidly. Fig. 3.4 shows a rate equation simulation of laser gain-switching. A square wave current alternates between below- and above-threshold, leading to periodic pulses of light when the carrier density reaches it's threshold level. The photon and carrier density do not exactly track the input current, due to the finite bandwidth of semiconductor laser. This is discussed in more depth below, in Sec. 3.4.1.

Gain-switching can produce short ($<$100 ps) pulses at GHz rates by only modulating the driving current. Additionally, under appropriate driving current settings, gain-switching produces naturally phase randomised pulses, without the need for external modulators. When the laser is driven below threshold, the laser output is dominated by spontaneous emission. Each spontaneously emitted photon has a random phase, and therefore the laser phase quickly randomises while it is below threshold. When the laser is next driven above threshold, the photons generated by stimulated emission will inherit their phase from the prior spontaneous emission, leading to each generated pulse having a random phase. Importantly, spontaneous emission

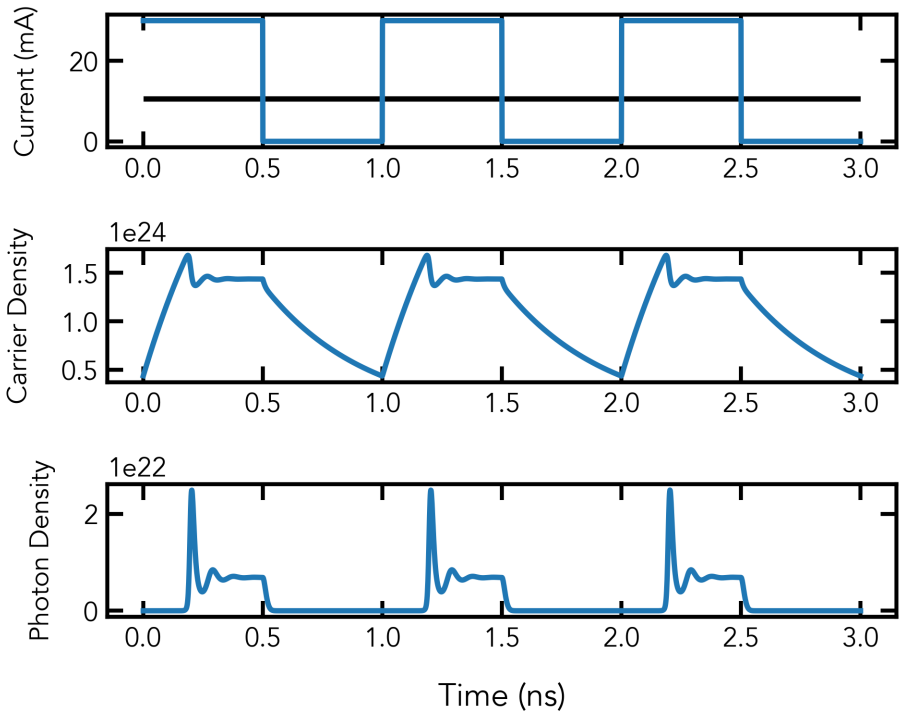

Figure 3.4: When the laser current input alternates between above and below threshold (indicated by horizontal black line in top figure), a train of pulses can be generated. When the current is turned on, carriers build up in the cavity until lasing begins. The carriers overshoot the threshold carrier density, leading to damped relaxation oscillations in both the carrier density and photon density.

is a quantum effect, and the resulting randomness is therefore also quantum in origin. Therefore, gain-switching represents an effective way of generating pulses of light with high quality randomness.

Fig. 3.5 shows plots of the simulated phase of a gain-switched laser. There are two components to the laser phase: the deterministic evolution of phase due to the changing carrier density in the laser cavity, seen in Fig. 3.5 (a). Superposed on this deterministic phase evolution is a stochastic component due to spontaneous emission in the laser cavity. Fig. 3.5 (b) plots just this stochastic component. Fig. 3.5 (b) is generated by solving the rate equations twice: first the non-stochastic rate equations, i.e. without the Langevin noise terms, are solved to obtain the deterministic evolution of phase due to changes in carrier density. Second, the stochastic equations are solved, and the deterministic component is subtracted such that we are left with just the stochastic component, as plotted in Fig. 3.5 (b). Note the increased phase noise at times when the laser is below threshold. This illustrates the phase-randomising effects of spontaneous emission between pulses.

Gain-switched lasers can produce short, naturally phase randomised pulses of light at GHz clock rates only by adjusting the current signal driving the laser and are therefore widely used in modern QKD implementations [11].

Gain-switching does come with its own disadvantages. High speed direct modulation of SLs leads to frequency chirp, which leads to frequency dependent dispersion in optical fibres. It also reduces the interference visibility between pulses. Visibility quantifies the contrast of interference at the output of an interferometer. It is defined as:

$$\nu = \frac{I_{\max} - I_{\min}}{I_{\max} + I_{\min}} \tag{3.21}$$

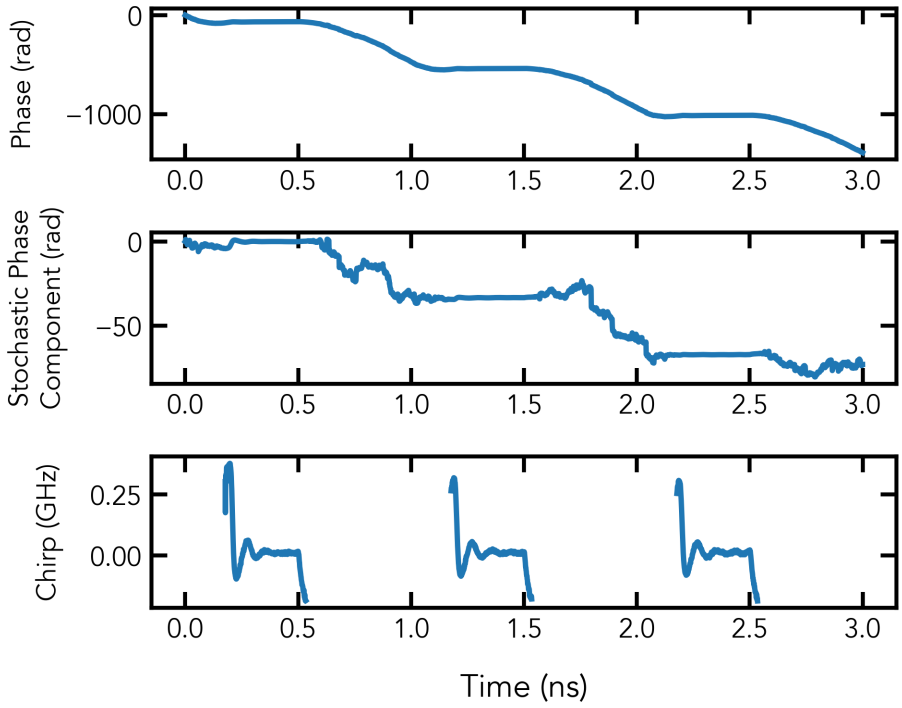

Figure 3.5: The laser phase has both a deterministic component, due to changes in the carrier density, and a random component due to spontaneous emission. The top figure plots the overall phase evolution, while the middle figure plots just the random evolution, by subtracting out the deterministic component. The bottom figure plots the laser chirp, which is equal to the rate of change of the phase. Gain switching leads to highly chirped pulses, especially during the initial relaxation oscillations.

where $I_{\max}$ and $I_{\min}$ are the maximum and minimum intensity at the interferometer output, measured over a range of phase-offset values. If complete destructive interference is observed, then the visiblity is 1. However, if the two interfering fields are not exactly the same frequency, or if there are other sources of noise such as jitter, or intensity noise, then these can act against the interference, and reduce the visibility.

Chirp is the change in laser frequency about the unmodulated frequency. Chirp can therefore reduce the interference visibilty if the two interfering pulses have different frequencies. It is an undesirable side effect of gain-switching. Chirp can be modelled by the rate equations, since it is simply equal to the rate of change of the phase:

$$\Delta f = \frac{1}{2\pi}\frac{d\phi}{dt} \tag{3.22}$$

Fig. 3.5 (c) plots the chirp of the gain-switched pulses. The chirp is only plotted at times when the laser is lasing and therefore has a well-defined frequency. Fig. 3.5 (c) shows a fast changing frequency due to the laser relaxation oscillations. High quality interference is only obtained between pulses with equal frequencies. Due to timing jitter, however, each pulse will be emitted at a slightly different time, and have a slightly different shape. When the pulses are highly chirped, as in Fig. 3.5 (c), the quality of interference degrades since the frequencies of the pulses are not exactly equal along the length of the pulse.

The chirp is most acute during the large relaxation oscillations at the beginning of a gain-switched pulse. Therefore, it is common for phase noise QRNGs to produce pulses long enough for the relaxation oscillations to dampen, and only measure the interference between two pulses during their steady-state output, after the relaxation oscillations have decayed [105]. By carefully controlling the driving current, it is possible to minimise the relaxation oscillations, and

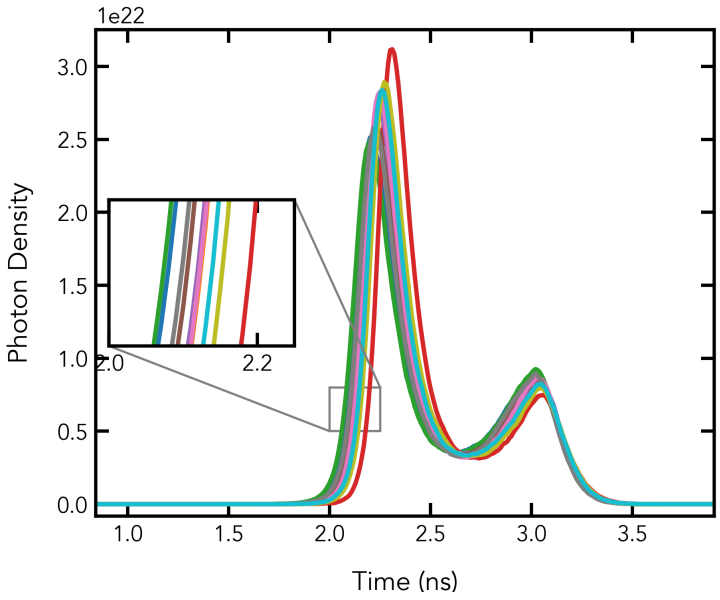

Figure 3.6: Each gain switched pulse starts with a random spontaneous emission event in the cavity. This randomness leads to a randomness in turn-on delay, producing jitter. The time at which the pulse ends, however, is much more deterministic since it does not depend on spontaneous emission.

achieve steady state emission more quickly [106].

Interference is also negatively affected by jitter, that is, the random variation in the timing of the emitted pulses. Jitter is caused by spontaneous emission: when the laser is driven above threshold, the stimulated emission is triggered by spontaneously emitted photons in the cavity. Depending on the timing of the spontaneous emission each new pulse will be triggered at a slightly different time, due to the random nature of spontaneous emission. Using the stochastic rate equations, we can simulate the effects of jitter. Fig. 3.6 shows many simulations of a single gain-switched pulse, showing the variation in temporal location between different pulses.

In Section 3.6 we will see how optical injection locking (OIL) can be used to greatly reduce these negative effects of gain-switching and enable high visibility interference between short pulses from independent lasers [107].

3.4.1 High Speed Modulation

One key characteristic of a gain-switched laser is its intensity modulation (IM) response. For an ideal laser, the light emitted would exactly track the input current. For example, if a perfect square wave current was input, then a perfect square wave of light intensity would be output, according to the current-power relationship as measured by a P-I curve. And, for modulation frequencies up to around 10MHz, this is approximately true. For higher modulation frequencies, the finite bandwidth of semiconductor lasers comes into play, and leads to significantly different behaviour. In particular, if a laser is driven by a step-like current-pulse like the one depicted in Fig. 3.4 (a), then at high frequencies the optical output will have some *turn-on delay* and will undergo damped oscillations around the steady-state power output, called *relaxation oscillations*. The frequency of these oscillations determines the maximum modulation frequency of the laser quantified by the *modulation bandwidth*. In the following, we elaborate on these issues.

3.4.2 Turn-on delay

The "turn-on delay" of a semiconductor laser refers to the time it takes for the laser to start emitting light after an electrical signal is applied. This can be observed clearly in the above simulations, Figs. 3.4. In Fig. 3.4 it can be seen that the current modulation is turned on at 1 ns, for example, but the laser does not begin lasing until well after 1 ns. This delay is due to the time required for carrier density to build up and reach its threshold value after the current is turned on. Two important factors that contribute to the turn-on delay are the carrier lifetime and the threshold carrier density.

The carrier lifetime (τ_n) is the average time a charge carrier (electron or hole) spends in the

active region before recombining. The threshold carrier density (N_{th}) is the minimum density of carriers required in the active region to achieve population inversion and, consequently, lasing action.

We can model the carrier buildup using the rate equations. During the buildup there is negligible stimulated emission, so the rate of change in carrier density is:

$$\frac{dN}{dt} = \frac{I}{Ve} - \frac{N}{\tau_n} \tag{3.23}$$

If the current is changed abruptly from 0 to I at $t = 0$, then we can solve the differential equation to obtain:

$$N(t) = \frac{I\tau_n}{eV}\left[1 - \exp\left(\frac{-t}{\tau_n}\right)\right] \tag{3.24}$$

When the laser is lasing, then the carrier density is clamped to a steady state value, N_{th} where the rate at which carriers are injected equals the rate at which they recombine. In other words $N_{\text{th}}/\tau_n = I_{\text{th}}/Ve$. By setting $N = N_{\text{th}}$, we can solve for t to find the turn-on delay:

$$t_{\text{d}} = \tau_n \ln\left[\frac{I}{(I - I_{\text{th}})}\right] \tag{3.25}$$

Interestingly, Eq. 3.25 provides an experimental method to estimate the carrier lifetime, by measuring the turn on delay at different driving current values I [108].

3.4.3 Relaxation Oscillations

Relaxation oscillations are a fundamental characteristic of semiconductor lasers, arising due to the interaction between the carrier and photon dynamics in the laser cavity. These oscillations manifest as damped sinusoidal variations in the output power of the laser, typically observed when the laser is subjected to a sudden change in input current or optical injection. Relaxation oscillations can again be observed in the above simulations, Figs. 3.4 and 3.5. Understanding the origin and behaviour of relaxation oscillations is crucial for high-speed optical communication systems, including QKD, as well as QRNG, since they determine the modulation characteristics of the laser.

The behaviour of relaxation oscillations can be analysed by considering the rate equations for carriers and photons, Eqs. 3.3 and 3.4, and using small-signal approximations. Consider a laser which is driven with an above-threshold DC current (I_{DC}), with a small AC current superimposed (I_{AC}). We can express the current and carrier and photon densities using complex frequency domain notation:

$$\begin{aligned} I &= I_{\mathrm{DC}} + I_{\mathrm{AC}} e^{j\omega t} \\ N &= N_{\mathrm{th}} + N_{\mathrm{AC}} e^{j\omega t} \\ S &= S_{\mathrm{DC}} + S_{\mathrm{AC}} e^{j\omega t}. \end{aligned} \tag{3.26}$$

where we ignore possible higher harmonics of the drive frequency ω. Note also that the DC carrier density term is the threshold carrier density N_{th}, since above threshold the carrier density is clamped to this value.

Substitute these into the corresponding rate equations:

$$j\omega N_{\text{AC}} = \frac{I_{\text{AC}}}{qV} - \frac{N_{\text{AC}}}{\tau_n} - gS_{\text{DC}}\frac{N_{\text{AC}}}{1+\epsilon S_{\text{DC}}} - g\left(N_{\text{th}} - N_0\right)\frac{S_{\text{AC}}}{1+\epsilon S_{\text{DC}}} \tag{3.27}$$

$$j\omega S_{\text{AC}} = \Gamma g\frac{N_{\text{AC}}S_{\text{DC}}}{1+\epsilon S_{\text{DC}}} + \Gamma g\frac{\left(N_{\text{th}} - N_0\right)S_{\text{AC}}}{1+\epsilon S_{\text{DC}}} - \frac{S_{\text{AC}}}{\tau_p} + \frac{\Gamma\beta N_{\text{AC}}}{\tau_n} \tag{3.28}$$

From here, it is clear that N_{AC} and S_{AC} can be expressed as a function of I_{AC}, by solving the set of linear equations. The transfer function can then be calculated as

$$\frac{S_{\text{AC}}(\omega)}{I_{\text{AC}}(\omega)} = \frac{gS_{\text{DC}}/(1+\epsilon S_{\text{DC}})}{gS_{\text{DC}}/(\tau_p(1+\epsilon S_{\text{DC}})) - \omega^2 + j\omega\left[gS_{\text{DC}}/(1+\epsilon S_{\text{AC}}) + 1/\tau_n\right]} \tag{3.29}$$

We can observe that the first term in the denominator is the square of a resonance frequency, and so we can define

$$\omega_R^2 \equiv \frac{gS_{\text{DC}}}{\tau_p(1+\epsilon S_{\text{DC}})} \tag{3.30}$$

as the *relaxation oscillation frequency* and rewrite Eq. 3.29 in a more normalised way

$$\frac{P_{\text{AC}}(\omega)}{I_{\text{AC}}(\omega)} = \frac{\eta h\nu/q}{1 - (\omega/\omega_R)^2 + j(\omega/\omega_R)\left[\omega_R\tau_p + 1/(\omega_R\tau_n)\right]} \tag{3.31}$$

where we have now expressed it in terms of power.

At low modulation frequencies the denominator is one and we recover the proportional relationship between power and current that is expected of a laser above threshold. At higher frequencies, the term $1 - (\omega/\omega_R)^2$ creates a resonance in the response. Fig. 3.7 shows the response of an idealised laser diode modulated at different frequencies, at different levels of power output. In Chapter 4 we will experimentally measure this response for a real laser diode and fit the measured response to Eq. 3.31.

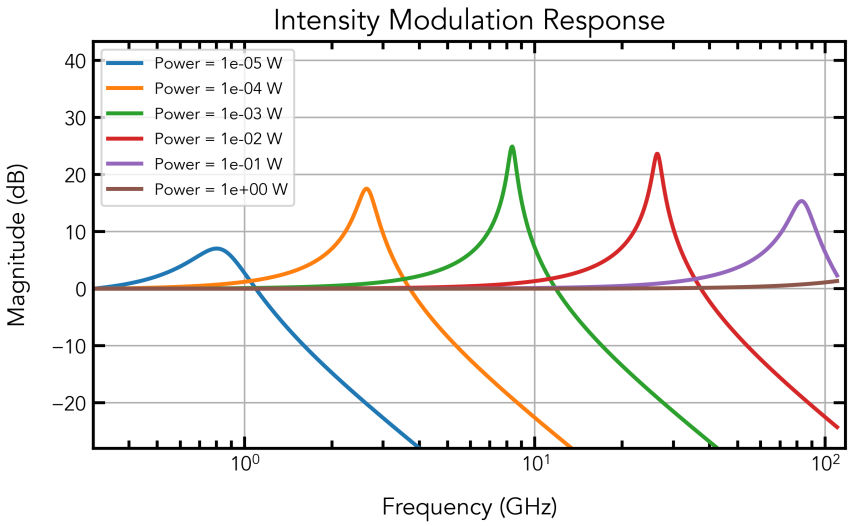

Figure 3.7: The ideal intensity modulation response of a semiconductor laser at different power outputs. The resonance frequency peak shifts to higher frequencies at higher power outputs. The 3 dB modulation bandwidth likewise increases. However, the damping *also* increases, reducing the resonance frequency peak, leading to a maximum achievable bandwidth, as expressed in Eq. 3.35

The third term in the denominator, $gS_{\text{DC}}/(1+\epsilon S_{\text{AC}})+1/\tau_n$ is referred to as the *damping factor* (γ). From Eqs. 3.29 and 3.30, the damping factor can be seen to be proportional to the square of the resonance frequency:

$$\gamma = 4\pi^2 \tau_p f_R^2 + \frac{1}{\tau_n} \tag{3.32}$$

The constant of proportionality $K = 4\pi^2\tau_p$ is referred to as the K-factor.

An important property of semiconductor lasers used in high-speed communication systems is their modulation bandwidth, that is, the range of frequencies over which the laser can be modulated without large degradation of the signal. It is common to quantify this in terms of the 3-dB bandwidth, defined at the frequency at which the laser response is reduced by 3 dB with respect to the DC response, that is

$$\left| \frac{P_{\text{AC}}(\omega_{3\,\text{dB}})}{P_{\text{AC}}(0)} \right| = \frac{1}{\sqrt{2}}. \tag{3.33}$$

Solving for $\omega_{3\,\mathrm{dB}}$ yields [10]

$$f_{3\,\mathrm{dB}} \approx f_R\sqrt{1+\sqrt{2}} \approx 1.55 f_R, \quad (\gamma/\omega_R \ll 1) \tag{3.34}$$

Note also that the relaxation oscillation frequency, and therefore the 3 dB bandwidth, increase with increasing power. The damping also increases, in proportion to the ω_R^2, according to the K-factor. At some point, the response will drop below the 3 dB level at frequencies lower than ω_R, implying a maximum achievable bandwidth. This maximum bandwidth occurs when the resonance peak is equal to the DC response, and $\omega_R = \omega_{3\,\mathrm{dB}}$, resulting in a maximum bandwidth of

$$f_{3\,\mathrm{dB}}|_{\max} = \sqrt{2}\frac{2\pi}{K}. \quad \left(\gamma/\omega_R = \sqrt{2}\right). \tag{3.35}$$

The K-factor, and therefore the photon lifetime τ_p, determines the modulation-bandwidth capabilities of a laser.

In summary, the relaxation oscillation frequency and damping factor provide insights into the dynamic response of the laser and can be influenced by the device parameters and operating conditions. Understanding and controlling relaxation oscillations are crucial for achieving high performance lasers in quantum cryptography. For example, a key factor in the performance of a QKD or QRNG system is the repetition rate of the gain-switched laser source. The modulation bandwidth of the laser can be a factor that limits the maximum achievable repetition rate, and therefore performance. From the above discussion we can see that increasing the driving current can be a way to increase the bandwidth, up to $f_{3\,\mathrm{dB}}|_{\max}$. Further, it may be desirable to select lasers based on their K-factor, which determines this maximum bandwidth. The K-factor is straightforwardly measured, as will be demonstrated in Chapter 4. Another

factor which influences performance is laser chirp, especially when modulating lasers at high-speeds. Chirp is a direct consequence of the fluctuations in carrier density caused by relaxation oscillations, and so minimising them can lead to better interference between pulses.

3.5 Phase Noise

Phase noise in semiconductor lasers refers to the fluctuation of the phase of the laser output field over time, which affects its coherence. While phase noise is typically something to be minimised, in quantum cryptography phase noise can be used as a useful resource. In QKD, gain-switching can be used to increase phase noise between pulses to achieve phase randomisation, which is crucial to security. In QRNG, phase noise is a source of quantum randomness which can be measured and digitised to produce random numbers. Phase noise is quantum in origin because it is caused by spontaneous emission, which is a quantum effect. Phase noise QRNGs can use both CW and gain-switched lasers as sources of randomness.

Phase noise is closely associated with the linewidth of a laser. Laser linewidth quantifies the width of a laser's optical spectrum. An ideal laser should emit light of a single frequency, but due to phase noise, the emission spectra is widened. We saw in Eq. 3.46 that the instantaneous change in frequency (chirp) is equal to the rate of change of phase. Spontaneous emission leads to changes in phase, and therefore of frequency, broadening the laser's optical spectrum.

Schawlow and Townes calculated a fundamental limit for the linewidth, even before the first laser was experimentally demonstrated [109]. Certain types of lasers have a linewidth which approaches this fundamental limit, however semiconductor lasers have a significantly higher linewidth. This fact was eventually explained by C. H. Henry as being due to a coupling between the phase and the carrier density in semiconductor lasers. Henry introduced

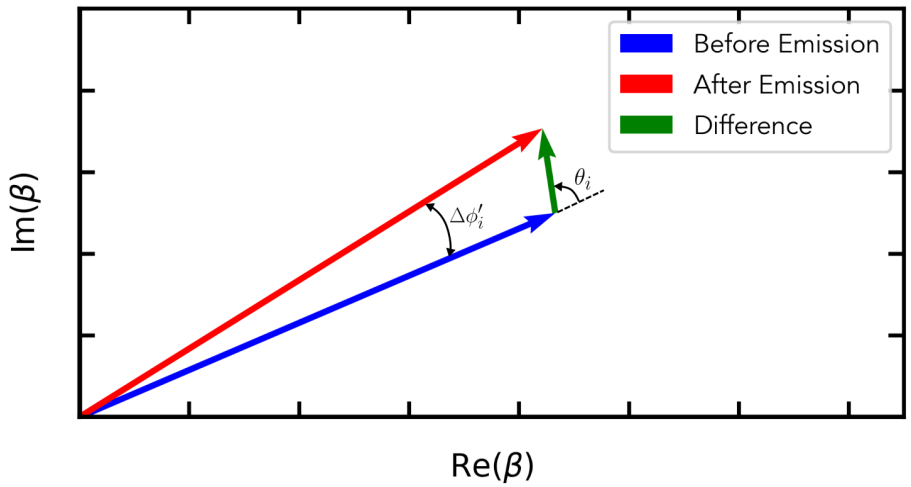

Figure 3.8: The instantaneous changes of the phase ϕ and intensity S of the optical field caused by the ith spontaneous emission event. The field amplitude $\beta = S^{1/2}\exp(i\phi)$ changes by $\Delta\beta_i$, which has an amplitude of Γ/V, corresponding to the addition of a single photon. The phase changes θ_i relative to ϕ where θ_i is a random angle, for an overall phase change of $\Delta\phi_i'$. (After [95], [110]).

the *linewidth enhancement factor* α or *Henry factor* to quantify this coupling. The phase-carrier density coupling is due to a unique feature of semiconductor lasers which is that the refractive index of the active lasing medium changes with the carrier density. This fact amplifies the effect of spontaneous emission on the phase of a laser: not only does a spontaneous emission event introduce a new photon with a random phase, it also removes a carrier from the laser cavity. The photon with a random phase contributes to phase noise as in any other type of laser, but the change in the number of carriers leads to a change in the refractive index of the lasing medium, and hence a change in the phase. Henry showed that the linewidth of semiconductor lasers is increased by a factor of $1 + \alpha^2$, in good agreement with experimental data [95], [110], [111].

3.5.1 Phase Noise in CW Lasers

Consider a single spontaneous emission event, depicted in Fig. 3.8, producing a photon with a random phase θ_i. This photon makes two contributions to the phase of the overall field. First,

there is an instantaneous change, $\Delta\phi_i'$, due to the addition of a new photon with a random phase. As is clear from Fig. 3.8, this instantaneous phase change is given by:

$$\Delta\phi_i' = \frac{\sin(\theta_i)}{\sqrt{S}} \tag{3.36}$$

The second contribution is delayed, and is due to the change in refractive index of the semiconductor lasing medium. To restore the steady-state field intensity after a spontaneous emission event, the laser will undergo relaxation oscillations. Integrating over these relaxation oscillations, Henry showed that the total contribution of this delayed phase change approaches:

$$\Delta\phi_i'' = -\frac{\alpha}{2S}\left(1 + 2S^{1/2}\cos(\theta_i)\right) \tag{3.37}$$

where α is the linewidth enhancement factor.

