ICFO-INSTITUT DE CIÈNCIES FOTÒNIQUES &
UPC-UNIVERSITAT POLITÈCNICA DE CATALUNYA

Quantum random number generators for industrial applications

Carlos Abellan

Thesis Advisor: Prof. Valerio Pruneri
Thesis Tutor: Prof. Morgan Mitchell

PhD Thesis - 2018

To my family.

Abstract

Randomness is one of the most intriguing, inspiring and debated topics in the history of the world. It appears every time we wonder about our existence, about the way we are, e.g. *Do we have free will? Is evolution a result of chance?* It is also present in any attempt to understand our anchoring to the universe, and about the rules behind the universe itself, e.g. *Why are we here and when and why did all this start? Is the universe deterministic or does unpredictability exist?* Remarkably, randomness also plays a central role in the information era and technology. Random digits are used in communication protocols like Ethernet, in search engines and in processing algorithms as page rank. Randomness is also widely used in so-called Monte Carlo methods in physics, biology, chemistry, finance and mathematics, as well as in many other disciplines. However, the most iconic use of random digits is found in cryptography. Random numbers are used to generate cryptographic keys, which are the most basic element to provide security and privacy to any form of secure communication.

This thesis has been carried out with the following questions in mind: *Does randomness exist in photonics?* If so, *how do we mine it and how do we mine it in a massively scalable manner so that everyone can easily use it?* Addressing these two questions lead us to combine tools from fundamental physics and engineering. The thesis starts with an in-depth study of the phase diffusion process in semiconductor lasers and its application to random number generation. In contrast to other physical processes based on deterministic laws of nature, the phase diffusion process has a pure quantum mechanical origin, and, as such, is an ideal source for generating truly unpredictable digits.

First, we experimentally demonstrated the fastest quantum random number generation scheme ever reported (at the time), using components from the telecommunications industry only. Up to 40 Gb/s were demonstrated to be possible using a pulsed scheme. We then moved towards building prototypes and testing them with partners in supercomputation and fundamental research. In particular, the devices developed during this thesis were used in the landmark loophole-free Bell test experiments of 2015. In the process of building the technology, we started a new research focus as an attempt to answer the following question: *How do we know that the digits that we generate are really coming from the phase diffusion process that we trust?* As a result, we introduced the randomness metrology methodology, which can be used to derive quantitative bounds on the quality of any physical random number generation device. Finally, we moved towards miniaturisation of the technology by leveraging techniques from the photonic integrated circuits technology industry. The first fully integrated quantum random number generator was demonstrated using a novel two-laser scheme on an Indium Phosphide platform. In addition, we also demonstrated the integration of part of the technology on a Silicon Photonics platform, opening the door towards manufacturing in the most advanced semiconductor industry.

Resum

L'aleatorietat és un dels temes més intrigants, inspiradors i debatuts al llarg de la història. És un concepte que sorgeix quan ens preguntem sobre la nostra pròpia existència i de per què som com som. *Tenim free-will? És l'evolució resultat de l'atzar?* L'aleatorietat és també un tema que sorgeix quan intentem entendre la nostra relació amb l'univers mateix. *Per què estem aquí? Quan o com va començar tot això? És l'univers una màquina determinista o hi ha cabuda per a l'atzar?* Sorprenentment, l'aleatorietat també juga un paper crucial en l'era de la informació i la tecnologia. Els nombres aleatoris es fan servir en protocols de comunicació com *Ethernet*, en algoritmes de classificació i processat com *Page Rank*. També usem l'aleatorietat en els mètodes *Monte Carlo*, que s'utilitzen en els àmbits de la física, la biologia, la química, les finances o les matemàtiques. Malgrat això, l'aplicació més icònica per als nombres aleatoris la trobem en el camp de la criptografia o ciber-seguretat. Els nombres aleatoris es fan servir per a generar claus criptogràfiques, l'element bàsic que proporciona la seguretat i privacitat a les nostres comunicacions.

Aquesta tesi parteix de la següent pregunta fonamental: *Existeix l'aleatorietat a la fotònica?* En cas afirmatiu, *com podem extreure-la i fer-la accessible a tothom?* Per a afrontar aquestes dues preguntes, s'han combinat eines des de la física fonamental fins a l'enginyeria. La tesi parteix d'un estudi detallat del procés de difusió de fase en làsers semiconductors i de com aplicar aquest procés per a la generació de nombres aleatoris. A diferència d'altres processos físics basats en lleis deterministes de la natura, la difusió de fase té un origen purament quàntic, i per tant, és una font ideal per a generar nombres aleatoris.

Primerament, i fent servir aquest procés de difusió de fase, vam crear

el generador quàntic de nombres aleatoris més ràpid mai implementat (en aquell moment) fent servir, únicament, components de la indústria de les telecomunicacions. Més de 40 Gb/s van ser demostrats fent servir un esquema de làser polsat. Posteriorment, vam construir diversos prototips que van ser testejats en aplicacions de ciència fonamental i supercomputació. En particular, alguns dels prototips desenvolupats en aquesta tesi van ser claus en els famosos experiments *loophole-free Bell tests* realitzats l'any 2015. En el procés de construir aquests prototips, vam iniciar una nova línia de recerca per a intentar contestar una nova pregunta: *Com sabem si els nombres aleatoris que generem realment sorgeixen del procés de difusió de fase, tal com nosaltres creiem?* Com a resultat, vam introduir una nova metodologia, la metrologia de l'aleatorietat. Aquesta es pot fer servir per a derivar límits quantificables sobre la qualitat de qualsevol dispositiu de generació de nombres aleatoris físic. Finalment, ens vam moure en la direcció de la miniaturització de la tecnologia utilitzant tècniques de la indústria de la fotònica integrada. En particular, vam demostrar el primer generador de nombres aleatoris quàntic totalment integrat, fent servir un esquema de dos làsers en un xip de Fosfur d'Indi. En paral·lel, també vam demostrar la integració d'una part del dispositiu emprant tecnologia de Silici, obrint les portes, per tant, a la producció a gran escala a través de la indústria més avançada de semiconductors.

Resumen

La aleatoriedad es uno de los temas más intrigantes, inspiradores y debatidos a lo largo de la historia. Es un concepto que surge cuando nos preguntamos sobre nuestra propia existencia y de por qué somos como somos. *¿Tenemos libre albedrío? ¿Es la evolución resultado del azar?* La aleatoriedad es también un tema que surge cuando intentamos entender nuestra relación con el universo. *¿Por qué estamos aquí? ¿Cuándo y cómo empezó todo esto? ¿Es el universo una máquina determinista o existe espacio para el azar?* Sorprendentemente, la aleatoriedad también juega un papel crucial en la era de la información y la tecnología. Los números aleatorios se usan en protocolos de comunicación como *Ethernet*, y en algoritmos de clasificación y procesado como *Page Rank*. También la utilizamos en los métodos Monte Carlo, que sirven en los ámbitos de la física, la biología, la química, las finanzas o las matemáticas. Sin embargo, la aplicación más icónica para los números aleatorios la encontramos en el campo de la criptografía y la ciberseguridad. Aquí, los números aleatorios se usan para generar claves criptográficas, proporcionando el elemento básico para dotar a nuestras comunicaciones de seguridad y privacidad.

En esta tesis partimos de la siguiente pregunta fundamental: *¿Existe la aleatoriedad en la fotónica?* En caso afirmativo, *¿Cómo podemos extraerla y hacerla accesible a todo el mundo?* Para afrontar estas dos preguntas, se han combinado herramientas desde la física fundamental hasta la ingeniería. La tesis parte de un estudio detallado del proceso de difusión de fase en láseres semiconductores y de cómo aplicar este proceso para la generación de números aleatorios. A diferencia de otros procesos físicos basados en leyes deterministas de la naturaleza, la di-

fusión de fase tiene un origen puramente cuántico y, por lo tanto, es una fuente ideal para generar números aleatorios.

Primeramente, y utilizando este proceso de difusión de fase, creamos el generador cuántico de números aleatorios más rápido nunca implementado (en ese momento) utilizando únicamente componentes de la industria de las telecomunicaciones. Más de 40 Gb/s fueron demostrados utilizando un esquema de láser pulsado. Posteriormente, construimos varios prototipos que fueron testeados en aplicaciones de ciencia fundamental y supercomputación. En particular, algunos de los prototipos desarrollados en esta tesis fueron claves en los famosos experimentos *Loophole-free Bell tests* realizados en el 2015. En el proceso de construir estos prototipos, iniciamos una nueva línea de investigación para intentar dar respuesta a una nueva pregunta: *¿Cómo sabemos si los números aleatorios que generamos realmente surgen del proceso de difusión de fase, tal y como nosotros creemos?* Como resultado introdujimos una nueva metodología, la metrología de la aleatoriedad. Esta se puede usar para derivar límites cuantificables sobre la calidad de cualquier dispositivo de generación de números aleatorios físico. Finalmente, nos movimos en la dirección de la miniaturización de la tecnología utilizando técnicas de la industria de la fotónica integrada. En particular, creamos el primer generador de números aleatorios cuántico totalmente integrado utilizando un esquema de dos láseres en un chip de Fosfuro de Indio. En paralelo, también demostramos la integración de una parte del dispositivo utilizando tecnología de Silicio, abriendo las puertas, por tanto, a la producción a gran escala a través de la industria más avanzada de semiconductores.

Acknowledgments

There are countless experiences after +5 years at ICFO surrounded by so many amazing colleagues and friends. From ICFOnians to international collaborators, there are plenty of people to thank for. I will try to add as little personal references as possible since I would surely forget important names in the attempt of listing them all. Instead, I will thank the 7 groups of people that played a crucial role in the process of completing this Ph.D.

First, I'd like to thank ICFO for giving me this beautiful and challenging opportunity. ICFO has been a fantastic place to carry out the Ph.D, not only providing unique facilities and support for your research, but also exposing you to a wide rage of researchers working in the field of photonics. From human resources to purchasing, projects, logistics, front desk, maintenance, or management, I owe you an enormous thank you for making the Ph.D. here an easier journey to navigate than I could have ever imagined.

Second, I'd like to thank a long list of collaborators and colleagues from all over the world for having shared lots of physics and engineering conversations with me. From long days testing photonic components in Valencia to whiteboard discussions on randomness in Delft, inspiring quantum optics conversations in Vienna, tech discussions with scientists at NIST, and many chats with colleagues in conferences and meetings. I'm honoured for having had the chance to speak with some of the smartest scientists and engineers in the world.

Third, my admiration to the people working at the engineering offices at ICFO. Thank you José Carlos Cifuentes, Daniel Mitrani and the rest of the team at the electronic workshop. Thank you Xavi Menino and the rest of the team at the mechanical workshop, and thank you Gonçal Badenes,

Juli Cespedes and the rest of the IT team. Your help and support have been essential to achieving many of the results of this thesis.

Fourth, I'd like to thank Sergi Ferrando, Silvia Carrasco and the rest of the team at the Knowledge and Technology Transfer (KTT) unit. From the very beginning, they spent time sharing their vision on how basic research can be turned into technology, and how this technology can ultimately have an impact on society in the form of a product. I also had the chance to work with them on many outreach projects, this teaching so many lessons on how to understand science and its role in society. I can only thank you for having dedicated so much time to this project, shaping it and shaping me in the process.

Fifth, I'd like to thank everyone at ICFO that, directly or indirectly, has been there to share knowledge and time with me. To those who spent countless 4 pm coffees chatting about vacuum. To those who shared their research and experiments. To those who asked the smartest and toughest scientific and technical questions. To those who played music. To those who played football. To those that just said hi in the corridor, thank you for having made this journey and unforgettable experience.

Sixth, my most sincere thank you to my supervisors Valerio Pruneri and Morgan Mitchell, and to Waldimar Amaya. Thank you for having spent an infinite amount of time and brightness with me. Thank you for always having the door open even when the last thing you had was time. Thank you for having trusted me, sometimes even blindly, such as with the solo trip to Japan demoing one of our first prototypes when I was still an undergrad or the time I got into your office proposing some weird project on quantum physics and people. I'm truly honoured by the chance of having shared more than 5 years working with you.

Last, and definitely not least, the seventh group of people to thank for. Those that were home supporting, listening, asking, following and encouraging me at every single step of the process. My warmest thanks to my mum and dad, my brother Victor, and especially to Alba, who has suffered and enjoyed this thesis with me every single day, even dreaming (literally) with the technology from time to time.

Contents

List of Publications

Publications included in this thesis

A (Rude et al., 2017) M. Rude, **C. Abellan**, A. Capdevila, D. Domenech, M. W. Mitchell, W. Amaya, and V. Pruneri, Quantum random number generator on a Silicon Photonics chip, *Submitted* (2017).

B (Abellan et al., 2016a) **C. Abellan**, W. Amaya, D. Domenech, P. Muńoz, J. Capmany, S. Longhi, M. W. Mitchell, and V. Pruneri, Quantum entropy source in an integrated Indium Phosphide chip, *Optica* **3**, 9, 989-994 (2016).

C (Abellan et al., 2015b) **C. Abellan**, W. Amaya, D. Mitrani, V. Pruneri, and M. W. Mitchell, Fresh and pure random number generation for loophole-free Bell tests, *Phys. Rev. Lett.* **115**, 25, 250403 (2015).

D (Abellan et al., 2014a) **C. Abellan**, W. Amaya, M. Jofre, J. Capmany, A. Acin, M. W. Mitchell, and V. Pruneri, "Ultra-fast quantum random number generation using accelerated phase diffusion in a pulsed laser diode", *Opt. Express* **22**, 2, 1645-1654 (2014).

E (Mitchell et al., 2015) M. W. Mitchell, **C. Abellan**, and W. Amaya, Strong experimental guarantees in ultrafast quantum random number generation, *Phys. Rev. A* **91**, 012314 (2015).

Other relevant publications and conference contributions

F (Abellan et al., 2018) C. Abellan et al., Challenging local realism with human choices, *Nature* **557**, 212-216 (2018).

G (Hensen et al., 2015) B. Hensen, et al., Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometers, *Nature* **526**, 682-686 (2015).

H (Giustina et al., 2015) M. Giustina et al., Significant-Loophole-Free Test of Bell's Theorem with Entangled Photons, *Phys. Rev. Lett* **115**, 250401 (2015).

I (Shalm et al., 2015) K. Shalm et al., Strong Loophole-Free Test of Local Realism, *Phys. Rev. Lett* **115**, 250402 (2015).

J (Abellan et al., 2014b) **C. Abellan**, et al., "Ultrafast quantum random number generation using off-the-shelf components", *2014 Conference on Lasers and Electro-Optics (CLEO) - Laser Science to Photonic Applications. Optical Society of America*.

K (Abellan et al., 2015a) **C. Abellan**, et al. "Towards an Optically-Integrated Quantum Random Number Generator", *Joint Symposium in Integrated Quantum Optics. 2015 European Conference on Lasers and Electro-Opttics - European Quantum Electronics Conference. Optical Society of America.*

L (Abellan et al., 2017) **C. Abellan**, et al., "Game, cloud, and Architecture for the Big Bell Test", *Americal Physical Society March Meeting* (2017).

M (Abellan et al., 2016b) **C. Abellan**, W. Amaya, and M. W. Mitchell, Un test de Bell sin escapatorias, *Investigacion y Ciencia* **472**. Panorama (2016).

Chapter 1

Randomness in the information era

Randomness is one of the most profound topics in science and philosophy, present not only in modern society due to its practical relevance, but also in ancient philosophy because of its close connection with the concepts of physical determinism and free will. However, since the beginning of the 20th century, randomness has taken a completely new direction. The development of the first computers moved randomness from pure philosophical debates into practically-driven discussions. One example is in connection with the Monte Carlo method, a technique to numerically solve complex analytical problems using randomised trials, which finds application in multiple fields, including physics, finance, biology and chemistry. Another relates to cryptography, the art of encrypting and protecting information. While cryptographic methods have been used for thousands of years, the use of random number generators in connection with cryptography is relatively new, and seems to appear in response to the new cryptanalysis possibilities opened up by digital computers.

Today, random number generators are essential components in any connected device. In this chapter, we discuss the topic of randomness first from the application point-of-view. We then give a historic perspective of the evolution of the field of randomness, including the basic concepts that will be used throughout the thesis. Finally, we describe efforts towards building dedicated devices for random number generation over the last 70

years. We start with the first technologies that were built, then move on to the first photonic devices, and finally we review the origin of a specific set of schemes, the so-called continuous-variable quantum random number generators.

1.1 Random numbers uncovered

Randomness, in contrast to other natural resources like oil or water, is something that we will never run short of, as far as we know. Our current understanding of physics provides strong evidence that randomness is basically everywhere in the universe. However, "mining" it is not an obvious task. Pure randomness easily interacts with nearby non-random phenomena, masking its pure properties or even destroying them completely. Extracting good randomness from such mixed *raw material* is, however, possible, but requires sophisticated procedures, much like refining oil.

At this point, the question that some readers might be asking is, *"Why on earth would we want to mine randomness?"* Throughout history, the principal objective of humans has been to efficiently use natural resources, firstly to survive, and then to improve quality of life. This long and slow evolution process reached its maximum exponent during the industrial revolution, when machines took over manual and heavy processes. One of the most important consequences is that humans moved from being valued for their strength to being valued for their brains. The world today bears very little resemblance to the place where our great-great-grandparents used to live. Today, information is more valuable than any other natural resource, but similarly to what happened in the past, humans are now concerned with how to use information to improve our quality of life and to create growth and progress. Remarkably, and again very similarly to what happened with other valuable resources, humans are also tremendously concerned about protecting this *new gold*.

And guess what? In most of these areas, especially the protection of data and for understanding better the universe we live in, random numbers are of extreme necessity. In the following pages, we describe the role of randomness in multiple everyday life applications.

1.1.1 Randomness in computer science

Seemingly counter-intuitive at first, randomised algorithms play an important role in computer science and communications. It turns out that many problems would not be solvable without an external random input. Some examples include the original page rank algorithm by Google, communication systems on shared channels as Ethernet, and the Monte Carlo method.

In the case of page rank, the algorithm is trying to classify webpages based on their popularity, so that the most popular results can be shown to the users. Roughly speaking, the algorithm works as follows: a webpage $\mathcal{A}$ is ranked as popular if it has multiple inbound links from independent webpages. In order to calculate the number of inbound and outbound links, the algorithm operates by going to the source code of a webpage, looking for the outbound links, and jumping to a new webpage. By doing this repeatedly, an accurate picture of the complex network of links can be drawn. However, it can happen that a series of webpages might be pointing to one another in order to try to fool the algorithm and gain popularity maliciously. To avoid this trap, one possible solution is that the algorithm jumps randomly to a webpage $\mathcal{B}$ (with a probability p) which is not necessarily in the list of outbound links of the current webpage. By throwing in a random number, the algorithm will decide to follow a link or to randomly jump to a website, escaping eventual traps.

Randomness is also a basic resource in shared communication channels, such as Ethernet or mobile networks. The actual transmission of information happens through a given physical support, such as wires in the case of electrical signals, wires or air in the case of radio-frequency signals, or optical fibres in the case of optical signals. When multiple users make use of the shared resource simultaneously, collisions might occur, making it impossible for the receiver to extract the information. In such events, information is lost, and the senders have to retransmit the messages. But what happens if both senders retransmit at the same time? Of course, if their messages were to collide over and over again, the network would collapse, and no information would be able to be transmitted. In order to avoid this situation, every time a collision happens, the senders generate a random number before resending the message. This random number represents a waiting time, so before retransmitting, they have to

wait a given amount of time. In this way, the probability that both senders transmit at the same time again is largely minimised.

Another very important application of random numbers in computer science is the so-called Monte Carlo method, which is a statistical sampling technique extremely useful in solving complex analytical problems without known solutions or closed formulae. The technique has been known for a long time, but it gained a lot of traction after Stanislaw Ulam and John Von Neumann used it to solve neutron diffusion problems in nuclear reactions during World War II. Monte Carlo methods are used across science and engineering, including physics, biology, mathematics, chemistry, aeronautics, telecommunications and risk analysis. They are also used in politics and many others fields.

Unfortunately, low quality random number generation and patterns have led to several examples of incorrect results in solving specific problems (Click et al., 2011). A famous example is the failure to find the parameters of the Ising model (Ferrenberg et al., 1992; Lin et al., 2013).

1.1.2 Randomness in cryptography

Secret communications are as old as our knowledge of ancient civilisations. One of the first evidences that we have of employing encryption devices for secure communications is found in the work of a Greek poet, Archilochus (7th century BC). The device is known as the Scytale, and is based on scrambling the positions of the letters in a message. During the time of the Roman Empire, especially during Julius Caesar's ruling, several cryptographic methods were proposed. The so-called Caesar cipher is one of them. Basically, by taking each letter of the message and replacing it with the one three positions after it in the alphabet, the encrypted message was unintelligible to the eyes of the curious enemy. This type of algorithm, in which letters do not change position, but rather their "identity", is known as a substitution cipher. Substitution ciphers seem to have remained secure for a long time, until Al-Kindi, one of the most celebrated philosophers of the Islamic world, introduced the first form of hacking: the frequency analysis technique. The idea is that in every language there are some letters that are more common than others. In English, for instance, the letter e is the most common and frequently used. Thus, if we calculate

the probability of every letter in a message encrypted by a substitution cipher, we can identify each substitution by just looking at the frequency of the relevant symbol. For instance, if we get an English text and we see the symbol ζ being used most frequently, we can guess it represents the letter e. Many workarounds were introduced by code makers to improve the security against frequency analysis, for example by adding so-called code words to the development of polyalphabetic ciphers, like the Vigener cipher or the Engima machine. However, codebreakers also introduced more sophisticated techniques, allowing them to break increasingly advanced methods.

In order to build a cryptographic system, one of the first things that we need is (i) an algorithm that scrambles our message so that it becomes unintelligible, and (ii) an algorithm that unscrambles the data so it recovers meaning again. These algorithms are typically public and known by everyone, so that both senders and receivers know what to do to establish a secure communication. However, because these algorithms are known a priori, it is not enough to distribute information securely. To add secrecy, we add random digits into the recipee. By combining the message, the private random digits and the scrambling algorithm, we can now send information with high confidence that no attacker can gain information about our message (since he or she does not have access to the secret random digits). To close the crypto-system, the last remaining task is to distribute these random digits to the intended recipients, so that they can recover the original information by using the unscrambling algorithm and the secret random digits. In cryptography, we must assume that the enemy has full access to every single element of the cryptographic chain, except for one thing: the random digits (Kerckhoff principle). As a result, a cryptographic system is only secure if the random digits are truly unpredictable and if they are properly distributed between the intended recipients.

The one-time-pad (OTP) method, first developed by Frank Miller in 1882 and reinvented by Gilbert S. Vernam in 1917, is the most secure encryption algorithm currently known. It is unconditionally secure no matter how powerful our enemy is and how many resources he has. It is a simple variation of the Caesar cipher, in which now, instead of shifting the letters by a fixed value, every letter is shifted by a random value. Provided that each letter is substituted randomly (a random number de-

termines how many positions we should shift each letter), the encrypted message remains unbreakable forever. Two conditions have to be met: (i) the cryptographic key, the secret, has to be as long as the message, i.e. we need one random number for every letter in the message, and (ii) the random numbers have to be totally unpredictable to the enemy. The OTP method is, unfortunately, hard to implement because of the difficulty in generating long keys and, also, because of the difficulty in distributing those keys.

Algorithms requiring shorter cryptographic keys as well as algorithms to distribute the keys efficiently were required to bring encryption into practice. The most iconic examples today are the Advanced Encryption Standard (AES) and the Rivest-Shamir-Adleman (RSA) algorithms. AES-like methods are used to actually encrypt information, whereas RSA-like algorithms are used to exchange cryptographic keys. For the encryption process, both the sender and the receiver typically share the same encryption key, as with the OTP. However, keys of only 256 bits are typically required. These methods, in which sender and receiver use the same key, are known as symmetric encryption. For the distribution of the keys, a different type of algorithm is used, known as public key cryptography. The RSA is probably the most famous example of this type. Currently, key sizes of around 1024 or 2048 bits are used. In this case, sender and receiver do not use the same keys, and so these methods are known as asymmetric encryption. All algorithms other than OTP are based on so-called one-way functions, i.e. mathematical problems that are easy to calculate in one direction but very hard to compute in the opposite direction. For instance, in the case of RSA, the trick is that given two prime numbers a and b it is very easy to calculate $c = a \times b$, but it is very hard to find a and b given only c. As a result, these methods are known as being computationally secure, meaning that it is very hard for computers to perform a brute force attack to break the key. However, hard means hard, not impossible. In fact, the RSA algorithm was found by (Shor, 1999) to be easily breakable using a quantum computer. A huge effort is currently being made on building and implementing new algorithms that are quantum-safe, i.e. that cannot be broken easily by a quantum computer. For further information on quantum-safe algorithms, see (Bernstein et al., 2009).

Quantum key distribution (QKD) is an alternative to asymmetric encryption methods for implementing the key exchange step. The basic idea is that by using the laws of quantum physics, we can distribute strings of random numbers in an unconditionally secure manner between two parties. In this way, the distribution problem mentioned would be solved, and thus we would have a totally secure method to share keys between sender and receiver. Building scalable QKD systems is a technological challenge, and tremendous effort are being made towards global quantum key distribution infrastructures. When deployed, the combination of QKD and OTP would allow us to build perfectly secure cryptographic systems, ending forever the war between code makers and codebreakers. For a review on QKD, see (Gisin et al., 2002).

In any crypto-system, thus, the key exchange task is of fundamental importance. However, there is a prior step required before the key distribution stage: the key generation. Generating random numbers for creating cryptographic keys is far from a trivial task. There are many examples of faulty implementations that led to serious vulnerabilities. These include the attacks on the SSL keys generated in the Netscape browser (Goldberg et al., 1996; Shepherd, 1996), which used predictable sources for randomness generation (e.g. the time of the day), or the attacks on the OpenSSL protocol, which used a very limited entropy source space (Ahmad, 2008). (Lenstra et al., 2012) also found significant vulnerabilities in around two out of every 1,000 RSA keys. By scrutinising public records of RSA keys, they found an alarming number of around 27,000 vulnerable keys. The failure to generate good random numbers also allowed hackers to recover the private key used by Sony to sign software licenses for the Play Station. Similarly, collisions on the Java random number generator allowed hackers to steal Bitcoins (Nakamoto, 2008) from digital wallets, the cryptocurrency that at the time of writing is worth $\$4.225,91$. There are typically two incentives for breaking a cryptographic system: making money, or gaining private information. Using the best possible cryptographic keys to secure our systems is therefore a basic step in the protection of our data.

1.1.3 Randomness in other areas

Cryptography and computer science are two of the most randomness-consuming industries. However, many other applications rely heavily on random number generation, such as the gambling industry or fundamental research. In the case of gambling, for both the online format and the physical format, randomness is essential. In online format, the winning and losing of people's money is decided from the results of random number generators. From the distribution of the cards in a Poker game, to the outcome of an online roulette. It would be totally unacceptable if online casinos knew the digits that were going to be used. In physical casinos, random number generators are also crucial on non-croupier-based games, such as slot machines. In fact, flaws in the generation of random numbers inside slot machines was recently in the news when a group of hackers was found to be gaining huge profits by predicting the results from low-quality pseudo-random number generators. It was estimated that a single individuals could make more than $10k in a single day, and that coordinated groups of four people could make up to $250k a week.

Fundamental research also needs high quality random digits for a variety of purposes. A clear example is discussed thoroughly in this thesis, and is related to tests of local realism by means of Bell theorem implementations, in which a very special form of random digits is required to select the measurement basis in every experimental round.

1.2 From solitaire to quantum technologies

Throughout the 20th century, application-driven research has dramatically changed the field of randomness generation, from recording random samples in tables and printing them in books to using quantum dynamics and electronic devices directly plugged into computers and communication devices. In this section, we review the progress of the field in the 20th century[1].

[1] Randomness is a very multidisciplinary topic ranging from mathematics, engineering, computer science, philosophy, computer science, and physics. The literature on the topic is very extensive (see e.g. a bibliographic chronology (Sowey, 1972, 1978; Sowey, 1986) including about 750 highlighted publications on the topic. In this section, we attempt to

1.2.1 From tables to algorithms

In 1927, (Tippett, 1927) published a book with 41,200 random numbers extracted from census registers. A few years later, (Mahalanobis et al., 1934) reported a similar list, this time with normally distributed random numbers. Then, (Fisher et al., 1938) reported a new table emphasising its use in biology, agriculture and medical research, and (Kendall et al., 1939a; Kendall et al., 1939b) published 100,000 numbers read from a spinning disk illuminated by a flash lamp. Since then, a number of other tables have followed. A relevant example is *"A Million Random Digits with 100,000 normal deviates"* by (Rand Corporation, 1955), in which an "electrical roulette wheel" was used for the production of the digits.

Random tables were useful for solving certain mathematical problems later known as Monte Carlo methods. The first known example of a Monte Carlo calculation was by the French naturalist Georges-Louis Leclerc, Comte de Buffon, in the 18th century. Starting with a pure probabilistic problem, he estimated the value of π by counting how many needles thrown randomly into a horizontally-divided grid had intersections with the grid lines themselves. However, the real expansion of the Monte Carlo[2] method can be traced back to Stanislaw Ulam, when he reinvented the statistical sampling technique after sitting sick at home and trying, unsuccessfully, to calculate the probability of winning in a solitaire game. He eventually thought that if he were to play multiple times, he could count the number of wins versus the number of losses, thereby getting an approximate answer to the initially complex problem in an straightforward manner. Ulam and his colleague at the Los Alamos National Laboratory, John Von Neumann, used this statistical sampling technique to solve neutron diffusion problems in the ENIAC computer during World War II. In Ulam's own words (Eckhardt, 1987)

> *"The first thoughts and attempts I made to practice [the Monte Carlo method] were suggested by a question which occurred to me in 1946 as I was convalescing from an illness and play-*

give an overall idea of the direction that the field has taken, and why and how we got to where we are now.

[2] An interesting review on the Monte Carlo method with a perspective of the early days of the field can be found in (Chambers, 1967).

> *ing solitaires. The question was what are the chances that a Canfield solitaire laid out with 52 cards will come out successfully? After spending a lot of time trying to estimate them by pure combinatorial calculations, I wondered whether a more practical method than "abstract thinking" might not be to lay it out say one hundred times and simply observe and count the number of successful plays. This was already possible to envisage with the beginning of the new era of fast computers, and I immediately thought of problems of neutron diffusion and other questions of mathematical physics, and more generally how to change processes described by certain differential equations into an equivalent form interpretable as a succession of random operations. Later... [in 1946, I] described the idea to John von Neumann and we began to plan actual calculations"*

Unfortunately, when combining statistical sampling concepts, such as the Monte Carlo technique, with computers, previous methods based on getting the random samples from tables was no longer viable. Firstly, these methods were extremely slow and limited - Monte Carlo calculations on computers required much longer sequences of random digits. Secondly, the quality of those methods was not sufficient. For instance, (Yule, 1938) scrutinised Tippett's numbers and reported evidence of *"patchiness"*. The longer the sequence of random digits is, the easier it is to detect imperfections.

In order to implement the Monte Carlo approach in the ENIAC computer, Von Neumann devised a smart strategy for generating random numbers directly on the computer. The method introduced by Von Neumann is known as the mid-square method. It consists of calculating the square of an n-digits number to obtain a $2n$-digits number, then keeping the n digits in middle of the resulting number, and finally repeating these steps periodically. Generally known as pseudo-random number generators, these methods have the advantages of being fast, and, more importantly, directly available to the calculation machines. The main drawback is that they are very predictable, in other words, not random. Pseudo-random number generators produce digits with statistically-good properties, like those observed in truly random sequences. This complete lack of

randomness seemed to have some advantages for certain applications. Quoting (Von Neumann, 1951)'s thoughts on the topic

> *"Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin. [...] The real objection to this procedure [using physical randomness] is the practical need for checking computations. If we suspect that a calculation is wrong, almost any reasonable check involves repeating something done before. At that point, the introduction of new random numbers would be intolerable. I think that the direct use of a physical supply of random digits is absolutely unacceptable for this reason and for this reason alone. The next best thing would be to produce random digits by some physical mechanism and record them, letting the machine read them as needed. At this point we have manoeuvred into using the weakest portion of presently designed machines - the reading organ."*

In 1949, D. H. Lehmer proposed a new algorithm for producing pseudo-random digits (Lehmer, 1949). This method, known as the linear congruential generator, is based on the following recursive equation

$$x_{i+1} = (ax_i + c) \mod m, \tag{1.1}$$

where a, c, and m are the parameters of the generator. In order to obtain a statistically robust generator, one has to be careful on how to select these parameters. A famous example of this arithmetic method is the RANDU generator, proposed in the by the RAND Corporation. The RANDU generator is found by setting $a = 65539$, $c = 0$, and $m = 2^{31}$. A few years later, (Marsaglia, 1968) published in a seminal paper that any linear congruential pseudo-random number generator, such as the one in Eq. (1.1), fails to generate uniformly distributed random numbers. He showed that, when grouping the sequence in n-tuples, these tuples are always distributed in at most $(n/m)!$ parallel hyperplanes. Hence, while pseudo-random number generators are easy to implement and to use, one has to pay special attention when using this type of generators in practice. Some of the most relevant features of pseudo-randomness that have to be taken into account include:

- /a/ The seeding problem. Pseudo-random algorithms have to be initialised, a.k.a. as seeded. In the Lehmer method, the seeding process corresponds to the selection of the initial value x_0. If we set the same x_0 twice, we will obtain the exact same sequence of random numbers, so we have to be careful when seeding a pseudo random algorithm. Typically, the seeding process is performed using some kind of external randomness source, such as getting the current time in timestamp format, and then storing that result. Then, using only this number, one can re-generate the entire sequence for the simulation in the future by using the same algorithm.

- /b/ The finite length problem. All pseudo-random algorithms have a finite repetition length. This means that after some time, they start repeating themselves in exactly the same order. For instance, in the linear congruential generator described in Eq. (1.1), if we let x_0 be the initial state of the generator, whenever $x_i = x_0$, the exact same sequence is going to be generated again.

- /c/ The internal algebraic structure problem. Some pseudo-random algorithms have been found to lead to incorrect results in specific physical models, while leading to correct results in other systems. This issue has been observed multiple times when solving the Ising model (Ferrenberg et al., 1992; Lin et al., 2013), as well as in other problems (Click et al., 2011). As a result, pseudo-random algorithms have to be tested for every specific problem and problem size.

Pseudo-random number generators are generally believed to be good-enough for Monte Carlo purposes, even though they are not random at all. For computation purposes, many such algorithms are still used today for the generation of random digits in this way for computation purposes. The Mersenne-Twister (Matsumoto et al., 1998) is one of the most widely used schemes in Monte Carlo methods. However, progress in the field and in technology has evidenced that this lack of randomness might lead to incorrect results in some problems, and therefore, arguments such as the following one by (Von Neumann, 1951), deserved further consideration:

"We are here dealing with "cooking recipes" for making digits;

probably they can not be justified, but should merely be judged by their results. [...] If the digits work well on one problem, they seem usually to be successful with others of the same type."

1.2.2 The concept of randomness

In light of the above, randomness moved from being just a fundamental concept to becoming a basic resource for solving important problems. As a result, the concern with what randomness was and whether or not the methods being developed were good enough for solving problems became a fascinating debate. One of the first attempts at formalising randomness was based on the idea of frequency stability, influenced by the concept of *Kollectiv* by von Mises. Intuitively, a sequence is said to be random according to this definition if (i) being $f(r)$ a function counting the number of ones in a sequence of length $|r|$, $f(r)/|r|$ approaches a limit p as $|r|$ approaches infinity, and (ii) an infinite sub-group extracted from the original sequence, and $g(r)$ the function counting the number of ones in this new sequence, $g(r)/|r|$ goes to the same p as $|r|$ goes to infinity. The second rule avoids the possibility that sequences of the type 1010101010 are considered random even when perfectly satisfying condition one. Several authors refined Von Mises' concept of Kollectiv in an attempt at formalising the notion of randomness, for example (Church, 1940; Kendall, 1941).

The frequency stability approach has, however, some serious issues with respect to a formal definition of randomness. For instance, the digits of π, which look totally random and satisfy many of the properties of a perfectly random sequence, also satisfies the frequency stability requirement, in spite of the sequence being totally predictable. Using concepts from computation, three authors, (R. Solomonoff, 1964; R. J. Solomonoff, 1964), (Kolmogorov, 1965), and (Chaitin, 1969), independently and almost simultaneously introduced the concept of *compressibility* as a necessary element to define randomness. The intuition is that the shortest way to represent a patternless, irregular, or unpredictable string, is by giving the string itself. Note that in the case of the digits of π, the Kolmogorov complexity works well to identify the lack of randomness, since we can write a very short program that describes precisely the digits of

π without having to write them all. For instance, we can simply describe them by writing *"divide the perimeter of a circumference by twice its radius and you will find all the digits of π"*.

More formally, the Kolmogorov complexity $K(x)$ of a sequence x, which is the term coined to this new definition of randomness, is defined as the length of the shortest computer program whose output is x. Namely, if x has length n and is perfectly random, $K(x) = n$. However, if the sequence is not random, $K(x) < n$. For instance, the sequence of "$10,000$ zeros" can be easily written in a computer program as *"print 10,000 zeros"*, which clearly takes much less space than actually writing ten thousand zeros one after the other. Remarkably, (Martin-Löf, 1966) proved that, in the asymptotic limit, a sequence that is random according to the Kolmogorov complexity criterion would pass any computable statistical test for randomness. Unfortunately, the Kolmogorov complexity is also proven not to be computable, and, as a result, cannot be used to prove the randomness of a sequence. In addition, the Kolmogorov complexity does not provide any insight on what randomness actually is, but rather on whether a specific sequence of digits satisfies a given definition.

In general, there are two general ways to look at randomness and attempt to describe it. Firstly, it can be looked at from the perspective of sequences of digits that have to fulfil certain properties, as with the frequency stability or the Kolmogorov complexity, and secondly, from the perspective of the origin of the random digits or the nature of the generation process. In this second approach, the process by which the numbers are generated must fulfil certain properties. For example, a process that faithfully records the time of nuclear decay events generates numbers that are random in a way that numbers generated by running an algorithm on a deterministic computer are not. For those interested in this second approach, the question *does randomness exist in the universe?* becomes of fundamental importance. If randomness did not exist, as in a Newtonian description of the world in which any dynamical system can be predicted from a proper model and initial conditions, then random number generation would be simply impossible. However, when physics moved from classical physics to quantum physics, new and important elements were brought into the discussion. Quantum mechanics is a probabilistic theory and randomness is inherent in almost any physical process.

Today, generating random digits is therefore possible within a quantum mechanical world. However, there is still some work to be done to produce random digits from quantum processes. Note that even if we have access to a perfect quantum system, and this quantum system is totally random, how do we know that the bits that are produced are truly coming from that process alone? How do we know that all the electronics that we use are not introducing weaknesses or predictabilities? To answer these questions there are generally two approaches. The first one is based on the sequence idea and employing statistical testing methods to test digits. We will review progress in this direction in the next section. The other option is to use the origin approach to randomness and derive entropy estimates from the physical device. We will review this second option afterwards.

1.2.3 Testing random digits

Imagine that we are in Las Vegas playing the roulette table. To simplify the explanation, let's imagine that only red and black outcomes are possible. In this case, the probability of a red or a black outcome are both $1/2$, and the probability that a specific combination of n outcomes appears is $1/2^n$. Imagine now that 19 reds have appeared in a row. What will our next bet be? A lot of people would bet on the belief that *"the probability that the next is red is very low because there have been already 19 reds"*, and thus place the next bet on blacks. The wheel spins again, but, unfortunately, the outcome turns out to be red again. Angry, and with a feeling of having been tricked, we decide to go to the director of the Casino to make a complaint. The director, however, who is a quantum physicist, kindly tells us that it is simply impossible that we have been tricked because the outcome of the roulette is based on sampling a quantum process. We might have a hard time believing it, but he continues, *"Well, the roulette table has been here for 2 years now, and it generates a new outcome every second. This means that more than 63 million values have been generated already. It's true that the sequence that has just occurred is unlikely and not typical (the probability of this happening is $1/2^{20} \approx 0.95 \times 10^{-6}$ to be more precise). However, since so much data has been generated during these two years, the 20-red-long sequence*

should have happened approximately 60 times already". To prove himself, he goes to the records, processes the data, and detects that such a sequence has actually occurred 57 times. So, indeed, probabilistically speaking, that was a perfectly random sequence.

This toy example is useful to get an idea of how statistical testing works, and what the limitations are. In general, a statistical test "looks" at sequences, and if they are outside of what we might call, loosely speaking, typical, it concludes that the sequence is not random. This brings some limitations of course, since perfect random number generators, like the one in the example above, also generate "non-typical" sequences from time to time. The most relevant implication of this fact is that perfect random number generators are expected to fail statistical tests with non-zero probability when, by chance, they produce "non-typical" sequences. To fully test a random number generation device, we would have to test a string of infinite data generated by it, but, unfortunately, this is not possible.

Nowadays, statistical testing of random number generators is typically carried out via batteries of statistical tests. (Knuth, 1997) covers some of the most important tests. A more recent overview with benchmarking of some commercial generators can be found in (Jakobsson, 2014). The most commonly used batteries of statistical tests today are the NIST SP 800-22 test suite (Rukhin et al., 2010), the Test U01 by (L'Ecuyer et al., 2007), and the Diehard and Dieharder suits (Brown, 2016; Marsaglia, 1985). Statistical testing is a useful tool when it comes to the detection of patterns. Basically, it can be used to proof the lack of randomness, but not as a tool to proof the existence of randomness. In the next section, we discuss the second approach to testing random number generators, which is based on thoroughly analysing the functioning of a physical device, understanding the physical process, and tracing back to fundamental principles the generation of every random digit.

1.2.4 Entropy estimation and randomness extraction

Computer algorithms cannot generate randomness due to their full deterministic nature. In contrast, physical processes can be used to create random digits based on the assumption that certain physical processes

are random. Unfortunately, there is a price to pay. Even if the physical system is perfectly random, the conversion from an ideal physical process into digital bits requires many steps that reduce the purity of the original bits. Some examples of device imperfections, present in any physical device, include electronic noise, digitisation noise, thermal effects, electromagnetic interference, and mechanical vibrations, among many others. Fortunately, nearly perfect random digits can be obtained from the output of an imperfect device by using a set of mathematical methods known as randomness extractors[3].

In Fig. (1.1), we illustrate the effect of device imperfections on the quality of the output bits from a physical random number generator. Typically, we start with a well-identified physical system which exhibits a physical property whose value changes in time in a way that is unpredictable. Then, a detection system converts these random dynamics into, typically, an electrical signal. Finally, an analogue-to-digital converter translates this electronic signal into the digital domain by means of a digitisation process. All of the processes following the *pure* physical process reduce the quality per bit of the raw data, introducing therefore fluctuations that do not originate from the physical process that we trust. Note that this is clearly an undesired effect, but the question is: *"can we quantify the 'quality' of a random number generator?"* or *"can we quantify how the effect of all these untrusted processes on the trusted signal?"* The conditional min-entropy (Chor et al., 1988), a variant of the concept of entropy that was introduced into the field of information by (Shannon, 1949), turns out to be a very useful measure for this task. The conditional min-entropy quantifies the amount of unpredictability or extractable randomness in a given physical process conditioned on everything that happened in the past, including all the previous values generated by the process itself as well as any other physical process potentially influencing the trusted entropy source mechanism. Then, once the conditional min-entropy of a source is found, a randomness extractor can generate a quasi-perfect string by applying a data compression, albeit at the expense of losing some bits. We will first describe the process of min-entropy estimation and then review the evolution of randomness extraction.

[3] A review on randomness extraction can be found in (Vadhan, 2012).

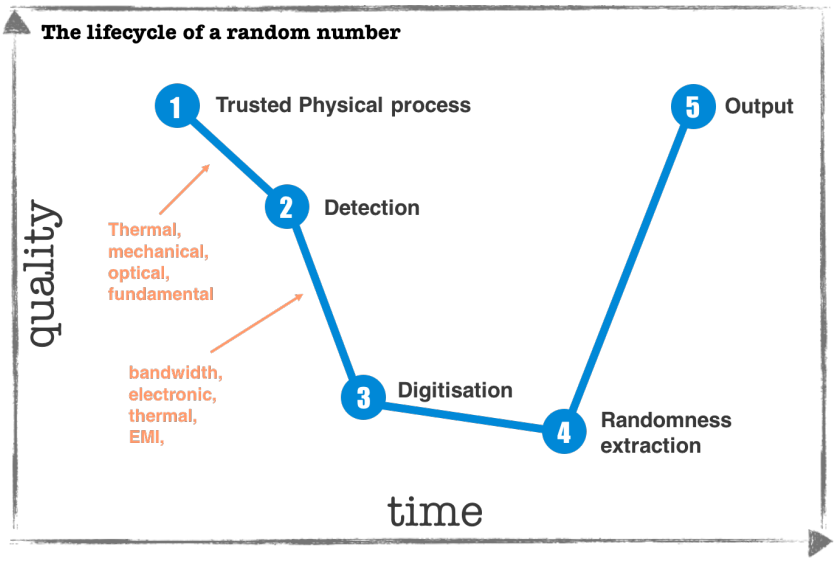


Figure 1.1: In any physical random number generator, the quality of the digital data is degraded due to the unavoidable imperfections of real devices. The detection and digitisation of the trusted physical process reduce the quality of the digital data. By rigorously quantifying the amount of interference of these undesired effects, one can recover the original quality by using a randomness extraction method.

Min-entropy estimation

Randomness extractors create nearly perfect random sequences from imperfect raw data by compressing the input space and by *sacrificing* some input bits. The question is: *how many bits do we have to sacrifice*? Intuitively, if we have a signal with k bits of *available* randomness, but we produce $n > k$ bits in our measurement process, at the end, we can get k bits of randomness at most, but never more. But what does this k represent and how do we measure it? The conditional min-entropy H_∞ was introduced into the field of randomness extraction in order to estimate the amount of extractable randomness from a given source, conditioned on all the prior knowledge that someone attempting at predicting the next value has. This includes, but is not limited too, all the prior values generated by

the source, and any other physical signal that can interact with the trusted process. If we let X be the trusted physical process and H all the prior history or knowledge available before the next value is generated, we can write

$$H_\infty(X|H) \equiv -\log \max_x P[X = x|\ H = h]. \tag{1.2}$$

The conditional min-entropy quantifies the guessing probability of a random variable X given H. In other words, it represents the best chance that someone (e.g. an adversary) has to correctly guess the next value in the sequence. Using the definition of conditional min-entropy, the concept of k-source is introduced. From now on, we will use min-entropy and conditional min-entropy indistinguishably. Basically, a random variable X (or a weak entropy source) is said to be a k-source if $H_\infty(X|H) \geq k$, or, equally, that $P[X = x|H = h] \leq 2^{-k}$.

Estimating the min-entropy or conditional min-entropy on a real device is a complicated problem. Imagine, for instance, that we have a trusted random variable Q (a process that is trusted to produce unpredictable dynamics), but due to electronic noise E and thermal effects T, the signal that we have access to will be given by $S = f(Q,T) + E$, $f(Q,T)$ being a function whose amplitude depends on both Q and T. In other words, the amplitude of the trusted process depends on the temperature and any electronic noise added to the signal. Thus, have access to S but not directly to Q. The role of the experimenter is to devise a measurement strategy that allows her or him to bound the effect of E and T on the predictability of the process S.

The connection between min-entropy and randomness extraction is simple. Imagine that we have a device producing random strings of n numbers. Imagine also that the device is a k-source, being $k < n$, but that our estimation of the min-entropy results in k'. When configured properly, the output of a randomness extraction will be a k'-source. Thus, it is of vital importance that the entropy estimation process never overestimates the min-entropy, or what is the same, that k is a strict upper bound for k'.

Randomness extraction

One of the first randomness extractors was proposed by John Von Neumann, and was designed to eliminate a constant bias in a sequence of bits. Basically, if we have a sequence $\mathbf{x} = \{x_1, x_2, \cdots\}$, the Von Neumann extractor takes two subsequent input bits and puts a 0 at the output if the combination is 01, puts a 1 if the combination is 10, or puts nothing if the combination is either 00 or 11. Thus, given a source with $P[0] \neq P[1]$, with both $P[0]$ and $P[1]$ constant over time, the output from the Von Neumann extractor will be unbiased, since $P[01] = P[10] = P[1]P[0]$. For example, if the sequence 0010110110 were processed with the Von Neumann extractor, the output 101 would be produced. There are several considerations with Von Neumann's extractor. Firstly, it assumes independent and identically distributed (IID) bits, secondly, it has an efficiency of at most 50% (i.e. we lose at least half of the input bits), and thirdly, the output rate is not constant. In order to design a randomness extractor, we need a randomness for the input string. In the case of Von Neumann, this is the IID assumption, which is very restrictive, since no real device satisfies it. (Blum, 1984) introduced a more general randomness model for sources based on deterministic finite state Markov chains. By using this more general randomness model, Blum's extractor, which consists of carefully applying the Von Neumann extractor depending on the state of the Markov chain, can be used with physical devices satisfying the Markov assumption. These type of randomness extraction algorithms, in which a pre-determined computation defines the extraction process, is known as a deterministic extractor.