The total contribution of a single spontaneously emitted photon is then:

$$\Delta\phi_i = \Delta\phi_i' + \Delta\phi_i'' = -\frac{\alpha}{2S} + \frac{1}{S^{1/2}}\left[\sin(\theta_i) - \alpha\cos(\theta_i)\right] \tag{3.38}$$

The first term represents a constant phase change, and so we focus on the second term, which introduces noise due to the random phase θ_i of each spontaneous emission event. Consider now many (N) spontaneous emission events. The overall contribution to the phase will be:

$$\Delta\phi = \sum_{i=1}^{N} S^{-1/2}\left(\sin(\theta_i) - \alpha\cos(\theta_i)\right) \tag{3.39}$$

If the average rate of spontaneous emission is R, we can easily calculate the variance of the phase after a time t by squaring Eq. 3.39. For random angles, the average of all cross terms

vanishes, giving:

$$\left\langle \Delta\phi^2(t) \right\rangle = \frac{R\,(1+\alpha^2)\,t}{2S}. \tag{3.40}$$

Because each spontaneous emission event contributes a random phase, the phase as depicted in Fig. 3.8 will execute Brownian motion, and is therefore a Gaussian random variable (due to the Central Limit Theorem), with zero mean. The variance of the phase, $\langle \Delta\phi^2 \rangle$, quantifies the phase noise. Indeed, it is common to define the coherence time t_c of a laser as the time it takes for the phase variance to reach some threshold, typically 2 radians, although other definitions can be found in the literature [95], [112]:

$$\left\langle \Delta\phi^2(t_c) \right\rangle \equiv 2 \implies \left\langle \Delta\phi^2(t) \right\rangle = \frac{2t}{t_c}. \tag{3.41}$$

Phase noise in a CW laser can be simulated by solving the stochastic rate equations, setting the input current to a constant value. Fig. 3.9 (left) shows one such simulation. By repeating the stochastic simulation several times, we can begin to visualise the statistics of the resulting phase values. In conclusion, we can calculate the phase variance analytically using Eq. 3.40. Alternatively, and more painstakingly, we can solve the stochastic rate equations many times in a Monte Carlo simulation, and then calculate the variance of the resulting phase values to quantify the phase noise over time.

In the case of a CW laser, Eq. 3.40 is clearly more useful for quantifying the phase noise. However this equation does not apply for a gain-switched laser in which the laser dynamics are highly non-linear. In that case, the numerical approach can be used.

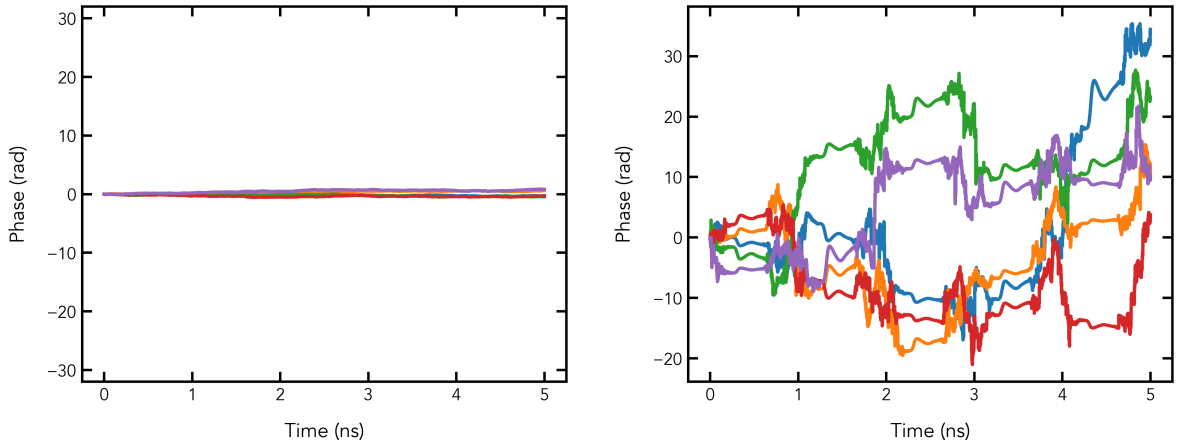

Figure 3.9: The random phase evolution in a CW (left) and gain switched (right) laser. The CW laser phase drifts over time. When the variance of the phase drift exceeds some threshold, typically π, then the laser is said to have lost coherence, and this defines the coherence time of the laser. With gain switching, the laser undergoes rapid phase randomisation when the laser is below threshold.

3.5.2 Phase Noise in Gain-Switched Lasers

Fig. 3.9 (right) shows a simulation of the phase of a gain-switched laser. Each line is a different solution of the stochastic rate equations, where the input current was set to a square wave that alternates between below- and above-threshold. Clearly, the laser phase rapidly randomises between pulses, when the laser is below threshold.

By solving the stochastic rate equations many times in a Monte Carlo simulation, we can calculate the variance of the phase at any point in time. This allows us to quantify the phase noise even for gain-switched lasers. This approach will be expanded upon in Chapter 4, to quantify the phase noise in a gain-switched laser in a quantum cryptography context, where it is essential to ensure enough phase randomisation between pulses.

3.6 Optical Injection Locking

Optical injection locking is a specific instance of the more general injection locking effect in which two oscillators, be it mechanical, electrical or in this case optical, become coupled and their oscillation frequency synchronises [113], [114]. The phenomenon was first observed by C. Huygens when he noticed that the oscillation of two pendulum clocks synchronises if they are placed close together on a common surface. This was found to be due to small vibrations caused by the clocks that travel through the wall and introduce a coupling between the two oscillators [115].

In the case of OIL, the phase of two lasers can become synchronised if sufficient light from one of the lasers, termed the "master" laser is injected into the other laser, termed the "slave" laser. If the frequency of both lasers is sufficiently close, then the slave laser will "lock" onto the phase and frequency of the master laser. OIL has been studied extensively in the field of classical optical communications, where laser synchronisation finds many applications. For example, synchronised lasers are used as local oscillators in coherent optical receivers.

In QKD, OIL finds several applications. Firstly, OIL can reduce the chirp and jitter of a gain-switched laser, which improves interference visibility at the receiver [107]. Second, OIL has been used to synchronise the phase of lasers in TF-QKD experiments [116]. TF-QKD requires the use of phase-synchronised lasers which may be separated by hundreds of kilometres, which OIL can achieve. Lastly, OIL has been used to devise a directly phase modulated QKD transmitter which does not use phase modulators to encode information on the phase [26], [117]. In the following, we will explore all three of these effects using the rate equations to model an OIL system.

3.6.1 Operating Principle

OIL can be modelled and studied using a modified form of the laser rate equations. The OIL rate equations include extra terms to account for the extra photons injected into the slave laser cavity. They are:

$$\frac{dN(t)}{dt} = \frac{dN_{\text{fr}}(t)}{dt} \tag{3.42}$$

$$\frac{dS(t)}{dt} = \frac{dS_{\text{fr}}(t)}{dt} + 2\kappa\sqrt{S_{\text{inj}}\,(t)S(t)}\cos(\Delta\phi(t) - \Delta\omega_{\text{inj}}t) \tag{3.43}$$

$$\frac{d\phi(t)}{dt} = \frac{d\phi_{\text{fr}}(t)}{dt} - \kappa\sqrt{\frac{S_{\text{inj}}(t)}{S(t)}}\sin(\Delta\phi(t) - \Delta\omega_{\text{inj}}t) \tag{3.44}$$

where the subscript $_{\text{fr}}$ denotes the standard rate equations for a free running laser given by Eqs. 3.3-3.5. $\Delta\phi = \phi(t) - \phi_{\text{inj}}(t)$ is the difference between the secondary laser phase and the phase of the injected light, κ is a coupling coefficient which quantifies the rate at which injected photons enter the secondary laser cavity, S_{inj} is the injected photon density and $\Delta\omega_{\text{inj}}$ is the difference in free-running optical angular frequency between primary and secondary lasers. We note that Eq. 3.44 describes the phase of the laser into which light is injected, although OIL rate equations are also occasionally expressed in the literature in terms of the phase difference between that laser's emitted light and the injected light—in this case, the frequency detuning $\Delta\omega_{\text{inj}}$ appears outside the sine term and without a dependency on t, which can simplify numerical calculations [114].

The locking effect of optical injection can be seen by considering the sine term in Eq. 3.44. For zero detuning, when the phase difference $\phi - \phi_{\text{inj}}$ is positive (in the interval $[-\pi, \pi)$), the term will be negative and vice versa. This has the effect of locking the secondary laser phase to the primary laser (up to a fixed phase offset). However, a non-zero detuning $\Delta\omega_{\text{inj}}$ acts against

this locking effect. Stable OIL can therefore only be obtained provided the detuning falls within the "locking bandwidth", which can be derived from the steady state solutions of the OIL rate equations [114]:

$$-\kappa\sqrt{1+\alpha^2}\sqrt{\frac{P_{\text{inj}}}{P_0}} < \Delta\omega_{\text{inj}} < \kappa\sqrt{\frac{P_{\text{inj}}}{P_0}} \tag{3.45}$$

where P_{inj} is the injected optical power and P_0 is the free-running secondary laser power. The injection ratio P_{inj}/P_0 and primary-secondary detuning $\Delta\omega_{\text{inj}}$ are crucial parameters in OIL dynamics. Even when an OIL system is within the stable locking range, the exact impact upon modulation bandwidth and pulse performance depends strongly on both detuning and injection ratio, thus requiring careful design of OIL systems for each target application.

OIL has numerous effects which can be usefully applied in QKD. In the following section we elaborate on three such applications.

3.6.2 Chirp and Jitter Reduction in Gain-Switched Lasers

In the context of gain-switched semiconductor lasers, jitter and chirp are two critical factors that can affect the performance of QKD transmitters and QRNG systems. As described in Sec. 3.4, jitter is caused because each new gain-switched pulse is seeded by a random spontaneous emission event. The randomness inherent to spontaneous emission creates variation in the turn-on delay from pulse to pulse. Chirp on the other hand is caused by the fluctuations in carrier density due to relaxation oscillations. Optical injection locking suppresses both of these effects, leading to improved performance.

In an optically injection-locked laser, the injected light can effectively stabilise the output of the slave laser, reducing the jitter in the pulse timing and suppressing the chirp. Without OIL, each pulse is seeded by a random spontaneous emission event, whereas with OIL there

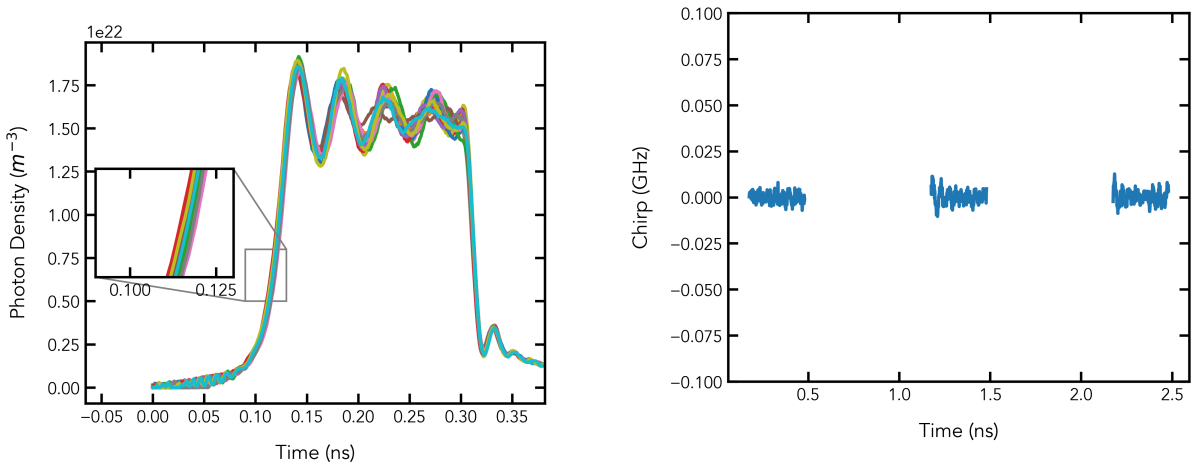

Figure 3.10: (Left) With OIL, each pulse from a gain switched laser is seeded by the injected light, rather than spontaneous emission, reducing jitter. (Right) The external light also reduces the carrier buildup and subsequent overshoot, which reduces relaxation oscillations and therefore chirp (compared to Fig. 3.5).

is a constant supply of external photons to seed each pulse, reducing jitter. This also leads to a reduced turn-on delay, which in turn reduces the buildup of carriers that lead to relaxation oscillations. The result is a significant improvement in the spectral purity and pulse stability of the gain-switched laser diode. This, in turn, can lead to a higher secure key generation rate and improved overall performance of the QKD system. Fig. 3.10 demonstrates, using a rate equation simulation, this improvement in both reduction of chirp and jitter.

3.6.3 Laser Synchronisation in TF-QKD

Twin-field quantum key distribution (TF-QKD) is a recent advancement in the field of QKD, which has demonstrated the potential to overcome some of the distance limitations encountered by conventional QKD systems [22], [23], [116], [118]–[121] . In a TF-QKD setup, two remote parties, Alice and Bob, each have a laser source, and they aim to establish a secure key by exchanging quantum states through an untrusted relay, named Charlie. The key to the TF-QKD is the single-photon interference which occurs at Charlie, requiring Alice and Bobs lasers

to be phase synchronised, even when they are physically separated by hundreds of kilometres.

OIL can address this challenge, since it produces phase synchronisation between the master and slave lasers. There are several possible approaches: either Alice can send part of her laser output directly to Bob, or vice versa, or the master laser can be placed at Charlie, and be used to seed both Alice and Bob's lasers. Of course, travelling hundreds of kilometres of fibre will introduce massive levels of phase noise, and a central challenge in TF-QKD implementations is stabilising and compensating for this noise. But the underlying physical mechanism by which the lasers are synchronised in phase, is OIL. Other methods of phase synchronisation exists, including active feedback mechanisms like optical phase-locked loops (OPLL) [22]. Recently TF-QKD has been demonstrated without the need for phase synchronisation at all [122], [123]. However, OIL is an appealing solution due to its ease of implementation and low cost and complexity.

3.6.4 Directly Phase Modulated QKD Transmitter

In conventional quantum key distribution (QKD) systems, external modulators are commonly used to encode quantum states into the phase or polarisation of the transmitted photons. However, these modulators can introduce additional complexity, cost, and potential vulnerabilities to the QKD system. To address these issues, Yuan et al. proposed a novel approach in 2016 that utilises OIL to design a "modulator-free" or "directly phase-modulated" QKD transmitter [117]. This innovative technique offers several advantages over traditional QKD systems and can lead to more efficient, secure, and cost-effective quantum communication networks.

In the modulator-free QKD transmitter scheme, a gain-switched master laser is used to inject light into a gain-switched slave laser diode. However the master laser is gain-switched at half

the repetition rate as the slave laser, so that a single master pulse seeds two slave laser pulses. This ensures that each pulse pair produced by the slave laser is phase coherent, but with a random phase with respect to other pulse pairs which were seeded by other master laser pulses. Information is encoded as the phase difference between pulse pairs, and this can be achieved by introducing a small modulation in the master laser driving current, in the middle of the pulse, as in Fig. 3.11. This small modulation briefly changes the carrier density in the master laser cavity, leading to a phase shift that depends on the size of the modulation and its duration. The result is that the first half of the master pulse has a phase difference with respect to the second half, determined by the small electrical modulation in the middle. This is illustrated in Fig. 3.11. When this long master laser pulse is used to seed a slave laser pulse pair, the two pulses will inherit the phase difference between the first and second half of the master pulse.

Key to this scheme is achieving deterministic control of the master laser phase just by adjusting the driving current in the middle of the pulse. We can quantify the relationship between the current modulation and the resulting phase modulation using the rate equations. Recall that the instantaneous change in frequency (chirp) is equal to the rate of change of phase. Using Eqs. 3.3-3.5 and Eq. 3.11 it is possible to express the chirp directly in terms of the laser power output [124]–[126]:

$$\Delta\nu(t) = \frac{1}{2\pi}\frac{d\phi(t)}{dt} = \frac{\alpha}{4\pi}\left\{\frac{d}{dt}\ln P(t) + \kappa P(t)\right\} \tag{3.46}$$

Note that Eq. 3.46 describes the change in frequency due to changes in the carrier density only. Temperature also affects the refractive index, and hence frequency, of semiconductor lasers. However, changes in temperature occur over slow timescales and the effects on frequency are negligible at the high speed modulations (> 100 MHz) used for direct phase modulation in quantum communications [126].

The first term in Eq. 3.46, proportional to the rate of change of the (natural log) power, represents changes in frequency due to relaxation oscillations of the carrier density after the applied current is suddenly changed. Relaxation oscillations are damped and so this term is called the "transient" chirp. If a laser is modulated up and back down, such that the power before and after the modulation is equal, then the phase change induced by the transient chirp is exactly zero. We can therefore focus on the second term, called the "adiabatic" chirp, which represents changes in frequency between different steady state values of power. Adiabatic chirp is a consequence of gain compression: at high power outputs non-linear effects reduce the gain. The main effect is spectral hole burning, where spontaneous emission leads to a dip or "hole" in the inhomogeneously broadened laser gain spectrum at the lasing frequency [112], [125], [127]. The carrier density must then increase to recover the same level of gain required for lasing. The carrier density is therefore not exactly clamped above threshold, rather it varies in proportion to the power and the gain compression factor, producing adiabatic chirp.

We can now express a change in phase as a function of power. Integrating Eq. 3.46 and considering only the adiabatic chirp, gives:

$$\Delta\phi = \frac{\Gamma\alpha\varepsilon}{V\eta hv}\int_{t}^{t+t_m} P(t)dt \tag{3.47}$$

where t_m is the duration of the modulation. As an approximation we can consider the ideal case where the power is simply proportional to the injected current above threshold $P = \frac{\eta hv}{2q}(I - I_{\text{th}}$ (neglecting the turn-on delay and relaxation oscillations)[126]. For an ideal square pulse modulation, as in Fig. 3.11, the change in phase is therefore:

$$\Delta\phi = \frac{t_m\Gamma\alpha\varepsilon}{2qV}\Delta I \tag{3.48}$$

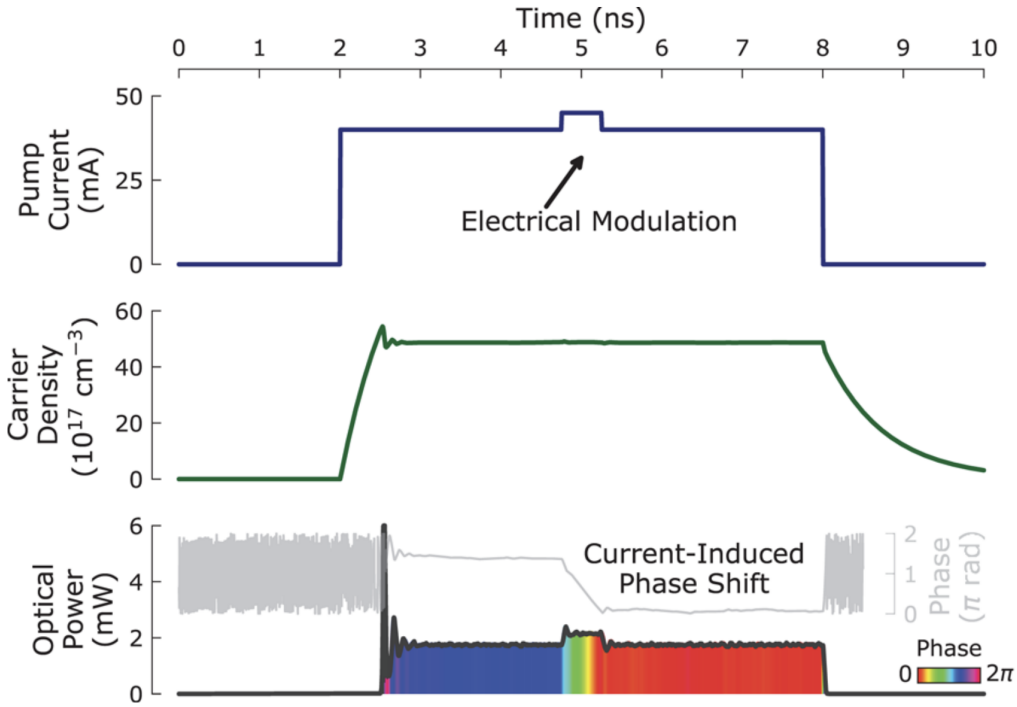

Figure 3.11: By adding an electrical modulation "notch" to the input current the phase of a laser pulse can be deterministically controlled by tuning the height and duration of the modulation. By using this directly modulated phase to lock another (slave) laser using OIL, the slave laser phase can likewise be controlled, removing the need for discrete phase modulators. Reproduced from Ref. [11].

For realistic laser parameters (Table 3.1), and a modulation time of 250ps, a $\sim 7.4\,\text{mA}$ modulation would be required to achieve a π phase shift.

In conclusion, using OIL it is possible to encode phase differences within pairs of coherent pulses, while ensuring phase randomisation between different pairs of pulses, only by adjusting the driving current of the master laser. No modulators are required.

A further recent work has shown that a directly-phase modulated transmitter can also produce *intensity modulated* pulses of light, which is essential for implementing decoy state QKD [128]. This removes the need for any intensity modulators.

The application of OIL for designing modulator-free QKD transmitters offers several significant benefits. By eliminating the need for external modulators, the overall complexity and cost of the QKD system can be reduced [128], [129]. This can lead to more accessible and affordable

quantum communication technologies, particularly for large-scale and resource-constrained deployments.

3.7 Summary

In this chapter we provided an introduction to laser physics. We focused on three aspects of semiconductor lasers most relevant to quantum cryptography and this thesis, namely gain-switching, phase randomisation and optical injection locking.

In the following chapter we will draw on and build upon the knowledge presented in this chapter, and the wider semiconductor laser literature, to quantify phase noise in gain-switched laser diodes.

Chapter 4

Characterising Phase Noise in Semiconductor Lasers

The contents of this chapter are based on results previously published in [12].

Phase noise is typically an undesirable property of laser light. Coherence is the defining feature of laser light, and phase noise degrades this coherence. In quantum cryptography, however, phase noise is a valuable resource which is used to minimise the information available to an eavesdropper in QKD, and generate random numbers in QRNG. Of course, both QKD and QRNG also require coherence. For example, a typical QKD transmitter produces a train of pairs of pulses with a fixed phase relationship within each pair, but with no phase relationship between pairs. This shows how in quantum cryptography there is a subtle interplay between phase randomisation and phase coherence, allowing information to be carried by coherent phase differences between pulses, but using phase randomisation to limit the amount of information available to an eavesdropper.

Given the importance of phase randomisation and phase coherence in quantum cryptography, it is important to accurately quantify and characterise both quantities. This is true both for

QKD and QRNG. In the following, however, we will focus on QRNGs, since we will be using tools and methods from the field of QRNG to interpret our results. In a way, using a gain-switched laser for phase randomisation in QKD is equivalent to having a phase noise QRNG "built-in" to the transmitter. The underlying physics are the same.

4.1 Quantifying Phase Noise

Quantifying phase coherence is straightforward, by e.g. measuring interference visibility. Quantifying phase noise on the other hand, is more difficult. In QRNG, we want to ensure that the phase is random due to spontaneous emission in the laser cavity, which is a quantum process, and not some other classical process such as temperature fluctuations or electronic noise. But we can't determine this is the case just by measuring the phase of the light emitted by the laser. In order to guarantee a random phase that is quantum in origin, it is necessary to have a theoretical model of the quantum process. This way, any claims of randomness are backed up by a theoretical model and understanding of the underlying physical process.

In the previous chapter, Sec. 3.5.1, we saw that the phase is a Gaussian random variable, and is quantified by the phase variance. For a CW laser, we reproduced equations by Henry to show that the phase variance $\langle \Delta\phi^2(t) \rangle$ increases linearly over time, and determines the coherence time t_c of a laser:

$$\left\langle \Delta\phi^2(t) \right\rangle = \frac{R\,(1+\alpha^2)\,t}{2S} = \frac{2t}{t_c} \tag{4.1}$$

Typical coherence times for a semiconductor laser are on the order of 100 ns. This means that one must wait $\gg$ 100 ns for the laser phase to become fully random. This requirement would severely limit the repetition rate of modern QKD or QRNG systems, which are commonly operated at GHz speeds. Gain-switching drastically increases the phase randomisation between

pulses, increasing the rate at which the phase noise can be sampled, and is therefore widely used in high-speed QRNG and QKD systems.

However, quantifying the phase noise of a gain-switched laser diode is not as straightforward as using Eq. 4.1. In this chapter we present a method of quantifying the phase noise, due to spontaneous emission, of a gain-switched laser diode by using a laser rate equation model. With this method we are able to quantify the phase noise of a laser with any arbitrary driving current, including gain-switching. First, we implement state-of-the-art techniques from the field of fibre-optic communications to calibrate the rate equation parameters based on experimental measurements. For engineering high-end telecommunication devices, it is essential to predict what the diode performances will be with different modulation regimes and for this reason an extensive literature has developed on the subject of semiconductor laser modelling and characterisation [8], [9], [112], [130]. With these analytical and numerical tools we build a model that can be used to identify the operational limits within which semiconductor lasers should be operated for random number generation.

Second, we develop simple method for measuring phase noise in gain-switched semiconductor lasers. This allows us to validate the operational limits established by the model by comparing measurements of the phase noise to the model predictions. The device characterisation can be performed at the beginning of the operational lifetime of the device, as part of a certification process. Once the model parameters have been determined, verified, and the operational limits established, the QRNG can be programmed to monitor certain key parameters, such as bias current, or level of phase noise, and take corrective action if these parameters fall outside the operational range established by the characterisation. Furthermore, the model can be used to explore different parameters and select optimal ones to maximise performance.

4.2 Prior Literature

Previous works have attempted to address the challenge of quantifying the phase noise of a gain-switched laser. The use of gain-switching to maximise laser phase noise for QRNG was pioneered by Jofre et al. [87]. In Ref. [89] the authors use a rate equation model to estimate the phase noise. The model parameters were a combination of typical parameters for semiconductor lasers, not specific to their own laser, and parameters that were selected to best fit the observed gain-switched power output of the laser. They quantify the phase noise using Eq. 4.1 as a *lower bound* of the phase noise over time. By solving the rate equations they calculate R and S for their measured gain-switching current input, and use Eq. 4.1 to establish the lower bound on the phase noise generated over one period.

Ref. [131] presents a method of measuring phase randomness by observing the visibility of interference between successive pulses from a gain-switched laser. This technique was used to verify that a gain-switched laser diode can be operated at 10 GHz with sufficient phase randomisation for the secure implementation of QKD protocols.

Another rate equation-based approach is presented in Ref. [132]. The authors implement a stochastic rate equation model to analyse the phase noise. They use the Monte Carlo method to estimate the variance of the phase due to phase noise. This approach has the advantage of not relying on linear approximations such as Eq. 4.1 and accounting for non-linear effects, such as relaxation oscillations, which are significant for gain-switched lasers.

In this work we build upon previous results [89], [131], [132] and develop a stochastic rate equation model to quantify laser phase noise. We provide two main improvements: first, we borrow established techniques from the field of classical optical communications to extract the rate equation model parameters for our specific laser. Second, we develop a novel method for

measuring laser phase noise in a gain-switched laser. Together, these improvements allow us to make accurate quantitative simulations of the laser power output and phase noise, and to verify the accuracy of these simulations with comparisons to experimental measurements. This work therefore presents a complete picture, from modelling to calibration measurements and experimental verification of the model.

4.3 Extracting the laser rate equation parameters

The values for the laser rate equation parameters we used in Section 3.2 were typical values for a semiconductor lasers. However, in practice, every laser will have a unique set of rate equation parameters, even if the lasers are produced by the same manufacturer and in the same production batch. To accurately model the behaviour of the specific laser being used in a QKD or QRNG system, it is therefore important to estimate, or extract, the parameters based on measurements of that laser. In the following section we implement a parameter extraction method based on simple measurements of three quantities [102]–[104]: the laser intensity modulation (IM) response, the transfer function of a dispersive optical fibre and the power-current (P-I) curve of the laser. Analytical expressions for these quantities can be derived from the rate equations, thereby relating the rate equation parameters to experimentally observable quantities. By fitting these measurements to their analytical expressions, we can estimate all the rate equation parameters. These three measurements were selected for being simple to implement using standard fibre optic laboratory equipment, while fully constraining the rate equation parameters.