(Santha et al., 1984) (SV) introduced an even more general model for random sequences. A source can be described by the SV model if for any i, every $x_1, \cdots, x_n$, and some constant $\delta > 0$,

$$\delta \leq P[X_i = 1 | X_1 = x_1, \cdots X_{i-1} = x_{i-1}] \leq 1 - \delta. \tag{1.3}$$

Using this model for random sequences, which applies to any physical device, Santha and Vazirani proved that deterministic randomness extraction was impossible using only one weak, a.k.a. corrupted, entropy source or k-source. In contrast, they also showed that by combining the output of multiple independent weak sources using a simple

bitwise xor operation, randomness extraction was possible. In particular, they proved that by combining the output of m independent weak sources $x_1, x_2, \cdots, x_m$ as $y = x_1 \oplus x_2 \oplus \cdots \oplus x_m$, the bias is bounded by $|P[y = 1] - P[y = 0]| \leq (1 - 2\delta)^m$. Note, however, that m bits are required to generate 1 single output bit and that on physical grounds. This method, in which multiple weak sources of random digits are combined, is known as independent-source randomness extraction.

Faced with the impossibility to design randomness extractors using only single weak sources, researchers began to look for new extraction methods that could be applied to the output of single devices. One of the most relevant developments was the seeded extraction method introduced by (Nisan et al., 1996). Nisan and Zuckerman proved that by using a small number of independent random digits, a.k.a. seeds, randomness extraction is possible from just a single weak source. In general, a seeded extractor is a function $Ext : \{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\}^m$, which takes as an input a sequence of n-bits from a k-source X, combines it with d independent random bits (the seed), and generates a sequence of m bits. Here, the seed is assumed to be a sequence of perfect random bits. A seeded extractor is called a (k, ϵ)-extractor if for every k-source X on $\{0,1\}^n$, the m-dimensional output block is ϵ-close to the uniform distribution in $\{0,1\}^m$. Two distributions are said to be ϵ-close if the trace distance between them is at most ϵ (Frauchiger et al., 2013). Hash functions are a special and very common construction of seeded extractors. Toeplitz matrices, imported from the privacy amplification step in quantum key distribution, are efficient implementations for constructing hashing-based extractors for weak entropy sources. There are many other constructions, like the Trevisan extractor, which was proven to be secure even against quantum adversaries. (X. Ma et al., 2013) present a benchmarking between a Toeplitz extractor and a Trevisan extractor for their physical random number generator.

1.3 Physical random number generators

In this section we review efforts and developments made over the last 70 years on physical generators. We start with the first physical devices that were built in the 1950s, then we move on to photonic implementations,

which started in the 1980s, and finally, we review progress towards a specific type of photonic technology known as continuous-variable quantum random number generation.

1.3.1 First physical random number generators

With the rise of computation capacity, the development of electronic random number generators expanded (Hull et al., 1962). One of the first proposals was by (Pawlak, 1956). He proposed the use of flip-flop elements in a configuration such that every time a contact was activated, the circuit collapsed into one of two possible outcomes. Other researchers focused on exploiting the inherently random nature of the radioactive decay process (Isida, 1956; Manelis, 1961). By using a fast clock and a counter, for example, one can count the number of clock cycles between any two subsequent radiocative decay events. Given that these decay events happen at random times (described by Poisson statistics), the number of clock cycles between any two events will also be a random variable. The theory behind random number generation based on radioactive decay has been very influential, and similar schemes based on the time of arrival of photons at a single photon detector can be found commercially today.

An interest by the telecommunication industry emerged also in the 1950s in order to improve traffic simulations. One of the first dedicated devices for physical random number generation was developed by the Telecommunications Research Laboratory of Denmark for their Monte Carlo simulations at the Danish Electronic Digital Solution (DASK) (Isaksson, 1959). The motivation by Isaksson et al., was to eliminate the repetition pattern effect present in pseudo-random number generators. He developed a device based on the shot noise effect in a diode operating at 5 kb/s. Shortly after the first patent on the topic at the European Patents Office (EPO) (Sterzer, 1962), the authors proposed a device based on parametric oscillators. In that case, their motivation was to improve the quality of the random numbers, which they felt was not sufficient for the algorithms of the day when long computations were performed. By using a parametric oscillator with intrinsic noise and by driving the circuit with a radio-frequency signal that interrupts the oscillation periodically, the re-

Reference	**Physical process**
(Pawlak, 1956)	Metastability flip-flop
(Isida, 1956)	Radioactive decay
(Isaksson, 1959)	Shot noise in a diode
(Sterzer, 1959)	Subharmonic oscillator
(Manelis, 1961)	Radioactive decay
(Sterzer, 1962)	Parametric oscillators
(Lancaster, 1967)	Oscillators and counters
(Whitaker et al., 1967)	Sampling wide band noise
(Vincent, 1970)	Radioactive decay
(Schmidt, 1970)	Radioactive decay
(George et al., 1971)	Oscillators and counters
(Maddocks et al., 1972)	Pulsed noise source
(Inoue et al., 1983)	Radioactive decay

Table 1.1: List of some physical random number generation papers and patents until the introduction of photonic methods for random bit generation in the 1980s. This list does not aim at being complete, but rather at illustrating some general traits in the progress made on physical randomisers during the second half of the 20th century.

sulting device oscillates with a random phase in every new modulation cycle. A few years later, a second patent on the topic was disclosed to the EPO, (Whitaker et al., 1967). Here, a device comprising a randomly fluctuating signal from a wide-band source, e.g. a gas discharge tube, was proposed, and random digits were extracted by sampling the amplitude of the signal. The main motivation for this work was to outsource the generation of random digits to a dedicated device, so that the main compute node could focus on the specific calculation at hand.

During the 1970s, work on physical random number generation increased, targeting also the gaming industry. In an article published in 1967 in Popular Electronics, (Lancaster, 1967) proposed a physical random number generator to simulate the throwing of a pair of dice, to be used in board games. Based on a 3 kHz oscillator driving a pair of coun-

ters, every time the user pressed a button, the counters stopped. The random number was given by the current value of the counters. Following on from this work, the General Electric Company patented technological improvements that overcame some limitations from the prior scheme published by (George et al., 1971). During this decade, several patents were presented in Japan by companies such as Cassio, NEC Corp., Hitachi, Fujitsu, and Nippon Electric.

Following the landmark contribution by (Shamir, 1981) and (Blum et al., 1982), the use of physical generators in cryptography to generate cryptographically strong sequences of random digits gained a lot of traction. Clearly, pseudo random numbers were not strong enough for cryptographic use, since gaining information about the internal state of an algorithm eliminates all the security of the protocol. To mitigate this effect, (Blum et al., 1982; Shamir, 1981) introduced the concept of cryptographically strong pseudo-random number generation. In order to build these new type of generators, they proposed the combination of some sort of physical randomness to act as a random seed for strong pseudo-random number generation algorithms.

Currently, most system integrators use dedicated random number generation devices based on physical processes, including, for example, the Intel RdRand instruction, which is based on metastability effects on transistors caused by thermal fluctuations.

1.3.2 Photonic quantum random number generators

The first optical implementation of random number generators was proposed in the 1980s by (Morris, 1985). Following on from those results, (Marron et al., 1986) experimentally demonstrated the first optical random number generator by exploiting the random speckle pattern from a laser source in a 2-D array of photon detectors. By thresholding the output of each one of the pixels of the array, an arbitrary distribution function for the random numbers could be obtained, being very useful for Monte Carlo calculations requiring specific distributions. (Morris, 1989) patented the optical method for random number generation in 2D arrays of photon detectors. Laser speckle was also the basis of the scheme proposed by (Ticknor et al., 1987), which was designed to provide a negative expo-

nential distribution function for an optical Boltzmann machine. Following this work, a massively parallel array of cellular processors, each with its own binary random bit generator, was proposed by (Devos et al., 1987). (Lalanne et al., 1990) then studied the speckle pattern in multimode fibres, and (Martino et al., 1991) introduced a novel approach based on the location of the detection events rather than the time.

(Rarity et al., 1994) proposed one of the most iconic photonic random number generation schemes. It was based on sending a single photon into a beam splitter and placing a single photon detector in each output. This idea was further explored by (Stefanov et al., 2000) and (Jennewein et al., 2000), and commercialised by the Swiss company ID Quantique. Similarly to the physical functioning of the first radioactive decay generators, the random arrival time of the photons was used by (H.-Q. Ma et al., 2005), who measured the time of arrival of the photons from a strongly attenuated pulsed laser source. Multiple variations and proposals have since been reported using the arrival time uncertainty of photons (Dynes et al., 2008; Stipcevic et al., 2007). These schemes for the spatial and temporal distribution of single-photon detection schemes are known as discrete variable quantum random number generators. These methods rely on single-photon detection technology, which is typically slow and expensive. After 2010, the literature on quantum random number generation and patent applications exploded. Schemes building on top of previous ideas continued to appear, and new promising quantum devices, requiring no single photon technologies, were also produced.

1.3.3 Continuous variable approaches

Continuous variable quantum random number generators are physical random devices based on sampling quantum systems with macroscopically-observable dynamics. In this section, we will review two of these schemes. The first one is based on measuring the vacuum fluctuations in a homodyne detection scheme, introduced by (Gabriel et al., 2010). The second one is based on measuring phase noise caused by spontaneous emission, first proposed by (Qi et al., 2010). Other schemes based on measuring amplified spontaneous emission, such as (Williams et al., 2010) have also attracted a lot of attention. Many papers have been published

Reference	Speed	Physical process
(Morris, 1985)	-	Photon counting
(Marron et al., 1986)	100 kb/s	Clipped laser speckle
(Devos et al., 1987)	-	Laser speckle
(Morris, 1989)	100 kb/s	Spatial distribution of light
(Martino et al., 1991)	100 kb/s	Spatial distribution
(Lalanne et al., 1990)	$\sim$ 1 Mb/s	Multimode fibre speckle
(Rarity et al., 1994)	-	Single photon splitting
(Stefanov et al., 2000)	100 kb/s	Single photon splitting
(Jennewein et al., 2000)	1 Mb/s	Single photon splitting
(H.-Q. Ma et al., 2005)	80 kHz	Time of arrival
(Stipcevic et al., 2007)	1 Mb/s	Time of arrival
(Dynes et al., 2008)	4 Mb/s	Time of arrival
(Qi et al., 2010)	500 Mb/s	Phase noise CW laser
(Gabriel et al., 2010)	6.5 Mb/s	Vacuum fluctuations
(Guo et al., 2010)	20 Mb/s	Phase noise in CW laser
(Wayne et al., 2010)	110 Mb/s	Time of arrival
(Xu et al., 2012)	6 Gb/s	Phase noise in CW laser
(Fürst et al., 2010)	50 Mb/s	Time of arrival
(Jofre et al., 2011)	1.1 Gb/s	Phase noise in GS laser
(Williams et al., 2010)	12.5 Gb/s	ASE Source
(Wahl et al., 2011)	150 Mb/s	Time of arrival
(Symul et al., 2011)	2 Gb/s	Vacuum fluctuations
(Li et al., 2011)	20 Gb/s	ASE
► (Abellan et al., 2014a)	42 Gb/s	Phase noise in GS laser

Table 1.2: List of photonic random number generators prior to the start of this thesis. Bitrate comparison should be analysed carefully, since some authors reported raw entropy production whereas others reported post-extracted bit rate capabilities. The first publication of this thesis is marked with ►.

during the development of this thesis, and are not reported in this state-of-the-art review. An in-depth description of both discreet and continuous variable approaches can be found in (Herrero-Collantes et al., 2017).

Homodyne detection of vacuum fluctuations

(Gabriel et al., 2010) introduced one of the first continuous variable quantum random number generation methods. The experimental setup comprises a polarisation beam splitter in a homodyne configuration with one input port connected to a strong local oscillator and the other to vacuum fluctuations (i.e. no input connected). The intensity of the two outputs of the polarisation beam splitter are photo-detected and subtracted (homodyne detection) to recover one of the quadratures of the field. By describing the vacuum field as $|0\rangle \equiv \int \psi(x)|x\rangle dx$, with $\psi(x)$ being the ground-state wave function, which is a Gaussian function centred around $x = 0$, and $|x\rangle$ being the amplitude quadrature eigenstates, the result of a projective measurement is a random variable x with a probability distribution function (PDF) given by $|\psi(x)|^2 = \langle x|0\rangle$, where $\langle x|$ is the projection vector. In order to account for untrusted additive noises Gabriel et al. proposed a simple entropy estimation technique by means of the Shannon entropy measure. Basically, if we let X be the quadrature measurement, they first calculated the entropy of the total signal $H(X)_{\text{total}}$ and then switched off the local oscillator to calculate the contribution from electronic noise $H(X)_{\text{elec}}$. Finally, by assuming that (i) the electronic noise and the quantum signal are combined in an additive form, and (ii) that they are mutually independent, they found the entropy of the quantum signal contribution by subtraction, i.e. $H(X)_{\text{quantum}} = H(X)_{\text{total}} - H(X)_{\text{elec}}$. (Symul et al., 2011) then reported a similar entropy source scheme with special focus on the entropy estimation and randomness extraction tasks. In particular, they proposed a smart thresholding technique allowing them to filter out the contribution of the noise by just dropping the least significant bits. They implemented the post-processing randomness extraction tasks on a field-programmable-gate-array (FPGA) in real-time. Later, an even more refined entropy estimation procedure was proposed by Haw et al., 2015.

Quantum phase noise schemes

(Qi et al., 2010) published the first manuscript on continuous variable methods for quantum random number generation. Their method consisted of measuring the phase noise effect in semiconductor lasers. Quantum phase noise is a direct consequence of spontaneous emission (Henry, 1982), and therefore a full quantum mechanical process. In (Qi et al., 2010), a continuous-wave-operated semiconductor laser is used. The light from the laser is sent to an unbalanced Mach Zehnder interferometer with a delay length of 650 ps. At the output of the interferometer, the amplitude of the detected signal is a function of the phase difference between the signals travelling from each path, in particular, the output intensity $I(t) \propto \cos \Delta\phi(t)$, where $\Delta\phi(t) \equiv \phi_1(t) - \phi_2(t-\tau)$. Here, $\phi_1(t)$ and $\phi_2(t-\tau)$ are the phases of the signal arriving via the short and long paths of the interferometer respectively. Provided that the phase of the laser diffuses sufficiently in the time interval τ due to spontaneous emission fluctuations, the detected signal will contain an inherently unpredictable component. (Guo et al., 2010) reported a very similar implementation of the phase noise scheme, and (Xu et al., 2012) reported a 1 order of magnitude rate improvement with respect to prior publications as well as a strict min-entropy estimation procedure.

(Jofre et al., 2011) proposed a variation of the above scheme by operating the laser source in gain-switching mode instead of continuous wave mode. In this way, by bringing the laser from below to above the threshold level periodically, the phase of the laser source diffuses much faster than in the continuous wave case. The average phase diffusion is proportional to $\langle \Delta\phi(T)^2 \rangle \propto I^{-1}$, where I is the intensity of the intracavity laser field. Hence, for a given time budget between subsequent measurements, the pulsed scheme diffuses several orders of magnitude faster than its continuous wave counterpart. The experimental configuration is exactly the same as in the previous scheme, but the delay length of the Mach Zehnder interferometer is now given by the pulse repetition frequency of the laser source. Effectively, the interferometer carries out the interference between two subsequent pulses from the laser. Again, by placing a digitiser directly at the output of the photodetector, random numbers can be extracted.

Phase noise approaches, both in continuous wave and gain-switching

modes, translate quantum phase noise information into the amplitude domain by means of an interferometer. Direct detection of macroscopic signals bring the advantage that telecommunication components, which are cost-effective and fast, can be used. In addition, the phase is an ideal variable for random number generation, since it is very robust to amplitude fluctuations as well as classical phase fluctuations.

1.4 Main results and outline

1.4.1 Main results

The main results of this thesis include

- **Theoretical framework for phase diffusion quantum random number generators in pulsed schemes and record speed demonstration**. We formalise the concept of phase diffusion in connection with quantum random number generation, and experimentally demonstrate the process at up to 42 Gb/s, a world-record for quantum random number generation at the time of publication.
- **Introduction of the randomness metrology procedure**. We introduce a methodology to estimate the min-entropy in real devices taking into account digitisation noise and memory effects. We have applied the methodology in several publications and prototypes, and this represents an important step towards building certifiable devices. This type of guarantees is important for certification agencies, which already have similar approaches in their regulatory frameworks.
- **First fully integrated quantum random number generation chip**. By using an Indium Phosphide platform and a new entropy source configuration based on a two-laser scheme, we demonstrate the first full photonic integration of a quantum random number generation device. In addition, we also report the integration of the scheme on a Silicon Photonics platform with an external laser source, providing a route towards production in the most advanced semiconductor industry.

- **Development of an enabling technology for loophole-free Bell test experiments**. By using the ultrafast scheme developed in this thesis and the randomness metrology framework, we develope and characterise a series of six prototypes that played a key role in the three 2015 loophole free Bell Test experiments. By developing an ultra-low latency technology and by providing strict min-entropy bounds, the developed prototypes constituted a unique device for the needs of the experiments.

1.4.2 Outline

This thesis is organised as follows:

- In **Chapter 2**, we introduce the concept of phase diffusion quantum random number generation in a pulsed configuration. We start by introducing the theoretical framework supporting the phase diffusion process. We follow this with a Monte Carlo simulation illustrating the average phase diffusion experienced in a pulsed laser, and show a comparison between pulsed and continuous wave schemes. We then show the results for the ultrafast (42 Gb/s) experiment, and we conclude with an intuitive introduction to the randomness metrology procedure that is used in Chapter 4.

- In **Chapter 3**, we describe progress towards the integration of the phase diffusion quantum random number generation technology in an integrated chip. We first describe the full optical integration in an Indium Phosphide chip using a new two-laser scheme. Then, we show the integration of a self-delayed scheme using Silicon Photonics with an external light source.

- In **Chapter 4**, we demonstrate the development of the fresh and pure random number generation technology employed in the loophole free Bell test experiments of 2015. We illustrate the design considerations as well as giving an in-depth description of the experimental work carried out to quantify and bound the unpredictability of the source and the freshness time.

Chapter 2

Phase-diffusion in pulsed semiconductor lasers

Spontaneous emission is the process by which an atom decays from an excited state into a lower energy state without any apparent cause. In each of these quantum jumps, energy is released in the form of a photon, whose frequency is proportional to the energy difference of the initial and final atomic states. The phenomenon of spontaneous emission can only be theoretically framed within a full quantum description of both matter and radiation. In the 1980s, Charles Henry pioneered the study of the effect of spontaneous emission in semiconductor lasers, and recently, these principles have been used in the development of quantum random number generators (Jofre et al., 2011; Qi et al., 2010; Xu et al., 2012). In this chapter, we present progress towards the understanding of the phase diffusion process in gain-switched semiconductor lasers.

2.1 Spontaneous emission as an entropy source

Laser technology, first proposed in (Schawlow et al., 1958), has been one of the most disruptive technologies of the last century, transforming many industries, such as industrial manufacturing and medical procedures, and enabling the heart of the Internet today, namely optical communications. One of the most particular features of laser radiation is its extremely nar-

row spectrum. Understanding the linewidth of the laser attracted a lot of interest during the second half of the 20th century, since the first predictions by Schwalow-Townes, and after posterior adjustments to the theory by (Lax, 1967). However, none of this predictions were capable of predicting the experimental observations made in semiconductor lasers (Fleming et al., 1981). In 1982, C. Henry presented the first theoretical description capable of predicting the linewidth enhancement observed in semiconductor lasers (Henry, 1982). Henry's intuitive description was that for every single spontaneous emission event, the global intracavity laser field experienced a phase and an intensity change. Immediately after, the laser would undergo relaxation oscillations to restore the steady state of emission, inducing delayed phase and amplitude changes. Based on this microscopic description of the spontaneous emission process, Henry derived a set of coupled stochastic differential equations with Langevin noise sources, describing the exchange of energy between carriers and photons, as well as introducing the spontaneous emission effect that was ultimately responsible for the linewidth effect. Using a derivation from (Henry, 1983), we can write a lower-bound on the average-phase diffusion in a semiconductor laser cavity (i.e. how much the phase change per unit time on average) as

$$\langle \Delta\phi(t)^2 \rangle > \frac{R}{2I}(1+\alpha^2)t, \tag{2.1}$$

where R is the spontaneous emission rate, I is the average number of photons inside the laser cavity, and α is the so-called linewidth enhancement factor, a.k.a. Henry's factor. As observed, the average phase diffusion increases linearly with time, is proportional to the spontaneous emission rate, and, most importantly, is inversely proportional to the intensity of the field. Hence, the smaller the number of photons inside the cavity the larger the average phase diffusion for a given time interval.

In coherent optical communications, laser diodes are operated well above the threshold level so that phase noise effects are minimised. In short-reach links, such as in fibre-to-the-home, on-off modulation schemes are more frequent because of the simplified nature of the receiver. In this section, we describe the principle of operation of our quantum random number generation scheme, which is based on an on-off modulation scheme going well below the threshold level in each modulation cycle to

randomise the phase. This combines the use of the gain-switching technique to maximise the phase noise during the off-time of the modulation cycle (very low number of photons inside of the cavity), with the use of coherent communication demodulation techniques to retrieve phase information during the on-time of the modulation cycle (large number of coherent photons). Basically, we combine techniques for short and long reach optical communications for the purpose of random number generation.

2.1.1 Measuring the phase of an optical field

If we let $s(t)$ be the number of photons inside of a laser cavity, $\phi(t)$ be the phase, and ω be the resonant frequency of the laser cavity, we can write the intracavity field as

$$\mathcal{E}(t) = \sqrt{s(t)}\,\mathrm{exp}[-\imath\omega t]\,\mathrm{exp}[\imath\phi(t)], \tag{2.2}$$

In order to detect this electromagnetic signal in the optical domain, we use a photodetector. The measurement reading corresponds to $u(t) \equiv \eta|\mathcal{E}(t)|^2 = \eta\mathcal{E}(t)\mathcal{E}^*(t)$, with * being the complex conjugate and η the transmission coefficient of the laser cavity. Applied to the cavity field, the observed signal would therefore be given by $u(t) = \eta s(t)$. Effectively, we are detecting a fraction of the photons inside the cavity and losing all phase information. For completeness, the average power detected in the interval $[0, T)$ will be given by $\mathcal{P}(t) \equiv \hbar\omega/T \int_0^T dt\ u(t)$, where $\hbar\omega$ is the energy of each photon, $\hbar$ being the reduced Planck constant. In general, if we want to retrieve phase information we have to use an interferometric scheme. In this thesis, we will use two such detection schemes. One is a self-delayed interferometer using an unbalanced Mach-Zehnder configuration and the other is an heterodyne scheme with a local oscillator. In the following, we will formalise the interference process in general as well as its statistical behaviour.

Let $\mathcal{E}_A(t)$ and $\mathcal{E}_B(t)$ be two electromagnetic fields described by Eq. (2.2). The total field after interfering, i.e. combining, the two sources is

given by $\mathcal{E}^{(out)}(t) = \mathcal{E}_A(t) + \mathcal{E}_B(t)$, and the detected intensity by

$$\begin{aligned} u^{(out)}(t) \equiv |\mathcal{E}^{(out)}|^2 &= \Big(\mathcal{E}_A(t) + \mathcal{E}_B(t)\Big)\Big(\mathcal{E}_A(t) + \mathcal{E}_B(t)\Big)^* \\ &= |\mathcal{E}_A(t)|^2 + |\mathcal{E}_B(t)|^2 + 2\mathsf{Re}\{\mathcal{E}_A(t)^*\mathcal{E}_B(t)\} \\ &= u_A(t) + u_B(t) + 2\sqrt{u_A(t)u_B(t)}\cos\Big(\int_0^t d\xi\Delta\Omega(\xi) + \Delta\phi(t)\Big), \end{aligned} \tag{2.3}$$

where $\Delta\Omega(t) \equiv \omega_A(t) - \omega_B(t)$ and $\Delta\phi(t) = \phi_A(t) - \phi_B(t)$. The first two terms correspond to the intensity of the fields travelling the two paths of the interferometer, whereas the last term corresponds to the interference term. Without losing generality, we will now assume that (i) the two fields oscillate at the same frequency, which corresponds to the case of the self-delayed interference scheme, and (ii) the two signals are operated in continuous wave, i.e. constant intensity. As a result, the previous expression can be simplified by eliminating the time dependence of $u_{A,B}$. We can write

$$u^{(out)}(t) = u_A + u_B + 2\sqrt{u_A u_B}\cos\Delta\phi(t), \tag{2.4}$$

in which we can directly associate a change in the phase $\Delta\phi(t)$ to a change in the intensity $u^{(out)}$. Depending on the phase difference between the two fields, constructive and destructive interference is observed, as illustrated in Fig. (2.2) for $u_A = u_B = 1$. Because of the interferometer, a change in the phase is translated into a change in the amplitude. Thus, if $\Delta\phi$ is a random process, for example because of phase noise, then $u^{(out)}$ will be a random process too.

2.1.2 Statistical behaviour: the arcsine distribution

In general, if x is a random variable with density function $P_x(x)$ and y is another random variable given by $y = f(x)$, where f a differentiable function, we can analytically find the density function of y by solving

$$P_y(y) \equiv \sum_k \Big|\frac{\partial}{\partial y} f_k^{-1}(y)\Big| P_x\big(f_k^{-1}(z)\big), \tag{2.5}$$

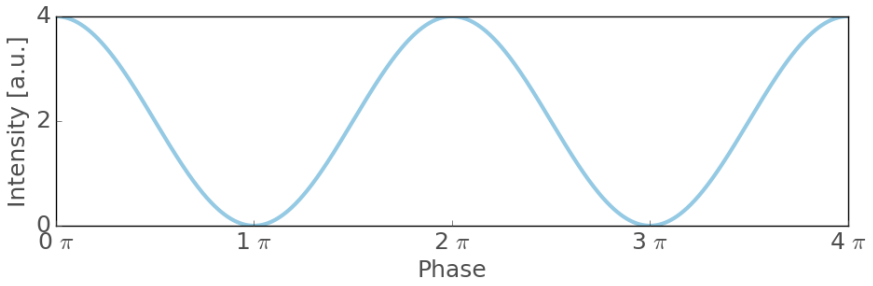


Figure 2.1: Interference intensity values as a function of the phase difference between the two fields. Note that although the input intensities are fixed to 1, the output intensity takes values ranging from 0 up to 4. When the two fields are in phase, i.e. their difference is a multiple of $2\pi k$, constructive interference is observed (maximum intensity), whereas when the phases are shifted by multiples of $\pi(2k-1)$, destructive interference is observed (minimum intensity).

where f_k^{-1} is the k-th root of the equation $y = f(x)$. Using Eq. (2.4), we find in the interference scenario that

$$f_k^{-1} = \arccos \underbrace{\left[\frac{u^{(out)} - u_A - u_B}{2\sqrt{u_A u_B}} \right]}_{\xi} + 2\pi k \tag{2.6}$$

and

$$\frac{\partial f_k^{-1}}{\partial u^{(out)}} = -\frac{1}{2\sqrt{u_A u_B}\sqrt{1-\xi^2}}. \tag{2.7}$$

Let us first start by analysing what the distribution of y is when $\Delta\phi \sim \mathcal{U}\left[-\pi, \pi\right)$ is uniformly distributed in $[-\pi, \pi)$ and $u_{A,B}$ are constant. While this uniform distribution of the phase does not correspond to a phase diffusion process (which is, typically, normally distributed), the distribution of $u^{(out)}$ when the phase uniformly covers the domain of the signal will reveal the distribution of a process in which the phase is totally random. In

this simplified scenario, we can easily find the output distribution by using the fact that (i) the distribution of $z = \cos\Delta\phi$ is described by the arcsine probability distribution function $\mathcal{A}(-1, 1)$, being

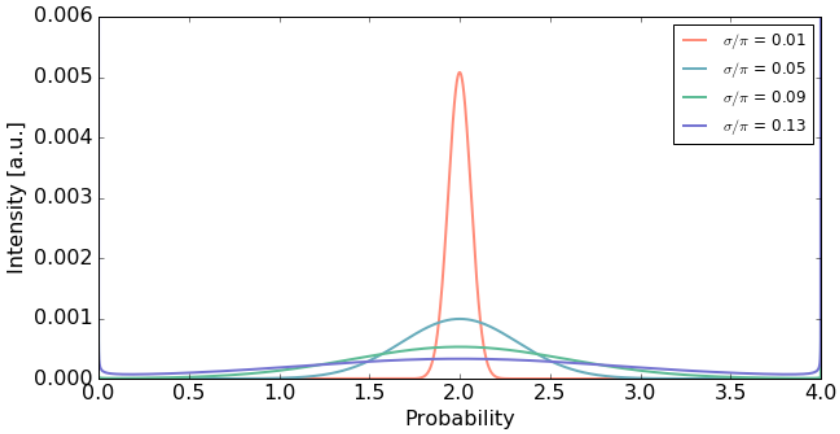
$$\mathcal{A}(a, b) \equiv 1/\pi\sqrt{(b - x)(x - a)}$$

and (ii) the arcsine distribution is closed under translation and scaling by a positive factor, i.e. if $\xi \sim \mathcal{A}\ (a, b)$, then $k\xi + x \sim \mathcal{A}(ak + c, bk + c)$.

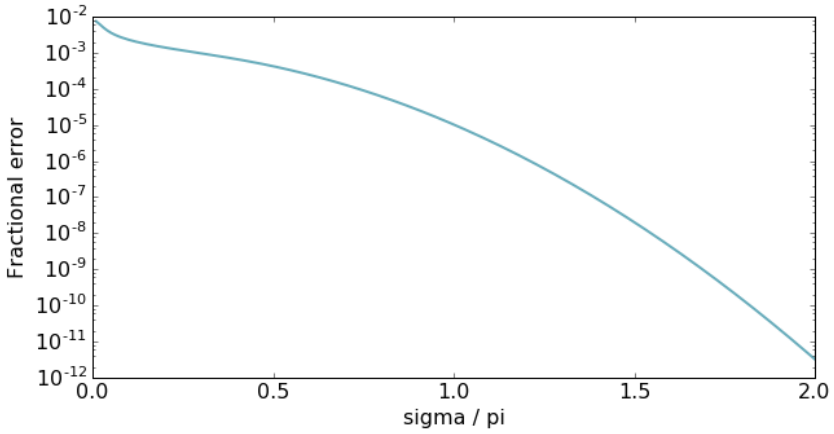
By inspecting Eq. (2.4), we find that the distribution of $u^{(out)}$ is given by the arcsine distribution with transformation parameters $k = 2\sqrt{u_A u_B}$ and $c = u_A + u_B$. Effectively, in the noiseless case, the resulting distribution is an arcsine with parameters (a, b) given by the destructive $u_{\text{min}}^{(out)}$ and constructive $u_{\text{max}}^{(out)}$ interference terms, i.e;

$$P_{u^{(out)}}(x) = \frac{1}{\pi\sqrt{(x - u_{\text{min}}^{(out)})(u_{\text{max}}^{(out)} - x)}} \tag{2.8}$$

For full phase randomisation, the intensity distribution is, therefore, described by the arcsine distribution in Eq. (2.8). Now, let us analyse the physical scenario in which the phase undergoes phase diffusion dynamics, i.e. it is described by Gaussian statistics. As described already in Eq. (2.1), the average phase diffusion increases linearly with time, i.e. $\langle\Delta\phi(t)^2\rangle \propto t$, so in principle, by waiting long enough, an arbitrarily large deviation can be observed. Intuitively, if the distribution of $\Delta\phi$ is sufficiently broad (e.g. infinitely broad), we would expect the phase to be fully randomised, and therefore the intensity distribution would look, exactly, like the distribution in Eq. (2.8), obtained when the phase spreads uniformly in $[-\pi, \pi)$. In the phase diffusion scenario, the phase is distributed according to normal statistics. However due to the modular nature of the cosine, values exceeding $-\pi$ and π wrap back into the domain range. By taking $\Delta\phi \sim \mathcal{N}(0, \sigma)$, and by folding it around the domain $[-\pi, \pi)$, we can compare the mean square error between this new variable and a uniform distribution in the same domain. In Fig. (2.2) we show the fractional error for increasing values of σ. We find that $\sigma > \pi$ has a fractional error $\epsilon < 10^{-5}$, whereas $\sigma > 2\pi$ has a fractional error $\epsilon < 10^{-11}$.



(a) Intensity distribution function



(b) Fractional error

Figure 2.2: Intensity distribution and deviation from full randomisation as a function of the average phase diffusion. (a) Numerically calculated intensity distribution function for several average phase diffusion values. (b) Fractional error between numerically evaluated distribution functions with gaussian phase noise and the ideal and analytically calculated intensity distribution for the uniform scenario. The fractional error is defined as $\epsilon^2 = \langle P_G - P_U \rangle$. We find that for $\sigma > \pi$, the fractional error drops below 10^{-5}. Or in terms of average phase diffusion $\langle \Delta\phi(t)^2 \rangle$, the fractional error is below 10^{-5} for $\langle \Delta\phi(t)^2 \rangle > \pi^2$

2.2 Numerical analysis of the phase diffusion process

The dynamics of semiconductor lasers are described by a set of coupled stochastic differential equations that govern the exchange of energy between charge carriers and the electromagnetic field. In general, if we let $\vec{x}$ be a vector of stochastic variables, we can write a set of coupled differential equations as (Oksendal, 2003)

$$dx_i = g_i(\vec{x}) + \sum_j h_{ij}(\vec{x}) dW_j(t), \tag{2.9}$$

where $g_i(\vec{x})$ represents the drift or deterministic evolution of the i-th stochastic variable, $dW_j(t)$ is a Wiener processes, and h_{ij} is the coefficient describing the correlation between the i-th and j-th random processes. For the laser rate equations we introduce the array of stochastic variables $\vec{x} = \{s, n, \phi\}$, where s and ϕ are the intensity and the phase of the cavity field, respectively, and n is the number of carriers. Following the equations derived by (Agrawal et al., 1988), we write the drift terms as

$$g_s(\vec{x}) = (\tilde{G} - \gamma) \cdot s + R \tag{2.10}$$

$$g_n(\vec{x}) = I/q - \gamma_e n - \tilde{G} s \tag{2.11}$$

$$g_\phi(\vec{x}) = \frac{\alpha}{2}(G_L - \gamma) - \frac{\beta}{2} \frac{G_L \cdot s}{1 + \sqrt{1+p}} \tag{2.12}$$

where γ is the cavity decay rate, $R = R_0 \gamma_e n$ is the spontaneous emission rate, I the electrical current, q is the electron charge, γ_e is the electron decay rate, α is the linewidth enhancement or Henry's factor, β is the chirp parameter or nonlinear phase term and

$$\tilde{G}(\vec{x}) = \frac{G_L}{\sqrt{1+p}} = G_n \frac{n - n_0}{\sqrt{1+p}} \tag{2.13}$$

is the intensity-dependent gain coefficient with saturation term $p = s/s_{sat}$, s_{sat} being the saturation intensity. The noise-correlation matrix $\vec{h} = \vec{D}^{1/2}$ can be calculated by computing the square-root of the diffusion matrix as:

$$\vec{D}(\vec{x}) = \begin{pmatrix} Rs & -Rs & 0 \\ -Rs & Rs + \gamma_e n & 0 \\ 0 & 0 & R/4s \end{pmatrix} \tag{2.14}$$

whose coefficients have been derived from first principles for steady-state operation (Agrawal et al., 1988; Henry, 1983). When an equilibrium is not achieved, however, the exact form of the diffusion matrix is unknown. Nevertheless, these coefficients have been used with satisfactory results even in non-equilibrium problems (Balle et al., 1993a,b, 1991).

Box 1. Method for solving the stochastic rate equations

In order to solve the rate equations numerically, we need, firstly, to derive the coefficients of the h matrix in Eq. (2.9). Since the diffusion matrix $D = hh^{\dagger}$ is symmetric and has a maximum rank for $R \neq 0$, we can calculate the matrix h by applying the transformation $h = Uf(h')U^{\dagger}$, h' being a diagonalised version of h and $f(x) = \sqrt{x}$. By carrying out simple linear algebra manipulations, we find

$$h_{ss}(\vec{x}) = (1+d)F_- - (1-d)F_+ \tag{2.15}$$

$$h_{sn,ns}(\vec{x}) = -2R_0(F_+ - F_-) \tag{2.16}$$

$$h_{nn}(\vec{x}) = (1+d)F_+ - (1-d)F_- \tag{2.17}$$

$$h_{\phi\phi}(\vec{x}) = \sqrt{D_{\phi\phi}} = \sqrt{R/4s}, \tag{2.18}$$

and $h_{s\phi} = h_{\phi s} = h_{n\phi} = h_{\phi n} = 0$, where

(2.19)

$$F_+ = \kappa^{-1}\sqrt{1+2R_0 s+d} \qquad \kappa = 2\sqrt{2}d/\sqrt{n\gamma_e} \tag{2.20}$$

$$F_- = \kappa^{-1}\sqrt{1+2R_0 s-d} \qquad d = \sqrt{1+4R_0^2 s^2} \tag{2.21}$$

In Section 2.2.1, we will use this set of coupled stochastic differential equations to compare the average phase diffusion obtained in continuous wave mode and pulsed mode. We will use the Euler-Maruyama method for solving the above equations. In other words, we calculate iteratively for the n-th step

$$x_i\,[n] = x_i\,[n-1] + dt \cdot g_i\,(\vec{x}\,[n-1]) + \sum_j h_{ij}(\vec{x}\,[n-1])\Delta W_j\,[n], \tag{2.22}$$

where dt is the time step, and $\Delta W_j[n] = W_j[n] - W_j[n-1]$ are independent and identically distributed normal random variables with zero mean and $\sigma = \sqrt{dt}$.

2.2.1 Accelerated phase diffusion process

In this section we will describe the generation of random numbers from the phase diffusion process in a semiconductor laser. The indispensable blocks in the creation of raw random bits are (i) a semiconductor laser undergoing phase diffusion dynamics, (ii) an interferometric scheme to translate phase information into the amplitude domain, (iii) a photodetector to generate an electrical signal proportional to the optical intensity, and (iv) a digitiser taking samples from the photo-detected signal with a sampling rate $f_s \equiv 1/\tau_s$. In the previous section, we found that the average phase diffusion $\langle \Delta\phi(t)^2 \rangle$ increases linearly with time. Also, we discussed the fact that for a sufficiently large $\langle \Delta\phi(t)^2 \rangle$, the intensity distribution after the interference process is practically indistinguishable from a fully randomised phase. By using these two conditions, we can find an upper limit to the sampling rate f_s, being the maximum sampling rate that we can use so that the phase has enough time to diffuse between two subsequent samples. In continuous wave mode, and using Eq. (2.1), we find that the minimum time between samples has to be:

$$\tau_s > \frac{2D_\phi s}{R(1+\alpha^2)}, \tag{2.23}$$

where s is the number of photons inside the cavity, R is the spontaneous emission rate, α is the linewidth enhancement factor, and D_ϕ is a free parameter representing the average phase diffusion value that the experimenter considers gives a sufficiently small fractional error compared to the fully randomised case. For instance, as shown in Fig. (2.2), $D_\phi = \pi^2$ gives a fractional error below 10^{-6}. Clearly, the quantity described in Eq. (2.23) depends only on (i) the laser structure (i.e. R and α) and (ii) the operating power. In this thesis, in order to increase the phase diffusion rate for a given sampling interval τ_s, we use the gain-switching technique, i.e. the generation of optical pulses by switching the laser from well below the threshold level (off-time) to well above the threshold level (on-time). In this way, we can brutally increase the phase diffusion rate during the off-time of the optical pulses, when the number of photons in the cavity is hugely reduced.

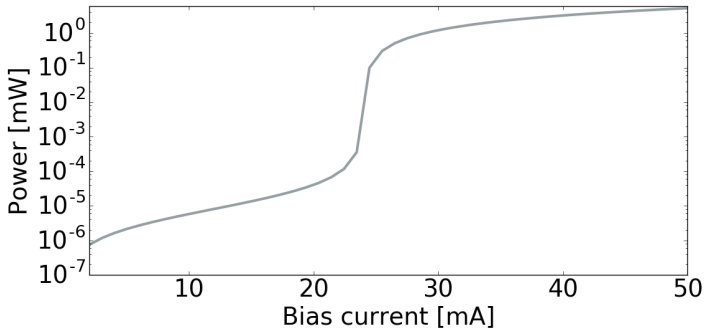


Figure 2.3: Simulation of the number of photons as a function of the bias current for the simulated laser with parameters given in Table 2.1

2.2.2 Average phase diffusion in CW and GS

Parameter	Symbol	Value
Cavity decay rate	γ_o^{-1}	3×10^{11}
Carrier decay rate	γ_e^{-1}	2.5×10^{-9}
Spontaneous emission rate	R_0	0.18×10^{-4}
Gain	G_n	5.4×10^{4}
Linewidth enhancement factor	α	2
Nonlinear phase	β	0
Saturation intensity	s_{sat}	10^{6}
Transparency level	N_0	5.4×10^{7}

Table 2.1: Simulated semiconductor laser parameters. Typical semiconductor laser parameters are chosen (Balle et al., 1993a). The transparency level is calculated as $N_0 = N_{th} - \gamma_o/G_n$, being $N_{th} = I_{th}/q\gamma_e$.

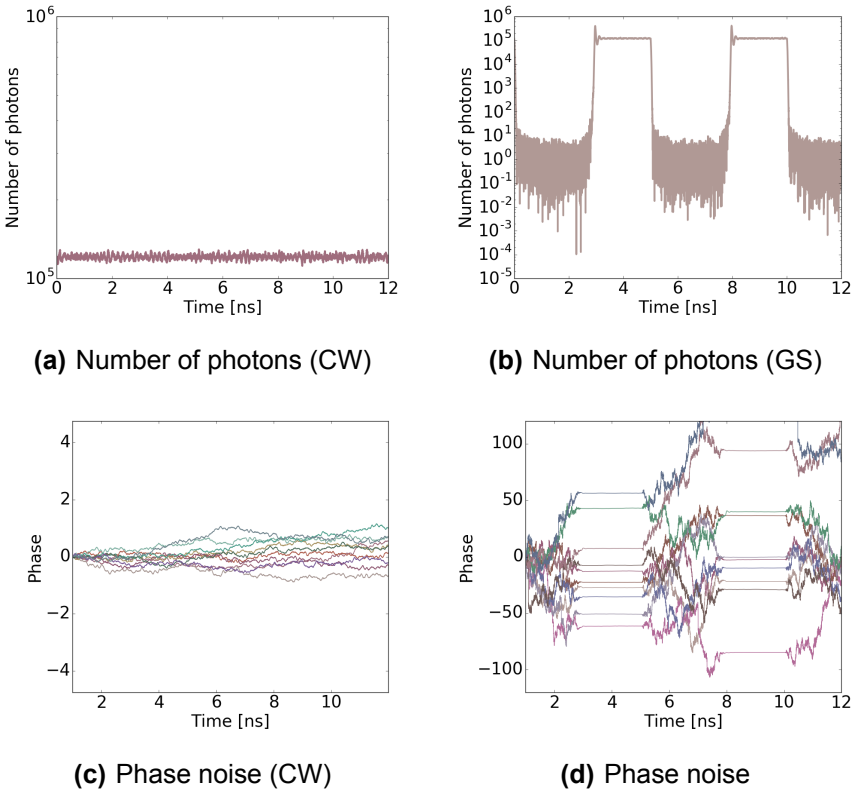
In this subsection, we compare the average phase diffusion enhancement for a given laser and fixed sampling interval in the continuous wave and the gain-switching operation modes. The simulated laser parameters are given in Table 2.1. The laser's threshold level is set at ~ 24 mA - see simulated current-power graph in Fig. (2.3). In the continuous wave case,

the biasing point is set at $I_b = 25$ mA. In the gain-switched case, the biasing point is $I_b = 15$ mA and during the on-time, it increases to 30 mA. In both simulations, the Monte Carlo time step is fixed at $h = 100$ fs. In the gain-switched case, the pulse repetition frequency is set at 200 MHz. The temporal evolution of the intensity and the phase in both operation modes is depicted in Fig. (2.4). Clearly, in the continuous wave scenario, a moderate phase noise is observed, whereas in the gain-switching case, a very rapid (moderate) phase diffusion rate is experienced during the off-(on-)time of the modulation.

From the solution of the phase from the stochastic rate equations, we can easily calculate the average phase diffusion as a function of time by evaluating the standard deviation of the phase noise at different times. In theory, the average phase diffusion is described by a normal distribution with a variance $\langle \Delta\phi(t)^2 \rangle$ increasing linearly in time, or equivalently, with a standard deviation growing as $\sqrt{t}$. In the simulation, we perform $N = 100$ Monte Carlo steps, obtaining N phase traces $\phi_i(t)$. For each trace, we first subtract the ordinary solution $\phi^{(ord)}(t)$ (i.e. the deterministic part), keeping the phase noise component only, namely, $\phi_i'(t) = \phi(t)_i - \phi^{(ord)}$. Then, by calculating the standard deviation at different times, we obtain $\sigma_\Delta(t) = \sqrt{\langle \Delta\phi(t)^2 \rangle}$. In Fig. (2.5), we show the results for the gain-switched scenario simulated above, as well as the solution for two continuous wave cases, one with a biasing point near threshold $I_b = 25$ mA and the other for $I_b = 30$ mA. The standard deviation in the gain-switched case is around 60 and 135 times larger when compared to the continuous wave results, which corresponds to a $3500-$ and 18000-fold increase in the phase diffusion rate, respectively.

2.3 Ultrafast quantum random number generation experiment

In the previous section we described the accelerated phase diffusion mechanism for random number generation. In this section, we show the results of an ultrafast experiment implementing the pulsed scheme in a self-delay configuration with an unbalanced Mach-Zehnder interferometer. A preliminary version of the experiment and data analysis was presented in



(a) Number of photons (CW)

(b) Number of photons (GS)

(c) Phase noise (CW)

(d) Phase noise

Figure 2.4: Solution of the stochastic rate equations in continuous wave (CW) and gain-switching (GS) modes. (a-b) Calculated number of photons for CW (a) and GS (b). (c-d) Phase noise, obtained by subtracting the ordinary solution from the stochastic solution for CW (c) and GS (d). Note that the vertical scale for the GS case is almost two orders of magnitude larger than for the CW case.

(Abellan, 2013). The main novelty presented in this section is the estimation of the average phase diffusion. The experiment and results are described here again for completeness. An off-the-shelf 10 Gb/s distributed-feedback (DFB) semiconductor laser was biased with a constant current of 15 mA and directly modulated with a 5.825 GHz radio frequency (RF)

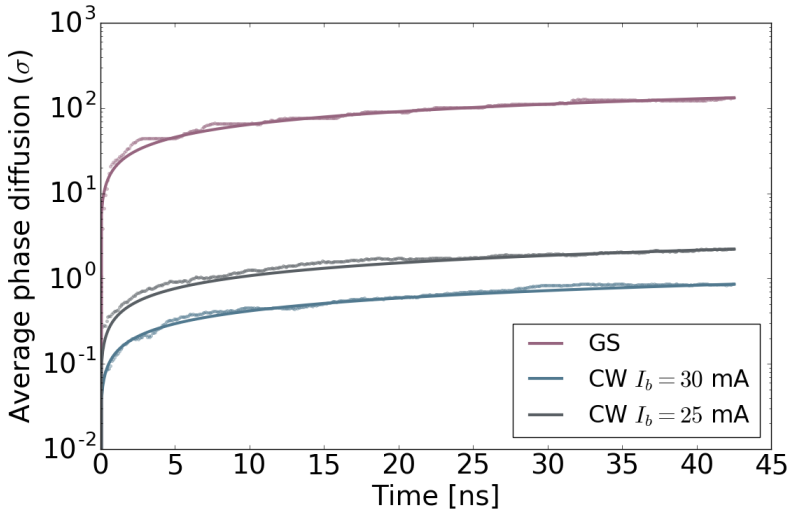


Figure 2.5: Average-phase diffusion for a simulated laser operating in gain-switching and continuous wave modes. The standard deviation in the gain-switched case is ~ 60 and ~ 135 times larger than the continuous wave result for $I_b = 25$ mA and for the $I_b = 30$ mA, respectively, corresponding to a 3500- and 18000-fold increase in the phase diffusion rate, respectively.

electrical signal. In Fig. (2.6), we show the electrical signal as recorded by a 20 GHz and 80 GSa/s digital oscilloscope. Since the RF signal brings the laser from below to above the threshold level in each cycle, the diode experiences two completely different regimes. Firstly, for ~ 40% of the time, the diode goes below the threshold level and undergoes strong phase diffusion dynamics. Then, it goes well above the threshold level, generating a coherent optical pulse and reaching the saturation intensity. The resulting optical output, also shown in Fig. (2.6), consists of ~ 85 ps optical pulses with a peak power of ~ 7.65 mW. To avoid back reflections into the laser cavity, the DFB incorporates a 30 dB internal optical isolator.