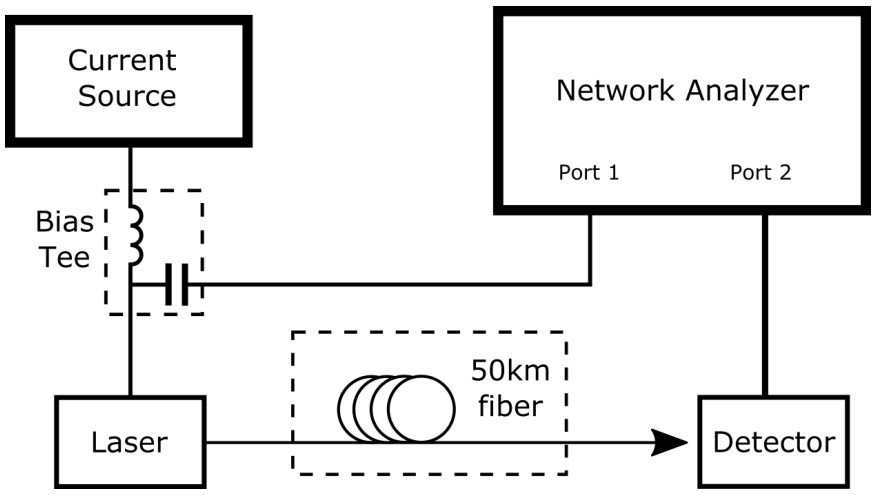

Figure 4.1: Setup for measuring the laser IM response (without the fibre) and the transfer function of 50km of dispersive fibre. Port 1 of the network analyser sends a small modulation signal to the laser, and Port 2 measures the response at the detector. The current source sets the bias current of the laser.

4.3.1 Experiment

Our experimental setup is shown in Figure 4.1. We use a commercial DFB laser (Gooch & Housego, AA0701 series) at telecom wavelength (1550nm) and an in-built isolator (>30 dB). The laser has an in-built bias-tee and a direct SMA connection for the RF modulation signal, enabling a high modulation bandwidth (>10 GHz). It also has an in-built TEC and thermistor, which are controlled by an external TEC controller (ThorLabs TTC001).

A network analyser (13.5 GHz) is used to measure the intensity modulation response of the laser and the fibre. One port of the network analyser is connected to the laser using a bias tee to superimpose a small AC current over the DC bias current. The second port of the network analyser is connected to the detector in order to measure the response of the laser to the input AC modulation sent from the first port. The network analyser is able to sweep the AC modulation over the full range of its bandwidth, and at each modulation frequency along the way measure the response. The network analyser therefore gives us a straightforward experimental method to measure the laser intensity modulation response.

The laser rate equation parameters are extracted by fitting these experimental measurements to analytical equations. In order to achieve a proper fit from the measurement, it is important to measure the main features of the response, in particular the peak of the response near the relaxation oscillation frequency, and the steep drop-off of the response at higher frequencies. A typical value for the relaxation oscillation frequency is a few GHz, and so each component in the experimental setup should have a bandwidth well above this. As mentioned, our network analyser has a bandwidth of 13.5 GHz. The detector is a photodiode with a 10 GHz bandwidth. The cables carrying the AC currents to the laser, and from the photodiode are coaxial cables with DC-26 GHz bandwidths.

For the measurement of the transfer function of a dispersive optical fibre, we employ ~ 50 km of single-mode optical fibre that connects the laser with the detector. When measuring the laser IM response, we connect the laser to a variable optical attenuator, which is then connected to the photodiode with a single-mode fibre patch cord.

The third measurement we carry out is of the laser P-I curve. For this measurement, we connect the laser output directly to a power meter, and the network analyser is not used.

In the following, we describe each measurement in turn along with the analytical equations, derived from the rate equations, used to fit the measurements. To verify the accuracy of the extracted rate equation parameters, we compare the model predictions of the power output of a gain-switched laser to experimental measurements.

4.3.2 Laser Intensity Modulation Response

In Sec. 3.4.3 we presented an expression (Eq. 3.31) for the intensity modulation response of a laser, that is, the output power modulation which is produced from a given input current

modulation, as a function of frequency. This expression depends on several rate equation parameters, such as the gain compression factor, and the photon lifetime. We can measure the intensity modulation response experimentally using a network analyser in the setup depicted in Fig. 4.1, and fit the results to Eq. 3.31 using the rate equation parameters as fitting parameters. This gives us experimental access to these parameters.

Recall the intensity modulation response is given by:

$$H(\omega) = \frac{P_{\mathrm{AC}}(\omega)}{I_{\mathrm{AC}}(\omega)} = \frac{\omega_R^2 \eta h v/q}{\omega_R^2 - \omega^2 + j\omega\gamma} \tag{4.2}$$

where:

$$\omega_R^2 = \frac{gS}{\tau_p(1+\epsilon S)} \tag{4.3}$$

$$\gamma = K f_R^2 + 1/\tau_n \tag{4.4}$$

$$K = 4\pi^2 \tau_p \tag{4.5}$$

We can rewrite Eq. 4.3 in terms of what we actually control and measure in experiment, that is, bias current and frequency respectively, using Eqs. 3.19 and 3.11:

$$f_R^2 = \frac{\Gamma g}{4\pi^2 q V}(I - I_{\mathrm{th}}) \tag{4.6}$$

Fig. 4.2 (left) plots the measured IM response at different levels of bias current. The resonance frequency peak can clearly be observed, and can be observed to shift towards higher frequencies for higher bias currents, as expected. However, we cannot yet fit these measurements to Eq. 4.2. The measurements in Fig. 4.2 are affected by the responses of the detector,

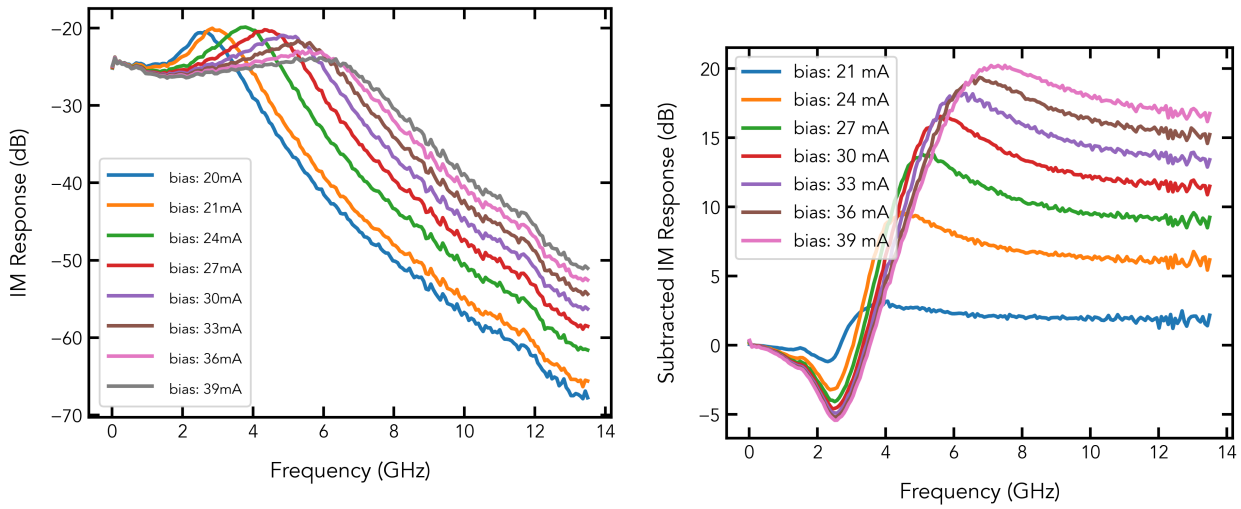

Figure 4.2: We measure the IM response at different bias currents above threshold. These measurements include non-laser effects due to the response of the detectors, electronics, etc. To remove the non-laser contributions, we subtract the IM response at 20 mA from each of the other measurements. The subtracted response depends only on the laser, and can therefore be fitted using the rate equations.

and the laser driving circuitry.

In order to get rid of these non-laser contributions to the overall response, first note that these contributions are independent of the bias current. Therefore, if we subtract two IM response measurements at different bias currents, all non-laser contributions will cancel out, and we will be left with the pure laser (subtracted) response. Fig. 4.2 (right) plots the corresponding subtracted response curves, where the IM response at 20 mA has been subtracted from all other measurements.

The subtracted response can then be fit to a modified expression, subtracting the IM response at two different bias currents:

$$S(f) = \frac{H(f, \omega_R, \gamma)}{H(f, \omega_{R0}, \gamma_0)} \tag{4.7}$$

where ω_{R0} and γ_0 are the resonance frequency and damping factor at the baseline bias current, which we chose to be 20 mA.

We use ω_R, γ, ω_{R0} and γ_0 as fitting parameters to fit each measured subtracted response. Note that ω_{R0} and γ_0 should be constants, however each fitted measurement will yield slightly different values, due to statistical variations between measurements and randomness in the optimisation algorithm. We therefore carry out the fitting process in two steps: first, we fit all the subtracted response curves using all four fitting parameters. We then fix the values of ω_{R0} and γ_0 to their average value across measurements. We then redo the fitting of all measurements using the average values obtained in the previous step for ω_{R0} and γ_0.

Fig. 4.2 (a) shows the resulting fitted subtracted IM response curves, at three different bias currents. Each of these fits will result in a value for the resonance frequency and the damping factor, at a given bias current. By plotting the resonance frequency (squared) against the bias current above threshold, and fitting to Eq. 4.6, we can obtain an estimate for the differential gain coefficient g. Next plotting the damping factor against the resonance frequency squared, we can obtain an estimate of the K-factor from the gradient, and of the carrier lifetime from the y-intercept, by fitting to Eq. 4.4. Our results our shown in Fig. 4.3, giving values of $g = 1.70 \times 10^{-6}\text{cm}^3/\text{ s}$, $\tau_n = 0.15$ ns and $K = 2.51 \times 10^{-10}$ s.

4.3.3 Fibre Transfer Function

The optical spectrum of a directly modulated laser contains modulation side-bands which travel at different velocities through dispersive optical fibre. After a certain distance these side-bands will interfere destructively, leading to a characteristic sharp dip in the fibre transfer function [133]. An analytical expression for the fibre transfer function, using a directly modulated laser, was derived in Ref. [134] and is given by [135]:

$$H_{\text{fibre}}(f) = \cos(\theta) - (\alpha - j\alpha f_c/f)\sin(\theta) \tag{4.8}$$

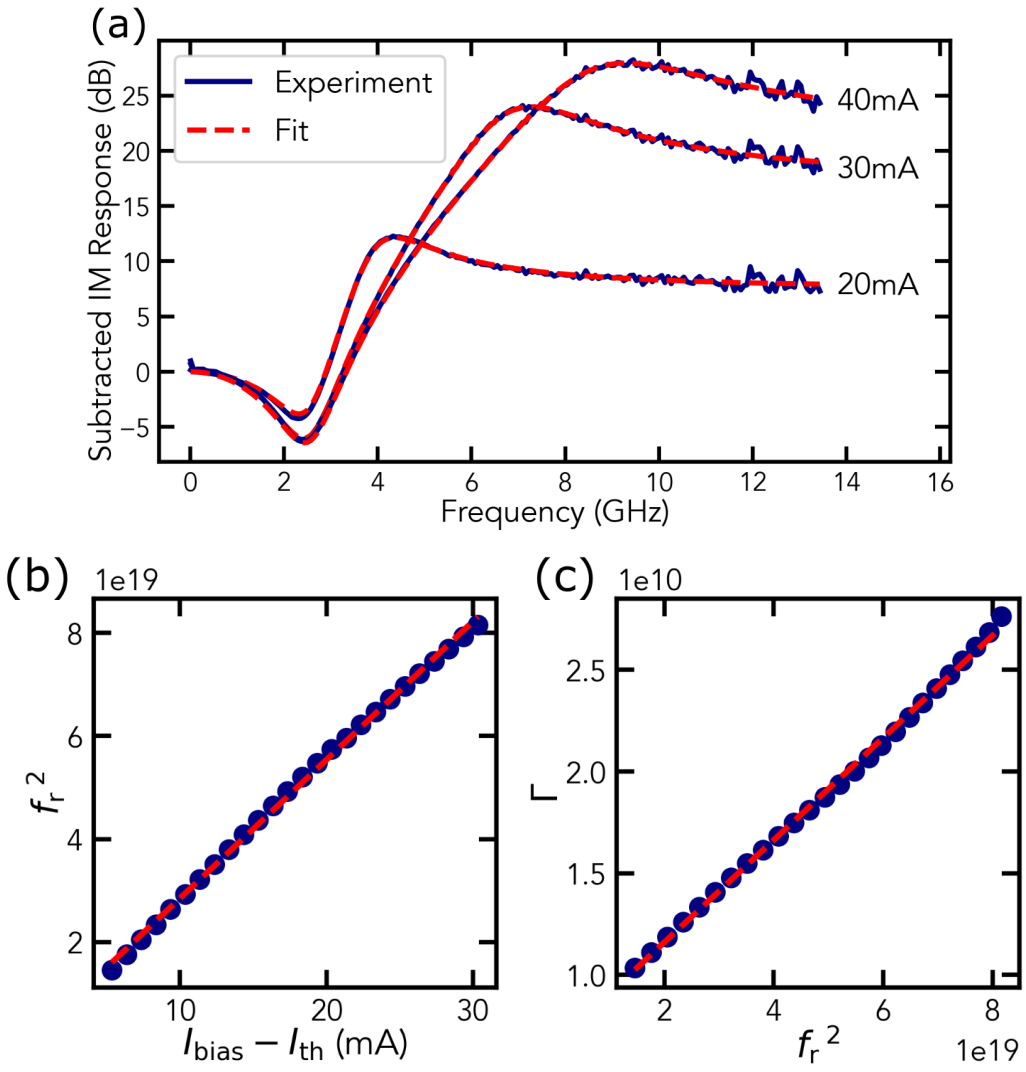

Figure 4.3: (Top) The laser IM response is fitted to Eq. 4.7 to obtain estimates for Γ and f_r at different bias currents. (Bottom) Using the fitted Γ and f_r values we can plot Eqs. 4.6 and 4.4. Linear fits give estimates for g, τ_n and the K-factor.

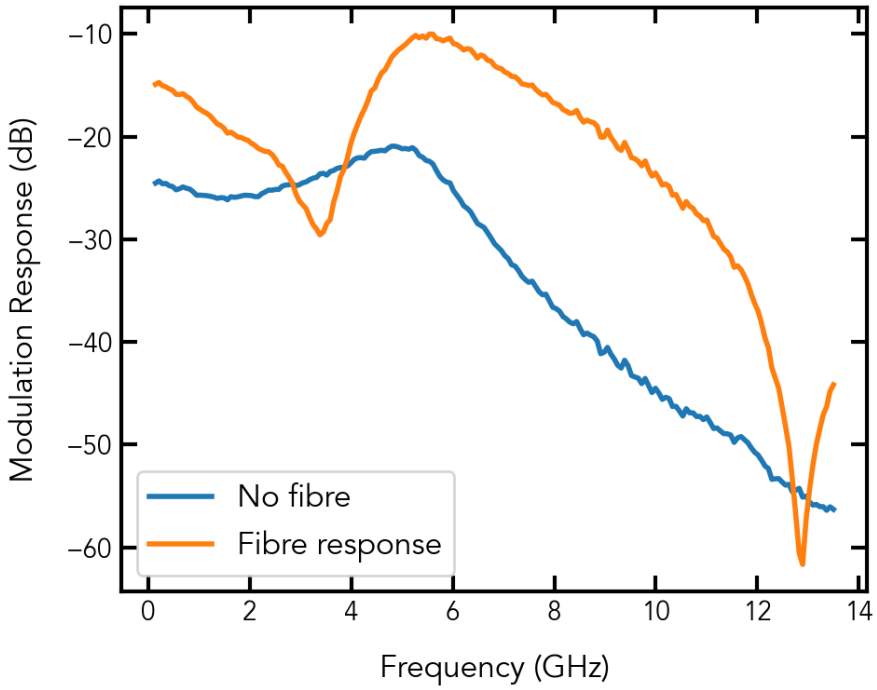

Figure 4.4: The modulation response of 50 km of single mode optical fibre (orange). The fibre response includes contributions from other experimental components, including the laser. To remove the non-fibre contributions, we subtract from the fibre response the IM response measured without the fibre (blue). The laser is biased at 30 mA. The ∼10 dB difference at 0 Hz between the fibre and no-fibre measurements is due to the optical attenuation introduced by the optical fibre.

where $\theta = f^2\pi\lambda^2 DL/c$ and $f_c = \Gamma\varepsilon\left(I - I_{\text{th}}\right)/(2\pi qV)$, D is the dispersion coefficient of the optical fibre, L is the length of the fibre and f_c the frequency at which the adiabatic and transient chirps (from Eq. 3.46) are equal [135]–[139]. The fibre transfer function can be measured using the same setup as for the laser IM response, and including ~ 50 km of standard single mode fibre between the laser and detector. The fibre can be of any length, however the sharp dips in the modulation response occur at smaller frequencies for longer lengths of fibre. Given the finite bandwidth of the network analyser (13.5 GHz in our case), a sufficiently long fibre must be used so that at least one of the dips occurs at a measurable frequency in order to properly constrain the fitting parameters.

As before, by fitting the measured response to the analytical expression we can estimate α

and f_c (and D, which we disregard). Again, the measured response will include contributions from the laser packaging and detector. Additionally, here we are interested in isolating the response of the optical fibre, so the laser response should be removed as well. All of the non-fibre contributions can be eliminated by making two measurements, one with the fibre, and one without, and subtracting them.

Fig. 4.4 plots the laser modulation response with and without the optical fibre. To account for the time-delay introduced by the 50km of fibre, the sweep time of the network analyser needed to be increased. Note also that the 50km of fibre adds significant attenuation ($\sim$10 dB) to the system, as can be seen by the $\sim$10 dB difference in the transfer function at $\sim$0 Hz, as seen in Fig. 4.4. We account for the additional attenuation introduced by the optical fibre, we add extra attenuation to the no-fibre measurement in order to equalise them. We measure the attenuation of the fibre using a power meter, and match that attenuation using a variable optical attenuator. Alternatively, the laser light for the fibre response measurement could be boosted using a coherent amplifier such as an Erbium-Doped Fibre Amplifier (EDFA).

The resulting subtracted response is plotted in Fig. 4.5. For this measurement, we can freely choose the laser bias current, since in principle this should not affect the (subtracted) fibre response. We select a bias current of 30 mA to obtain a reasonable power output, and this led to the best fit with the analytical expression, Eq. 4.8. Fitting the measurement to Eq. 4.8 gives values for for $\alpha = 2.95$ and $f_c = 5.85 \times 10^8$ Hz.

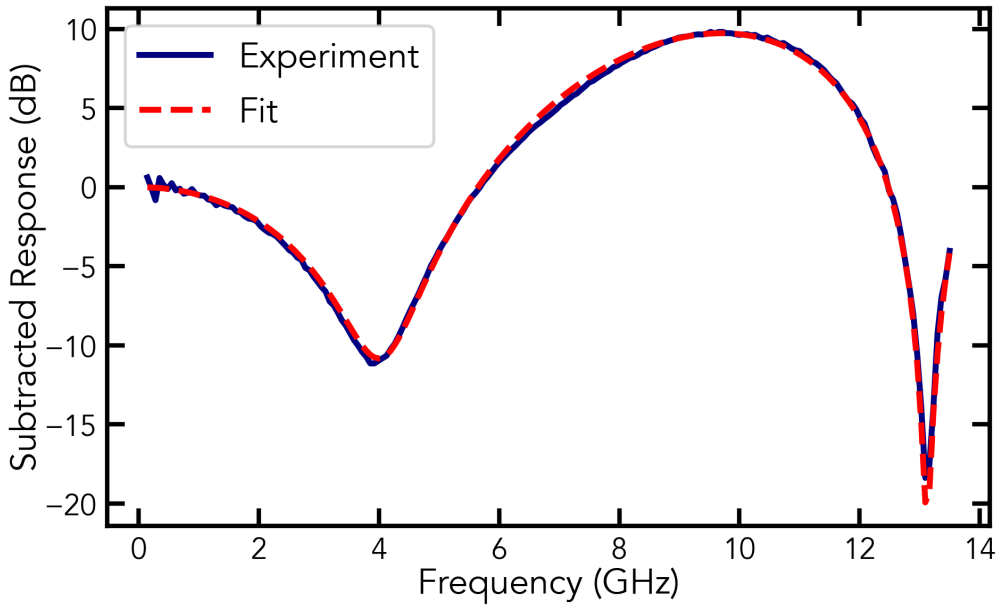

Figure 4.5: The fibre transfer function is fitted to Eq. (4.8) to obtain estimates for α and f_c. The laser is biased at 30 mA.

4.3.4 Steady State Power vs. Bias Current

Finally, in Chapter 3 we provided an expression for the power-current relationship of semiconductor laser, Eq. 3.20:

$$(\frac{2e}{\eta h\nu}P)^2 - (I - I_{\text{th}} - I_s)\frac{2e}{\eta h\nu}P - I_s I \approx 0 \tag{4.9}$$

where $I_s = \beta eV/(\Gamma g \tau_n \tau_p)$ and recall that the threshold current is related to the carrier density at threshold by:

$$I_{\text{th}} = \frac{eVN_{\text{th}}}{\tau_n} \tag{4.10}$$

We can express this in terms of the carrier density at transparency N_0 by considering that the at threshold, the laser gain is equal to to the cavity losses:

$$\Gamma g(N_{\text{th}} - N_0) = \frac{1}{\tau_p} \tag{4.11}$$

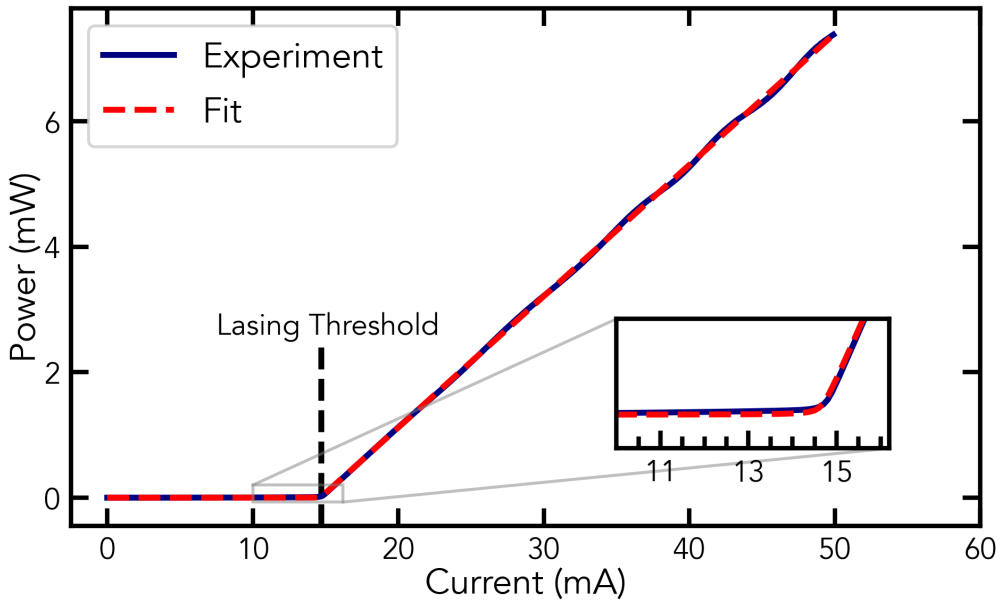

Figure 4.6: Fit of the laser P-I curve to Eq. 3.20, using F, I_s and I_{th} as fit parameters. The inset shows a good fit around the lasing threshold $I_{\text{th}} = 14.7\text{mA}$.

where we neglect the gain compression term because we are in near-threshold conditions. Re-arranging gives:

$$N_{\text{th}} = N_0 + \frac{1}{\Gamma g \tau_p} \tag{4.12}$$

Substituting into Eq. 4.10:

$$I_{\text{th}} = \frac{eV}{\tau_n}\left(N_0 + \frac{1}{\Gamma g \tau_p}\right) \tag{4.13}$$

The measured P-I curve can then be fitted to Eq. 3.20 to access these parameters. Our results are plotted in Fig. 4.6, giving values of $\eta = 0.52$, $I_s = 6.16 \times 10^{-4}$ mA and $I_{\text{th}} = 14.7$ mA.

In total, the fitted parameters are $g, \tau_n, K, \alpha, f_c, F, I_s$ and I_{th}, giving eight constraints to the rate equation parameters. There are ten rate equation parameters, however V and Γ just reflect the choice of expressing the rate equations in terms of number or density of carriers and photons. They do not affect the simulation results, and so we can assume a reasonable value for each: $V = 2 \times 10^{-17}\text{m}^3$ and $\Gamma = 0.2$. The remaining eight rate equation parameters are

Table 4.1: The extracted rate equation parameters, based on the measurements shown in Figs. 4.3, 4.5 and 4.6

Parameters	Values	Description
τ_n (ns)	0.15	Carrier lifetime
τ_p (ps)	4.47	Photon lifetime
g ($\times 10^{-6}$ cm^{3}s^{-1})	1.70	Differential gain coefficient
ε ($\times 10^{-17}$ cm^3)	3.24	Gain compression factor
N_0 ($\times 10^{18}$ cm^{-3})	3.79	Carrier density at transparency
β ($\times 10^{-5}$)	4.44	Spontaneous emission factor
α	2.95	Linewidth enhancement factor
η	0.52	Differential quantum efficiency
V ($\times 10^{-11}$ cm^3)	2	Active layer volume
Γ	0.2	Mode confinement factor

fully constrained by the fitted parameters, and can be calculated using the relationships stated above: $\varepsilon = 2\pi q V f_c/[\Gamma(I - I_{\text{th}})]$, where $I = 30$ mA; $\tau_p = K/(4\pi^2)$; $\beta = \Gamma g \tau_n \tau_p I_s/(eV)$; finally $N_0 = I_{\text{th}}\tau_n/(eV) - (\Gamma g \tau_p)^{-1}$. Alternatively, the rate equations can be rewritten in terms of the fitted parameters [102]. The extracted rate equation parameters for our laser, based on the measurements plotted in Figs. 4.3 - 4.6, are shown in Table 4.1.

In this study, while the rate equation parameters have been extracted, the associated uncertainties have not been quantified. Quantifying the uncertainty associated with these parameters is an important factor, particularly when these parameters are used to inform decisions related to device security. Developing a robust methodology to estimate these uncertainties is a key area for future research.

4.3.5 Comparison to Experiment

To confirm the accuracy of the model and extracted parameters, we compare the model predictions to experimental measurements. For a given current $I(t)$ the rate equations can be solved numerically to simulate the power output of the laser. We use the ordinary rate equations, Eqs. 3.3-3.5, without noise terms since we are here interested in the average power output.

Fig. 4.7 shows a comparison between the simulated and measured intensity output of the laser when driven at a repetition rate of 1 GHz for different bias currents. The good agreement between simulation and experiment was achieved after several adjustments to the rate equation simulations and experimental method. First, we noticed that using a square wave RF signal to drive the laser led to poor agreement with simulation due to high frequency parasitics from the laser circuitry and packaging. To minimise distortions to the driving current, we use a pure 1 GHz sinusoidal signal to drive the laser. Additionally, we measure the driving signal using an oscilloscope, and use this measured signal as input to the rate equations (instead of an ideal sinusoidal wave). Additionally, we model the finite-bandwidth (10 GHz) of the detector, which is the lowest bandwidth component in our setup, by applying a 10 GHz first-order low-pass filter to the rate equation solutions. This has the effect of reducing the amplitude of the relaxation oscillations, and we find it agrees better with the rate equation simulations.