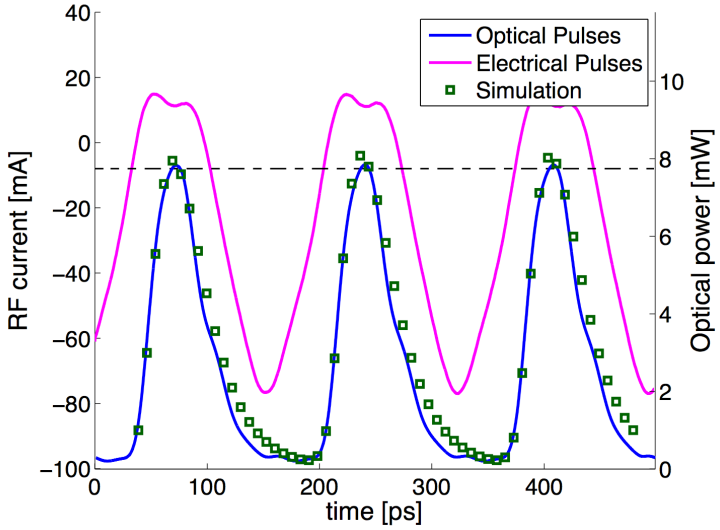


Figure 2.6: Electrical and optical pulse trains. Magenta, (upper trace): electrical current drive applied to the laser, with a period of 172 ps. Blue, (lower trace): photo-detected optical pulses of 85 ps time width and 7.65 mW peak power and (black, dashed line) 9 mA LD current threshold. Simulation (green squares) is a conservative fitting of the rate equations such that the predicted detected output power vs. time is always larger than the observed output power vs. time.

2.3.1 Estimating the average phase diffusion

As a result of the gain-switching modulation process, a string of optical pulses with nearly identical waveform and randomised phases is generated. To estimate the average phase diffusion between subsequent optical pulses we fit the solution of the ordinary rate equations Eqs (2.10-2.11) to the observed optical signal. In order to do this, we first need to estimate the following unknown parameters from the laser: the saturation intensity s_{sat}, the cavity length L that goes into calculating the cavity losses, the number of carriers at threshold n_{th}, the gain G_N, the transparency level n_0 and the rate of spontaneous emission R_0. In addition, since the optical

signal is detected by limited bandwidth components, the oscilloscope being the most limiting component $B_{osc} = 12.5$ GHz, we low pass filter the solution of the rate equations with a single-pole recursive filter with time constant $\tau_f = 0.35/B_{osc}$. The following recursive method is employed:

1. We set s_{sat} to a *typical* value, and L to either 100, 200, 500, $1000\ \mu m$.
2. We solve the steady state solution of Eqs (2.10-2.11) for the number of photons and carriers near the threshold level, i.e. with $n \sim n_{th}$, which read:
$$0 = \gamma\Big(\frac{1}{\sqrt{1+p_{th}}} - 1\Big)s_{th} + R_0\gamma_e n_{th} \tag{2.24}$$
$$0 = I_{th}/q - \gamma_e n_{th} - \frac{\gamma s_{th}}{\sqrt{1+p_{th}}}, \tag{2.25}$$
where the subscript $_{th}$ refers to the *threshold* value, and $p_{th} \equiv s_{th}/s_{sat}$. By using the fact that the laser emits 0.3 mW when it is biased with $I = 10$ mA, from the solution of this equations we find n_{th} and R_0.
3. We choose G_N, which mainly controls the speed dynamics, such that the calculated detected power vs. time is always larger than the observed output power vs. time. In this way, the calculation is conservative since the larger the power, the slower the phase diffusion will be. By setting G_N, we immediately define n_0 via $G_N = \gamma/(n_{th} - n_0)$.
4. We repeat steps 1-3 to find the values of s_{sat} and L that minimised the root-mean-square deviation of the calculated solution and the observed signal.

Following this iterative procedure, we find $s_{sat} = 7.7\times10^5$, $L = 500\,\mu$m, $n_{th} = 5.62 \times 10^7$, $R_0 = 8.8 \times 10^{-4}$, $G_N = 2.3 \times 10^4$, and $n_0 = 3.46 \times 10^7$. The calculated solution is depicted in Fig. (2.6). By using the linear bound from Eq. (2.1) in differential format

$$\frac{d}{dt}\langle\Delta\phi(t)^2\rangle = \frac{R}{2s}(1+\alpha^2), \tag{2.26}$$

and numerically integrating this with the values estimated above, we find an average phase diffusion $\langle\Delta\phi(\tau_s)^2\rangle > (9.45\ \text{rad})^2$, where $\tau_s = 1/5.825$ GHz ≈ 172 ps, which, for all practical pulses, randomise the phase.

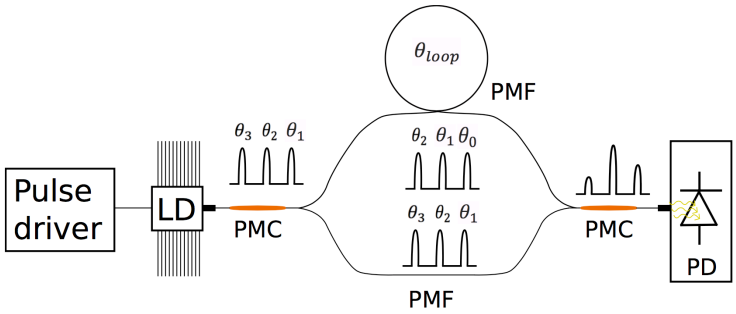


Figure 2.7: Unbalanced Mach-Zehnder interferometer (U-MZI). Phase-randomised coherent optical pulses interfering at the output of the U-MZI produce random intensities. (Pulse driver) denotes the electrical pulse generator that directly modulates the laser, (LD) is the laser diode, (PMC) is the polarisation maintaining coupler, (PMF) are the polarisation maintaining fibres, (θ_{0-3}) are optical phases of different consecutive pulses, (θ_{loop}) is the phase introduced by the delay line and (PD) is a fast photodetector.

2.3.2 Measurements and statistical characterisation

Once a phase-randomised string of optical pulses is produced, the next step in the generation of random numbers is to translate phase information into the amplitude domain. An unbalanced Mach-Zehnder interferometer (uMZI) is used for this task. As illustrated in Fig. (2.7), the uMZI first splits the signal into two paths. Then, a phase delay θ_{loop} is introduced into one of the two arms by means of a fibre delay line, and then the two fields are recombined at the output. In our case, θ_{loop} is selected so that the pulse travelling the long path of the interferometer is delayed by one period of the modulation signal, effectively achieving at the output of the interferometer an interference between the i-th and the $(i-1)$-th pulses at the output of the interferometer. The uMZI is a self-delayed interferometer, and, therefore, when the interference occurs between the fields coming from the two arms, the instantaneous frequency of the two interfering beams is nearly the same. In a period of ~ 172 ps, which corresponds to the path time difference between the two arms of our interferometer, we measure

phase variations caused by the stretching of the fibres and laser drifts below 2×10^{-7} root-mean-square, negligible compared to the quantum fluctuations described above. As a result, following on from Eq. (2.3), we can apply the simplification $\omega_1 = \omega_2$, with $\omega_{1,2}$ being the instantaneous frequency of the fields in each path, and write the output intensity as

$$u^{(out)}(t) = u_A(t)+u_B(t)+2|g^{(1)}(t)|\sqrt{u_A(t)u_B(t)}\cos\Delta\phi(t)+u_n(t), \quad (2.27)$$

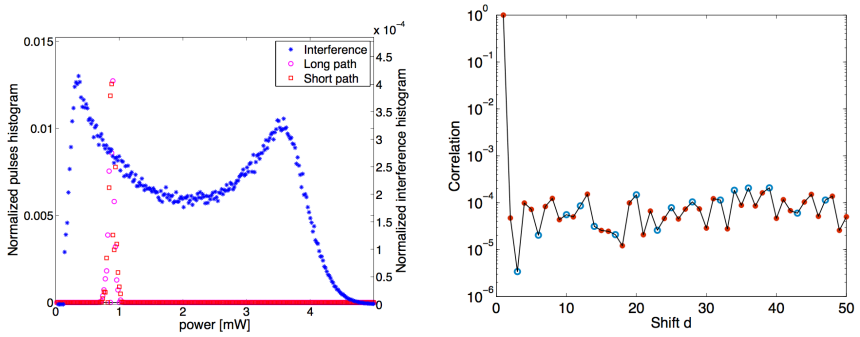
where we introduce the visibility or first-order coherence function $g^{(1)}(t)$ and the term $u_n(t)$, which represents electronic noise as well as other additive noises.

A fast, 14-bit sampling oscilloscope is used to acquire data. For each pulse, a single sample is taken 13 ps after the pulse peak. This delay is chosen in order to let the laser frequency stabilise. During the build-up of the cavity field, a large variation on the instantaneous frequency occurs (Balle et al., 1991). As a result, either no interference or bad visibility is observed during this time. Once this transient period damps out, the instantaneous frequency stabilises and high visibility is observed. Experimentally, we found that 13 ps maximised the width of the observed distribution. In total, 120×10^6 pulses were recorded for data analysis. We took data over the course of 5 days, and high stability was observed. To analyse the visibility of the interference process, we first measured the distribution of the pulses travelling the two paths of the interferometer, obtaining mean values of 0.97 mW and 0.9 mW and a standard deviation of 45 μW. These fluctuations arise from background noise and intensity noise in the laser, and produce narrow density functions, as shown in Fig. (2.8a). In contrast, due the interference between optical pulses with similar intensities and random phases, a broad distribution following an arcsine density pattern is detected at the output.

In Fig. (2.8(b)) we show the autocorrelation Γ for the $n = 120 \times 10^6$ dataset measured above. We estimate the autocorrelation with the unbiased estimator

$$\Gamma_x(d) = \frac{1}{n-d}\sum_{i}^{n-d} x_i x_{i+d} - \mu_x^2 \quad (2.28)$$

where μ_x is the mean of the input data. This form of the unbiased correlation estimator is valid for small correlation distances and large sample



(a) Histogram **(b)** Autocorrelation

Figure 2.8: Statistical characterisation of the raw data. (a) Input power distributions (left y-axis) and the resultant output power distribution (right y-axis). The visibility achieved for the interferometer is 0.9. The power distribution has clearly widened due to the random phase generated by amplified spontaneous emission (ASE). (b) Normalised correlation of 50 subsequent sampled pulses. The autocorrelation has been evaluated with 120×10^6 14-bit samples. As expected, it follows a delta-function like behaviour indicating the random nature of the process.

sizes, i.e. $d \ll n$. The low correlation values for $d > 0$ indicate the random nature of the process.

2.3.3 Entropy estimation and randomness extraction

In the process of generating raw random bits, the digitised signal contains information about the physical process that we trust (accelerated phase diffusion, in our case) as well as other noise contributions from processes such as electronic noise, electromagnetic interference and thermal fluctuations, among others. All of these noise sources will introduce fluctuations that might look random, but, since they probably do not come from a quantum phenomenon, we cannot trust them. To eliminate these contributions as well as to obtain a uniform output distribution, a randomness extractor (RE) is used. As described in the Chapter 1, in order to apply

a randomness extractor we first need to quantify the min-entropy H_∞ of our source. In this experiment, we quantify the min-entropy using second order statistics of the observed distributions. By computing the variance of the two sides of Eq. (2.27) and assuming independence between the four terms that compose the right-hand side, we can estimate the visibility as

$$|g^{(1)}(t_{loop})|^2 = \frac{\mathrm{var}(u^{(out)}) - \mathrm{var}(u_A) - \mathrm{var}(u_B) - \mathrm{var}(u_n)}{2E[\sqrt{u_A}]^2 E[\sqrt{u_B}]^2}. \tag{2.29}$$

In the experiment we find $\mathrm{var}(u^{(out)}) = 1.4$ mW^2, $\mathrm{var}(u_A) = 2.0 \times 10^{-3}$ mW^2, $\mathrm{var}(u_B) = 2.1 \times 10^{-3}$ mW^2, $E[u_A] = 0.97$ mW, and $E[u_B] = 0.90$ mW, and we find $E[\sqrt{u_A}] = 0.98$ and $E[\sqrt{u_B}] = 0.95$ numerically. From measurements with the laser off, we find the contribution of detection and digitisation noise $\mathrm{var}(u_n) = 1.45 \times 10^{-4}$ mW^2. Substituting in Eq. (2.29), we obtain $|g^{(1)}(t_{loop})| \approx 0.89$.

Box 2. Deriving Equation 2.29

If we assume independence between the three terms in Eq. (2.27) and take the variance, we can write

$$\mathrm{var}(u^{(out)}) = \mathrm{var}(u_A) + \mathrm{var}(u_B) + 4|g^{(1)}(t_{loop})|^2 \mathrm{var}(\sqrt{u_A u_B}\cos\Delta\phi) + \mathrm{var}(u_n). \tag{2.30}$$

Using the independence assumption, we can easily calculate the variance of the third term. In general, the variance of the product of n independent random variables ξ_i is given by

$$\begin{aligned}\mathrm{var}\Big(\prod_{i=1}^{n}\xi_i\Big) &= \prod_{i=1}^{n} E[\xi_i^2] - \prod_{i=1}^{n} E[\xi_i]^2 \\ &= \prod_{i=1}^{n}\left(\mathrm{var}(\xi_i) + E[\xi_i]^2\right) - \prod_{i=1}^{n} E[\xi_i]^2\end{aligned} \tag{2.31}$$

where the operator $E[\xi_i]$ represents the expected value of ξ_i. To simplify this equation, we will neglect the terms $\mathrm{var}(u_A)$ and $\mathrm{var}(u_B)$, since they are almost 3 orders of magnitude smaller than the corresponding mean values.

Substituting in Eq. (2.31), we find

$$\begin{aligned}\mathrm{var}(\sqrt{u_A u_B}\cos\Delta\phi) &= E[\sqrt{u_A}]^2 E[\sqrt{u_B}]^2\big(\mathrm{var}(\cos\Delta\phi) - E[\cos\Delta\phi]\big) \\ &\quad - E[\sqrt{u_A}]^2 E[\sqrt{u_B}]^2 E[\cos\Delta\phi] \\ &= E[\sqrt{u_A}]^2 E[\sqrt{u_B}]^2 \mathrm{var}(\cos\Delta\phi) \end{aligned} \tag{2.32}$$

Then, since $\langle\Delta\phi\rangle^2 > (9.45\,\mathrm{rad})^2$, the distribution of $\cos\Delta\phi$ is nearly equal to the arcsine distribution - see Fig. (2.2). We can use the analytical results that the mean and variance of an arcsine distribution $\mathcal{A}(a,b)$ are given by

$$E[\mathcal{A}(a,b)] = \frac{1}{2}(a+b) \tag{2.33}$$

$$\mathrm{var}\Big(\mathcal{A}(a,b)\Big) = \frac{1}{8}(b-a)^2 \tag{2.34}$$

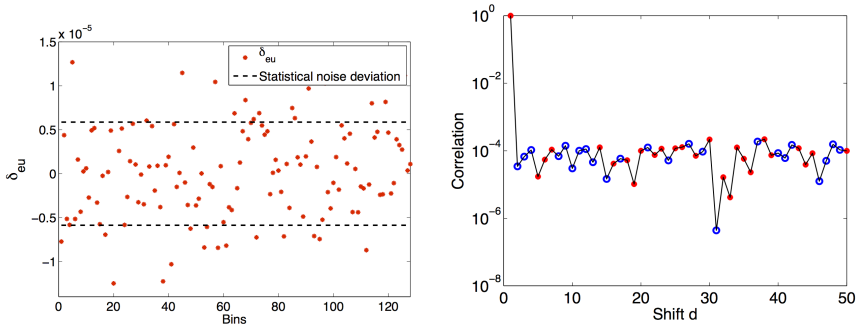
and for the distribution $\cos\Delta\phi$, which is an arcsine with extreme values $a=-1$ and $b=1$ we get $E[\cos\Delta\phi] =$ and $\mathrm{var}(\cos\Delta\phi) = 1/2$. Replacing these results in Eq. (2.32) and rearranging the terms in Eq. (2.30), we can write the visibility as

$$|g^{(1)}(t_{loop})|^2 = \frac{\mathrm{var}(u^{(out)}) - \mathrm{var}(u_A) - \mathrm{var}(u_B) - \mathrm{var}(u_n)}{2E[\sqrt{u_A}]^2 E[\sqrt{u_B}]^2} \tag{2.35}$$

In a noiseless scenario, and as shown in Eq. (2.8), the density function of $u^{(out)}$ is described by an arcsine with parameters $u_\pm = E[u_A + u_B \pm 2|g^{(1)}(t_{loop})|^2]$. We calculate the min-entropy using

$$H_\infty \approx \frac{b}{2} - \frac{1}{2}\log_2\Big(\frac{4\Delta_{\mathrm{ADC}}}{\pi^2(u_+ - u_-)}\Big), \tag{2.36}$$

where Δ_{ADC} is the range of the scope's digitiser and b the resolution. In the units of optical power, we measure in the experiment $\Delta_{\mathrm{ADC}} = 5$ mW, $b = 14$ bits, and $u_+ - u_- = 4|g^{(1)}(t_{loop})|^2 E[\sqrt{u_A u_B}] = 2.99$ mW, finding $H_\infty = 7.28$ bits. Thus, since the repetition rate of the DFB laser was $f_c = 5.825$ GHz, a real time randomness generation rate of up to $R = f_c \times H_\infty \approx 42.41$ Gb/s could be achieved if real time extraction at this speed were possible. In practice, however, performing randomness extraction at such high speed is hard. In the experiment, we implemented an offline randomness extractor based on the Whirlpool hash function (Jofre



(a) Histogram **(b)** Autocorrelation

Figure 2.9: Statistical characterisation of the post-processed data. (a) Deviation from the ideal 7-bit uniform distribution. Dashed lines show plus/minus 1σ expected variation. (b) Normalised autocorrelation of the hashed data. The correlation coefficients for $d > 0$ are at the -40 dB level, corresponding to the expected statistical variation at this sample size.

et al., 2011). We applied a compression factor of $b/H_\infty \approx 1.93$, reducing the initial 120×10^6 14-bit numbers to $\sim 125 \times 10^6$ 7-bit numbers. In Fig. (2.9) we show the deviation of the hashed data with the ideal 7-bit uniform distribution and the autocorrelation. At the output of the hash function, the data is uniformly distributed and uncorrelated.

Box 3. Deriving Equation 2.36

In general, the min-entropy H_∞ of a weak entropy source is given by

$$H_\infty(x) \equiv -\log_2\left(\max_{\forall x_k} P_x(x_k)\right), \tag{2.37}$$

where $\max_{\forall x_k} P_x(x_k)$ is defined as the predictability $\mathcal{P}$ of the source. Using the facts that (i) our distribution is nearly equal to an arcsine, and (ii) an arcsine density function is peaked at the extremes $u_\pm$, we can estimate an

upper bound on the predictability of the source by calculating

$$\mathcal{P}_{u^{(out)}} < \frac{1}{\pi}\int_{u_-}^{u_-+\Delta} d\xi \frac{1}{\sqrt{(\xi-u_-)(u_+-\xi)}} = \frac{2}{\pi}\arcsin\sqrt{\frac{\Delta}{u_+-u_-}},$$

where $\Delta = \Delta_{\text{ADC}}/2^b$, Δ_{ADC} is the range of the digitiser and b is the resolution. With the predictability estimated, we can immediately derive the min-entropy as $H_\infty \equiv -\log_2 \mathcal{P}_{u^{(out)}}$, finding

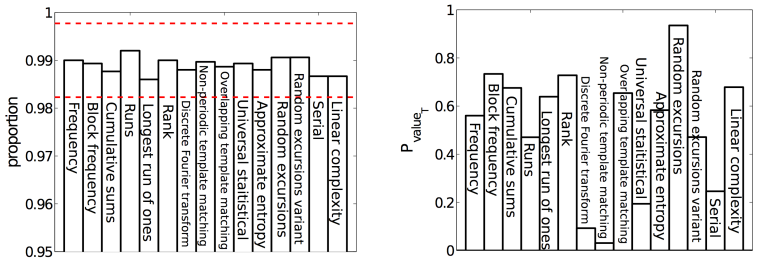
$$H_\infty = -\log_2 \frac{2}{\pi}\arcsin\sqrt{\frac{\Delta}{u_+-u_-}} \approx -\log_2 \frac{2}{\pi}\sqrt{\frac{\Delta}{u_+-u_-}},$$

where we used that $\arcsin x \approx x$ for x small. Rearranging terms, we can find a conveniently closed form given by

$$H_\infty \approx \frac{b}{2} - \frac{1}{2}\log_2\left(\frac{4\Delta_{\text{ADC}}}{\pi^2(u_+-u_-)}\right).$$

2.3.4 Statistical testing

In this experiment, we used the 15-test battery proposed by NIST, which is applied on the hashed data to assess its randomness. The significance level (α_{SL}) is set at 0.01, meaning that one in every hundred sequences is expected to be rejected even if it is produced by a fair random generator. In order to evaluate the results of the tests, two statistics are calculated. Firstly, the ratio of accepted to rejected sequences, which must fall within the confidence interval defined by $1-\alpha_{SL} \pm 3\sqrt{(1-\alpha_{SL})\alpha_{SL}/m}$, where $m = 1500$ is the number of 1 Mbit sequences tested, see Fig. (2.10(a)). It's worth emphasising that the NIST battery of tests requires at least 1 Gbit of data. Here, we used 1.5 Gbits. Second, the ϵ-uniformity of the p-values is examined. The idea is to compute p-value$_T$, a 'P-value of P-values'. The procedure is as follows: for each test, (i) calculate a 10-bit histogram of the obtained p-values, (ii) compute the $\chi^2 = s/10\sum_{i=1}^{10}(F_i - s/10)^2$, being s the number of p-values per test and F_i the number of p-values in the i-th bin, and (iii) calculate the incomplete gamma function $\Gamma(9/2, \chi^2/2)$, which must be larger than 10^{-4}, see Fig. (2.10(b)).



(a) Proportion test **(b)** p-value test

Figure 2.10: Summary of the results of the NIST test suite to assess randomness. (a) Proportion test. Red dashed lines represent the confidence interval in which the proportion of accepted/rejected sequences per test must fall. (b) P-value test. We plot the p-value$_T = \Gamma(9/2, \chi^2/2)$ for each test. All p-value$_T > 10^{-4}$. The smallest coefficient is obtained for the non-periodic template matching test, giving a value of p-value$_T = 0.0926$.

2.4 Randomness metrology

One of most intriguing aspects in randomness and random bit generation is that randomness *per se* cannot be tested. Still, batteries of statistical tests are carried out on a daily basis as well as in regulatory frameworks to test the quality of random number generators (L'Ecuyer et al., 2007). These tests are useful to detect patterns and defects in certain processes, but unfortunately that is all they can do. For fundamental reasons, statistical tests cannot confirm randomness of finite sequences. Passing statistical tests is a necessary condition for randomness claims, but it is not a sufficient one. This is because firstly, only finite strings of digits are tested, and secondly, only a limited number of statistical anomalies are tested for. In order to detect predictabilities on any scale, we need new tools, and physics provides us with such tools.

Quantum mechanics tells us that some physical events are completely unpredictable from first principles, and therefore, that by measuring them, we can extract truly unpredictable bits. However, from the ideal quantum

mechanical realisation of the process until its conversion into the digital domain, several untrusted physical mechanisms are involved, which corrupt the quality of the original signal, opening the door for potential predictabilities in the produced bitstream. New schemes based on Bell inequality violations (BIV) allow for so-called device-independent randomness generation protocols (Pironio et al., 2010) as well as self-testing randomness generation schemes (Lunghi et al., 2015; Vallone et al., 2014). At different confidence levels, both methods allow for the derivation of unpredictability bounds based only on the laws of quantum mechanics and the non-local behaviour of certain quantum states. These schemes are interesting because of the fact that no characterisation of the hardware is required. However, they typically require (i) seed input randomness to select the measurement settings, and (ii) entanglement-based technologies as building blocks. The seed input randomness requires, in turn, randomness validation, which cannot be provided by using the same methods (similarly to the chicken and egg problem). Additionally, the requirement for loophole-free entanglement-based technologies poses performance limitations for today's communication systems.

In this section we introduce the randomness metrology methodology (Mitchell et al., 2015), which, in terms of confidence levels, sits somewhere between the naïve statistical testing approach, and the extreme paranoia of the device-independent approach. The randomness metrology methodology is based on the understanding and modelling of the statistical behaviour of a trusted entropy source, and a thorough characterisation of the hardware components that convert the pure physical process into strings of zeros and ones. As detailed in Chapter 1, by rigorously placing bounds on the unpredictability of a physical random number generator, randomness extractors (Shaltiel, 2002) can then be used to convert the corrupted raw data into fully unpredictable random bits (Frauchiger et al., 2013).

2.4.1 Untrusted noises and *min*-entropy estimation

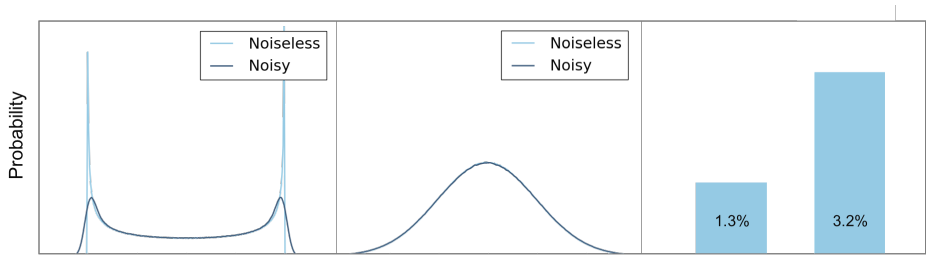
The presence of untrusted noise in real devices leads to smoothed distribution functions, which in general, may lead to overestimated *min*-entropy values. The simplest example is the presence of an additive normally

distributed noise, e.g. electronic noise. If we let $y = x + n$ be the observed signal, x being the process that we want to measure and n an additive Gaussian noise, the observed probability distribution function of y is given by $P_y \equiv P_x * P_n$, where $*$ is the convolution operator. If, for simplicity, we assume that P_x and P_n are both normally distributed with parameters μ_x, μ_n, σ_x and σ_n, it is well known that the resulting distribution function will be normally distributed also, with parameters $\mu_y = \mu_x + \mu_n$ and $\sigma_y^2 = \sigma_x^2 + \sigma_n^2$. Clearly, since the deviation is larger around the mean, the distribution spreads over a larger range, and, therefore, the maximum value of the new distribution is lower than the original distribution, i.e. $P_y(\mu_y) < P_x(\mu_x)$. As a result, when computing the min-entropy H_∞ on this distribution (see Chapter 1 for an introduction on the min-entropy), defined as:

$$H_\infty(X) \equiv -\log_2 \max_{X_i} P(X_i), \tag{2.38}$$

we find that, since max P_y is smaller than max P_x, the min-entropy $H_\infty(y)$ is larger than $H_\infty(x)$. In other words, the estimated min-entropy is larger than the entropy originally available in the trusted process. This smoothing effect is depicted in Fig. (2.11) for a Gaussian additive noise and two input distributions for the trusted process, an arcsine distribution and a Gaussian distribution. The smoothing effect is clearly visible in the arcsine scenario, whereas it remains visually negligible in the Gaussian case. However, when we move into the digital domain, i.e. we digitise the input analogue signal, this situation changes. We calculate the number of digitisation errors made, finding that fewer errors are made in the arcsine case. We define a digitisation error as an output bit that does not correspond to what was expected for a given input value. In Fig. (2.11c) we show the number of digitisation errors made in the arcsine and Gaussian cases due to the presence of untrusted noises when using a 1-bit digitisation scheme. Remarkably, the fact that the arcsine is peaked at the extremes, far from the mean value where the comparison threshold is placed, leads to a smaller number of mistakes in the analogue-to-digital conversion process. In contrast, in the Gaussian scenario, where the signal is peaked at the mean value, the number of mistakes is larger.

The challenge in entropy estimation for random number generators is to quantify and measure all these untrusted effects and derive rigor-



(a) Arcsine scenario **(b)** Gaussian scenario **(c)** Digitisation errors

Figure 2.11: Effect of an additive noise on the observed distribution for an arcsine distribution (left) and a Gaussian distribution (centre). The smoothing effect on the arcsine distribution is clearly seen, whereas the effect on the Gaussian can be barely appreciated. However, when taking the arcsine and Gaussian random signals into an analogue-to-digital process, and quantifying the difference between the digitised signal in the presence of noise and in the noiseless scenario, the Gaussian distribution suffers from more errors than the arcsine case. This is intuitive, since the Gaussian is peaked at the centre (i.e. values around the mean occur more frequently) whereas the arcsine is peaked at the extremes. As a result, when placing a comparator at the mean value of the signal to convert the analogue domain into the digital domain, the arcsine is more insensitive to the noise, since a smaller number of events happen around the mean value.

ous bounds on the available min-entropy, avoiding all smoothing effects that may lead to undesired overestimations. Unfortunately, this process is challenging. First, we cannot measure the trusted signal alone - it is always affected by the noises. Second, if multiple untrusted noises are present, it might be hard to measure them independently and to assess their joint probability distribution function.

2.4.2 Digitisation noise on the min-entropy estimation

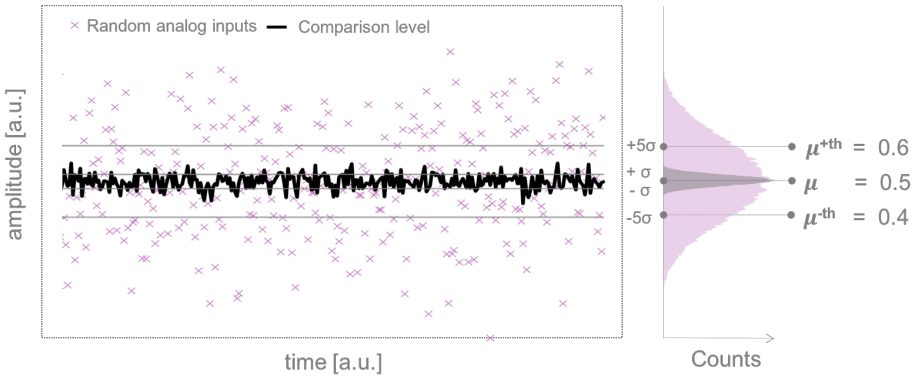
The analogue-to-digital (A/D) conversion process is a significant source of errors and predictabilities when building a random number generator (Mitchell et al., 2015). A/D converters are a fundamental element of any information system, and act as a bridge between the physical quantity and the observation that we make. An A/D converter takes an input analogue signal, and converts it to one of the 2^b possible output values, b being the resolution of the A/D conversion. In the following section, we will describe a simple situation that illustrates the limitations of the A/D conversion process in a 1-bit resolution A/D system, and then we will introduce a generalisation to a multiple-bit A/D converter.

Toy example: digitisation effects on random bit generation

To illustrate the limitations of the A/D conversion process in the entropy estimation problem, let us consider the simple example depicted in Fig. (2.12). A normally distributed analogue random signal $x(t)$ (purple crosses) is digitised using a 1-bit resolution A/D system (a comparator), which has a noisy reference voltage level $\mu(t)$ (black line). The digital value d_i obtained at time i is given by

$$d_i = \begin{cases} 0 & \text{if } x(t_i) < \mu(t_i) \\ 1 & \text{if } x(t_i) \geq \mu(t_i) \end{cases} \tag{2.39}$$

In a noiseless scenario, a given input analogue value is always converted to the same output digital value. However, in a real system, the comparison level $\mu(t)$ fluctuates in time, and, as a result, the same input analogue value can be converted into different outputs depending on the instantaneous value of the reference voltage. Unfortunately, due to the fact that the distribution function of the analogue signal and the comparison level are symmetric, the errors made in the conversion process average out, leading to the naive observation that $P(0) = P(1) = 1/2$. If we limit ourselves to measuring this output distribution without considering the fluctuations in the reference voltage, the min-entropy that we find is $H_\infty = -\log_2 \max\{P(0), P(1)\} = -\log_2 1/2 = 1$. Therefore, we conclude that the source is totally unpredictable. However, if we inspect



(a) Time trace **(b)** Histogram

Figure 2.12: Simple description of the effect of A/D noise on the randomness analysis with a 1-bit resolution A/D conversion. (a) Simulated analogue stochastic process (purple) and a noisy comparison level for the reference level (black). As observed, due to the fluctuations in the comparison level, a given input value might be converted to different output digital values depending on the instantaneous strength of this signal. (b) Probability distribution function for the analogue input signal and the comparison noise level. The signal levels μ and $\mu^{\pm th}$ are used as boundary thresholds in the randomness analysis presented in this section.

the comparison noise signal and the analogue signal, we immediately observe that many input values have been mistakenly converted due to the instantaneous value of the reference voltage - see Fig. (2.11).

In order to include the effect of the instantaneous fluctuations of the A/D noise, we propose the following methodology. First, we need to measure and statistically characterise the comparison reference noisy signal. Then, using the distribution function of the trusted signal (obtained from first principles), we derive upper bounds $\bar{P}$ on the probability of every symbol as follows:

$$\bar{P}(d=0) \equiv P(x < \mu^{+th}) - P(x < -\infty) \equiv F_x(\mu^+) - 0 \tag{2.40}$$

$$\bar{P}(d=1) \equiv P(x < \infty) - P(x < \mu^{-th}) \equiv 1 - F_x(\mu^-), \tag{2.41}$$

where F_x is the cumulative distribution function of the trusted signal $x(t)$, μ^{+th} is the maximum input value that can give rise to a 0 output value, and μ^{-th} is the minimum input value that can give rise to a 1 output value. If we did not consider the instantaneous effect of the noise, we would use $\mu^{+th} = \mu^{-th} = \langle x(t) \rangle = \mu$ (the average value of the input signal), leading to the $P(0) = P(1) = 1/2$ as naively estimated above. In contrast, we can set $\mu^{\pm th}$ using our knowledge of the dynamics of the comparison level. For instance, as shown in Fig. (2.12), we can use $\mu^{\pm th} = \pm 5\sigma$, where σ represents the standard deviation of the comparison level. Using this strategy, the derived predictability of the source is conservative with respect to the A/D noise. Only with a probability of $\sim 6 \times 10^{-5}$ is the instantaneous predictability of the source larger than $\mu^{\pm th}$.

Generalisation to multiple bit digitisers

If $x(t)$ is an analogue signal taking any possible value between $-\infty$ and ∞, an A/D converter quantises that information into one of the 2^b possible digital values $d \in d_0, \cdots, d_{2^b-1}$. Here, b is known as the resolution of the digitiser. Basically, the A/D conversion process discretises the input space in 2^b equally spaced bins Δ_d. If an input value falls within the boundaries of $\Delta_d = [\mu_d^-, \mu_d^+)$, the digital outcome d is produced. The probability of the digital outcome d in this ideal scenario is given by

$$P(d) \equiv F_x(\mu_d^+) - F_x(\mu_d^-), \tag{2.42}$$

where F_x represents the cumulative distribution function of the input signal x. For the extreme values $d = 0$ and $d = 2^b - 1$, $\mu_0^- = -\infty$ and $\mu_{2^b-1}^+ = \infty$ respectively, and therefore $F_x(\mu_0^-) = 0$ and $F_x(\mu_{2^b-1}^+) = 1$.

Unfortunately, as described in the simplified 1-bit resolution A/D conversion example above, the boundary levels $\mu_d^\pm$ are noisy, and this directly influences the generated random bitstream. Following the same procedure as described above, if we can find upper and lower limits for all the

boundaries, we will be able to bound the effect of the digitisation noise. If we let $\mu_d^{\pm}(t)$ be functions of time, describing the instantaneous value of the threshold levels, we want to find the adapted bounds

$$\bar{\Delta}_d = \big[\min_t \mu_d^-(t), \max_t \mu_d^+(t)\big) \equiv [\xi_d^-, \xi_d^+), \tag{2.43}$$

i.e. the lowest and highest analogue inputs that can give rise to the output d. There are multiple ways to treat this problem, depending on the statistical model that we use for the threshold levels $\mu_d^{\pm}$. One possibility is to assume that these threshold levels are normally distributed, statistically characterise $\mu_d^{\pm}$, find the mean and standard deviations, and write $\xi_d^{\pm} = \langle \mu_d^{\pm} \rangle + \kappa\sigma_{\mu_d^{\pm}}$, with κ being the desired confidence levels. Here, $\sigma_{\mu_d^{\pm}}$ is the standard deviation of $\mu_d^{\pm}$. Another statistical model is to use the worst case observation on every interval Δ_d, finding $\xi_d^+ = \max\{\mu(t)|d\}$ and $\xi_d^- = \min\{\mu(t)|d\}$. From this analysis we can also derive confidence intervals depending on how many data points have been used to find the minimum and maximum observations.

In Chapter 4, we describe the process we followed to quantify digitisation noise in the 1-bit A/D conversion scenario. For a 8-bit commercial digitiser, we bounded the size of the digitisation errors in the following way. We used an electronic signal generator (Tabor WW1281A) followed by a low-pass filter to produce a 1 kHz triangle wave, which is, from the perspective of the 2 GS/s digitiser, quasi-static. Then, we digitised this signal with our fast 8-bit digitiser (Acqiris U1084A) and simultaneously with a 14-bit oscilloscope (Agilent infiniium 86100C with an electronic module Agilent 86112A) for reference. In Fig. (2.13 we show the distribution of the digitisation errors (i.e. of the deviation of the digitised value from the ideal value), based on $\approx 2^{14}$ samples per digitisation value. This allows us to identify the limits $\xi_d^{\pm}$. In other words, the minimum and maximum voltages that were observed to produce a given digitisation value d.

2.4.3 Adding memory effects and other untrusted noises

A digitisation process is a fundamental step in any physical random number generator, so the procedure described above applies transversely to the construction of any real device. Similarly, there is another noise source that is common to any device: limited bandwidth electronics. When

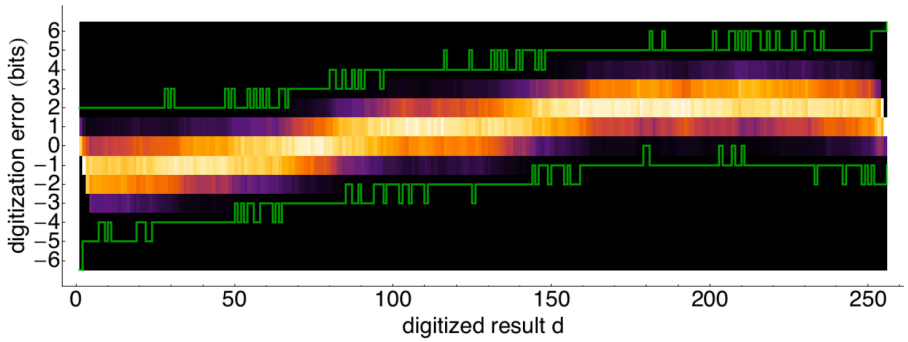


Figure 2.13: Measured digitisation error frequencies and error limits. Colour indicates relative frequency from zero (black) to maximum (white). It is interesting to note the presence of both a large-scale nonlinearity in the con- version (the general trend) and small-scale regularities (e.g. the period-two patterns clearly visible between 50 and 60). Green traces above and below indicate the largest and smallest errors observed, respectively. Approximately 2^{14} samples per digitisation value were used to obtain the frequencies, so the confidence that a new event will fall within the limits is $\approx 1 - 2^{-14}$

a digital sample is taken, the detection system is still responding (possibly weakly) to analogue inputs it received at earlier times. If we let $H(t)$ be the impulse response of the detection system and $x(t)$ the input signal, then the detected signal $y(t)$ is given by

$$y(t) = H(t) * x(t) \equiv \int_{-\infty}^{t} dt' H(t - t')x(t'), \tag{2.44}$$

where $*$ is the convolution operator.

Again, there are multiple ways to determine memory effects, which may depend on the construction of the random number generator. As an example, we measured memory effects (a.k.a. hangover errors) from the autocorrelation data in the 8-bit digitisation experiment (Mitchell et al., 2015). In contrast, in the prototypes built in 2015 (Abellan et al., 2015b), we calculated the hangover errors by periodically interrupting the modulation of the laser using a radio-frequency switch in an unbalanced Mach-

Zehnder configuration, and measuring the distribution of the last pulse of every radio-frequency cycle (see Chapter 5 for further details).

Similarly to the A/D noise, upper bounds on memory effects (as well as on other untrusted noises specific to a particular scheme) can be measured. Then, by incorporating these quantities into our analysis, we can adjust the digitisation threshold values, finding conservative bounds on the predictability of a real random number generation device. A possible approach is to quantify the fluctuations introduced by all the untrusted noises and then add these fluctuations into the digitisation bounds described above. As done above for the digitisation noise, the goal now is to include the effect of all the other noises in the estimation process. To derive conservative bounds, we can use multiple strategies depending on how paranoid we want to be about the effect of the noises.

Following with the scenarios described above, one possibility is to assume that all the noises are mutually independent and normally distributed and adapt the bounds by adding the noise fluctuations in quadratures, i.e.

$$\xi_d^{\pm} = \langle \mu_d^{\pm} \rangle + \kappa \sigma_T, \tag{2.45}$$

with κ defining the ratio of events that satisfy the condition, and

$$\sigma_T^2 = \sigma_{\mu_d^{\pm}}^2 + \sum_i \sigma_i^2$$

the joint contribution from untrusted noises. Here, $\sigma_{\mu_d^{\pm}}$ is defined as above, and σ_i represents the standard deviation of the i-th noise.

A more paranoid solution might be to add the fluctuations of the noises linearly, instead of doing it in quadratures. It corresponds to assuming that all the noises are correlated. In this case, we would calculate

$$\sigma_T = \sigma_{\mu_d^{\pm}} + \sum_i \sigma_i.$$

2.4.4 Minimising the worst-case predictability

We understand the predictability $\mathcal{P}$ of a random number generator to be the maximum probability for an adversary, with all possible information and resources in the universe, to guess what the next outcome from a

device will be. Following the methodology presented here, we can only find bounds on the predictability of the source if we understand the digitisation process of our device and the contribution from untrusted noises. If we are able to bound the effects of all the noises, we can find physically-guaranteed bounds on the predictability of the source. Basically, we have to maximise

$$\mathcal{P}(d) \equiv \max_d P(d|x) \equiv \max_d \left\{ F_d(\bar{\xi}_d^+) - F_d(\bar{\xi}_d^-) \right\} \tag{2.46}$$

Different experimental techniques were applied to characterise and combine the effect of the untrusted noises. In the 1-bit A/D technology described in (Abellan et al., 2015b), we derived unpredictability bounds using 5σ bounds on the observed noises and combining them with different paranoia levels. In contrast, in the 8-bit A/D experiment (Mitchell et al., 2015), we calculated the worst-case scenario that was compatible with the available data set by solving a multi-dimensional linear programming optimisation procedure to find the average min-entropy as follows:

$$\langle H_\infty \rangle \equiv - \int d\mathbf{x'} P(\mathbf{x'}) \max_d \log_2 P^{(wc)}(d \,|\mathbf{x'}). \tag{2.47}$$

Remarkably, we found that in this worst-case scenario for the noises, $\langle H_\infty \rangle$ is still several bits per symbol, allowing efficient extraction of pure randomness from the dataset. Also, by leaving the classical phase as a parameter in the optimisation, we showed that classical phase fluctuations have an effect on the randomness of the digitised symbols that decreases rapidly with increasing quantum phase diffusion. In other words, no classical noise can make the phase predictable, provided the quantum noise is sufficient.

Deriving trustworthy min-entropy bounds is of fundamental importance in the field of randomness generation in order to guarantee the security and performance of cryptographic nodes. Cryptographic protocols rely on the availability of high quality random digits, and false security perceptions can exist if the entropy of the randomness source is not properly estimated. The methodology introduced here is, in fact, similar to industry efforts to standardise and regulate physical random number generation devices and their characterisation. The AIS 31 standard is an example,

proposed by the German *Bundesamt für Sicherheit in der Informationstechnik* (Killmann et al., 2011).

2.5 Conclusions

In this chapter, we have explored the phase diffusion process in semiconductor lasers and its application and suitability for random number generation. We have presented a numerical analysis of the average phase diffusion both in continuous wave and pulsed operational modes, finding a large phase randomisation advantage in the gain-switching scheme. We have also reported the results of an ultrafast experiment (above 40 Gb/s bit rate), proving successful phase randomisation in the hundreds of picosecond time scale. In this experiment, we have presented a min-entropy estimation procedure based on second-order statistics of the observed signals. Finally, we have introduced the randomness metrology methodology to derive trustworthy min-entropy bounds by combining a thorough characterisation of the hardware components with an in-depth knowledge of the physical process. The results of this chapter confirm the suitability of the phase diffusion process for ultrafast randomness generation, both theoretically and experimentally, and introduce techniques to quantify the quality of physical random number generators.

Chapter 3

On-chip quantum entropy sources

Photonic integrated circuit (PIC) technology (Heck et al., 2013; Smit et al., 2014) is a key ingredient for building scalable optical devices (Walmsley, 2015). The telecommunications industry is a clear example, already accounting for commercial products such as semiconductor lasers, 100 GHz photodetectors, and high-bandwidth optical interconnects and transceivers (Alduino et al., 2010). Recently, the quantum optics community has been making rapid progress by leveraging PIC technology, offering the possibility to design scalable quantum optics experiments. In the field of quantum computation, PIC technology in combination with additional bulk elements, such as lasers, is allowing for the development of novel experiments otherwise impossible using tabletop components. Some examples include quantum simulation (Tillmann et al., 2013) and quantum-enhanced sensing (Matthews et al., 2009). Quantum key distribution (QKD) functionalities have also been integrated using Indium Phosphide technology (Sibson et al., 2015) and a monolithically integrated QRNG, composed of a light-emitting diode (LED) and a single-photon avalanche photodetector (SPAD), has been recently demonstrated at 1 Mb/s using Silicon (Si) Photonics technology (Khanmohammadi et al., 2015). Si Photonics is a promising candidate for building scalable optical applications due to its compatibility with the microelectronics industry. However, the impossibility of monolithically integrating a laser source

poses serious limitations to the level of miniaturisation and performance of the PIC.

Multiple technologies and materials have been considered for the integration of the phase diffusion QRNG technology. In particular, we have experimented with silicon photonics (Si), silicon nitride (Si_3N_4), and indium phosphide (InP). The key features that were considered critical in our design include: (i) the availability of all the required optical components (i.e. laser source, waveguides, couplers and detectors), (ii) a low propagation loss in order to maximise the signal to noise ratio (quantum fluctuations versus classical noise), (iii) a high-density component integration, and (iv) a mature manufacturing industry. In order to achieve a high density of integration, high refractive index materials are desirable. The higher the refractive index contrast, the higher the confinement of the light in the waveguide mode, and the smaller the curvature radius that can be achieved.

Technology	Losses (dB/cm)	Refractive index
Si	3	3.4
Si_3N_4	< 1	2
InP	2	3.15

Table 3.1: Key parameters for three of the most common materials for photonic integration.

As shown in Table 3.1, silicon nitride is the best candidate in terms of propagation loss. In contrast, silicon photonics offers both the highest density of components (highest refractive index contrast) and the most advanced (by far) manufacturing industry. Finally, indium phosphide is the only platform offering monolithic integration of all the optical components, including light sources. In this chapter, we first describe the results of a tiny silicon photonics device taking a 1x0.1 mm^2 area with an external DFB laser source, and then we show the results of an all optically integrated device using indium phosphide in an area of less than 6x2 mm^2.

3.1 Self-delayed scheme on a Silicon Photonics chip

In this section, we report the results of the integration of the phase-diffusion QRNG scheme on a Silicon chip with an unbalanced Mach-Zehnder configuration. In contrast to the Indium Phosphide scheme, the Silicon chip is constrained in a reduced area, and due to the self-delayed nature of the scheme, the interference signal is almost immune to temperature variations.