Fig. 4.7 shows model correctly predicts the main features of the laser output: the steady-state power output, the turn-on delay and the amplitude, damping and frequency of relaxation oscillations.

4.4 Modelling Laser Phase Noise

Having verified the accuracy of the rate equation model for simulating the power output of a gain-switched laser, we now turn to simulations of the laser phase noise. Recall that the phase noise is quantified by the variance $\langle \Delta\phi^2(t) \rangle$ of the Gaussian-distributed phase. We cannot derive an analytical expression for this quantity, and instead we employ the Monte Carlo method: we repeatedly solve the stochastic rate equations, and calculate the variance of the resulting distribution of phase values to estimate $\langle \Delta\phi^2(t) \rangle$. To verify the accuracy of this estimate we again

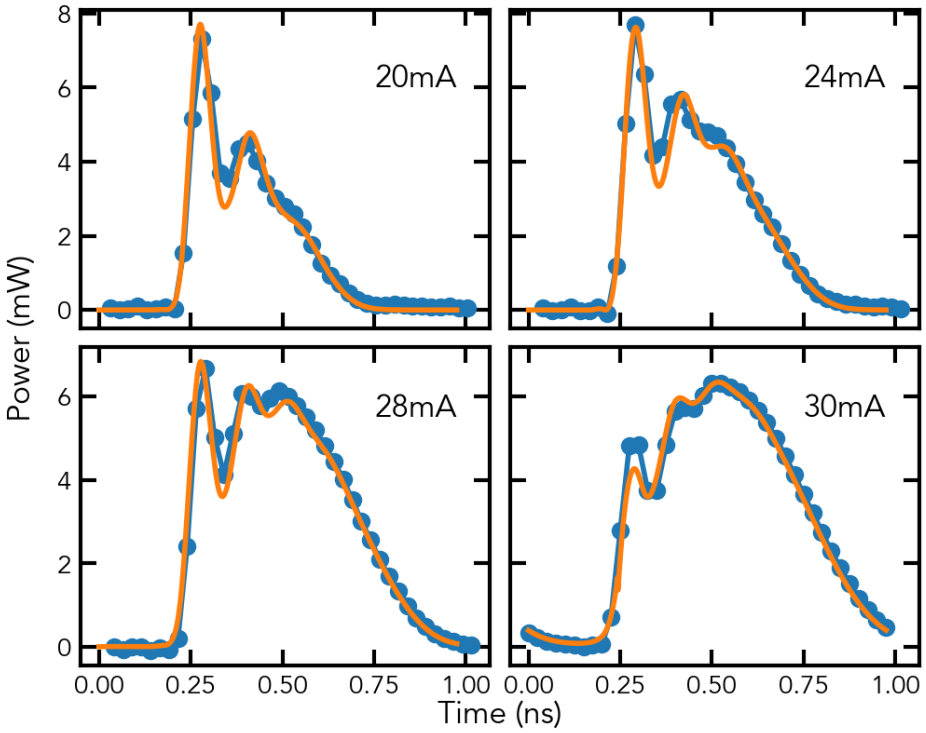

Figure 4.7: Measured and simulated laser pulses, at different bias currents (modulation current = 30 mA, repetition rate = 1 GHz). The good agreement is evidence that the extracted rate equation parameters are accurate.

compare the model predictions against experimental measurements. We cannot measure phase directly, but we can indirectly measure $\langle \Delta\phi^2(t) \rangle$ by observing the distribution of intensities at the output of an asymmetric interferometer, like in Fig. 2.5 [140]. The experimentally observable intensity distribution depends on $\langle \Delta\phi^2(t) \rangle$, giving experimental access to this quantity. What is needed, therefore, is an analytical expression that relates the observable intensity distribution to $\langle \Delta\phi^2(t) \rangle$. Ref. [140] achieves this by setting the fixed interferometer phase $\phi_0 = \pi/2$ and choosing a small interferometer delay such that $\sin(\Delta\phi) \approx \Delta\phi$. Eq. 2.9 then becomes:

$$I_{\text{out}} = \frac{I_{\text{in}}}{2}(1 + \Delta\phi) \tag{4.14}$$

such that the intensity is proportional to the phase and therefore the variance of the phase is simply proportional to the variance of the intensity, which can be measured. The shortcoming

of this method is that it is limited to small phase noise values for the small angle approximation to hold. We remove this constraint by using an analytical expression for the probability density function (PDF) of the intensity distribution for arbitrary phase noise values. This PDF was derived in Ref. [141], and here we quote the result. Box 3 provides a full and intuitive derivation. Let $Y = \cos(\Delta\phi + \phi_0)$ be the normalised intensity, ignoring units and displacements along the x-axis. Then the PDF of Y is:

$$f_Y(y,\sigma) = \sum_{n=-\infty}^{\infty} \frac{1}{\sqrt{1-y^2}} \Big[f_{\Delta\phi}(2(n+1)\pi - \cos^{-1}(y) + \phi_0, \sigma^2) + f_{\Delta\phi}(2n\pi + \cos^{-1}(y) + \phi_0, \sigma^2) \Big] \tag{4.15}$$

where f_Y is the PDF of the normalised intensity, $f_{\Delta\phi}$ is the PDF of the Gaussian distribution (with zero mean) and $\sigma^2 = \langle \Delta\phi^2(t) \rangle$. As required, this expression relates the distribution of the phase $f_{\Delta\phi}$ to the experimentally accessible distribution of the intensity, f_Y. By fitting measurements of f_Y to Eq. (4.15) we can estimate $\langle \Delta\phi^2(t) \rangle$ by using it as a fitting parameter. Eq. (4.15) includes an infinite sum, however, we can truncate the sum at $n = \pm 100$ with negligible effect on the results. One limitation of our method is that above a certain level of phase noise, f_Y becomes experimentally indistinguishable from an arcsine distribution. In fact, a wrapped Gaussian distribution with a large variance approaches a uniform distribution, so for large phase noise values f_Y approaches an arcsine distribution. Therefore, our technique is limited to measuring phase noise values below the threshold at which f_Y approaches an arcsine distribution. We find this happens around $\langle \Delta\phi^2(t) \rangle \approx 9$ which is in good agreement with previous results [89], [131], [141]. For our purposes this limitation is acceptable since we are exactly interested in determining whether the phase is approximately uniformly distributed, and hence do not need

to measure higher phase noise values. We refer to this threshold at which the wrapped Gaussian distribution approximates a uniform distribution as the "Uniform Distribution Threshold".

Box 3: Derivation of Eq. 4.15

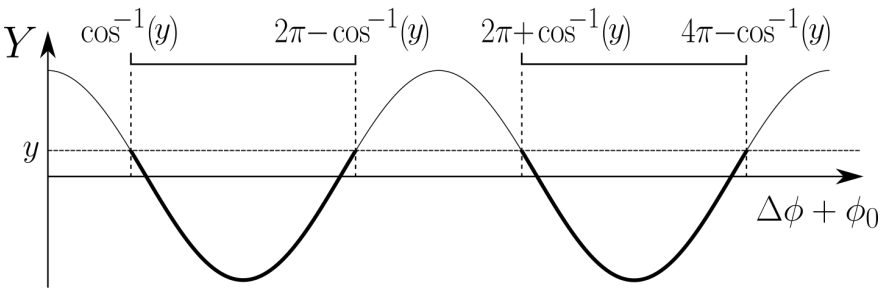

Figure 4.8: Visual aid to derivation of Eq. 4.15

We derive the PDF of the normalised intensity Y (f_Y) when the phase $\Delta\phi$ follows a Gaussian distribution ($f_{\Delta\phi}$). We first derive the cumulative distribution function (CDF) F_Y, and then differentiate it to obtain the PDF.

The CDF of $Y = \cos(\Delta\phi + \phi_0)$ is by definition:

$$F_Y(y) = \Pr(Y \leq y), \qquad y \in [-1, 1]$$
$$= \Pr(\cos(\Delta\phi + \phi_0) \leq y)$$

Fig. 4.8 shows a plot of Y.

The sections of the curve which are below y are drawn in bold. The probability that Y falls into one of these regions is therefore equal to the probability that the phase $\Delta\phi + \phi_0$ falls into one of the highlighted intervals on the x-axis. These intervals occur every 2π

radians and are given by

$$\begin{aligned}\Delta\phi + \phi_0 \in &[2n\pi + \cos^{-1}(y), 2(n+1)\pi - \cos^{-1}(y)] \\ \Delta\phi \in &[2n\pi + \cos^{-1}(y) - \phi_0, \\ &2(n+1)\pi - \cos^{-1}(y) - \phi_0]\end{aligned} \tag{4.16}$$

where $n \in \mathbb{Z}$. The probability that $\Delta\phi$ lies in one of these intervals is given by:

$$\begin{aligned}F_Y(y) = \sum_{n=-\infty}^{\infty} &\left[F_{\Delta\phi}(2(n+1)\pi - \cos^{-1}(y) - \phi_0)\right. \\ &\left. - F_{\Delta\phi}(2n\pi + \cos^{-1}(y) - \phi_0)\right]\end{aligned} \tag{4.17}$$

where $F_{\Delta\phi}$ is the CDF of the Gaussian phase distribution. The last step is to differentiate both sides of the equation, using the fact that $d/dy(F_{\Delta\phi}) = f_{\Delta\phi}$ and $d/dy(\cos^{-1}(y)) = -1/\sqrt{1-y^2}$, to obtain Eq. (4.15):

$$\begin{aligned}f_Y(y,\sigma) = \sum_{n=-\infty}^{\infty} &\frac{1}{\sqrt{1-y^2}} \\ &\left[f_{\Delta\phi}(2(n+1)\pi - \cos^{-1}(y) - \phi_0, \sigma^2)\right. \\ &\left. + f_{\Delta\phi}(2n\pi + \cos^{-1}(y) - \phi_0, \sigma^2)\right]\end{aligned} \tag{4.18}$$

Finally, we compare the model predictions with experimental measurements of the phase noise using the measurement technique just described. We perform a Monte Carlo simulation, calculating the laser phase evolution over one period (1 ns) 10,000 times by solving the stochastic rate equations under gain-switched conditions. We use a measurement of the pulse generator output to define the current $I(t)$ in the stochastic rate equations. An estimate for $\langle \Delta\phi^2(t) \rangle$

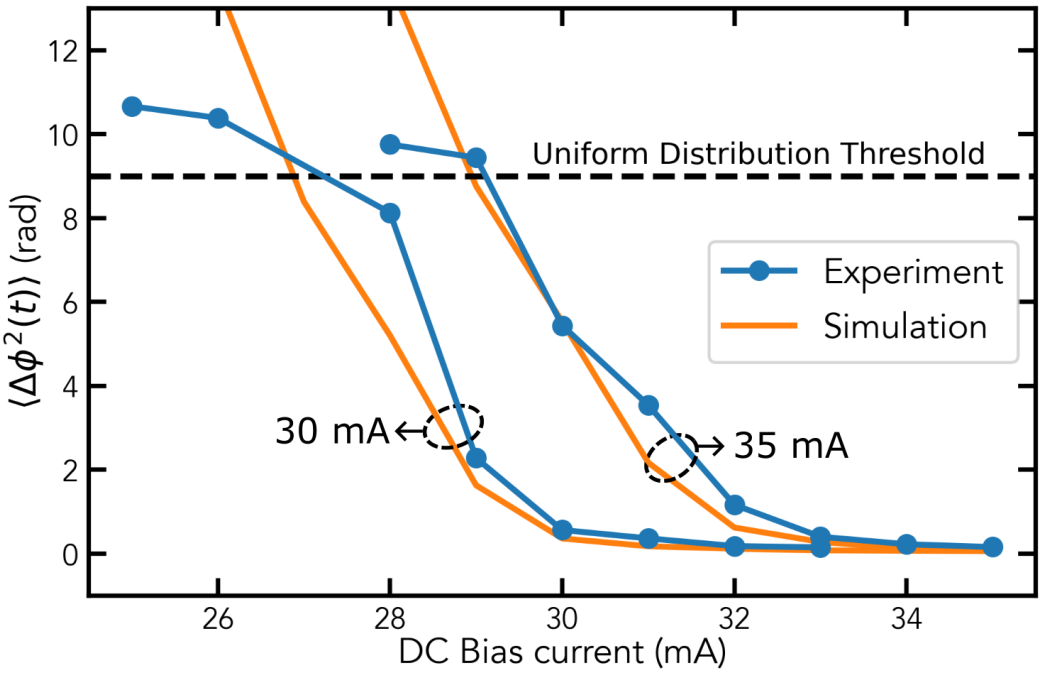

Figure 4.9: Comparison between measured and simulated values of the phase noise $\langle \Delta\phi^2(t) \rangle$ as a function of bias current. Measurements were taken for two different modulation currents (30 and 35 mA), as indicated. The threshold at which the wrapped Gaussian phase distribution becomes approximately uniform is marked with the dashed line labelled "Uniform Distribution Threshold". Above this threshold we are unable to measure higher phase noise values, since the phase noise distribution gets infinitesimally close to a uniform distribution. Therefore, at lower bias currents the experimental phase noise values plateau, while the simulation values continue to increase.

is then given by the variance of the 10,000 solutions for $\Delta\phi$. We use this approach to estimate $\langle \Delta\phi^2(t) \rangle$ as a function of the laser DC bias current, at two different modulation currents (30 and 35 mA). Our simulation results are shown in Fig. 4.9.

To measure the phase noise, we gain switch the laser using the same current parameters as in the simulation, and measure the output power over 25μs, corresponding to 25000 pulses. We sample the intensity of each pulse and plot a histogram which can be fit to Eq. (4.15), using $\langle \Delta\phi^2(t) \rangle$ as a fitting parameter[1].

[1]Note that when the measured distribution approaches an arcsine distribution, the optimisation can set $\langle \Delta\phi^2(t) \rangle$ to extreme values, since an arcsine distribution is compatible with phase noise values starting from around $\langle \Delta\phi^2(t) \rangle = 9$ to infinity. Therefore, in the optimisation, we implement a penalty to the value of $\langle \Delta\phi^2(t) \rangle$ which adds a cost to the objective function proportional to the size of $\langle \Delta\phi^2(t) \rangle$, preventing such extreme values. In practice, this leads to the fitted values of $\langle \Delta\phi^2(t) \rangle$ plateauing just above $\langle \Delta\phi^2(t) \rangle = 9$, as seen in Fig. 4.9

In our measurements we observed a slow drift of ϕ_0, on the order of rad/s, due to mechanical or thermal instabilities affecting the length difference between the short and long arm of the interferometer. This drift is much slower than our measurement time of 25μs, so the effect on individual measurements is negligible. However, ϕ_0 can take on different values for measurements at different times, and to account for this we include ϕ_0 as another fitting parameters. Additionally we model classical sources of noise, such as electronic noise, with a Gaussian distribution independent from ϕ_0 or $\langle\Delta\phi^2(t)\rangle$. The total intensity distribution from classical and quantum sources is then given by the convolution of the Gaussian classical noise, and the intensity distribution due to phase noise f_Y. We include the variance of the Gaussian classical noise as a third fitting parameter.

Fig. 4.10 shows examples of fitted intensity distributions for different bias currents of the laser, keeping other current parameters (modulation current = 30 mA; repetition rate = 1 GHz) constant. In Fig. 4.9 we plot the fitted values of $\langle\Delta\phi^2(t)\rangle$ alongside the simulation. We see that at low bias currents, the model predicts ever-higher phase noise values, while our measurements plateau around $\langle\Delta\phi^2(t)\rangle = 9$. This corresponds to the level of phase noise at which the intensity distribution becomes indistinguishable from an arcsine distribution. At this point, the phase noise distribution approximately uniform, and so we denote $\langle\Delta\phi^2(t)\rangle = 9$ as the "uniform distribution threshold".

At higher bias currents, with lower values of phase noise, we see a good agreement between experiment and simulation, verifying the accuracy of the model. Fig. 4.9 clearly shows the point at which the Gaussian phase becomes approximately uniform: when the intensity distribution becomes indistinguishable from an arcsine distribution at lower bias currents, the measured phase noise values plateau (around $\langle\Delta\phi^2(t)\rangle = 9$), while the simulation continues increasing. From our measurements we can therefore say that for a modulation current of 30 mA (35 mA),

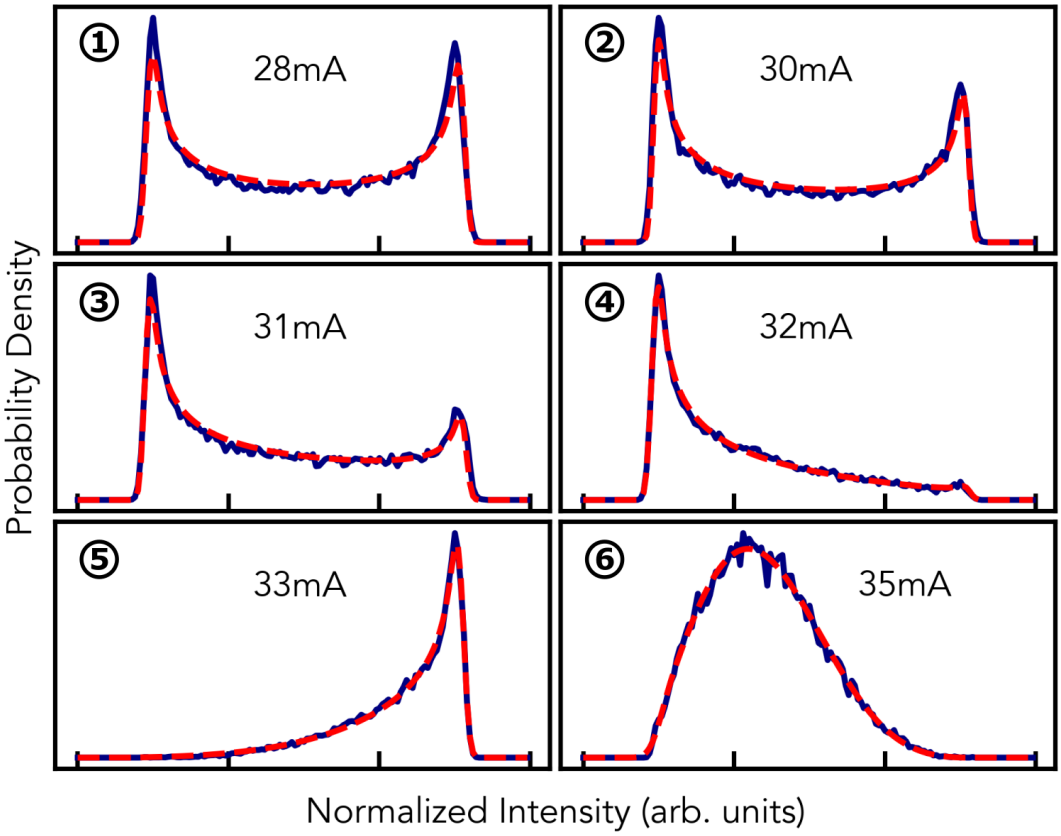

Figure 4.10: Measured intensity distributions at different bias currents, fitted to Eq. (4.15). The effect of the slow drift of the relative interferometer phase ϕ_0 can be seen by most clearly comparing the intensity distributions at 32 and 33mA. The peaks of the distributions are at different intensities, even when the phase noise is similar for both measurements.

a bias current below ∼26 mA (∼29 mA) is required to guarantee an approximately uniform phase, and hence the security of the QRNG.

4.5 Effects on performance

This contents of this section were primarily written by Davide Marangon as a co-author of Ref. [12].

The effect of poorly selected laser driving parameters on the performance of a phase-noise based QRNG can be made explicit by considering the min-entropy associated to the interference signal. The min-entropy quantifies the amount of identically and independently distributed (iid) bits in the digital codes, which are generated by an analogue-to-digital converter (ADC) sampling the photodiode current signal. We consider an (ideal) ADC with a resolution of d bits and a measurement range of R volts, such that the range is divided into 2^d intervals of width $\Delta = R/2^d$. We associate the random variable W to the ADC output codes, each code corresponding to the index of the voltage interval into which the PD signal is measured at the time of sampling, i.e., $[w\Delta, (w+1)\Delta)$, with $w \in \{0, 1, \ldots, (2^d - 1)\}$. The min-entropy of W is then defined as

$$H_{\min}(W) = -\log_2 \left[\max_w P_W(w)\right] \tag{4.19}$$

where the discretised sample probability $P_W(w)$ is given by

$$P_W(w) = \int_{w\Delta}^{(w+1)\Delta} f_Y(y, \sigma) dy \tag{4.20}$$

where f_Y is the PDF of the interference signal given by Eq. 4.15, allowing us to calculate the min-entropy as a function of phase noise[141]. In case of high phase randomisation, the in-

terferometer output intensity and therefore the amplitude of the PD signal, follows an arcsine distribution. In this case $\max_w P_W(w)$ corresponds to either the destructive or the constructive signal amplitudes, $Y = y_d$ and $Y = y_c$. For example, if y_d and y_c fall into intervals w and w' respectively, $\max_w P_W(w)$ will correspond to the largest between $\int_{y_d}^{(w+1)\Delta} f_Y(y,\sigma)dy$ and $\int_{w'\Delta}^{y_c} f_Y(y,\sigma)dy$. Ideally, in the absence of fluctuations and additive electronic noise, the distribution fits the whole range R such that codes $w = 0$ and $w = (2^d - 1)$ occur with the same discretised probability. Hence, if we assume a typical ADC resolution of $d = 8$, when the phase noise is uniformly distributed we obtain $H_{\min}(W) = 4.65$ bits.

We can now see how a non-uniform phase distribution will negatively affect the QRNG performance, by lowering the min-entropy of the raw output distribution. Fig. 4.11 plots the min-entropy as a function of phase noise $\langle \Delta\phi^2(t) \rangle = \sigma^2$ with $d = 8$ and $\phi_0 = 0$. When the phase is not fully randomised, the resulting intensity distribution will become more asymmetric, as shown in Fig 4.10. Crucially, this asymmetry will lead to a decreased min-entropy: since one of the peaks in the distribution becomes larger, the probability of the most-likely outcome likewise increases. The physical reason for this behaviour is that the smaller $\langle \Delta\phi^2(t) \rangle$ the less the phase changes from pulse to pulse and hence the higher becomes the probability constructive and near constructive interference events.

We can combine this result with our simulations of the min-entropy as a function of phase noise (Fig. 4.9) to directly relate the min-entropy to the bias current. We indicate in Fig. 4.11 the points along the min-entropy curve corresponding to different levels of bias current, as measured in Figs. 4.9 and 4.10. In this way, combining the rate equation simulations with the analytical calculations of the min-entropy, we can quantify the effects on the performance of the QRNG as a function of the DC bias current directly, or any other current or laser rate equation parameter.

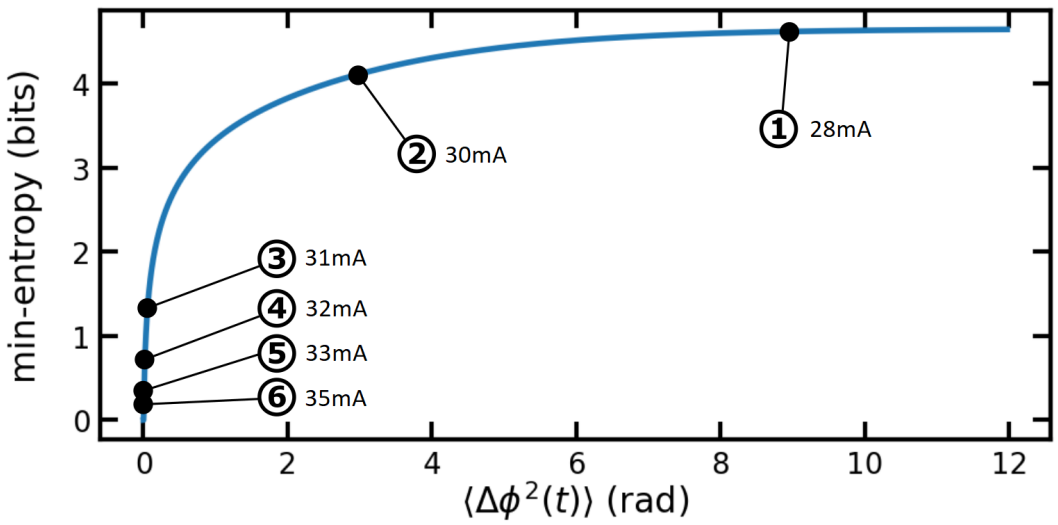

Figure 4.11: The min-entropy as a function of the phase noise, assuming 8-bit digitisation resolution. The min-entropy quantifies the extractable randomness of the QRNG and is proportional to the secure random number generation rate. The numbers correspond to the measurements plotted in Fig. 4.10 at different bias currents, indicating a clear connection between the bias current, the phase noise, and the performance as quantified by the min-entropy.

Given the min-entropy, the ADC output should be processed with a seeded randomness extractor, such as a 2-universal hash function, in order to actually distil the iid bits from the samples. It is worth stressing that $H_{\min}(Y)$ in Fig. 4.11 is not taking into account various factors such as dependencies among the samples, non-idealities of the ADC, electronic noise, laser fluctuations, so it overestimates the actual entropy content one would obtain in a realistic situation. However, since the post-processed generation rate is proportional to the min-entropy, Fig. 4.11 shows the critical loss of secure bits the QRNG user would experience in case the laser drifts away from the driving conditions that guarantee the larger phase randomisation. In this situation, although the rate diminishes, the distilled random bits are secure as long as the randomness extractor is re-calibrated on the actual min-entropy value.

This is not the case if instead of using a seeded randomness extractor, the user implements some unseeded post-processing algorithm. We consider an unbiasing algorithm based on finite impulse response (FIR) filters [90], [94], [142], in which the unbiased output code $u(n)$ is given

by scrambling together the last $n - M$ ADC codes $w(n)$, i.e., $u(n) = \sum_{i=0}^{M} b_i w(n-i) \mod 2^d$ where b_i are the coefficients of the filters. As FIR filter based processing does not compress the raw random numbers, the generation rate is constant. This makes them a practical solution for applications such as Monte Carlo simulations, which consume large amount of data but are less recommendable for cryptographic applications, since the generation rate does not depend on the actual min-entropy content.

As an experimental demonstration, we use the standard phase noise QRNG setup from Fig. 2.5 with the laser operated at 1 GHz, the PD sampled at 1 GSample/s by an ADC with 8 bit resolution, which we employ to generate 1 GB of raw output numbers at different levels of DC bias current while keeping constant the modulation amplitude. We then use the fifth order FIR filter, i.e., $M = 4$ and with binomial coefficients $b_i = \frac{M!}{i!(M-i)!}$ [90] and analyse the results using the batteries *Rabbit* and *Alphabit* of the suite TestU01 for statistical randomness assessment [143]. These batteries are applied to the whole $8 \cdot 10^9$ bit long strings and Fig. 4.12 shows the test results at each level of bias current. As one can appreciate, when the laser is properly driven with low bias current, the FIR filter is very effective in unbiasing the output, since the tests output acceptable p-values. However, starting at 32mA, the QRNG begin to fail more tests and from 33mA onward most of them fail catastrophically. Comparing these values of bias current to Fig. 4.9 we see that at these levels of bias current, the phase noise is well below the uniform distribution threshold. So, again, the rate equations help determine the operational limits of DC bias current, or any other rate equation parameter, required for the correct operation of the QRNG.