3.1.1 Chip design and experiment

The integrated device implements the critical interferometry and photodetection elements of the phase-diffusion QRNG strategy, as shown in Fig. (3.1). The laser component, which to date cannot be monolithically integrated in Si, is interfaced to the chip by a grating coupler (GC). A single-frequency DFB laser is operated in gain-switching (GS) mode, with a mean drive current of 14 mA and a sinusoidal modulation at 1 GHz, applied via a bias-tee. As the laser threshold is 10 mA, this takes the laser far above and below the threshold on each modulation cycle, producing a train of linearly-polarised optical pulses of duration $\sim$300 ps. Due to the phase diffusion process, subsequent pulses have random relative phases, while also having very similar wave-forms. In order to couple the light pulses into the Si chip, the laser output is directed towards a grating coupler (GC) via single mode fibres (SMF) at 10° incidence to couple the pulses into the Si chip. A ~ 10 dB Erbium-doped fibre-amplifier (EDFA) is used to compensate for the losses of the grating coupler and to improve in this way the signal to noise ratio at the output of the experiment. By measuring the transmission through a straight waveguide, losses due to the GC are estimated to be $\alpha_{\text{gc}} \sim 7$ dB.

In the chip, a first multimode interference coupler (MMI) splits the input light to the two arms of an unbalanced Mach-Zehnder interferometer (uMZI) with a power-splitting ratio of 2:98. The large deviation between the two output ports of the first MMI is chosen in order to pre-compensate for the losses that the signal in the long path will suffer due to the extra delay line. A delay line of 6.9 cm is integrated to introduce a 1 ns temporal delay, i.e. for 1 GHz modulation rate. Thus, the signal in the long arm

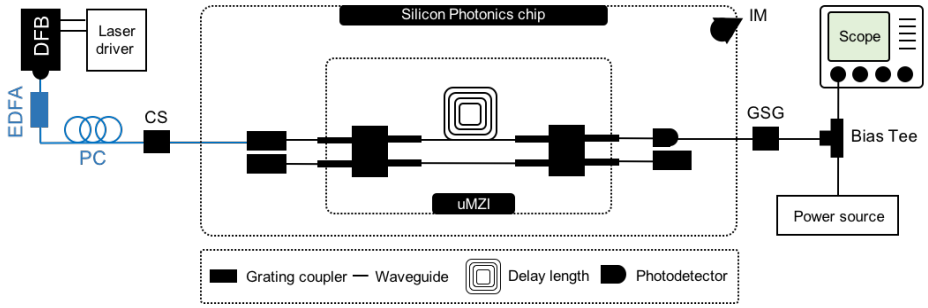


Figure 3.1: Experimental setup for the characterisation of the Si-based QRNG.A distributed feedback (DFB) laser is periodically modulated with a 1 GHz sinusoidal signal and biased close to the threshold level. An Erbium-doped fibre-amplifer (EDFA) is used to compensate for the losses of the grating coupler. The optical pulses travel through a polarisation controller (PC) and are sent to the Silicon chip through a coupling stage (CS). The CS is set up to couple light from the cleaved fibre to the chip at an incidence angle of 10°. A grating coupler brings the signal into the Si waveguide, which sends it directly into the unbalanced Mach Zehnder interferometer (uMZI). The uMZI is composed of two multimode interferometers (MMI) and a delay line introducing a $\sim$1 ns delay. Finally, a photodetector is reverse biased using a power source and the DC port of a bias-tee, and the RF signal is extracted using a groud-signal-ground (GSG) RF probe. The electrical signal is finally detected with a 4 GHz oscilloscope. An imagining system (IM) allows the chip to be viewed on a desktop computer.

suffers from approximately $\alpha_{\text{dl}} \approx 6.9$ cm $\times 3$ dB/cm ≈ 20.5 dB of propagation loss in the delay line. If we did not compensate for the loss in the first MMI, then the signal in the short arm, which experiences almost no propagation loss (only a few μm long waveguide), would reach the output MMI 20 dB stronger than the signal in the long arm, thereby killing in this way the interference visibility. By introducing the 2:98 splitting ratio in the first MMI, the signal travelling the short arm sees a loss of $\approx 10 \log 2/100 \approx 17$ dB of loss, reaching the output MMI with approximately the same strength as the signal from the long arm. After the uMZI structure, the interfered

signal is detected by a 10 GHz on-chip Germanium photodiode and sent to a 4 GHz real-time oscilloscope via a bias-tee. The detected intensity $I_{\text{det}}(t)$ can be written as:

$$I_{\text{det}}(t) = \alpha_s I(t) + \alpha_l I(t-\tau) + 2\mathcal{V}\sqrt{\alpha_s I(t)\alpha_l I(t-\tau)}\cos(\Delta\phi + \delta\theta), \quad (3.1)$$

where $I(t)$ is the instantaneous laser power at time t, $\alpha_l \approx 0.98\alpha_{\text{gc}}\alpha_{\text{dl}}$ are the losses experienced by the signal going through the long path of the interferometer and $\alpha_s \approx 0.02\alpha_{\text{gc}}$ the losses in the short path, $\tau = 1$ ns is the pulse repetition period, $\mathcal{V}$ is the interference visibility, $\delta\theta$ is the relative phase between subsequent optical pulses, and $\delta\phi$ is the optical phase acquired in the uMZI. Due to strong phase diffusion between subsequent optical pulses, $\Delta\theta$ is, to a very good approximation, random, and, therefore, an arcsine distribution is observed (Abellan et al., 2014a), irrespective of $\Delta\phi$.

A microscope image of the 4 x 7.5 mm^2 chip is shown in Fig. (3.2). Multiple uMZIs with different compensation values and delay lengths were present on it for testing purposes. More specifically, up to 20 uMZIs with optical-optical and optical-electrical input/output interfaces were integrated. Different splitting ratios for the MMIs and different path delay lengths were integrated too, in order to select the optimal structure. As well as the uMZI structures, a section of the chip is dedicated to test structures, in which all the building blocks forming the uMZIs are placed with input/output contacts for direct characterisation. All the tested components operate according to specifications. The measurements providing the best interference signals were performed in the 2:98 splitting ratio uMZIs, which introduced an amplitude compensation of around 20 dB, very similar to the losses expected in the long arm of the interferometer, i.e. ≈ 6.9 dB/cm $\times 3$ dB/cm $= 21$ dB. The overall size of a single QRNG detection structure is below 0.5 x 1 mm^2.

3.1.2 Performance tests

By measuring the statistics of the electrical signal when the laser is below the threshold level, one can obtain information about the overall noise of the system - see purple line in Fig. (3.3). While the electronic noise and

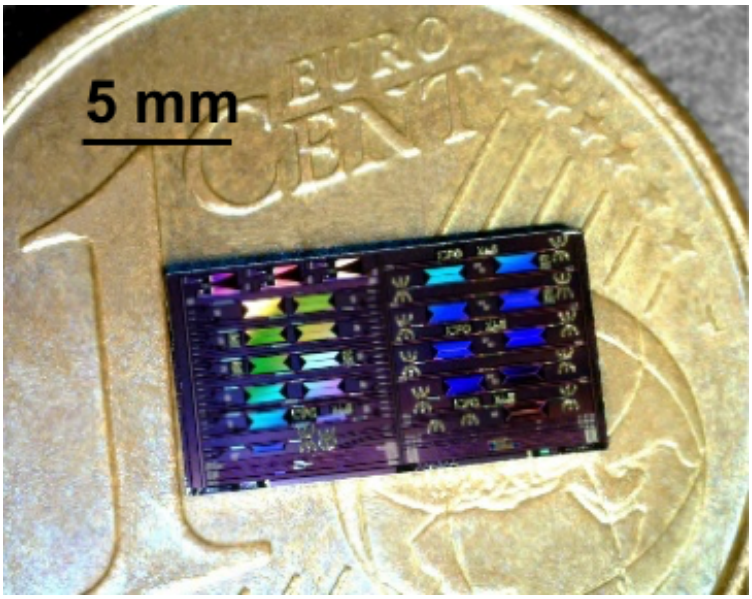


Figure 3.2: Microscope image of the 4 x 7.5 mm^2 Silicon Photonics integrated chip on top of a 1 euro cent coin. Up to 20 quantum random number generation (QRNG) structures are present on the chip, together with test structures of the various building blocks that form the QRNG device. A single QRNG block is less than 0.5 x 1 mm^2

optical power produce a strongly monomodal distribution (Gaussian-like shape), the interference signal (orange line in Fig. (3.3)) shows a strong bimodal behaviour (arcsine-like shape), reflecting the smoothed arcsine distribution due to the convolution with the electronic noise. 700k samples were acquired when calculating the histograms.

We ran a Monte Carlo calculation to find the interference parameters that best fits the observed distribution according to the model in Eq. (3.1). We set the waveguide losses to 3 dB/cm, as estimated experimentally, the splitting ratio to 98:2, as also verified experimentally in one of the test structures of the chip, and the electronic noise strength to $\sigma = 1.9$ mV, as extracted from the histogram in Fig. (3.3). By leaving the interference visibility $\mathcal{V}$, as well as the noise acquired by the signal in each path of the

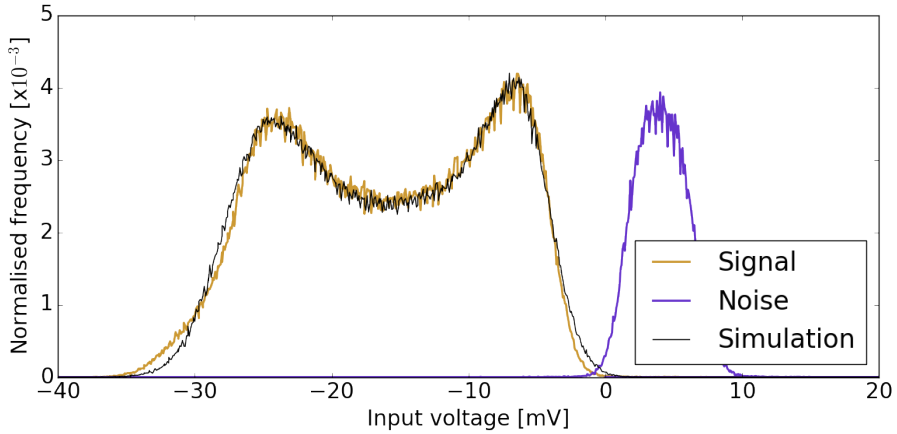


Figure 3.3: Histogram of the observed signal and noise by taking samples during the on and the off times of the modulation cycle. The normalised frequency of the signal fits well the expected arcsine behaviour, whereas the noise follows a Gaussian profile. A Monte Carlo simulation of the process fits well the observed frequencies.

interferometer, i.e. the standard deviation of $I(t)$ and $I(t-\tau)$, as free parameters, we found that the observed distribution is consistent with Eq. (3.1) with $\mathcal{V} = 0.74$ and random $\Delta\theta$. The mean square error between the observed and simulated distributions is $\approx 10^{-5}$. The signal to noise ratio (SNR), defined as the ratio between the standard deviation of the arcsine signal and the noise, was found to be SNR$\approx$ 4.1. The fitted distribution is also plotted in Fig. (3.3), showing good agreement between the observed and theoretical predictions.

In order to measure the correlation, we have introduced a new experimental method for situations in which high-speed digitisation is not available. Typically, a long sequence of digits is stored, and then the correlation is estimated from that data. In our case, for instance, since capturing data continuously with a pulsed source at 1 GHz was not possible, we devised a new strategy to do this directly on the oscilloscope. By using available measurement options in the oscilloscope, such as gaiting

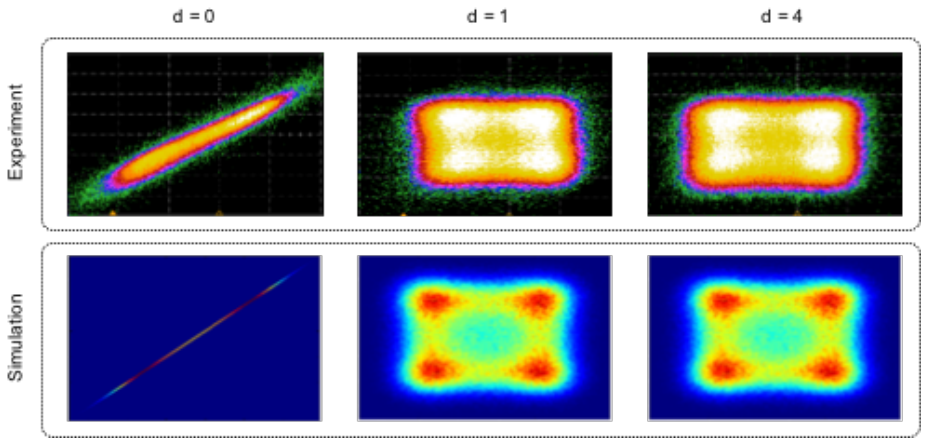


Figure 3.4: 2D autocorrelation of the raw data. By plotting the amplitudes corresponding to the n-th and $(n-d)$-th pulses on an XY plot directly on the oscilloscope, we can evaluate and visually inspect the autocorrelation of the raw data in real-time.

and skewing, we measured the amplitudes of the n-the and the $(n-d)$-th pulses and plot the pair of points using an XY plot. If we let A_n and A_{n-d} represent the amplitudes of the two pulses, we accumulate the pairs of pulses (A_n, A_{n-d}) on the screen and qualitatively analyse the results. This proposed technique is very useful as a first real-time screening method. A numerical simulation together with the measured XY plots for several correlation distances d are depicted in Fig. (3.4).

3.2 Two-laser scheme on an Indium Phosphide chip

In the unbalanced Mach-Zehnder interferometer approach presented in the previous chapter, a path length difference between the two arms of the interferometer of $\Delta L = c\tau_c/n$ is required, where c is the speed of light in vacuum, $\tau_c = f_c^{-1}$ the period of the modulated signal, and n the refractive index of the material. For instance, for a 1 GHz modulation frequency and an InP waveguide ($n = 3.15$), a path length difference of $L \sim 10$ cm

would be required. In order to observe high interference visibility, the losses in the short path should be increased to balance the signal levels in both paths of the interferometer. Hence, we immediately reduce the quantum signal to noise ratio, reducing the quality of the produced random numbers.

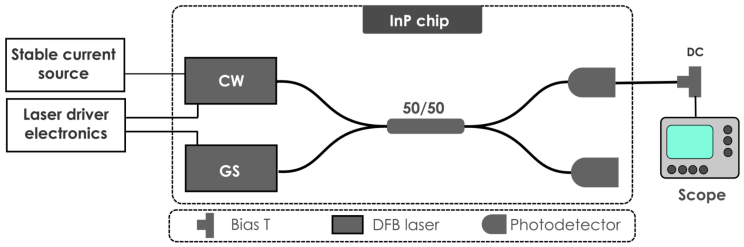


Figure 3.5: Schematic of the QRNG-PIC based on two-laser interference. The two DFB lasers are biased, each of them with its own current driver, and one of them operating in CW mode, while the other one is periodically GS using an external RF generator. The temperature of the entire chip is controlled through a Peltier element, while that of the entropy source area, including one of the lasers, is locally tuned by using a stable current source. The outputs from the two lasers are combined and interfered in a 2×2 MMI coupler, and two 40 GHz photodiodes are placed after the coupler. The detected signal is then recorded by a fast oscilloscope.

In this chapter, a new configuration is introduced. It uses heterodyne and gets rid of the need for long delay lines. As illustrated in Fig. (3.5), the proposed scheme combines two DFB lasers on the same chip. The first laser is operated in gain switching (GS) mode, while the second one can be operated in either continuous wave (CW) or GS modes. As described in Section 2.2.1, by continuously modulating the GS laser from below to above the threshold level, optical pulses with nearly identical waveforms and completely randomised phases are generated. Next, by beating the GS and CW (the local oscillator) lasers through a multimode interference (MMI) coupler, an intensity oscillation forms with a beating frequency equal to the difference of the two lasers' frequencies, which can then be detected by a photo-detector. The principle of operation is

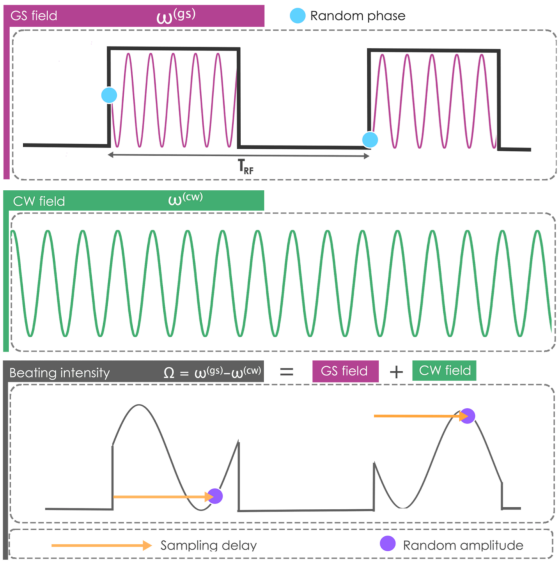


Figure 3.6: Principle of operation of the QRNG-PIC: optical pulses from a GS laser interfere with a CW laser, generating an interference modulation whose frequency is equal to the difference of the two lasers' frequencies. The random phase of the GS laser pulse produces a random phase of the interference oscillation that can be properly sampled into a random amplitude. In this way, after digitisation, one sample per GS pulse can be extracted.

qualitatively described in Fig. (3.6).

If we let $u_s(t) = u_A(t) + u_B(t)$ be the sum of the intensities from the two laser sources and $u_p(t) = \sqrt{u_A(t)u_B(t)}$ their geometric mean, we can write the interference signal at the output of the interferometer following Eq. (2.3) as

$$u^{(out)}(t) = u_s(t) + 2u_p(t)\cos\left(\int_0^t d\xi\Omega_C(\xi) + \Delta\phi(t)\right), \qquad (3.2)$$

where $\Delta\phi \equiv \phi^{(cw)} - \phi^{(gs)}$ is the phase difference between the two lasers' fields, and $\Omega_C(t) \equiv \Omega - \beta(t)$ their frequency detuning as a function of time. We introduce $\beta(t) = \beta_0 t$ phenomenologically to account for the fre-

quency chirp arising from fast thermal effects in the directly modulated laser (Zadok et al., 1998). Here, Ω represents the initial frequency detuning between the two lasers. As illustrated in Fig. (3.6), the resulting signal corresponds to a train of pulses in which the amplitude of each pulse oscillates at $\int_0^t d\xi \Omega_c(\xi)$ with a random phase $\Delta\phi$ (for simplicity $\beta_0 = 0$ in the illustration, i.e. the chirp is not represented). Finally, after the MMI coupler, a photodetector converts the optical signal into the electrical domain, and random numbers are obtained by taking one sample per pulse repetition period.

Box 4. Resolving the beating between two light sources

The interference between two light sources can be written as

$$u^{(out)}(t) = u_s(t) + 2u_p(t)\cos\big(\Omega t + \Delta\phi(t)\big), \tag{3.3}$$

where $u_s(t) = u_A(t) + u_B(t)$ is the sum of the intensities of the two sources and $u_p(t) = \sqrt{u_A(t)u_B(t)}$ the geometric mean. Unlike with Eq. (3.2), we here neglect the effect of the chirp without loss of generality, since we are analysing bandwidth effects associated with the frequency detuning. If $\Omega_D \approx 0.35/\tau_D$ is the bandwidth of the detector and τ_D its response time, the electrical signal at the output of the detector system $v(t)$, assuming linearity, is given by

$$v(t) = u^{(out)} * h_D(t), \tag{3.4}$$

where $*$ is the convolution operator and $h_D(t)$ the impulse response of the detection system. The impulse response can be well approximated by $h_D(t) \sim \theta(t)\exp\{-t^2/2\tau_D^2\}$, $\theta(t)$ being the heaviside step function and τ_D the width given by the response time. Using the linearity of the convolution operator:

$$(a + b) * c = a * c + b * c$$

we can focus on the oscillation term in Eq. (3.3), namely,

$$\begin{aligned}\cos\big(\Omega t+\Delta\phi\big)*h_D(t) &= \int_{-\infty}^{\infty} d\xi h_D(\xi)\cos\big(\Omega(t-\xi)+\Delta\phi\big)\\ &= \int_{0}^{\infty} d\xi\,\exp\{-\xi^2/2\tau_D^2\}\cos\big(\Omega(t-\xi)+\Delta\phi\big)\\ &\propto \exp\Big\{-\frac{\Omega^2}{18\Omega_D^2}\Big\}\Big\{\cos\big(\Omega t+\Delta\phi\big)\\ &\qquad +\mathrm{Erfi}\big[\frac{\Omega}{3\sqrt{2}\Omega_d}\big]\sin\big(\Omega t+\Delta\phi\big)\Big\}.\end{aligned}$$

Note that if the beating frequency Ω is much larger than the detection bandwidth (i.e. $\Omega/\Omega_D >> 1$), the exponential term tends to zero and therefore the oscillating term cannot be resolved. On the other hand, for $\Omega_D >> \Omega$, the exponential term tends to one, and the oscillation $\cos\Omega t+\Delta\phi$ can be recovered. Thus, in the two-laser scheme, the central frequency of the two lasers must be kept within the detection bandwidth.

Preliminary results with discrete components

The two-laser scheme was demonstrated using discrete components as a proof-of-concept test before integration. An Alcatel A1905LMI DFB laser was used as the GS source, and a tunable laser Photonetics Tunics Plus 3642 HE 10 as the CW reference, as illustrated in Fig. (3.7). A 2x1 polarisation maintaining coupler (PMC) was used to combine the two signals, and the beating was detected by a 10 GHz bandwidth photodetector (Nortel PP10G), and digitised by a 2 Gsps digitiser Acquiris U1084A with a 1 GHz electrical bandwidth. As seen in Eq. (3.2), the heterodyne signal oscillates at a frequency determined by the detuning between the two lasers. Thus, in order to resolve this beat note, the detuning should be kept within the detection bandwidth of the detector (see Box 4). Using an optical sampling scope (20 GHz bandwidth) and an optical spectrum analyser, we measured the interference visibility (RMS deviation of the distribution) as a function of the detuning between the two lasers. As shown in Fig. (3.8), high interference visibility was observed for detunings of up to 200 pm, which corresponds to a frequency difference of ~ 25 GHz, in agreement with the electronic bandwidth of the measurement device.

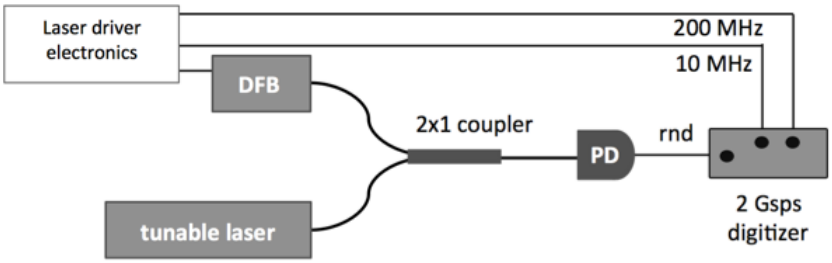


Figure 3.7: Bulk setup for the QRNG based on heterodyning two laser diodes. A DFB laser is directly modulated from below to above threshold with a 200 MHz signal. A tunable laser is operated in cw and the central frequency is set very close to the central wavelength of the GS laser. A 2×1 polarisation maintaining coupler combines the two signals and a photodetector (PD) detects the beating field. The random signal (rnd) is sent to a high-speed digitiser. The 200 MHz signal and the internal 2 GHz clock of the digitiser are synchronised with a 10 MHz reference clock.

For larger detuning frequencies, the visibility starts to decrease until it reaches almost zero for detunings of more than 500 pm. After characterising the visibility as a function of the detuning, we set the frequency difference between the two lasers below 1 GHz, which is the electrical bandwidth of the digitiser used to acquire large data sets.