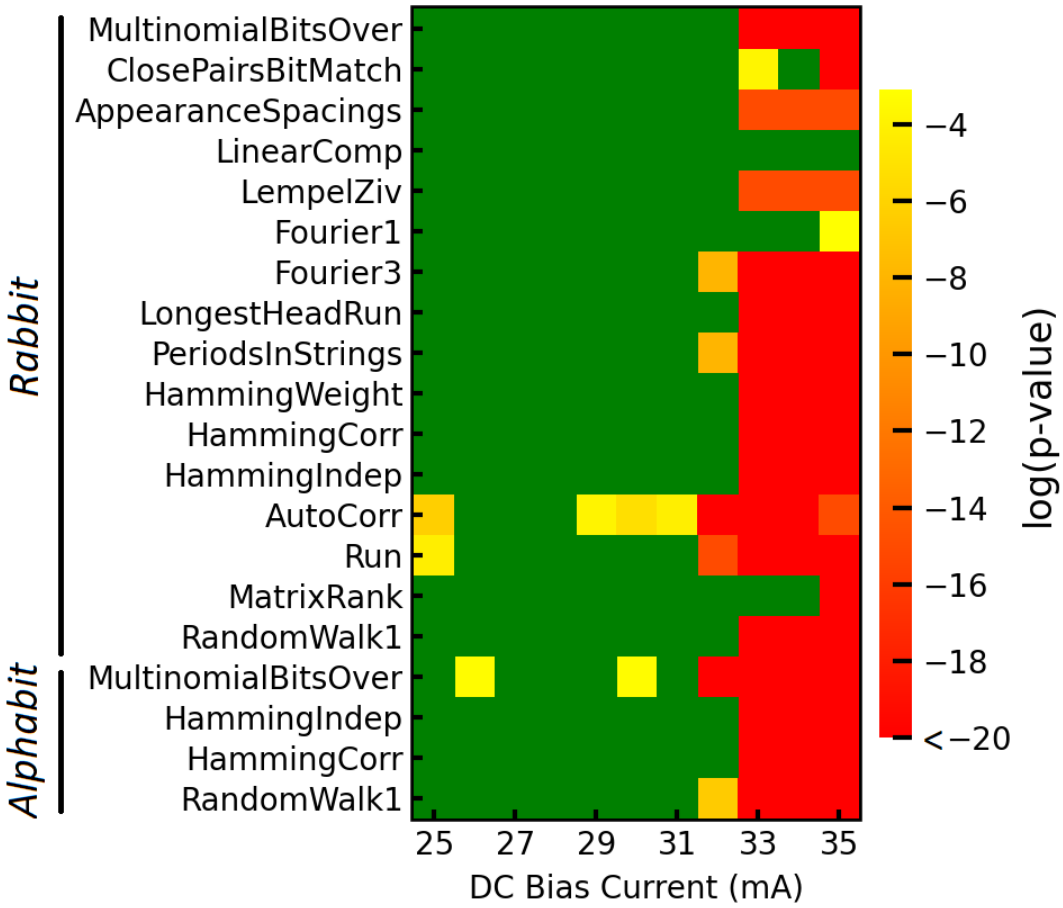

Figure 4.12: The p-values of different statistical tests from the TestU01 randomness testing suite applied to 1GB of raw data from the QRNG at different bias currents. The bottom four tests correspond to the Alphabit battery of tests, and the rest are from the Rabbit battery of tests. Passed tests are drawn in green, and the p-values of the failed tests (p-value below 0.001) are indicated by the colourbar. Starting at 32 mA, the QRNG fails several tests with very low p-values, indicating that the phase noise, and hence entropy, is too low for the unbiasing algorithm to completely remove bias and correlations from the generated numbers.

4.6 Maximising Min-Entropy with a Non-Uniform Phase

We have demonstrated how the rate equation model can be used to quantify the phase noise of a gain-switched laser. Further, we have linked the phase noise to the generation rate of a QRNG, using the min-entropy. Throughout our discussion we have assumed the typical operation of a phase noise QRNG where the phase is allowed to fully randomised between pulses. However, in this section we will demonstrate that, counterintuitively, we can achieve higher min-entropy with *lower* levels of phase noise.

Using the same analytical tools developed in the previous section, in particular Eq. 4.15, we can optimise the min-entropy as a function of phase noise. Remarkably, we find that the maximum min-entropy obtainable by a phase noise QRNG does not occur when the phase is fully random, that is, uniformly distributed. This is because with a phase noise QRNG we do not measure the phase directly, but rather the intensity after an AMZI, according to Eq. 2.9. The PDF of the output intensity is an arcsine distribution when the phase is uniformly distributed, and the arcsine distribution has a lower min-entropy than a uniform one. However, when the phase is not fully random, then the PDF of the output intensity depends on the fixed interferometer phase ϕ_0, as stated in Eq. 4.15. To illustrate, Fig. 4.13 plots the evolution of the PDF of the output intensity for different levels of phase noise, and different values of ϕ_0. We can see that when ϕ_0 is 0, the PDF is very asymmetric. For low values of phase noise almost all interference is constructive, leading to a sharp peak in the PDF at high-intensity. And as the phase noise increases, the PDF tends towards an arcsine as expected.

However, consider the case when $\phi_0 = \pi/2$. Then there is an equal likelihood of there being slightly constructive, or destructive interference, and the PDF is symmetric. For low phase values the PDF looks Gaussian, centred at $I_{\text{out}}/2$. And again, as the phase noise increases, the

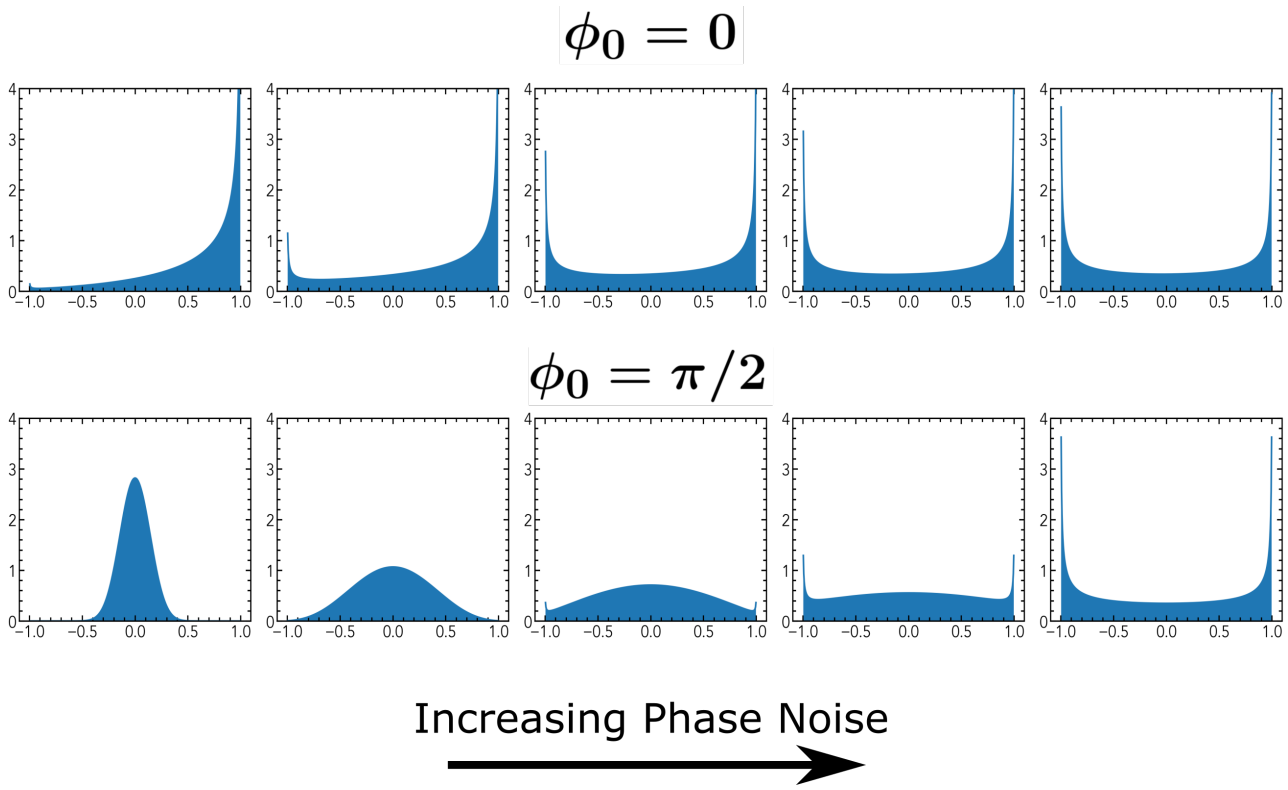

Figure 4.13: The intensity distribution at the interferometer output for not fully randomised phase, at two different values of the fixed interferometer phase ϕ_0. When $\phi_0 = 0$, most of the interference is constructive, leading to a large peak of the distribution at the highest intensity. However, when $\phi_0 = \pi/2$, the intensity distribution is symmetric and spreads out with increasing phase noise. We can see that the maximum min-entropy is obtained when $\phi_0 = \pi/2$ and the phase noise is not fully randomised (bottom, centre).

PDF tends to an arcsine distribution. But, crucially, for a certain range of phase noise values the min-entropy of the PDF, corresponding to the highest peak in the distribution, is actually lower than for an arcsine distribution. The min-entropy is therefore maximised for an interferometer phase difference of $\phi_0 = \pi/2$ and with a non-uniform phase distribution.

If we plot the min-entropy of the PDF when ϕ_0 as a function of the phase noise, we obtain Fig. 4.14. Note the discontinuity of the min-entropy around a phase noise value of ~ 0.5. This discontinuity arises because until that point, corresponding to Figs. 4.13 (bottom, left), the PDF looks mostly Gaussian with a single peak in the centre. The min-entropy is therefore defined by this central peak, and increases as the central peak spreads out and becomes shorter. However, once the PDF of the phase becomes broad enough, the two side peaks characteristic of the arcsine distribution begin to appear, as shown in Figs. 4.13 (bottom, centre-right). At a certain point these side peaks become taller than the central peak, and the min-entropy from that point onward is defined by the height of the side peaks. As the phase noise increases, so does the height of the side peaks, approaching an arcsine distribution, and so the min-entropy decreases. The maximum min-entropy is therefore obtained at the point where the central peak is exactly equal in height as the side peaks. And this makes intuitive sense: when all three peaks are equal, then we have obtained a maximally spread out PDF, which maximises the min-entropy.

Note that when we make a measurement of a random variable with some PDF, we do not measure the underlying PDF directly, but rather a digitised version of it, according to the precision of the ADC used. The probability of obtaining any given outcome is given by the probability mass function (PMF), obtained by quantising the PDF into bins according to the ADC resolution: for an n-bit ADC resolution, the corresponding PMF has 2^n bins.

Fig. 4.14 plots the min-entropy of the intensity distribution when $\phi_0 = \pi/2$, for different

ADC resolutions. We can observe the effect described above where the min-entropy is first defined by the central peak in the distribution, and increases with phase noise. At some point, the side peaks reach the same height as the central peak and the min-entropy is maximised. At higher phase noise, the side-peaks continue increasing in height and the min-entropy decreases, leading to a kink in the min-entropy curve at the maximum.

Note as well that the value of phase noise which maximises the min-entropy depends on the ADC resolution. The height of the central peak with respect to the side peaks depends on the bin widths of the ADC. A higher resolution ADC leads to a lower value of phase noise at which the min-entropy is maximised.

Finally, we observe that for a 1-bit ADC, the min-entropy is constant and equal to 1. This is because any symmetric 1-bit digitised PDF will have 2 bins of equal height. This corresponds to a uniform distribution, and so the min-entropy is maximal, which for a 1-bit ADC corresponds to a min-entropy of 1 bit.

4.6.1 Applications to a QRNG

We have found that the maximum min-entropy obtainable by a phase noise QRNG is 7.57 bits for an 8 bit ADC which is obtained for a phase variance of $\langle \Delta\phi^2(t) \rangle = 0.12$ and an interferometer phase of $\phi_0 = \pi/2$. Operating a QRNG with these parameters would not only have a higher min-entropy per measurement, but requiring $\langle \Delta\phi^2(t) \rangle = 0.12$ could allow for higher sampling rates than typical gain-switched phase noise QRNG. Consider that for a gain-switched phase noise QRNG, we require $\langle \Delta\phi^2(t) \rangle > 9$ to achieve a near-uniform phase distribution.

A phase noise of $\langle \Delta\phi^2(t) \rangle = 0.12$ could be achieved by a CW laser in a short enough time to still allow for high repetition rates. Recall that the phase noise is inversely proportional to the

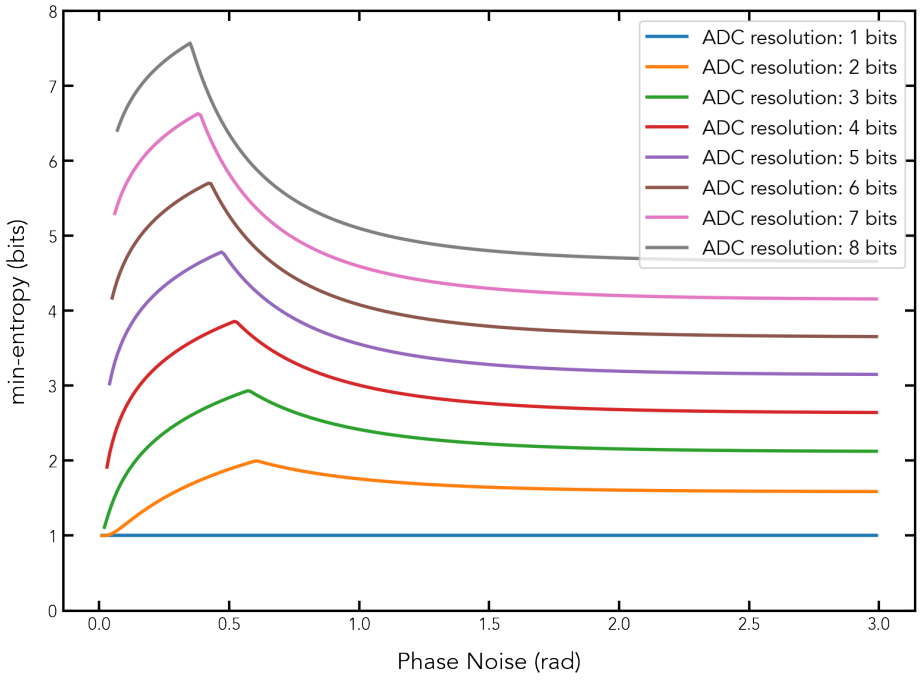

Figure 4.14: The min-entropy of the intensity distribution when the fixed interferometer phase $\phi_0 = \pi/2$. The min-entropy is at first defined by the central peak in the distribution (Fig. 4.13 bottom, left), and increases as the distribution spreads out and flattens. At a certain value of phase noise, when the central peak is equal in height to the side peaks, the min-entropy is maximised. At higher phase noise, the min-entropy switches to being defined by the height of the side peaks, leading to a kink in the min-entropy curve, and a decrease in the min-entropy as the side peaks increase in height.

coherence time:

$$\left\langle \Delta\phi^2(t) \right\rangle = \frac{2t}{\tau_c} \tag{4.21}$$

Assuming a typical coherence time of a CW DFB laser operated just above its threshold current of 10 ns [85], it would take 0.6 ns to achieve $\langle \Delta\phi^2(t) \rangle = 0.12$ and maximise the min-entropy. The corresponding maximum sampling rate is 1.7 GHz, comparable to the repetition rates of gain-switched phase noise QRNGs.

Gain-switched lasers require specialised electronics to drive them at GHz rates. Doing away with the complications of high-frequency modulation is a major benefit in terms of cost and simplicity.

The scheme just described was implemented previously by Ref. [91]. In that work, they employ a CW laser with a stabilised interferometer to operate the QRNG at its optimal min-entropy conditions. They, however, estimate the min-entropy in a significantly different way than presented here.

There are two main complications: first, the scheme just described requires a fixed interferometer phase of $\phi_0 = \pi/2$ whereas in the gain-switched version the interferometer phase does not matter, since the PDF at the output is an arcsine distribution regardless. This scheme therefore requires a phase-stabilised interferometer, adding cost and complexity [144]. Additionally the min-entropy is highly sensitive to the interferometer phase. Any deviation from $\phi_0 = \pi/2$ would lead to a sharp drop of the min-entropy. The phase stabilisation therefore needs to be accurate and, crucially, reliable. It is unclear whether this can be achieved in practice [145].

The second complication is that min-entropy is also highly sensitive to the phase noise. It is therefore a requirement to accurately model and measure the phase noise to ensure the QRNG is being operated at the optimal phase noise corresponding to the peak in the min-

entropy plot (Fig. 4.14). CW lasers are again beneficial in this sense, since their phase noise is straightforwardly related to their linewidth.

Finally, our above calculations of the maximal min-entropy, and optimal phase noise value assumed ideal and noiseless operation of the QRNG. Of course in practice, sources of noise will change the output distribution, and hence the min-entropy. Further work is required to analyse the effects of noise and other imperfections, as well as malicious attacks by Eve, on the extractable min-entropy.

4.7 Discussion

The assumption of a uniform phase distribution due to spontaneous emission, leading to an arcsine-distributed intensity, is fundamental to the security of phase noise QRNGs. Our work puts this assumption on stronger footing by quantifying the phase noise using a rate equation model. Rate equation modelling of laser diodes is a well established technique from the field of classical optical communications, giving confidence that our analysis rests on solid foundations. We have chosen a parameter extraction technique based on a small number of simple measurements. Our method for measuring phase noise can be implemented with a standard phase noise QRNG setup, with no need for additional equipment. This makes our analysis easy to replicate and implement as part of a certification process to guarantee the security of phase noise QRNGs. Although we have focused on quantifying the phase noise for the purposes of security, a rate equation model has other useful applications. Here we describe two such potential applications.

We have shown how a rate equation model can be used to quantify the phase noise in a gain-switched laser. Such a model can also be used to optimise the performance of a phase noise

QRNG, by selecting parameters to maximise the phase noise. The maximum sampling rate of the QRNG is limited by the time it takes for the laser to reach full randomisation. Increasing the phase noise can therefore allow for higher sampling rates. Fig. 4.9 shows that a 1GHz gain-switched laser is able to achieve full phase randomisation for appropriately selected current parameters. The model also gives insight into which rate equation parameters (intrinsic to the laser) affect the phase noise, notably the linewidth enhancement factor α and the spontaneous emission rate β. Choosing a laser with a high value of α or β could again improve the maximum sampling rate.

Laser phase noise is not the only consideration for maximising the QRNG performance. For example, laser chirp is a feature of directly modulated laser diodes which can lead to low visibility interference at the interferometer output. It is especially problematic at high repetition rates and large intensity modulations. The rate equations can again be used to select current parameters such that the chirp is minimised, or to find a suitable trade-off between high sampling rate and high visibility interference.

Even if suitable parameters have been chosen for the operation of the QRNG, the device can malfunction or its performance can degrade over time. QRNGs, like RNGs in general, can also be the targets of hacking attacks. For these reasons it is important to monitor the behaviour of the QRNG to detect malfunctioning or other deviations from normal behaviour. The standard approach consists of running statistical tests on the generated numbers to detect correlations or other signs of non-randomness. However, passing statistical tests of randomness is a necessary but not sufficient condition for establishing the correct operation of a QRNG. A seemingly random string of numbers can nonetheless be predictable and hence insecure. Having a strong understanding of the physical process by which the numbers are generated, backed up by a suitable model, is more reliable approach to certifying the randomness of the

output numbers. Our rate equation model can serve to establish a baseline of correct operation to which the device behaviour can be compared.

4.8 Summary

In this chapter, we used a laser rate equation model to quantify the phase noise of a gain-switched laser in the context of QRNG. We employed a parameter extraction method based on simple measurements, allowing us to quantitatively compare the model to experimental measurements. We found the model accurately predicts the power output and phase noise of the laser. By quantifying the phase noise using a model, we can give stronger guarantees that the generated numbers originate from quantum phase noise, improving the security of phase noise QRNGs.

In the following chapter, we study the laser seeding attack in QKD. We use both experiments and rate equation simulations to quantify the effects of this attack on a QKD transmitter and hence the required countermeasures.

Chapter 5

Quantified Countermeasures Against the Laser Seeding Attack in QKD

The contents of this chapter are based on results previously published in [13].

QKD implementation security vulnerabilities can be broadly classified as targeting either the transmitter or the receiver. Historically, the most serious proposed attacks against QKD systems have targeted the receiver. However, the development of MDI-QKD and its variants has provided a solution to all known and possible vulnerabilities in the receiver [23], [77], [78]. The focus of QKD implementation security has therefore shifted toward the transmitter [41].

5.1 Implementation Security of QKD Transmitters

The security of QKD transmitters is intuitively safer than for receivers. Transmitters can operate independently from the outside world, and only need to prepare and send specific quantum states without leaking information. They can use optical isolation, and monitor any incoming light for signs of malicious tampering. Receivers on the other hand by definition must interact

with the outside world: they must receive and measure light, which Eve has full control over. A multitude of attacks have been proposed that target the receiver, many of which involve Eve precisely modifying some property of the incoming light. For example, the detector efficiency mismatch attack requires Eve to precisely control the time of arrival of light pulses received by Bob [68], [71], [146], [147]. The degree of control which Eve has over QKD receivers is a major source of security vulnerabilities.

As discussed in Section 2.1.3, the discovery of MDI QKD provided a method for solving all current and potential security vulnerabilities of the detector and thus represented a huge step forward for the practical security of QKD systems. It also made the security of QKD transmitters comparatively more important.

Although QKD transmitters benefit from the use of optical isolation, they still must ensure that they do not leak information via side-channels. Table 5.1 provides an outline of the most prominent attacks on QKD transmitters. It is important to note that these attacks focus on the unique features of QKD transmitters, but classical side-channel attacks also apply to QKD transmitters. For example, power analysis involves measuring the power consumption of a cryptographic device to obtain information about the data being manipulated. Power analysis, and other classical side channel attacks apply as much to quantum cryptography devices as to classical ones.

5.2 Laser Seeding Attack

In this chapter we study a prominent attack on QKD transmitters known as the laser seeding attack (LSA) [69], [152]–[155]. This attack consists of an eavesdropper, named Eve, injecting light into the laser of a QKD transmitter to try and change the emitted light in some way that is ben-

Table 5.1: Prominent attacks on QKD transmitters

Security issue / attack	**Description**
Photon-number-splitting attack [61], [62]	The output of an attenuated laser is a weak coherent pulse, where the number of photons per pulse follows a Poisson distribution. An attacker could perform a quantum non-demolition measurement of the photon number to detect multi-photon pulses. They could then remove one photon from those pulses to measure, obtaining information without introducing any disturbance to the system. The PNS attack can be counteracted using the decoy state method [57], [148]–[151]
Trojan horse [65], [66]	QKD transmitters use encoding devices such as phase or polarisation modulators to encode information on photon pulses. Eve can inject light into a QKD transmitter and obtain information about the settings of the encoding device by measuring the backreflected light. The THA can be counteracted by using optical isolation to limit the amount of light that can enter a QKD transmitter, and using extra privacy amplification to remove any remaining information loss [63].
Laser seeding [69], [70]	Discussed in this chapter
Laser damage [64], [72]	Very bright light can damage optical components which can give an advantage to Eve. For example the attenuation of optical isolators can be permanently reduced. This attack can be counteracted by ensuring that any optical components used fail "gracefully" in that when a component is compromised, the QKD error rate increases to a level where the communications are aborted.

eficial to her (Figure 5.1). For example, Ref. [69] first demonstrated how the LSA can violate the assumption of a phase-randomised source: by seeding the QKD transmitter laser with light of a known phase, the LSA can give an eavesdropper full knowledge of the phase of the outgoing light, which drastically reduces the performance of a QKD system. Ref. [69] implemented the LSA using only two different levels of injected power. Additionally, they implemented the LSA

using an isolated laser diode. The isolation of an isolated laser diode is difficult to characterise, and so it is unclear exactly how much light was reaching Alice's laser cavity. Altogether, this means that we do not know accurately how the effects of the LSA depend the level of injected power (that reaches the laser cavity). This is a crucial consideration for Alice when implementing countermeasures to the attack: if Eve must inject a large amount of light for a successful attack, then the attack will be easier to detect. However, if Eve can implement a successful LSA with only a small amount of injected power, it will be more difficult to detect or prevent. In the first part of this work (Section 5.3), we implement the LSA experimentally and measure its effects on the phase randomisation of Alice's laser as a function of the injected optical power. We accurately measure the level of injected power that reaches Alice's laser cavity by using an unisolated laser, and measuring the incoming light with a power meter. We find that Eve can influence the phase of Alice's laser using much lower levels of injected power than may have been considered previously [69], [154]. Additionally, by accurately measuring how the effects of the LSA vary with increasing injected power, we are able to quantify the level of optical isolation required to limit the effects of the LSA on Alice's laser. This is of obvious practical relevance to the secure implementation of QKD systems.

Ref. [69] also suggested that the LSA could have other damaging effects apart from de-randomising the phase. Indeed, Ref. [154] demonstrated that the LSA can also increase the power output of a QKD transmitter, and quantified the effect of this increase on the secure key rate. However, there are still other effects of the LSA, such as a shift in the wavelength of Alice's laser [152], [155], a reduced turn-on delay, or a change in the shape of the emitted pulse, and Eve can try to use any of these to her advantage. In the second part of this work (Sections 5.4 & 5.4.2) we use a laser rate equation model that allows us to simulate the output of a laser subject to the LSA by modelling it as a form of optical injection locking (OIL). In Section 5.4 We

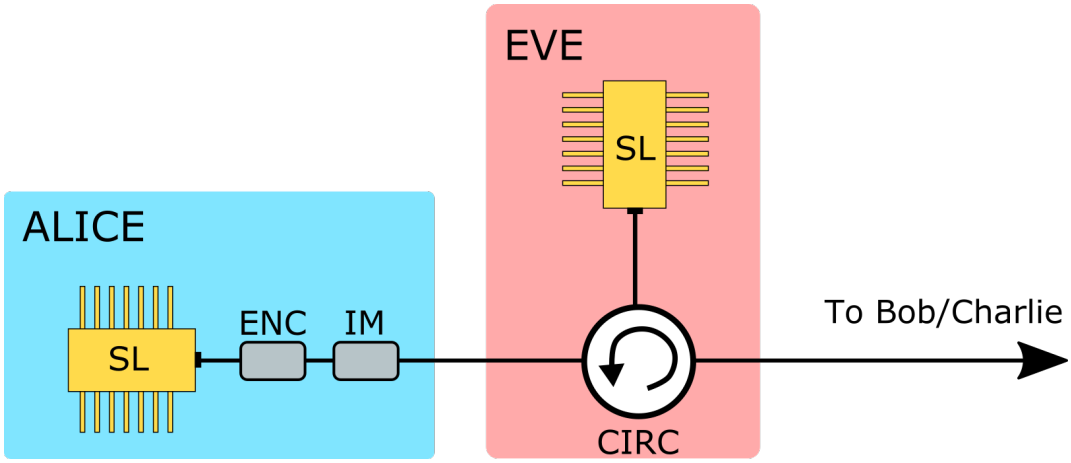

Figure 5.1: A simplified QKD transmitter (Alice), with a simple implementation of the LSA by Eve. Eve can add a circulator to the quantum channel between Alice and Bob such that she can inject light into Alice's transmitter while letting Alice's light pass through unimpeded. SL: semiconductor laser; ENC: encoder; IM: intensity modulator; CIRC: circulator.

argue that the laser rate equations are a useful tool for the study of the LSA and can be used as a general model of the LSA to investigate all of its various effects. To demonstrate this usefulness, we use the model to reproduce, in simulation, previous published experimental results in the literature [69], [154]. Further, we use the model to generate new insight into the effects of the LSA on QKD transmitters by examining how its effects on the power output of a gain-switched laser vary under different laser current driving conditions.

5.3 Effects on Phase Randomisation

QKD has been proven secure with and without phase randomised signals [156], [157]. However, the use of non-random phase leads to a significantly worse performance. Hence, current implementations of QKD use phase randomised pulses of light. The most widely used method for producing phase randomised signals for QKD is gain-switching, and we therefore assume the target of the LSA is a gain-switched laser diode [158], [159].

The current parameters of a gain-switched laser diode must be set carefully to ensure that

the laser cavity fully empties between each pulse. If photons from a previous pulse are still present in the cavity when the laser is driven above threshold, then the new pulse will inherit its phase from these photons. This will therefore lead to correlations between the phase of the emitted pulses, which is detrimental to the security of QKD [160].

The LSA works in a similar way: by injecting external photons into the laser cavity the generated pulses will inherit their phase from the external photons, rather than spontaneous emission, preventing the phase from randomising between pulses. Additionally, the attacker can deterministically control the phase of the injected photons, and therefore of the emitted pulses, which is a further security concern.

5.3.1 Phase-Randomised LSA

A simple implementation of the LSA consists in Eve injecting constant, continuous wave (CW) laser light into Alice's laser. As explained, this prevents the phase randomisation in Alice's laser, locking its phase to a constant value determined by the coherent injected light.

Alice may try to detect this attack by monitoring the phase at the output of her laser to check for signs of non-randomness. However, with a successful LSA, Eve can deterministically control the phase of Alice's laser. Therefore, we propose and experimentally demonstrate a new, more sophisticated version of the LSA, which we refer to as the "phase-randomised LSA". In this version of the LSA, Eve injects light with a seemingly random phase, but which is nonetheless completely known to her, into Alice's transmitter. For example, she can modulate the phase of her light with a phase modulator connected to a pseudo random number generator under her control, or alternatively she can gain-switch her laser and measure the phase before it is sent into Alice's transmitter. Either way, when Alice's laser locks to the injected light, it will

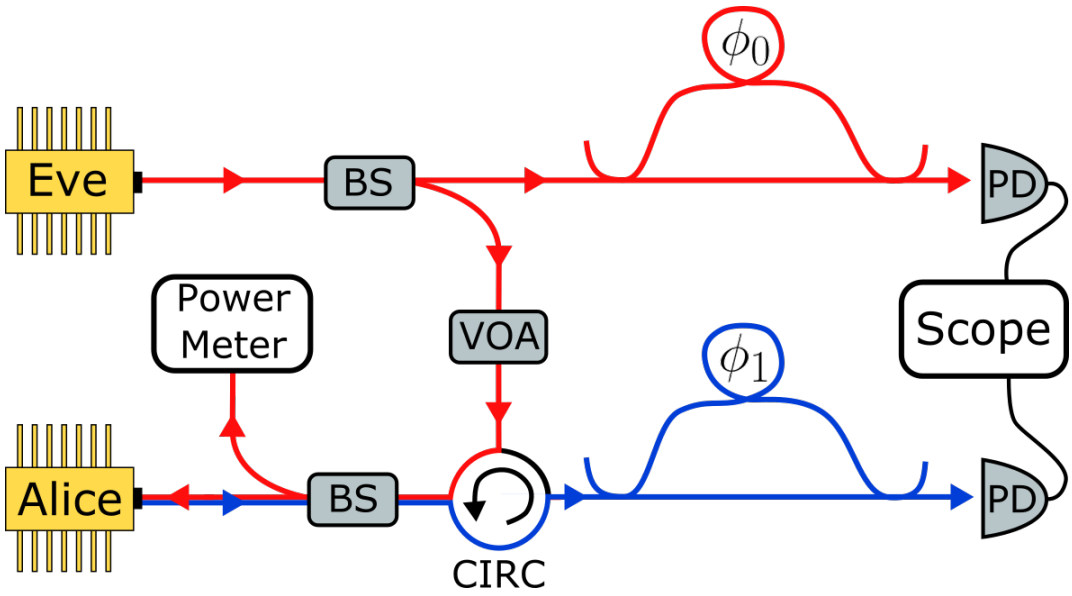

Figure 5.2: Experimental setup for quantifying the phase correlations between Alice and Eve's lasers due to the LSA. Using two asymmetric Mach-Zehnder interferometers we can simultaneously monitor the output of Alice's (red lines) and Eve's (blue lines) lasers. The interferometers in effect convert the specific phase of each laser into a specific intensity at the interferometer output, allowing us to monitor the phase of each laser and calculate their correlation. A power meter is used to measure the injected power reaching Alice's unisolated laser. VOA: variable optical attenuator; BS: beam splitter; PD: photodiode.

adopt the seemingly random phase of said light, which Eve has full knowledge of. If Alice tries to monitor the phase of her light, she will not detect any signs of non-randomness, even when the attack is successful. The phase-randomised LSA is more difficult to detect, and therefore is the one we implement and analyse in this work.

Because of the phase-randomised version of the LSA, Alice is forced to rely on optical isolation, or detecting the incoming light from Eve using a "watchdog" detector, to prevent the attack. It should be noted that neither optical isolation nor watchdog detectors are fool-proof solutions: optical isolation can be damaged, and detectors can be blinded, for example [67], [161].

Our experimental setup is shown in Fig. 5.2, where both Alice and Eve monitor the phase of their lasers by using asymmetric Mach-Zehnder interferometers (AMZIs). In the following we

demonstrate how the naive countermeasure of monitoring Alice's phase fails to detect Eve's attack, even when the attack is highly successful. Further, we use this experimental setup to quantify the degree to which Eve is successful in locking Alice's laser in phase as a function of the level of injected optical power. This allows us to in turn quantify the level of optical isolation needed to prevent the attack, in Section 5.3.4.

Note that some previous experimental demonstrations of the LSA made use of isolated laser diodes, requiring much higher injected power to compensate for the isolation losses. More importantly, it is difficult to accurately characterise the isolation of an isolated laser and therefore it is unclear exactly how much power actually reaches the laser cavity. In our work, we use an unisolated laser (for Alice) and a power meter to accurately measure the injected power that reaches the laser cavity. Therefore, in the following we use "injected power" to mean "injected power that reaches Alice's laser cavity".

We use two asymmetric interferometers to monitor the phase of both Eve's and Alice's laser. The intensity at the output of an asymmetric Mach-Zehnder interferometer (AMZI) is given by:

$$I_{\text{out}} = \frac{I_{\text{in}}}{2}[1 + \cos(\Delta\phi + \phi_0)] \tag{5.1}$$

where I_{in} is the input intensity, $\Delta\phi$ is the phase difference between the interfering pulses and ϕ_0 is the relative phase between both arms of the interferometer due to the difference in their length. We can therefore monitor the intensity at the interferometer output as a measure of the phase difference between successive pulses at the laser output. This allows us to measure the correlation between the phase of both lasers; if the output intensity of Eve's interferometer is highly correlated with Alice's, then this indicates a successful attack, giving Eve information about the phase of Alice's laser.

The intensity at the output of the interferometer depends on both the fixed interferometer phase ϕ_0 and the difference in phase between pulses due to phase noise $\Delta\phi$. Although we have been referring to ϕ_0 as "fixed", it in fact drifts over time as temperature variations or mechanical vibration affect the difference in length between both interferometer arms. This drifting phase presents a problem when trying to measure the correlations between Alice and Eve's lasers: even if both lasers are fully locked and $\Delta\phi = 0$, the output intensity will continue to vary because of a drifting ϕ_0.

Ideally we could phase stabilise the interferometers, keeping ϕ_0 truly fixed, so we can isolate the effects of $\Delta\phi$. However phase stabilisation is experimentally complicated, requiring a feedback mechanism connected to a phase modulator in one of the interferometer arms to correct any phase drift [144]. In the following we present a method to measure the correlations between the phase of Alice and Eve's laser, without the need of phase stabilised interferometers.

5.3.2 Measuring Correlations with Unstable Interferometers

Consider first an experiment with phase stabilised interferometers. Then when Alice and Eve's lasers are fully locked, absolute value of correlation will be 1[1]. Now if we remove the phase stabilisation, then the correlations will begin to drift between 1, when $\phi_0 = 0$, and -1, when $\phi_0 = \pi$.

Now consider again a phase stabilised interferometer, but with Alice and Eve's lasers only partially locked. In this case, the (absolute) correlations will be some non-zero value $0 < c < 1$. If we now remove the phase stabilisation, the correlations c will again begin to drift, but this time between c, when $\phi_0 = 0$, and $-c$, when $\phi_0 = \pi$.

[1] In practice of course the correlations will never reach exactly 1, due to other sources of noise reducing the correlations.

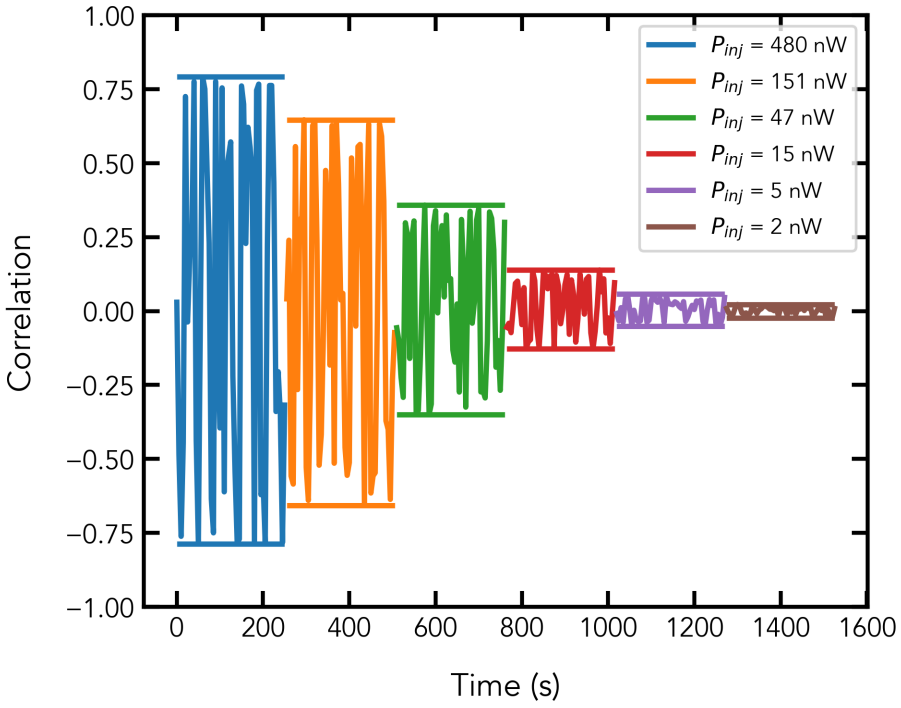

Figure 5.3: We measure the correlation between the intensity at the output Alice and Eve's interferometers, without phase stabilisation. The correlations therefore drift between a maximum and a minimum value. The horizontal lines represent our final estimate for the correlation at each level of injected power.

Therefore, if we want to measure the absolute value of the correlations c, we can continually measure the correlations, and c will correspond to the maximum and minimum values between which the correlation is drifting. This provides a way to experimentally measure the correlations, even with an unstable interferometer.

This method is illustrated in Fig. 5.3. We measure the correlation over time, at different levels of injected power, corresponding to different degrees of locking between Alice and Eve. At high injected power, the correlations reach large absolute values, indicative of full locking, while at lower injected power the correlations are also lower. The horizontal lines above each curve represent the maximum correlation value obtained for each level of injected power, and therefore represents our final estimate of the correlation.

In the following Section, we use this method to measure the correlations over a wide range

of injected powers, and determine at what level of injected power do correlations begin to appear.

5.3.3 Experiment

To set up the experiment, we gain-switch both lasers (DFB telecom laser diodes, unisolated for Alice and isolated for Eve) at 1 GHz using a 3.35 GHz pulse/pattern generator. We choose 1 GHz as it is representative of the modulation frequencies used in real-world QKD systems, and allows us to reliably generate fully phase randomised pulses. We set the current parameters (duty cycle, bias and modulation current) appropriately to ensure the phase of each generated pulse is random, as discussed in Chapter 4. We verify this for both lasers by measuring the autocorrelation of the intensity at the output of each interferometer. Both lasers are disconnected for this measurement, so none of Eve's laser light reaches Alice.

We then connect both lasers using the circulator and use a variable optical attenuator to adjust the level of injected power. We use polarisation maintaining components and fibre throughout, and a manual fibre polarisation controller, to match the polarisation of both lasers and maximise the effectiveness of the LSA. We measure the average injected power reaching Alice's laser using a power meter. Both lasers are 1550 nm and we additionally precisely match their frequencies by temperature tuning using TEC controllers and an optical spectrum analyser. The laser frequencies must be very closely matched, since optical injection locking requires the master-slave frequency detuning to be within the locking bandwidth. Further details on the effects of detuning on OIL are provided in Box. 4

Box 4: Locking Bandwidth

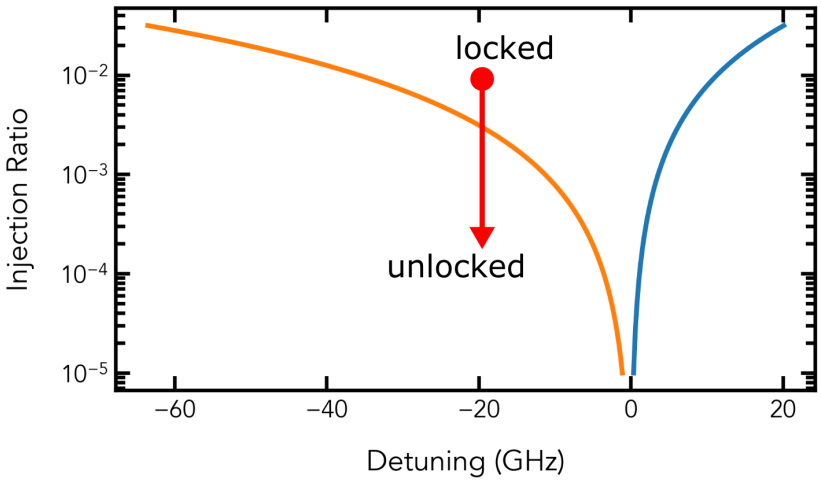

Figure 5.4: The locking bandwidth depends on the injection ratio. A higher level of injected power, relative to the slave laser power, means that the OIL can tolerate higher detuning. It is possible for the lasers to become unlocked at lower injected power (red line), even when a successful locking is possible. To maximise the effects of the LSA at all levels of injected power, it is important to minimise the detuning.

A successful LSA requires the frequency detuning between Eve (master) and Alice's (slave) lasers to fall within the locking bandwidth. Importantly for the LSA, the locking bandwidth is a function of the injection ratio, such that the lower the power Eve injects, the narrower the locking bandwidth, and the more stringent the detuning requirements for successful OIL. Fig. 5.4 plots a typical locking bandwidth for a semiconductor laser, showing its dependence on the detuning. Care must be taken because it is possible to obtain successful locking at a certain injected power, but for the locking to be lost when the power is decreased, as shown by the red arrow on Fig. 5.4.

This is crucial when measuring the correlation between master and slave laser: if the lasers become unlocked, then the correlations will decrease, even though a successful attack is still possible. To ensure that our correlation measurements accurately represent the optimal attack achievable by Eve it is therefore essential to minimise the master-slave

detuning.

Finally, we measure the intensity waveforms at the output of both interferometers for 25 μs, corresponding to 25000 pulses, using two high-speed photodiodes connected to two channels of a high-bandwidth (13 GHz) oscilloscope.

In the following we are particularly interested in the amount of injected power at which Eve just starts to induce measurable correlations between her and Alice's laser. However, since we are measuring the maximum and minimum values of correlation, rather than the mean, the measured correlations will never be zero, due to statistical fluctuations, even when no light is injected into Alice's laser. Therefore, at zero injected power there will be a minimum and maximum baseline correlation, and we are interested in the amount of injected power at which the correlation rises above this baseline. The measured maximum and minimum baseline correlations at zero injected power will increase as a function of the length of the measurement: the longer a measurement, the higher the likelihood of an outlier correlation measurement pushing the maximum higher or minimum lower. For this reason, it is important that the length of measurements throughout the experiment remain constant (in our case 25 μs). To measure the baseline, we simply disconnect Eve's laser from the circulator before making the correlation measurements. The measured baseline correlation is shown by the black dashed lines in Fig. 5.5, and any increase above the maximum correlation baseline must be due to Eve's injected light, and likewise for the minimum correlation.

The correlation measurements are plotted as the coloured lines in Fig. 5.5, showing the maximum and minimum values of correlation at each level of injected power. We can clearly see that at high levels of injected power, the LSA is very successful at locking Alice's laser in phase, with correlations between Alice and Eve's lasers reaching absolute values above 0.8. In

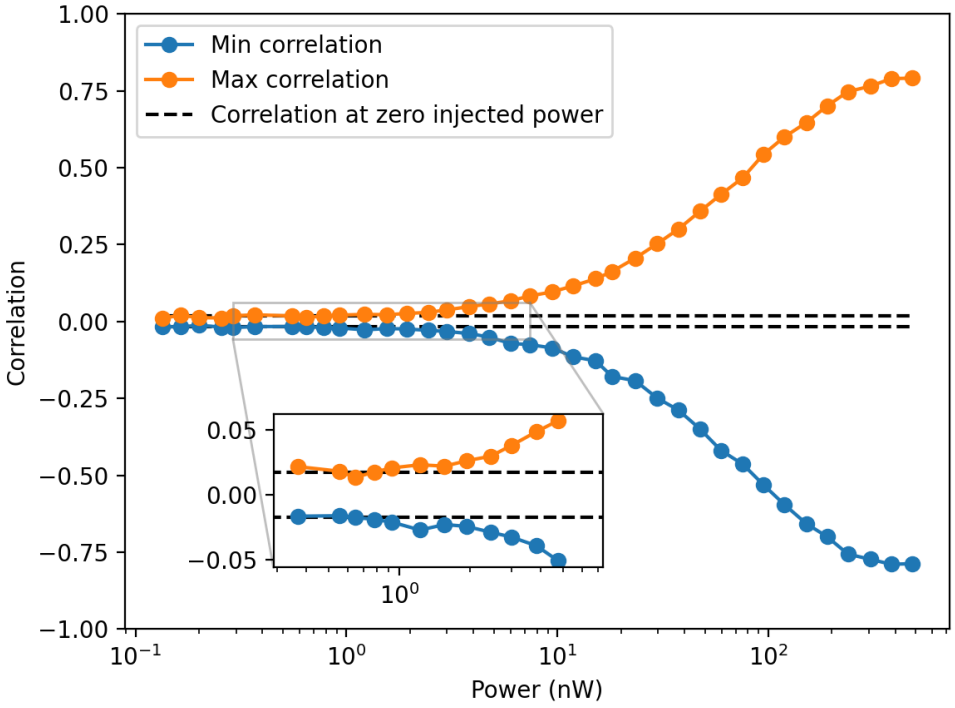

Figure 5.5: The measured correlation between Alice and Eve's lasers as a function of the injected power. Since our interferometers are not phase stabilised, the measured correlation between both lasers drifts along with the interferometer phase. We carry out 50 measurements of the correlations at each level of injected power and plot the maximum and minimum of the values obtained. The dashed black lines indicate the maximum and minimum measured correlations when Eve's laser is disconnected from Alice's. Since we are plotting the maximum and minimum values obtained over 50 measurements, rather than the mean, these lines are not zero due to noise and statistical fluctuations. Any correlations induced by Eve's attack will cause the measured correlations to deviate from this baseline. The inset zooms into the low-power region of the graph, showing that Eve can induce measurable correlations with as little as 1 nW of injected power, which is the point at which the measured correlations start to increase above the baseline.

practice, the maximum and minimum correlation values will never reach 1 and -1, since other sources of noise, such as intensity noise, or chirp, will also influence the interferometer output, acting against the locking effects of the LSA and reducing the correlation. With such high correlations, Eve has almost perfect knowledge of the phase of Alice's emitted pulses. From her perspective, the pulses are almost fully non-random, which undermines the security of the communications due to the drastically lower secure key rates of non-phase-randomised QKD. Of course, in our implementation of the attack, Eve uses a gain-switched laser diode and does not in fact know the absolute value of the phase, she only knows that Alice's laser has the same phase as hers. However, in principle Eve could use a reference laser and a phase modulator to measure the exact phase of her laser, and therefore also of Alice's.

Note that despite the large correlation between both lasers, the output of Alice's laser still appears to be random. Fig. 5.6 (left) plots the distribution of intensity at the output of Alice's laser, showing the signature arcsine distribution indicative of full phase randomisation. Additionally, Fig. 5.6 (right) plots the autocorrelation of the intensity, again showing no signs of non-randomness. This demonstrates that if Eve uses phase randomised light to perform the LSA, Alice cannot detect the attack by monitoring the output of her laser. If she uses an asymmetric interferometer to check whether the phase of her laser is random, by looking at the distribution of intensities and the correlation as in Fig. 5.6, she will not detect any signs of non-randomness, even though Eve's attack is highly successful. Instead, in order to prevent the attack, Alice is forced to either block the incoming light using optical isolation, or detecting the incoming light with a monitor detector.

As the injected power decreases, so do the correlations. The inset of Fig. 5.5 zooms into the lower-power measurements, showing that, in our experiment, Eve can induce measurable correlations with as little as 1 nW of injected power. Starting around 1 nW, the measured cor-

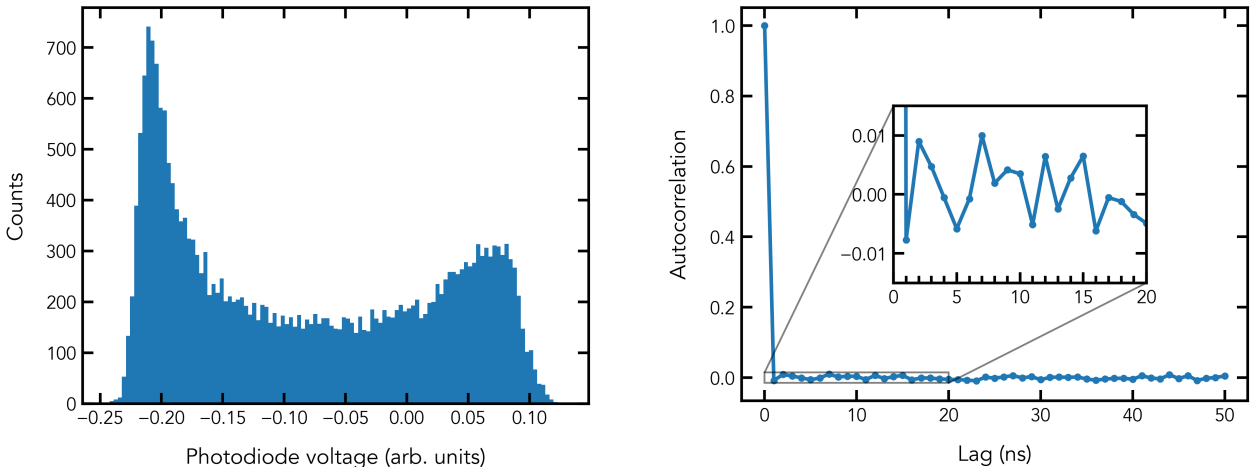

Figure 5.6: The distribution (left) and autocorrelation (right) of the intensity at the output of Alice's interferometer, when Eve is injecting 480 μW of optical power. This corresponds to the highest power measurement in Fig. 5.5, with a correlation between Alice and Eve's laser above 0.8. Despite Eve obtaining near perfect information about the phase of Alice's laser, Alice cannot detect this by monitoring the output of her laser, since both the distribution and the autocorrelations are indicative of a fully phase randomised laser.

relations rise above the zero injected power baseline, showing that Eve's attack increases the correlation between both lasers. We stress that this 1 nW threshold is specific to our experiment. Other experiments, and indeed practical QKD systems, will undoubtedly have different thresholds, depending on the lasers being used, experimental conditions such as temperature, and other factors. However, our observations and analysis are widely applicable to all QKD transmitters under the LSA.

1 nW is a much lower level of injected power than used by previous works analysing the LSA, and suggests that the LSA requires a lower level of injected power to be successful than previously thought [69], [154]. However, note that 1 nW is the threshold at which the effects of the LSA just start to become measurable, and are therefore still very small. Indeed, our results are still consistent with prior works: at 100 nW of injected power, similar to the injected power used in Ref. [154], we observe very large effects from the LSA consistent with their results.

Quantifying the effects of these correlations on the secure key rate is outside the scope of

this work. However, recent theoretical results have developed a security proof for QKD with imperfect phase randomisation [162]. We speculate that these results could be extended to the context of the LSA. Our results could then be used to provide an experimentally quantified measure of the degree of correlation, which could be inserted into the security proof to calculate the secure key rate. This is, however, outside the scope of this work, and instead in the following section: we ask: what level of optical isolation is needed to guarantee no measurable correlations between Alice and Eve? Based on the measurements reported in Fig. 3, to ensure no measurable correlations, Alice must not permit more than 1nW of light to enter her laser cavity. Using this minimum injected power threshold, in the next section we take a similar approach to Ref. [63] to quantify the optical isolation required to prevent a successful LSA.

5.3.4 Countermeasures

To prevent the LSA and guarantee the security of the QKD communications, the transmitter must implement countermeasures. This could consist of a “watchdog" detector placed at the entrance of the QKD transmitter, monitoring any incoming light [63]. If this detector registers incoming light above some threshold value, then the communications can be aborted. However, this solution comes with several drawbacks. Most obvious is the increased cost and complexity of the QKD system. Another disadvantage is that there are several known security vulnerabilities of detectors used in QKD systems [41]. For example it has been shown that certain types of detector can be “blinded" by shining bright light on them, making them unresponsive [67]. In general, active countermeasures, as opposed to passive ones, are less desirable because of their increased complexity which can introduce further avenues to attack like the aforementioned blinding. Instead, passive countermeasures are preferable. In particular, Alice can use

optical isolation to block any incoming light [163]. An optical isolator is a device which is transparent to light travelling in one direction, but opaque in the other. Clearly, an ideal optical isolator would be a suitable countermeasure. However, optical isolators are not ideal, and in particular they are not able to completely block light, but rather just attenuate the light by a large amount. Therefore, Alice cannot completely prevent light from entering her transmitter, but can only control the attenuation of the incoming light.

A key quantity is therefore the minimum amount of light that needs to reach Alice's laser for Eve's attack to be successful. Clearly, if any amount of injected light, however small, will lead to a successful attack, then no amount of optical isolation can prevent it. In the previous section we experimentally determined that, for our experimental apparatus and conditions, Eve can induce measurable correlations between the phase of her laser and that of Alice by injecting as little as 1 nW of (average) optical power. In the following, will use 1nW as an example minimum power threshold for a successful LSA, but we stress that other experiments and QKD systems may well have different thresholds, which should be verified independently. A second key quantity is the maximum amount of light that Eve can inject into Alice's transmitter. Clearly, if Eve can inject an unlimited amount of light, then no amount of optical isolation can guarantee the 1 nW limit.

One upper limit to the amount of light that Eve can inject is given by the laser-induced damage threshold (LIDT). The LIDT is defined as the maximum power that can be transmitted through an optical fibre without damaging it. Ref. [63] quotes a value for the LIDT of standard single-mode silica optical fibre of 55 kW, beyond which the fibre softens and begins to melt. Reducing 55 kW of optical power to 1 nW would require on the order of 140 dB of optical isolation. Alternatively, we can upper bound the amount of light Eve can inject by using an optical fuse, which is a device intended to break and stop the transmission of any light if the

power goes above some threshold. Ref. [164] introduces an optical fuse with a threshold of a few watts, reducing the required optical isolation to approximately 90 dB. There also exists so-called optical power limiters, which do not break above a certain threshold like an optical fuse, but rather prevent the transmitted optical power from increasing beyond that threshold. A recent proposal introduces a simple power limiting device with a widely tunable power threshold, down to values of around 1 μW, which would reduce the optical isolation requirement down to approximately 30 dB [165].

Although the 1 nW threshold leads to no measurable correlations in our experiment, it is still possible that with longer measurement times, or more accurate experimental apparatus, we could measure correlations even below 1nW of injected power. Indeed, if we make no assumptions about the capabilities of Eve, then we must assume that she can measure arbitrarily low correlations. The above countermeasure would therefore not be sufficient to account for these correlations below our measurement precision. Instead, a theoretical framework similar to the one presented in, for example, Ref. [162] would ultimately be needed.

Backreflection Tolerance

Optical backreflections from components like fibre pigtails can introduce feedback effects when the reflected light reenters the laser cavity [166]. This feedback, when it exceeds a specific threshold, can induce instabilities and introduce noise into the laser's output, thereby compromising its operation [167]. The term "backreflection tolerance" describes a laser's resilience to such feedback before noticeable performance degradation occurs.

The data illustrated in Fig. 5.5 measures the impact of the LSA on the phase of a QKD laser as a function of the external injected optical power. This analysis essentially assesses the QKD laser's "tolerance" to external light injection, where we note a conceptual parallel to "backreflec-

tion tolerance" concerning optical feedback. Future work could investigate these parallels and whether methods from the optical feedback literature can be used to further quantify the effects of the LSA on QKD laser performance, or suggest ways in which QKD lasers can be made more resilient to optical seeding attacks.

5.4 Numerical Model of the LSA

Although the effect of the LSA on the phase randomisation of a gain-switched laser is perhaps the most damaging, the LSA has many other effects on the laser output and Eve can try to use any of these to her advantage. In this section we use the optical injection locking (OIL) laser rate equations, introduced in Section 3.2, to model the LSA and all of its effects.

The LSA can be described as a form of OIL, where Eve controls the master laser and tries to lock, or otherwise influence, the slave laser controlled by Alice. The same constraints that come with OIL, minimal detuning, aligned polarisations, etc., also apply to the LSA. Additionally, all of the effects of OIL, discussed in Section 3.6, do too. We saw that OIL can reduce the jitter, chirp and turn-on delay of the laser pulses, and can be used to deterministically control the frequency of the slave laser. Any of these effects can in principle be used by Eve to compromise the security of the QKD communications. The effects of LSA on the phase of Alice's laser has been studied in Ref. [69], and Ref. [154] analyses the effects on the intensity of the emitted pulses. But still there are other effects which have not been studied, such as the impact on turn-on delay, and many of the effects that have been studied have not been studied exhaustively, and there is still room for further investigation.

We propose using the laser rate equations as a tool to investigate the LSA and all of its effects on Alice's laser. Investigating the LSA in simulation can help guide experimental work,

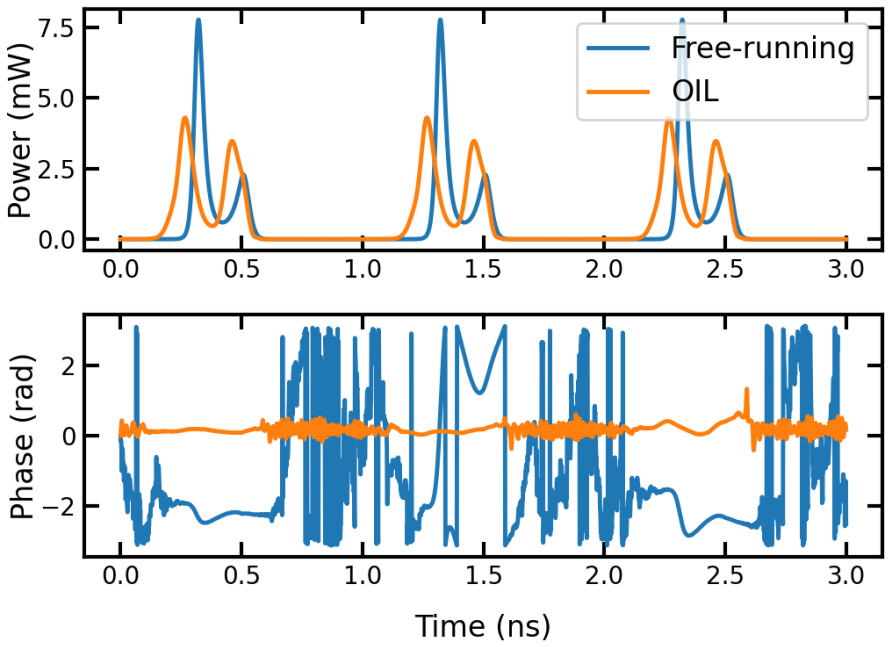

Figure 5.7: A rate equation simulation of the power output (top) and phase (bottom) of a gain-switched laser with and without the effects of OIL. (Top) With the parameters in this study, OIL causes the laser to start lasing sooner and a different pulse shape, leading to an overall increase in total energy emitted. (Bottom) The free-running laser experiences drastic phase diffusion while the laser is below threshold and not lasing. OIL suppresses this phase diffusion and keeps the phase around a constant value set by the master laser.

and generate new insight.

5.4.1 Reproducing Experimental Results in Simulation

Using the rate equations we can simulate the power output and phase of Alice's gain-switched slave laser, both with and without the effects of the LSA. The blue curve of Fig. 5.7 plots the power output and phase of a free-running gain-switched laser, and is obtained by solving the free-running laser rate equations, without OIL terms. It displays signature features of gain-switching: a train of pulses, each pulse with one or more relaxation oscillation peaks, and each with a random phase, due to rapid phase randomisation between pulses. The orange curve of Fig. 5.7 plots the power output and phase of a gain-switched laser under the effects of the LSA. It is obtained by solving the rate equations with OIL terms, and setting $P_{\text{inj}} = 100$ nW and

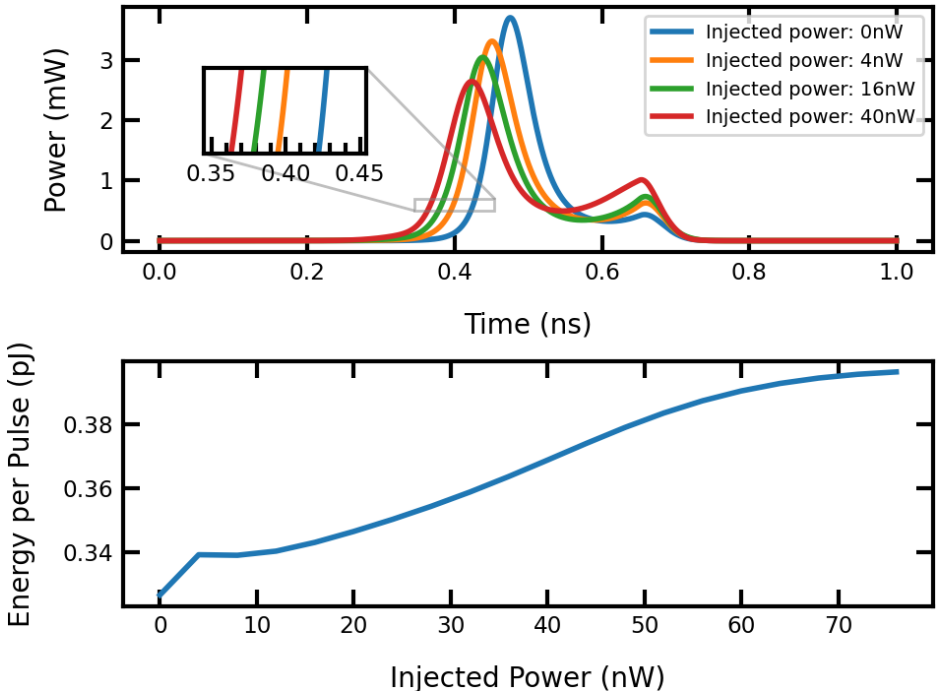

Figure 5.8: (Top) The change in power output of the laser under various levels of injected power. The pulse shape changes with the injected power and in particular there is a shorter turn-on delay (the laser starts lasing sooner, see inset), leading to an increase in total energy emitted per pulse which can be calculated by integrating the pulse over one period. (Bottom) The energy per pulse increases as a function of injected power. This simulation result is in good agreement with previous experimental measurements [154].

$\phi_{\text{inj}} = 0$. These two parameters can be set to any values to simulate the effects of the LSA under different levels of injected optical power and different phase differences between the master and slave lasers. P_{inj} and ϕ_{inj} do not even need to be constant, if for example Eve's master laser is itself gain-switched.

The orange curve of Fig. 5.7 displays several signature effects of the LSA on the output of a gain-switched laser. The effect on the phase randomisation is clear: the LSA prevents the slave laser phase from randomising, keeping it centred around a constant value set by the phase of the master laser ϕ_{inj} (in this case 0). This is in agreement with the experimental results of the first demonstration of the LSA in Ref. [69]. Likewise the effect on the power output is apparent: the slave laser begins lasing sooner (shorter turn-on delay), and the relaxation oscillation peaks are shorter and wider. Ref. [154] demonstrated that an increase in the photon number per pulse, or

equivalently energy per pulse, emitted by a QKD transmitter is detrimental to its performance and security. We can calculate the energy per pulse in simulation by integrating the simulated laser power output over one period.

To investigate how the energy per pulse changes as a function of injected optical power, we repeat the simulations under various levels of injected power P_{inj}. Fig. 5.8 (top) plots the resulting pulse shapes, indicating that at higher levels of injected power, the slave laser begins lasing sooner (reduced turn-on delay, indicated by the inset) while the first relaxation oscillation peak reduces, and the second peak increases in power. By integrating these curves over one period, we can plot the energy per pulse as a function of injected power, in Fig. 5.8 (bottom), showing an increase in energy with higher levels of injected power. These simulations again agree with previous experimental results, in Ref. [154], and demonstrate the usefulness of the rate equation model in studying the LSA. We have shown that the rate equation model can simulate the main effects of the LSA studied experimentally to date.

In the next section we demonstrate how the rate equation model can go further and be used to generate new insight into the LSA. We study how the effects of the LSA on the total energy emitted per pulse changes when using different laser current parameters, and we verify our numerical simulations with experimental measurements. We argue that a rate equation model can be a useful tool for exploring large ranges of parameters, which would be time-consuming to explore experimentally. But we stress that in principle, a rate equation model can be used to study any effect of the LSA, and how those effects depend on various laser parameters.

5.4.2 New insight into the LSA using a rate equation model

The laser power output is relevant to the security of QKD because in QKD, and in decoy-state QKD in particular, it is necessary to use pulses with a specific number of photons per pulse, that is, a specific energy [57]. An increase in the power output will lead to a larger number of photons per pulse, reducing the performance and hence the security of a QKD protocol if the increase is not detected. In particular, the quantity of interest is the percentage increase in energy per pulse, which is the relevant quantity for quantifying the impact on the secure key rate [70]. As before, we can simulate this quantity by solving the rate equations and integrating over a single period to get a measure of the energy. By comparing the energy per pulse with and without the LSA, we can calculate the percentage increase in energy per pulse by calculating the ratio of these two quantities.

Furthermore, we can re-do the simulations using different levels of injected power to see how the percentage increase in energy changes as a function of injected power. Fig. 5.8 shows our simulation results, which are in good qualitative agreement with previous experimental results [70].

The pulses emitted by a QKD transmitter need to be short, phase randomised and with a photon number close to zero [105]. The last requirement can be met with an arbitrary level of attenuation after the laser. The first two can instead be obtained by suitably adjusting the current signal that drives the gain-switched laser. Therefore, we can ask whether certain current driving parameters, are more susceptible to the LSA than others, in terms of energy increase. We can easily investigate this question in using the rate equation model by simply adjusting the current parameter $I(t)$ and calculating the energy increase. In this way, we can explore hundreds of parameters in simulation, before undertaking time-consuming experimental work.

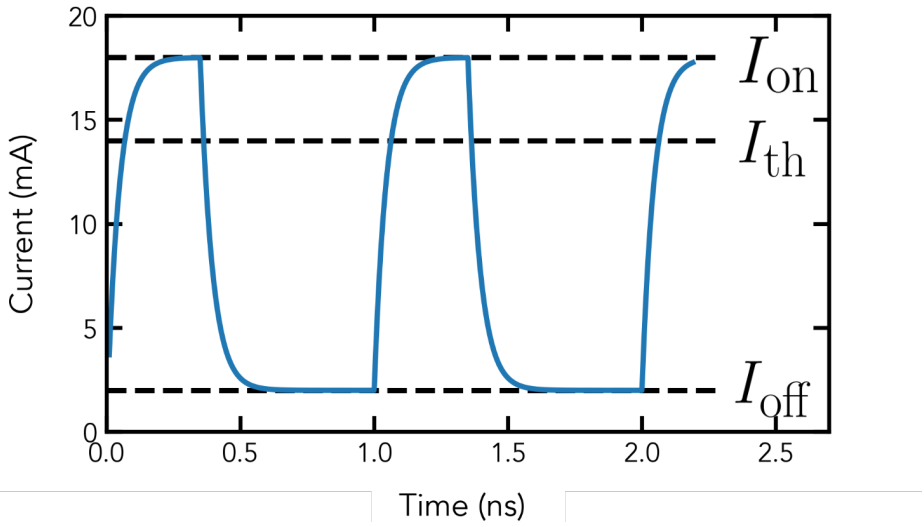

Figure 5.9: The laser driving current alternates between an on-time current I_{on} and off-time current I_{off}. The duty cycle is calculated to achieve single-peak emission, by setting the duration of the current on-time to equal the laser turn-on delay plus half the period of a relaxation oscillation. To account for the finite bandwidth of the driving electronics, a 3.5 GHz low-pass filter is applied to the current.

We can define the injected current as a 1 GHz pulse wave, with an on-time current of I_{on} and an off-time current of I_{off} and a variable duty cycle. We choose to define the current in terms of on- and off-time current, instead of the more typical bias and modulation current, because this makes it easier to define constraints such that e.g. the current is never negative.

To model the finite bandwidth of the pulse generator used to drive the laser, we apply a 3.5 GHz low-pass filter to the injected current. Fig. 5.9 gives a visual representation of the driving current.

We can then vary I_{on} and I_{off} across a wide range of values subject to the following constraints: the off-time current of the laser should never be negative, and should always remain below the threshold current, i.e. $0 < I_{\text{off}} < I_{\text{th}}$, where I_{th} is the threshold current; and the on-time current should always be above the threshold current, i.e. $I_{\text{on}} > I_{\text{th}}$. To guarantee the requirement of narrow pulses, we set the duty cycle such that the on-time of the pulse wave is equal the turn-on delay plus half the period of the relaxation oscillations [168].

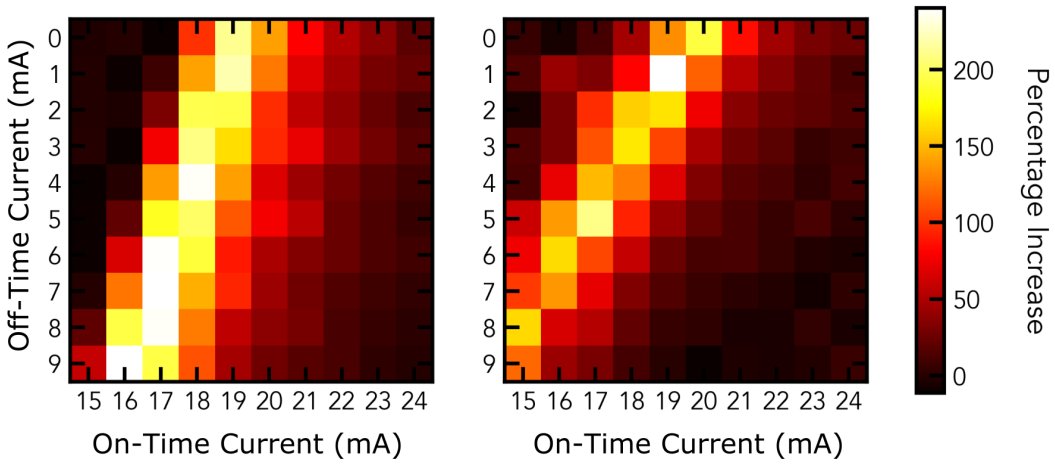

Figure 5.10: Simulated (left) and experimental (right) heatmaps of the percentage energy per pulse increase of Alice's laser with different current driving parameters. We drive the laser with a range of current parameters, from 0 to 9 mA off-time current, and from 15 to 24 mA on-time current. For each combination of current parameters (each square in the heatmaps) we calculate the percentage increase in intensity per pulse caused by the LSA. The correspondence between simulation and experiment is evidence that the rate equation model accurately describes the LSA. These measurements indicate that the effects of the LSA on the power output of a laser is highly dependent on the specific current parameters used to drive the laser.

Fig. 5.10 (a) shows our simulations results in the form of a heatmap. For each combination of current parameters $(I_{\text{on}}, I_{\text{off}})$, we calculate the percentage increase in energy due to the LSA by solving the rate equations with and without injected light. To calculate the energy per pulse without injected light, we set $P_{\text{inj}} = 0$ to model a free-running laser, and integrate the solution to the rate equations over one period. To calculate the energy per pulse with injected light, we set $P_{\text{inj}} = 100$ nW, which is a level of injected power used by previous experimental studies of the LSA [153], [154]. The heatmap colourbar indicates the calculated percentage increase in energy per pulse.

Using the same setup as in Fig. 5.2 we can experimentally verify the simulation results shown in Fig. 5.10 (a). For each combination of current parameters covered by the heatmap, we measure the average output power of Alice's laser with no injected light, and with 100nW of continuous wave (CW) injected light from Eve's laser. Our experimental results are shown

in Fig. 5.10 (b), which agrees well with the simulations. In particular, both heatmaps display a notable line of light-coloured squares rising diagonally from the bottom left corner, with darker squares elsewhere. The good agreement between experiment and simulation is evidence of the accuracy of the rate equation model in describing the LSA. Based on these simulations, we can see that the specific current parameters, i.e. the specific square on the heatmap, used to drive a gain-switched laser can have a large impact on the effect of the LSA on the power output of that laser.

There are many factors to consider when choosing the current parameters to drive a gain-switched laser in a QKD transmitter. The shape of the emitted pulses, their width, chirp and other factors are all important. The simulation and experimental results of Fig. 5.10 can serve as another data point and consideration when choosing these parameters. For example, Alice may choose to avoid a bright square in order to minimise the energy increase caused by the LSA. On the other hand, a large increase in energy could be used to detect the presence of Eve implementing the LSA on her laser. The heatmaps of Fig. 5.10 can serve as one factor among others when choosing the best current parameters for a gain-switched laser in a QKD system.

Alice should therefore choose her parameters carefully and could use these heatmaps to inform her selection. For example, she may choose to avoid a bright square in order to minimise the energy increase caused by the LSA. On the other hand, a large increase in energy could be used to detect the presence of Eve implementing the LSA on her laser. Of course, there are other factors to consider when choosing current driving parameters in a QKD context, such as the shape of the pulses, their width and chirp, and not all of the parameters covered by the heatmap will be suitable. However, the heatmaps can serve as one factor among others when choosing the best current parameters for a gain-switched laser in a QKD system.

These results demonstrate the usefulness of a rate equation model for studying the LSA.

Using the model, we were able to explore hundreds of parameters in simulation before undergoing time-consuming experimental work. Although we focused on the energy increase, other effects of the LSA can similarly be studied, such as the reduction in the turn on delay.

5.5 Summary

In this work we presented an experimental and numerical study of the laser seeding attack in QKD. We implemented the LSA experimentally and measured the effect on the phase randomisation as a function of injected optical power. This allowed us to quantify the level of optical isolation required to prevent the attack. Since the effect on the phase is just one of multiple effects of the LSA, we introduced the laser rate equations as a useful tool to study and model the LSA, drawing on the literature on optical injection locking from the field of classical telecommunications. Using this model, we were able to reproduce previously published experimental results, and demonstrate how the model can be used to study other properties of the LSA. In particular, we measured the increase in power output of a gain-switched laser when subject to the LSA under different laser current parameters. We found that certain parameters made the laser more vulnerable to the LSA, and we verified our findings experimentally. Altogether, our work contributes to the security of QKD transmitters, and provides a tool for further investigations of the LSA and other attacks which target the laser in a QKD transmitter.

Chapter 6

Conclusion

QKD promises unconditional security for private communications. However, the physical implementation of QKD systems introduces potential security issues that must be analysed and addressed for true security. Likewise with QRNGs, the promise of true randomness of quantum origin depends on the device operating as expected, reliably, and robust against side-channels. This thesis focused on implementation security issues related to one of the most critical components of QKD and QRNG systems: the semiconductor laser.

Through experiments and simulations, we investigated two important threats to QKD transmitters involving semiconductor lasers: laser phase noise in QRNGs and the laser seeding attack on QKD transmitters.

For QRNGs, we developed a method to accurately quantify the laser phase noise using laser rate equation modelling. By extracting the model parameters from experimental measurements, we achieved good agreement between simulations and experiments. This modelling approach demonstrates how phase noise QRNGs can operate within well-defined parameters that guarantee a sufficient level of randomness.

For the laser seeding attack, we experimentally demonstrated that sizeable correlations be-

tween attacked and eavesdropper lasers are achievable at the nanowatt level of injected optical power. We also modelled the effects of the attack using optical injection locking rate equations, enabling simulations of a wide range of attack scenarios. These quantitative results allow us to determine necessary countermeasures to mitigate the attack, such as the optical isolation required at the transmitter.

Overall, this thesis presents a strong case for the benefit of an in-depth theoretical understanding, backed up by accurate experimental characterisation, of a fundamental component such as the semiconductor laser. By closely examining the physical mechanisms underlying this key component of quantum cryptography systems, we can ensure that the implementation matches theoretical requirements and assumptions, leading to more robust and secure real-world quantum technologies. While the focus of this thesis was on semiconductor lasers, this holistic approach combining experiment, modelling and security analysis can and should be applied to other components as well in order to realise the full promise of quantum cryptography.

Bibliography

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, Mar. 2002.

[2] S. Pirandola, S. Pirandola, U. L. Andersen, *et al.*, "Advances in quantum cryptography," *Adv. Opt. Photon., AOP*, vol. 12, no. 4, pp. 1012–1236, Dec. 2020.

[3] M. Peev, C. Pacher, R. Alléaume, *et al.*, "The SECOQC quantum key distribution network in Vienna," *New J. Phys.*, vol. 11, no. 7, p. 075 001, Jul. 2009.

[4] D. Stucki, M. Legré, F. Buntschu, *et al.*, "Long-term performance of the SwissQuantum quantum key distribution network in a field environment," *New J. Phys.*, vol. 13, no. 12, p. 123 001, Dec. 2011.

[5] S.-K. Liao, W.-Q. Cai, J. Handsteiner, *et al.*, "Satellite-Relayed Intercontinental Quantum Network," *Phys. Rev. Lett.*, vol. 120, no. 3, p. 030 501, Jan. 2018.

[6] J. F. Dynes, A. Wonfor, W. W.-S. Tam, *et al.*, "Cambridge quantum network," *npj Quantum Information*, vol. 5, no. 1, pp. 1–8, Nov. 2019.

[7] J.-P. Chen, C. Zhang, Y. Liu, *et al.*, "Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas," *Nat. Photon.*, vol. 15, no. 8, pp. 570–575, Aug. 2021.

[8] G. P. Agrawal, *Fiber-Optic Communication Systems*. John Wiley & Sons, Feb. 2012.

[9] G. P. Agrawal and N. K. Dutta, *Semiconductor Lasers*. Springer Science & Business Media, Nov. 2013.

[10] L. A. Coldren, S. W. Corzine, and M. L. Mashanovitch, *Diode Lasers and Photonic Integrated Circuits*. John Wiley & Sons, Mar. 2012.

[11] T. K. Paraïso, R. I. Woodward, D. G. Marangon, V. Lovic, Z. Yuan, and A. J. Shields, "Advanced Laser Technology for Quantum Communications (Tutorial Review)," *Adv Quantum Tech*, p. 2 100 062, Aug. 2021.

[12] V. Lovic, D. Marangon, M. Lucamarini, Z. Yuan, and A. Shields, "Characterizing Phase Noise in a Gain-Switched Laser Diode for Quantum Random-Number Generation," *Phys. Rev. Applied*, vol. 16, no. 5, p. 054 012, Nov. 2021.

[13] V. Lovic, D. G. Marangon, P. R. Smith, R. I. Woodward, and A. J. Shields, "Quantified Effects of the Laser Seeding Attack in Quantum Key Distribution," *Physical Review Applied*, Accepted for publication, 2023.

[14] V. Lovic, "Quantum Key Distribution: Advantages, Challenges and Policy," Oct. 2020.

[15] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[16] P. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, Nov. 1994, pp. 124–134.

[17] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, Oct. 1997.

[18] S. Pirandola, U. L. Andersen, L. Banchi, *et al.*, "Advances in Quantum Cryptography," *arXiv:1906.01645 [math-ph, physics:physics, physics:quant-ph]*, Jun. 2019.

[19] R. Renner and R. Wolf, "Quantum Advantage in Cryptography," *AIAA Journal*, pp. 1–16, Feb. 2023.

[20] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *npj Quantum Information*, vol. 2, no. 1, pp. 1–12, Nov. 2016.

[21] C. Gobby, Z. L. Yuan, and A. J. Shields, "Quantum key distribution over 122 km of standard telecom fiber," *Appl. Phys. Lett.*, vol. 84, no. 19, pp. 3762–3764, May 2004.

[22] M. Pittaluga, M. Minder, M. Lucamarini, *et al.*, "600-km repeater-like quantum communications with dual-band stabilization," *Nat. Photonics*, Jun. 2021.

[23] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," *Nature*, vol. 557, no. 7705, pp. 400–403, May 2018.

[24] K. Azuma, S. E. Economou, D. Elkouss, *et al.*, *Quantum repeaters: From quantum networks to the quantum internet*, Dec. 2022.

[25] K. A. Patel, J. F. Dynes, I. Choi, *et al.*, "Coexistence of High-Bit-Rate Quantum Key Distribution and Data on Optical Fiber," *Phys. Rev. X*, vol. 2, no. 4, p. 041 010, Nov. 2012.

[26] T. K. Paraïso, I. De Marco, T. Roger, *et al.*, "A modulator-free quantum key distribution transmitter chip," *npj Quantum Inf*, vol. 5, no. 1, pp. 1–6, May 2019.

[27] J. A. Dolphin, T. K. Paraïso, H. Du, R. I. Woodward, D. G. Marangon, and A. J. Shields, "A hybrid integrated quantum key distribution transceiver chip," en, *npj Quantum Inf*, vol. 9, no. 1, pp. 1–8, Sep. 2023.

[28] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," *arXiv:quant-ph/0212066*, Sep. 2004.

[29] M. Pereira, M. Curty, and K. Tamaki, "Quantum key distribution with flawed and leaky sources," *npj Quantum Information*, vol. 5, no. 1, pp. 1–12, Jul. 2019.

[30] G. Currás-Lorenzo, K. Tamaki, and M. Curty, *Security of decoy-state quantum key distribution with imperfect phase randomization*, Oct. 2022.

[31] A. Koehler-Sidki, J. F. Dynes, M. Lucamarini, *et al.*, "Best-Practice Criteria for Practical Security of Self-Differencing Avalanche Photodiode Detectors in Quantum Key Distribution," *Phys. Rev. Applied*, vol. 9, no. 4, p. 044 027, Apr. 2018.

[32] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, "Quantum random number generation," *npj Quantum Inf*, vol. 2, no. 1, pp. 1–9, Jun. 2016.

[33] M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," *Rev. Mod. Phys.*, vol. 89, no. 1, p. 015 004, Feb. 2017.

[34] A. Acín and L. Masanes, "Certified randomness in quantum physics," *Nature*, vol. 540, no. 7632, pp. 213–219, Dec. 2016.

[35] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, "A fast and compact quantum random number generator," *Review of Scientific Instruments*, vol. 71, no. 4, pp. 1675–1680, Apr. 2000.

[36] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, "Optical quantum random number generator," *Journal of Modern Optics*, vol. 47, no. 4, pp. 595–598, Mar. 2000.

[37] M. Lucamarini and et al., *Implementation Security of Quantum Cryptography*, Jul. 2018.

[38] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, no. 3, pp. 1301–1350, Sep. 2009.

[39] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nature Photonics*, vol. 8, no. 8, pp. 595–604, Aug. 2014.

[40] N. Jain, B. Stiller, I. Khan, D. Elser, C. Marquardt, and G. Leuchs, "Attacks on practical quantum key distribution systems (and how to prevent them)," *Contemporary Physics*, vol. 57, no. 3, pp. 366–387, Jul. 2016.

[41] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," *Rev. Mod. Phys.*, vol. 92, no. 2, p. 025 002, May 2020.

[42] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *International Conference on Computers, Systems & Signal Processing*, Dec. 1984, pp. 175–179.

[43] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "Fast and simple one-way quantum key distribution," *Appl. Phys. Lett.*, vol. 87, no. 19, p. 194 108, Nov. 2005.

[44] M. Mafu, A. Dudley, S. Goyal, *et al.*, "Higher-dimensional orbital angular momentum based quantum key distribution with mutually unbiased bases," *Physical Review A*, vol. 88, no. 3, Sep. 2013.

[45] M. Lucamarini, K. A. Patel, J. F. Dynes, *et al.*, "Efficient decoy-state quantum key distribution with quantified security," *Opt. Express, OE*, vol. 21, no. 21, pp. 24 550–24 565, Oct. 2013.

[46] W. K. Wootters and B. D. Fields, "Optimal state-determination by mutually unbiased measurements," *Annals of Physics*, vol. 191, no. 2, pp. 363–381, May 1989.

[47] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, Oct. 1982.

[48] D. Dieks, "Communication by EPR devices," *Physics Letters A*, vol. 92, no. 6, pp. 271–272, Nov. 1982.

[49] S. M. Barnett and S. Croke, "Quantum state discrimination," *Adv. Opt. Photon., AOP*, vol. 1, no. 2, pp. 238–278, Apr. 2009.

[50] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*, Dec. 2010.

[51] S. Loepp and W. K. Wootters, *Protecting Information: From Classical Error Correction to Quantum Cryptography*. Cambridge University Press, Jul. 2006.

[52] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Transactions on Information Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995.

[53] P. W. Shor and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," *Phys. Rev. Lett.*, vol. 85, no. 2, pp. 441–444, Jul. 2000.

[54] D. Mayers, "Quantum Key Distribution and String Oblivious Transfer in Noisy Channels," in *Advances in Cryptology — CRYPTO '96*, N. Koblitz, Ed., ser. Lecture Notes in Computer Science, Springer Berlin Heidelberg, 1996, pp. 343–357.

[55] H.-K. Lo and H. F. Chau, "Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances," *Science*, vol. 283, no. 5410, pp. 2050–2056, Mar. 1999.

[56] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, "Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations," *Phys. Rev. Lett.*, vol. 92, no. 5, p. 057 901, Feb. 2004.

[57] H.-K. Lo, X. Ma, and K. Chen, "Decoy State Quantum Key Distribution," *Phys. Rev. Lett.*, vol. 94, no. 23, p. 230 504, Jun. 2005.

[58] T. Sasaki, Y. Yamamoto, and M. Koashi, "Practical quantum key distribution protocol without monitoring signal disturbance," *Nature*, vol. 509, no. 7501, pp. 475–478, May 2014.

[59] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *J. Cryptology*, vol. 5, no. 1, pp. 3–28, Jan. 1992.

[60] R. Alléaume, C. Branciard, J. Bouda, *et al.*, "Using quantum key distribution for cryptographic purposes: A survey," *arXiv:quant-ph/0701168*, Dec. 2014.

[61] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, "Limitations on Practical Quantum Cryptography," *Phys. Rev. Lett.*, vol. 85, no. 6, pp. 1330–1333, Aug. 2000.

[62] N. Lütkenhaus, "Security against individual attacks for realistic quantum key distribution," *Phys. Rev. A*, vol. 61, no. 5, p. 052 304, Apr. 2000.

[63] M. Lucamarini, I. Choi, M. B. Ward, J. F. Dynes, Z. L. Yuan, and A. J. Shields, "Practical Security Bounds Against the Trojan-Horse Attack in Quantum Key Distribution," *Phys. Rev. X*, vol. 5, no. 3, p. 031 030, Sep. 2015.

[64] A. N. Bugge, S. Sauge, A. M. M. Ghazali, J. Skaar, L. Lydersen, and V. Makarov, "Laser Damage Helps the Eavesdropper in Quantum Cryptography," *Phys. Rev. Lett.*, vol. 112, no. 7, p. 070 503, Feb. 2014.

[65] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, "Trojan-horse attacks on quantum-key-distribution systems," *Phys. Rev. A*, vol. 73, no. 2, p. 022 320, Feb. 2006.

[66] N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, "Trojan-horse attacks threaten the security of practical quantum cryptography," *New J. Phys.*, vol. 16, no. 12, p. 123 030, Dec. 2014.

[67] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," *Nature Photon*, vol. 4, no. 10, pp. 686–689, Oct. 2010.

[68] V. Makarov, A. Anisimov, and J. Skaar, "Effects of detector efficiency mismatch on security of quantum cryptosystems," *Phys. Rev. A*, vol. 74, no. 2, p. 022 313, Aug. 2006.

[69] S.-H. Sun, F. Xu, M.-S. Jiang, X.-C. Ma, H.-K. Lo, and L.-M. Liang, "Effect of source tampering in the security of quantum cryptography," *Phys. Rev. A*, vol. 92, no. 2, p. 022 304, Aug. 2015.

[70] A. Huang, A. Navarrete, S.-H. Sun, P. Chaiwongkhot, M. Curty, and V. Makarov, "Laser seeding attack in quantum key distribution," *arXiv:1902.09792 [quant-ph]*, Apr. 2019.

[71] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, "Time-shift attack in practical quantum cryptosystems," *arXiv:quant-ph/0512080*, Dec. 2005.

[72] V. Makarov, J.-P. Bourgoin, P. Chaiwongkhot, *et al.*, "Creation of backdoors in quantum communications via laser damage," *Phys. Rev. A*, vol. 94, no. 3, p. 030 302, Sep. 2016.

[73] C. Kurtsiefer, P. Zarda, S. Mayer, and H. Weinfurter, "The breakdown flash of silicon avalanche photodiodes-back door for eavesdropper attacks?" *Journal of Modern Optics*, vol. 48, no. 13, pp. 2039–2047, Nov. 2001.

[74] A. Koehler-Sidki, J. F. Dynes, T. K. Paraïso, *et al.*, "Backflashes from fast-gated avalanche photodiodes in quantum key distribution," *Applied Physics Letters*, vol. 116, no. 15, p. 154 001, Apr. 2020.

[75] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, "Device-independent quantum key distribution secure against collective attacks," *New J. Phys.*, vol. 11, no. 4, p. 045 021, Apr. 2009.

[76] U. Vazirani and T. Vidick, "Fully Device-Independent Quantum Key Distribution," *Phys. Rev. Lett.*, vol. 113, no. 14, p. 140 501, Sep. 2014.

[77] H.-K. Lo, M. Curty, and B. Qi, "Measurement-Device-Independent Quantum Key Distribution," *Phys. Rev. Lett.*, vol. 108, no. 13, p. 130 503, Mar. 2012.

[78] S. L. Braunstein and S. Pirandola, "Side-Channel-Free Quantum Key Distribution," *Phys. Rev. Lett.*, vol. 108, no. 13, p. 130 502, Mar. 2012.

[79] J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, "A high speed, postprocessing free, quantum random number generator," *Applied Physics Letters*, vol. 93, no. 3, p. 031 109, Jul. 2008.

[80] M. Wahl, M. Leifgen, M. Berlin, T. Röhlicke, H.-J. Rahn, and O. Benson, "An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements," *Applied Physics Letters*, vol. 98, no. 17, p. 171 105, Apr. 2011.

[81] Y.-Q. Nie, H.-F. Zhang, Z. Zhang, *et al.*, "Practical and fast quantum random number generation based on photon arrival time relative to external reference," *Applied Physics Letters*, vol. 104, no. 5, p. 051 110, Feb. 2014.

[82] B. Sanguinetti, A. Martin, H. Zbinden, and N. Gisin, "Quantum Random Number Generation on a Mobile Phone," *Phys. Rev. X*, vol. 4, no. 3, p. 031 056, Sep. 2014.

[83] D. G. Marangon, G. Vallone, and P. Villoresi, "Source-Device-Independent Ultrafast Quantum Random Number Generation," *Phys. Rev. Lett.*, vol. 118, no. 6, p. 060 503, Feb. 2017.

[84] C. H. Vincent, "The generation of truly random binary numbers," *J. Phys. E: Sci. Instrum.*, vol. 3, no. 8, pp. 594–598, Aug. 1970.

[85] B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, "High-speed quantum random number generation by measuring phase noise of a single-mode laser," *Opt. Lett., OL*, vol. 35, no. 3, pp. 312–314, Feb. 2010.

[86] H. Guo, W. Tang, Y. Liu, and W. Wei, "Truly random number generation based on measurement of phase noise of a laser," *Phys. Rev. E*, vol. 81, no. 5, p. 051 137, May 2010.

[87] M. Jofre, M. Curty, F. Steinlechner, *et al.*, "True random numbers from amplified quantum vacuum," *Opt. Express, OE*, vol. 19, no. 21, pp. 20 665–20 672, Oct. 2011.

[88] F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, "Ultrafast quantum random number generation based on quantum phase fluctuations," *Opt. Express, OE*, vol. 20, no. 11, pp. 12 366–12 377, May 2012.

[89] C. Abellán, W. Amaya, M. Jofre, *et al.*, "Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode," *Opt. Express, OE*, vol. 22, no. 2, pp. 1645–1654, Jan. 2014.

[90] Z. L. Yuan, M. Lucamarini, J. F. Dynes, B. Fröhlich, A. Plews, and A. J. Shields, "Robust random number generation using steady-state emission of gain-switched laser diodes," *Appl. Phys. Lett.*, vol. 104, no. 26, p. 261 112, Jun. 2014.

[91] Y.-Q. Nie, L. Huang, Y. Liu, F. Payne, J. Zhang, and J.-W. Pan, "The generation of 68 Gbps quantum random number by measuring laser phase fluctuations," *Review of Scientific Instruments*, vol. 86, no. 6, p. 063 105, Jun. 2015.

[92] H. Zhou, X. Yuan, and X. Ma, "Randomness generation based on spontaneous emissions of lasers," *Phys. Rev. A*, vol. 91, no. 6, p. 062 316, Jun. 2015.

[93] S.-H. Sun and F. Xu, "Experimental study of a quantum random-number generator based on two independent lasers," *Phys. Rev. A*, vol. 96, no. 6, p. 062 314, Dec. 2017.

[94] D. G. Marangon, A. Plews, M. Lucamarini, *et al.*, "Long-Term Test of a Fast and Compact Quantum Random Number Generator," *Journal of Lightwave Technology*, vol. 36, no. 17, pp. 3778–3784, Sep. 2018.

[95] C. Henry, "Theory of the phase noise and power spectrum of a single mode injection laser," *IEEE Journal of Quantum Electronics*, vol. 19, no. 9, pp. 1391–1397, Sep. 1983.

[96] G. Morthier and P. Vankwikelberge, *Handbook of Distributed Feedback Laser Diodes, Second Edition*. Artech House, Sep. 2013.

[97] R. Hui and M. S. O'Sullivan, *Fiber optic measurement techniques*. Amsterdam ; London: Elsevier/Academic Press, 2009.

[98] I. Fatadin, D. Ives, and M. Wicks, "Numerical simulation of intensity and phase noise from extracted parameters for CW DFB lasers," *IEEE Journal of Quantum Electronics*, vol. 42, no. 9, pp. 934–941, Sep. 2006.

[99] J. Troger, P.-A. Nicati, L. Thevenaz, and P. Robert, "Novel measurement scheme for injection-locking experiments," *IEEE Journal of Quantum Electronics*, vol. 35, no. 1, pp. 32–38, Jan. 1999.

[100] J. C. Cartledge and R. C. Srinivasan, "Extraction of DFB laser rate equation parameters for system simulation purposes," *Journal of Lightwave Technology*, vol. 15, no. 5, pp. 852–860, May 1997.

[101] D. J. Higham., "An Algorithmic Introduction to Numerical Simulation of Stochastic Differential Equations," *SIAM Rev.*, vol. 43, no. 3, pp. 525–546, Jan. 2001.

[102] L. Bjerkan, A. Royset, L. Hafskjaer, and D. Myhre, "Measurement of laser parameters for simulation of high-speed fiberoptic systems," *Journal of Lightwave Technology*, vol. 14, no. 5, pp. 839–850, May 1996.

[103] K. Czotscher, S. Weisser, A. Leven, and J. Rosenzweig, "Intensity modulation and chirp of 1.55-/spl mu/m multiple-quantum-well laser diodes: Modeling and experimental verification," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 5, no. 3, pp. 606–612, May 1999.

[104] I. Tomkos, I. Roudas, R. Hesse, N. Antoniades, A. Boskovic, and R. Vodhanel, "Extraction of laser rate equations parameters for representative simulations of metropolitan-area transmission systems and networks," *Optics Communications*, vol. 194, no. 1-3, pp. 109–129, Jul. 2001.

[105] Z. L. Yuan, M. Lucamarini, J. F. Dynes, B. Fröhlich, M. B. Ward, and A. J. Shields, "Interference of Short Optical Pulses from Independent Gain-Switched Laser Diodes for Quantum Secure Communications," *Phys. Rev. Applied*, vol. 2, no. 6, p. 064 006, Dec. 2014.

[106] X. Hachair, S. Barland, J. R. Tredicce, and G. L. Lippi, "Optimization of the switch-on and switch-off transition in a commercial laser," *Appl. Opt., AO*, vol. 44, no. 22, pp. 4761–4774, Aug. 2005.

[107] L. C. Comandar, M. Lucamarini, B. Fröhlich, J. F. Dynes, Z. L. Yuan, and A. J. Shields, "Near perfect mode overlap between independently seeded, gain-switched lasers," *Opt. Express, OE*, vol. 24, no. 16, pp. 17 849–17 859, Aug. 2016.

[108] K. Konnerth and C. Lanza, "Delay between current pulse and light emission of a gallium arsenide injection laser," *Appl. Phys. Lett.*, vol. 4, no. 7, pp. 120–121, Apr. 1964.

[109] A. L. Schawlow and C. H. Townes, "Infrared and Optical Masers," *Phys. Rev.*, vol. 112, no. 6, pp. 1940–1949, Dec. 1958.

[110] C. Henry, "Theory of the linewidth of semiconductor lasers," *IEEE Journal of Quantum Electronics*, vol. 18, no. 2, pp. 259–264, Feb. 1982.

[111] ——, "Phase noise in semiconductor lasers," *Journal of Lightwave Technology*, vol. 4, no. 3, pp. 298–311, Mar. 1986.

[112] K. Petermann, *Laser Diode Modulation and Noise*, ser. Advances in Opto-Electronics. Springer Netherlands, 1988.

[113] E. K. Lau, L. J. Wong, and M. C. Wu, "Enhanced Modulation Characteristics of Optical Injection-Locked Lasers: A Tutorial," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 15, no. 3, pp. 618–633, May 2009.

[114] Z. Liu and R. Slavík, "Optical Injection Locking: From Principle to Applications," *Journal of Lightwave Technology*, vol. 38, no. 1, pp. 43–59, Jan. 2020.

[115] M. Bennett, M. F. Schatz, H. Rockwood, and K. Wiesenfeld, "Huygens's clocks," *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, vol. 458, no. 2019, pp. 563–579, Mar. 2002.

[116] X.-T. Fang, P. Zeng, H. Liu, *et al.*, "Implementation of quantum key distribution surpassing the linear rate-transmittance bound," *Nature Photonics*, vol. 14, no. 7, pp. 422–425, Jul. 2020.

[117] Z. L. Yuan, B. Fröhlich, M. Lucamarini, G. L. Roberts, J. F. Dynes, and A. J. Shields, "Directly Phase-Modulated Light Source," *Phys. Rev. X*, vol. 6, no. 3, p. 031 044, Sep. 2016.

[118] M. Minder, M. Pittaluga, G. L. Roberts, *et al.*, "Experimental quantum key distribution beyond the repeaterless secret key capacity," *Nat. Photonics*, vol. 13, no. 5, pp. 334–338, May 2019.

[119] Y. Liu, Z.-W. Yu, W. Zhang, *et al.*, "Experimental Twin-Field Quantum Key Distribution through Sending or Not Sending," *Phys. Rev. Lett.*, vol. 123, no. 10, p. 100 505, Sep. 2019.

[120] X. Zhong, J. Hu, M. Curty, L. Qian, and H.-K. Lo, "Proof-of-Principle Experimental Demonstration of Twin-Field Type Quantum Key Distribution," *Phys. Rev. Lett.*, vol. 123, no. 10, p. 100 506, Sep. 2019.

[121] H. Liu, C. Jiang, H.-T. Zhu, *et al.*, "Field Test of Twin-Field Quantum Key Distribution through Sending-or-Not-Sending over 428 km," *arXiv:2101.00276 [quant-ph]*, Jan. 2021.

[122] L. Zhou, J. Lin, Y.-M. Xie, *et al.*, "Experimental Quantum Communication Overcomes the Rate-Loss Limit without Global Phase Tracking," *Phys. Rev. Lett.*, vol. 130, no. 25, p. 250 801, Jun. 2023.

[123] W. Li, L. Zhang, Y. Lu, *et al.*, "Twin-Field Quantum Key Distribution without Phase Locking," *Phys. Rev. Lett.*, vol. 130, no. 25, p. 250 802, Jun. 2023.

[124] T. L. Koch and J. E. Bowers, "Factors affecting wavelength chirping in directly modulated semiconductor lasers," in *Conference on Lasers and Electro-Optics (1985), paper WB2*, Optical Society of America, May 1985, WB2.

[125] T. L. Koch and R. A. Linke, "Effect of nonlinear gain reduction on semiconductor laser wavelength chirping," *Appl. Phys. Lett.*, vol. 48, no. 10, pp. 613–615, Mar. 1986.

[126] R. Tucker, "High-speed modulation of semiconductor lasers," *Journal of Lightwave Technology*, vol. 3, no. 6, pp. 1180–1192, Dec. 1985.

[127] J. Huang and L. W. Casperson, "Gain and saturation in semiconductor lasers," *Opt Quant Electron*, vol. 25, no. 6, pp. 369–390, Jun. 1993.

[128] Y. S. Lo, R. I. Woodward, N. Walk, *et al.*, "Simplified intensity- and phase-modulated transmitter for modulator-free decoy-state quantum key distribution," *APL Photonics*, vol. 8, no. 3, p. 036 111, Mar. 2023.

[129] R. I. Woodward, Y. S. Lo, M. Pittaluga, *et al.*, "Gigahertz measurement-device-independent quantum key distribution using directly modulated lasers," *npj Quantum Inf*, vol. 7, no. 1, pp. 1–6, Apr. 2021.

[130] L. N. Binh, *Advanced Digital Optical Communications*, 2nd ed. Boca Raton: CRC Press, Jan. 2017.

[131] T. Kobayashi, A. Tomita, and A. Okamoto, "Evaluation of the phase randomness of a light source in quantum-key-distribution systems with an attenuated laser," *Phys. Rev. A*, vol. 90, no. 3, p. 032 320, Sep. 2014.

[132] R. Shakhovoy, A. Tumachek, N. Andronova, Y. Mironov, and Y. Kurochkin, "Phase randomness in a gain-switched semiconductor laser: Stochastic differential equation analysis," *arXiv:2011.10401 [physics, physics:quant-ph]*, Nov. 2020.

[133] G. E. Shtengel, R. F. Kazarinov, G. L. Belenky, M. S. Hybertsen, and D. A. Ackerman, "Advances in measurements of physical parameters of semiconductor lasers," *Int. J. Hi. Spe. Ele. Syst.*, vol. 09, no. 04, pp. 901–940, Dec. 1998.

[134] J. Wang and K. Petermann, "Small signal analysis for dispersive optical fiber communication systems," *Journal of Lightwave Technology*, vol. 10, no. 1, pp. 96–100, Jan. 1992.

[135] R. Srinivasan and J. Cartledge, "On using fiber transfer functions to characterize laser chirp and fiber dispersion," *IEEE Photonics Technology Letters*, vol. 7, no. 11, pp. 1327–1329, Nov. 1995.

[136] K. Hinton and T. Stephens, "Modeling high-speed optical transmission systems," *IEEE Journal on Selected Areas in Communications*, vol. 11, no. 3, pp. 380–392, Apr. 1993.

[137] A. Royset, L. Bjerkan, D. Myhre, and L. Hafskjaer, "Use of dispersive optical fibre for characterisation of chirp in semiconductor lasers," *Electronics Letters*, vol. 30, no. 9, pp. 710–712, Apr. 1994.

[138] B. Wedding, "Analysis of fibre transfer function and determination of receiver frequency response for dispersion supported transmission," *Electronics Letters*, vol. 30, no. 1, pp. 58–59, Jan. 1994.

[139] F. Devaux, Y. Sorel, and J. Kerdiles, "Simple measurement of fiber dispersion and of chirp parameter of intensity modulated light emitter," *Journal of Lightwave Technology*, vol. 11, no. 12, pp. 1937–1940, Dec. 1993.

[140] B. Daino, P. Spano, M. Tamburrini, and S. Piazzolla, "Phase noise and spectral line shape in semiconductor lasers," *IEEE Journal of Quantum Electronics*, vol. 19, no. 3, pp. 266–270, Mar. 1983.

[141] M. W. Mitchell, C. Abellan, and W. Amaya, "Strong experimental guarantees in ultrafast quantum random number generation," *Phys. Rev. A*, vol. 91, no. 1, p. 012 314, Jan. 2015.

[142] I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, "An optical ultrafast random bit generator," *Nature Photon*, vol. 4, no. 1, pp. 58–61, Jan. 2010.

[143] P. L'Ecuyer and R. Simard, "TestU01: A C library for empirical testing of random number generators," *ACM Trans. Math. Softw.*, vol. 33, no. 4, 22:1–22:40, Aug. 2007.

[144] P. Roztocki, B. MacLellan, M. Islam, *et al.*, "Arbitrary Phase Access for Stable Fiber Interferometers," *Laser & Photonics Reviews*, vol. 15, no. 7, p. 2 000 524, Jul. 2021.

[145] R. Shakhovoy, M. Puplauskis, V. Sharoglazova, *et al.*, "Phase randomness in a semiconductor laser: Issue of quantum random-number generation," *Phys. Rev. A*, vol. 107, no. 1, p. 012 616, Jan. 2023.

[146] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems," *Phys. Rev. A*, vol. 78, no. 4, p. 042 333, Oct. 2008.

[147] N. Jain, C. Wittmann, L. Lydersen, *et al.*, "Device Calibration Impacts Security of Quantum Key Distribution," *Phys. Rev. Lett.*, vol. 107, no. 11, p. 110 501, Sep. 2011.

[148] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Phys. Rev. A*, vol. 72, no. 1, p. 012 326, Jul. 2005.

[149] X.-B. Wang, "Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography," *Phys. Rev. Lett.*, vol. 94, no. 23, p. 230 503, Jun. 2005.

[150] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, "Experimental Quantum Key Distribution with Decoy States," *Phys. Rev. Lett.*, vol. 96, no. 7, p. 070 502, Feb. 2006.

[151] X. Ma, *Quantum cryptography: Theory and practice*, Aug. 2008.

[152] M. S. Lee, M. K. Woo, J. Jung, Y.-S. Kim, S.-W. Han, and S. Moon, "Free-space QKD system hacking by wavelength control using an external laser," *Opt. Express, OE*, vol. 25, no. 10, pp. 11 124–11 131, May 2017.

[153] X.-L. Pang, A.-L. Yang, C.-N. Zhang, *et al.*, "Hacking Quantum Key Distribution via Injection Locking," *Phys. Rev. Applied*, vol. 13, no. 3, p. 034 008, Mar. 2020.

[154] A. Huang, A. Navarrete, S.-H. Sun, P. Chaiwongkhot, M. Curty, and V. Makarov, "Laser-Seeding Attack in Quantum Key Distribution," *Phys. Rev. Applied*, vol. 12, no. 6, p. 064 043, Dec. 2019.

[155] X.-X. Zhang, M.-S. Jiang, Y. Wang, *et al.*, "Analysis of an injection-locking-loophole attack from an external source for quantum key distribution," *Phys. Rev. A*, vol. 106, no. 6, p. 062 412, Dec. 2022.

[156] D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," in *International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings.*, Jun. 2004, pp. 136–.

[157] H.-K. Lo and J. Preskill, "Security of quantum key distribution using weak coherent states with nonrandom phases," *Quantum Info. Comput.*, vol. 7, no. 5, pp. 431–458, Jul. 2007.

[158] Z. Yuan, A. Plews, R. Takahashi, *et al.*, "10-Mb/s Quantum Key Distribution," *Journal of Lightwave Technology*, vol. 36, no. 16, pp. 3427–3433, Aug. 2018.

[159] A. Boaron, G. Boso, D. Rusca, *et al.*, "Secure Quantum Key Distribution over 421 km of Optical Fiber," *Phys. Rev. Lett.*, vol. 121, no. 19, p. 190 502, Nov. 2018.

[160] Y.-L. Tang, H.-L. Yin, X. Ma, *et al.*, "Source attack of decoy-state quantum key distribution using phase information," *Phys. Rev. A*, vol. 88, no. 2, p. 022 308, Aug. 2013.

[161] A. Huang, R. Li, V. Egorov, S. Tchouragoulov, K. Kumar, and V. Makarov, "Laser-Damage Attack Against Optical Attenuators in Quantum Key Distribution," *Phys. Rev. Appl.*, vol. 13, no. 3, p. 034 017, Mar. 2020.

[162] G. Currás-Lorenzo, K. Tamaki, and M. Curty, *Security of quantum key distribution with imperfect phase randomisation*, Apr. 2023.

[163] A. Ponosova, D. Ruzhitskaya, P. Chaiwongkhot, V. Egorov, V. Makarov, and A. Huang, "Protecting fiber-optic quantum key distribution sources against light-injection attacks," *PRX Quantum*, vol. 3, no. 4, p. 040 307, Oct. 2022.

[164] T. Shin-ichi and S. Inoue, "Optical fuse made of silica glass optical fibers spliced through low-melting glass with carbon-coating," in *Proceedings of the XXth International Congress on Glass, Report No. O-14-010*, Kyoto, Japan, 2004.

[165] G. Zhang, I. W. Primaatmaja, J. Y. Haw, X. Gong, C. Wang, and C. C. W. Lim, "Securing Practical Quantum Communication Systems with Optical Power Limiters," *PRX Quantum*, vol. 2, no. 3, p. 030 304, Jul. 2021.

[166] K. Petermann, "External optical feedback phenomena in semiconductor lasers," en, *IEEE J. Select. Topics Quantum Electron.*, vol. 1, no. 2, pp. 480–489, Jun. 1995.

[167] M. C. Soriano, J. García-Ojalvo, C. R. Mirasso, and I. Fischer, "Complex photonics: Dynamics and applications of delay-coupled semiconductors lasers," *Rev. Mod. Phys.*, vol. 85, no. 1, pp. 421–470, Mar. 2013.

[168] R. Shakhovoy, V. Sharoglazova, A. Udaltsov, A. Duplinskiy, V. Kurochkin, and Y. Kurochkin, "Influence of Chirp, Jitter, and Relaxation Oscillations on Probabilistic Properties of Laser Pulse Interference," *IEEE Journal of Quantum Electronics*, vol. 57, no. 2, pp. 1–7, Apr. 2021.