The system ran overnight in order to acquire and process up to 60 sequences of 1 GB (Gigabyte) each. In Fig. (3.8), we show the histogram, measured every 70 minutes, and high-interference visibility and repeatability is observed, indicating that the frequency detuning between the two lasers remained within the detection bandwidth over the entire measurement run. We also calculated the autocorrelation function for the raw data, showing a statistically significant correlation for $d < 200$, and falling into the statistical sensitivity afterwards. This correlation pattern is always observed with the employed photodetector (even in the unbalanced Mach-Zehnder scheme), and is attributed to its long-lived states. For completeness, we also implemented the randomness extraction step, as well as statistical testing of the output bits. We wrote a parallelised version of the hashing algorithm proposed by Frauchiger-Renner-Troyer in C++ to

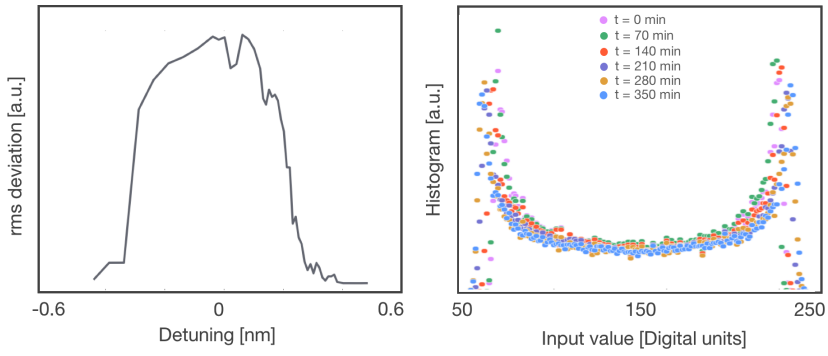
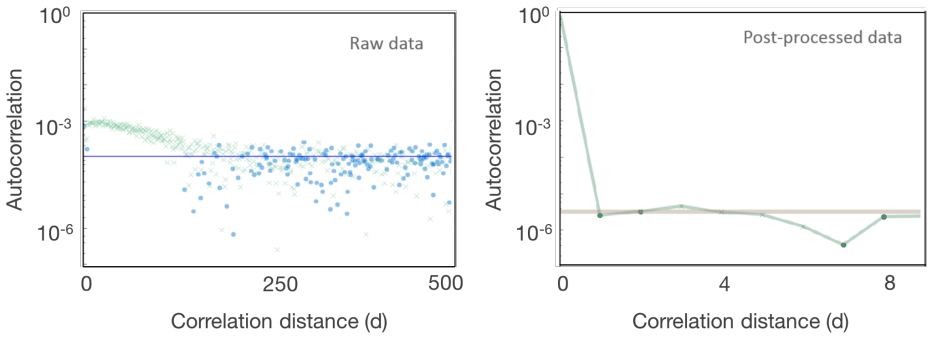


Figure 3.8: Stability of the two-laser scheme with discrete components. (a) RMS deviation of the interference signal as a function of the detuning between the CW reference laser and the GS laser. Note that for detunings larger than $\lambda = 400$ nm, the RMS deviation falls, indicating that the interference term oscillates at a frequency that cannot be resolved. (b) Histograms taken at time intervals of 70 minutes. The observed distribution is shown for every measurement. High interference visibility is observed during the entire measurement run.

increase the throughput (Frauchiger et al., 2013). After randomness extraction, we computed the correlation for a total dataset of 60 Gb, observing no statistically significant coefficients - see Fig. (3.9). We also applied the Alphabit battery of statistical tests to the 60 sequences of 1 Gb post-processed data, observing a rate of weak p-values below 2%. See the statistical testing section in Chapter 5 for more details.

3.2.1 Chip design and experiment

The integrated chip was fabricated at the Fraunhofer Heinrich Hertz Institute (HHI) in Berlin. The design of the chip was carried out in collaboration with VLC Photonics. For the implementation of the two-laser quantum entropy source chip, two DFB lasers, a 2x2 MMI coupler, and two photodetectors were utilised. HHI's standard building blocks were used for



(a) Raw data (b) Post-processed data

Figure 3.9: Autocorrelation for the two-laser scheme with discrete components. (a) Autocorrelation for the raw data calculated from a 100 Mb dataset. (b) Autocorrelation for post-processed data using the Frauchiger-Renner-Troyer randomness extractor (Frauchiger et al., 2013) computed from a 60 Gb dataset.

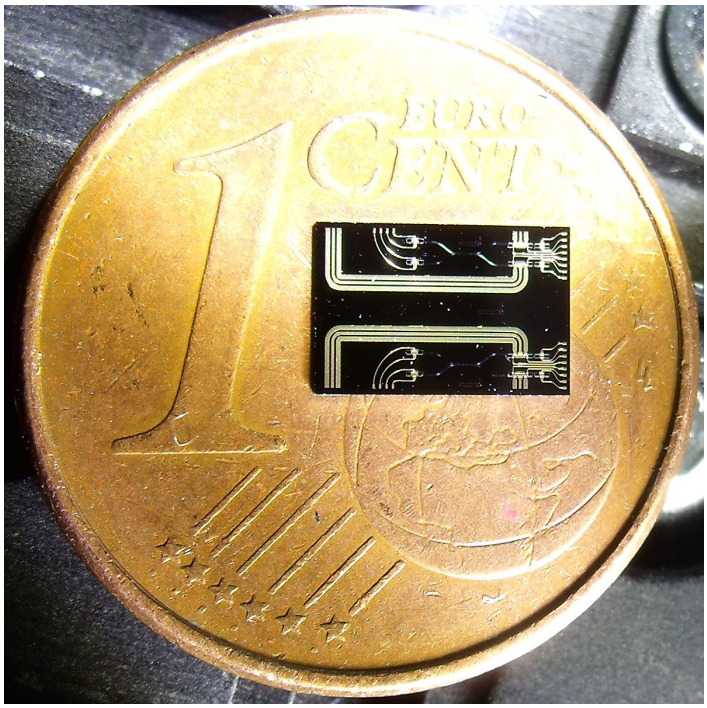
the laser sources and the photodetectors. MMIs are based on the self-imaging principle (Soldano et al., 1995), which is an effect observed in slab waveguides supporting multiple spatial modes. In such structures, an input field profile is periodically reproduced in single or multiple locations along the waveguide due to the interference between multiple supported spatial modes. Different modes propagate at different group velocities, and therefore, different patterns appear due to the local interference occurring at each point. In order to achieve the 2x2 functionality, two input and two output single mode waveguides are connected to a wide multimode waveguide at positions $\pm W_e/6$ from the centre, W_e being the effective width of the multimode waveguide. With this structure, the light from each input port splits with probability $1/2$ to each output port, at a distance of approximately $\sim L_\pi/2$ from the input. Here $L_\pi \equiv 4n_r W_e^2/3\lambda_0$ is the beat length of the two lowest-order modes, n_r being the refractive index and λ_0 the central wavelength of the field. For best performance, however, the dimensions of the MMI region are numerically optimised to minimise coupling losses from and to the single mode structure and the

multimode structure.

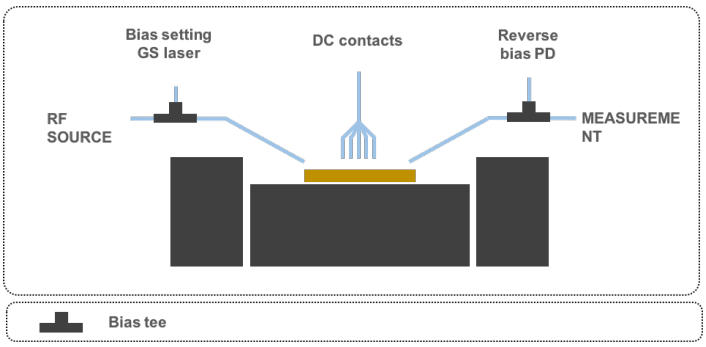
A microscope image of the two-laser quantum entropy source (QES) PIC is shown in Fig. (3.10). The chip was placed on top of a Peltier controller and its temperature was maintained at 25° with variations of less than 0.1°. Measurements were taken directly from the bare chip using ground-signal-ground RF probes, as well as DC contacts, in a configuration as shown in Fig. (3.2.1).

The first DFB laser, with a bias of 10 mA, was operated in GS mode by superimposing a 100 MHz modulation from an Anritsu MP1800A pulse generator through a bias-tee port. We chose this relatively low modulation frequency in order to capture properly the dynamics of the interference pattern within the GS pulse. Modulation frequencies above 1 GHz were demonstrated in the laboratory using the same integrated components, offering a very promising approach to achieve raw generation rates in the order of tenths of Gb/s. As discussed in previous chapters, the scheme will be limited by the stabilisation of the build-up dynamics of the laser intensity, i.e. the time it takes for the laser to create a stable single frequency mode starting from a below-threshold spectrum. In the experiment, we operated the CW laser with a constant 30 mA current. The beating signal was detected by an on-chip 40 GHz photodetector and digitised with a 20 GHz and 50 GSa/s real-time scope (Digital Phosphor Oscilloscope, Tektronix DPO72004C), providing a temporal resolution of 20 ps to analyse the beat note.

The central frequencies of the two lasers were independently tuned by injecting a constant current from a stable source (Keithley 2401) through a metallic contact on the grating structure. As expected, the injected current produced a heating effect on the grating structure, changing its average refractive index and, therefore, the Bragg resonance condition. As a result, the operating frequency (wavelength) of each laser could be independently tuned. Following this approach, the detuning frequency between the two lasers was reduced and brought within the detection bandwidth.



(a) Microscope image



(b) Measurement stage

Figure 3.10: (a) Schematic of the QES-PIC based on the two-laser interference scheme. Two QES-PIC structures are integrated on the 6x4 mm^2 chip, and a test structure with optical output can be observed in between. Each QES-PIC structure consists of two DFB lasers, a 2x2 MMI coupler, and two 40 GHz photodetectors. (b) Illustration of the experimental stage for the optical characterisation of the chips. The signal to modulate the GS laser is sent into the integrated DFB laser using a ground-signal-ground (GSG) RF probe, and is generated using an RF source for the AC component and a constant reference for the DC part. The AC and DC signals are combined using a bias-tee. The CW laser is biased using a DC contact line. Finally, a second bias-tee is used with the photodiode, firstly, to reverse bias it through the DC port, and, secondly, to extract the detected RF component. The two lasers are temperature controlled by injecting a DC current through metallic contacts.

3.2.2 Performance tests

Temporal dynamics and numerical simulations

In general, interfacing between different components in an integrated circuit produces back-reflections. In our scheme, in which we aim to extract phase information due to spontaneous emission photons in the cavity of the GS laser, photons coupling from the CW laser to the GS laser due to back-reflections would prevent the generation of phase randomised optical pulses. More specifically, this effect is significant when the frequencies of the two lasers are tuned close to each other, leading to phase-locking (frequency-locking) effects. This phenomenon can be explained on the basis of the general mechanism of Adler's synchronisation of two coupled nonlinear oscillators (Adler, 1946), and modelled by the Lang-Kobayashi rate equation analysis for two mutually coupled semiconductor lasers (Lang et al., 1980). With the effective coupling rate between the two laser cavities represented by κ, and the frequency detuning between the two bare longitudinal modes of the uncoupled cavities by Ω, it is known in simple Adler's theory of synchronisation that frequency locking occurs, if we neglect delay effects, for:

$$|\Omega| < 2\kappa. \tag{3.5}$$

In Fig. (3.11), we show the frequency beating between the two lasers measured by operating them both in CW mode, and sweeping the resonance condition of one of them. As observed, the frequency between the two lasers changes linearly with the applied current, except in the region where the two central frequencies are similar. In this central region, the frequency difference cannot be clearly measured, mainly because of two effects: (i) phase noise, which can be a few hundreds of MHz typically, and (ii) phase-locking effects. Experimentally, clear locking effects could be seen in this region for frequencies below ~ 1.5 GHz. Using Eq. (3.5), we can estimate $\kappa \sim 5$ ns^{-1} for this photonic integrated circuit. In (Abellan et al., 2016a), a more complete analysis based on the numerical solution of the Lang-Kobayashi rate equations is given.

In the experiments, we used two PICs: a high waveguide propagation loss PIC that ensures the absence of significant back reflection from the CW into the GS laser, and another one with a similar structure but lower

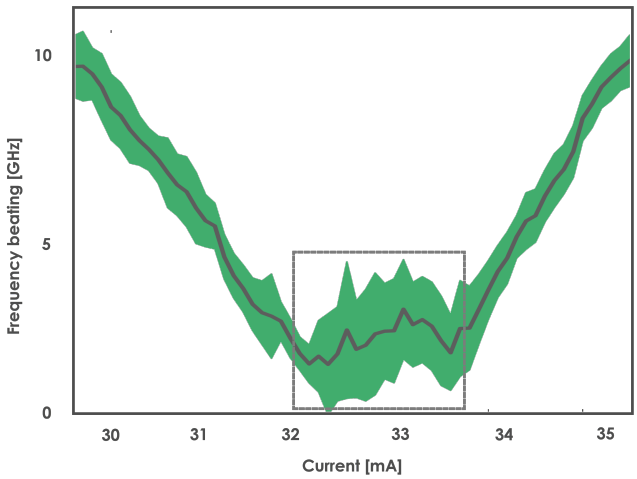


Figure 3.11: Beat-note frequency at the output of the MMI measured by sweeping one of the integrated lasers, while keeping the other one constant in the low-loss QRNG-PIC. The beat-note frequency can be continuously tuned by current control for large detuning frequencies, whereas for small detuning frequencies phase- (frequency-) locking may occur (gray square), leading eventually to disappearance of the oscillation.

loss. In the lower-loss PIC, back reflections at the MMI interface eventually induce phase-locking effects, preventing the generation of random oscillations. As detailed above, the coupling constant for the low-loss chip is given by $\kappa \sim 5$ ns^{-1}. With such a high coupling constant, spontaneous emission is too weak compared to the back-reflection, and thus phase-locking is observed. To obtain the QRNG functionality, it is, therefore, mandatory to reduce the feedback arising from spurious reflections at the MMI coupler. This goal was achieved by increasing the optical losses of the bus waveguides (~ 15 dB/cm), and, as a result, the coupling rate κ between the two laser cavities is reduced by ~ 30 dB from the previously discussed low-loss PIC. For the high-loss PIC, the coupling, if any, is very weak, and, thus, phase randomisation due to quantum noise prevails over phase-locking. In Fig. (3.12) we show the solution of the Lang-Kobayashi rate equations for different detuning parameters, and compare the results

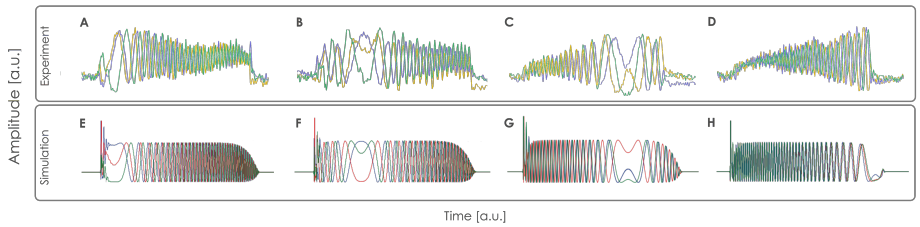


Figure 3.12: Temporal dynamics of the beating between the two lasers forming the high-loss QRNG-PIC and comparison with numerical results. (a)-(d) Experimental data with different temperature settings (currents). Chirp due to thermal effects and attenuation of beating amplitude due to the bandwidth limit of the detection electronics are evident. (e)-(h) Numerical results with initial detuning frequencies set to fit the experimental observations in (a).

with the experimental data.

For both the high- and low-loss PICs, the optical pulses of the GS laser were strongly chirped due to thermal effects, yielding a frequency-varying oscillation of the beating pattern, as depicted in Fig. (3.12). As a result, a nearly zero detuning (NZD) region was observed within the optical pulses when the chirped frequency of the GS laser coincided with the stable frequency of the CW laser. The position of the NZD region depended on the initial frequency separation between the GS and the CW emission lines. When both lasers were initially close in frequency, the NZD region occurred at the beginning of the pulse. Conversely, with a large frequency separation, the NZD region occurred at the end of the pulse - see Fig. (3.12). In the high waveguide-loss PIC (15 dB/cm), the interference amplitude within the NZD region changed from pulse to pulse, a clear signature that phase noise dominated. Instead, in the low-loss PIC (2 dB/cm), back-reflection from the CW into the GS laser was significant enough that phase-locking between the two lasers was observed. In this case, the interference amplitude in the NZD region did not appreciably change from pulse to pulse. In the experiment, the NZD region was tuned at the end of the pulse - see Fig. (3.12d) - maximising the detuning frequency between the two lasers in order to reduce residual phase-locking

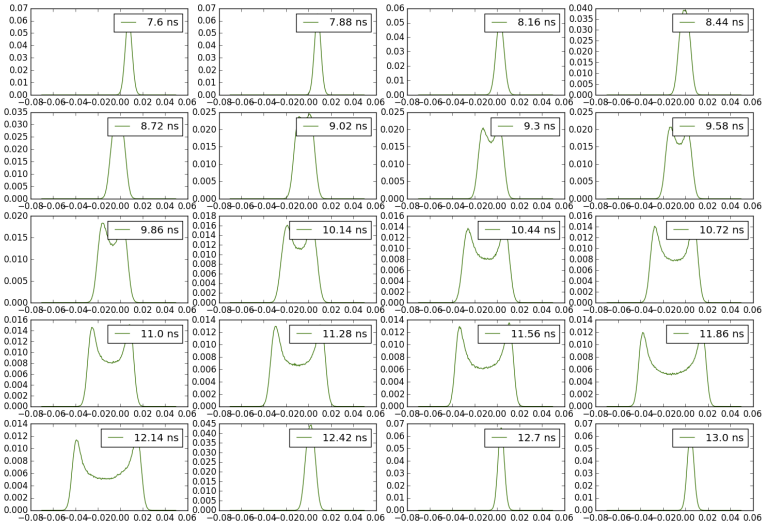


Figure 3.13: Statistical characterisation of the density function within the chirped pulses. In the nearly zero detuning (NZD) region, good interference visibility is observed, whereas outside this region, the interference cannot be resolved and a narrow distribution appears.

effects, if any. In Fig. (3.13), we show the histograms observed by taking samples at different positions within the pulse for a configuration in which the NZD region occurs at approximately the central position of the pulse. In this scenario, a Gaussian distribution is observed when the frequencies are far from each other (corresponding to fast oscillations), and an arcsine distribution arises within the NZD region.

PIC Stability and statistical characterisation

From a practical point of view, long-term stability of the scheme is a critical aspect. As we are interfering signals from two independent lasers, intrinsic phase noise and temperature drifts can severely affect the perfor-

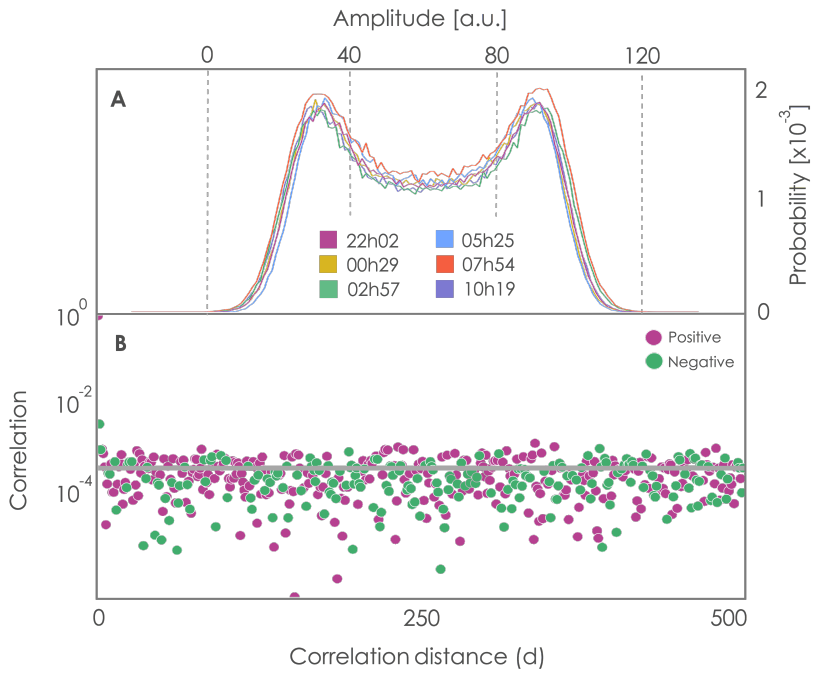


Figure 3.14: Statistics on the output of the QES-PIC. (a) Histograms on six sets of $200,000$ samples each taken over 14 h, confirming stable operation of the QES-PIC device. (b) Autocorrelation function for 10^7 random samples taken with a 20 GHz scope and a 50 GSa/s. Magenta and green circles correspond to positive and negative correlation coefficients, respectively.

mance. In Fig. (3.14a), we plot the histogram for six datasets with $200,000$ samples in each. High stability is observed between acquisitions taken over a 14-hours period. Compared with the bulk case, higher stability is observed with the integrated scheme. We attribute this effect mainly to the fact that the two lasers are closely located in a region with uniform temperature in the integrated case, whereas independent lasers with different packagings are used in the bulk experiment..

In Fig. (3.14b), we show the autocorrelation function $\Gamma_x[k] \equiv \langle x_i x_{i+k} \rangle -$

$\langle x \rangle^2$. Samples from the higher-loss PIC were acquired using a 50 GSa/s resolution and 20 GHz bandwidth real-time scope, followed by a 30 dB RF amplifier. The amplifier introduced noise at several frequency bands, so we employed a 30 MHz high pass- band digital filter to remove low-frequency components. In addition, in order to assess the quality of the QES-PIC, we are interested in estimating the correlation of the beat note only. In order to do so, we assume that the noise is independent of the beat signal, and then calculate $\Gamma_x = \Gamma_y - \Gamma_n$, where Γ_y is the autocorrelation of samples taken within the GS pulse, and Γ_n is calculated by taking samples outside of the GS pulse - see Box. 5. We emphasise that this technique is only valid for an estimation of the entropy source quality, but will not work to estimate the autocorrelation of the raw data produced in a real device. In the experiment, the use of a bare chip and RF probes introduced significant noises. With a proper packaging and PCB soldering, we expect these noises to be significantly reduced.

Box 5. Autocorrelation subtraction.

Let $y = x + n$ be the signal that we measure, with x and n being independent random variables. If $\Gamma_z[k] \equiv \langle z_i z_{i+k} \rangle - \langle z \rangle^2$ is the autocorrelation of a random variable z, we can calculate the autocorrelation of y as follows:

$$\begin{aligned} \Gamma_y[k] &= \langle (x_i + n_i)(x_{i+k} n_{i+k}) \rangle - \langle x + n \rangle^2 \\ &= \langle x_i x_{i+k} + x_i n_{i+k} + n_i x_{i+k} n_i n_{i+k} \rangle - \langle x \rangle^2 - \langle n \rangle^2 \\ &= \langle x_i x_{i+k} \rangle + \langle n_i n_{i+k} \rangle - \langle x \rangle^2 - \langle n \rangle^2 \\ &= \Gamma_x[k] + \Gamma_x[k] \end{aligned} \tag{3.6}$$

The autocorrelation is calculated from a sequence with $n = 10^7$ samples and for a correlation delay distance of up to 500 samples. For such a sequence length, the statistical uncertainty due to finite size effects is 3.16×10^{-4}. Except for the $d = 1$ coefficient, which is significantly larger than the statistical noise sensitivity, all the other coefficients fall within the statistical noise level. We attribute the larger correlation at $d = 1$ to limitations in the direct modulation of the DFB laser diode in the experiment, leading to residual photons in the cavity from pulse to pulse. If this coefficient were due to phase-locking effects, we would expect it to last for

much longer, not only for short correlation distances. Phase-locking is a constant effect due to the injection of photons from the CW laser into the GS laser, whereas residual photons due to not emptying the cavity fast enough represent a pulse-to-pulse effect that would rapidly decay with correlation distance. For the rest of coefficients ($d > 1$), we apply the D'Agostino-Person's normality test, finding a p-value of 0.18. Note that, for an ideal random sequence, the correlation coefficients for $d > 0$ should spread according to a normal distribution, with zero mean and standard deviation given by the finite size effect sensitivity.

3.3 Conclusions

In this chapter, we have shown the integration of the phase diffusion quantum random number generation technology on photonic integrated circuits (PICs). First, we showed an all-optical integration on an Indium Phosphide platform with a novel two-laser scheme and heterodyne detection. In this design, all the optical components, including laser, interferometer and detectors, were integrated on the chip. We demonstrated that GHz rates are possible in a form factor below 6 x 2 mm^2 with standard fabrication processes. Then, we also reported successful integration on a Silicon Photonics platform, in which the critical interferometer and detection components were integrated on the chip. By using an external laser source, we observed high-quality interference at 1 GHz modulation rates. The results of this chapter demonstrate the potential for large scale and commercial production of quantum devices with standard fabrication processes.

Chapter 4

Physical randomiser for Bell-inequality-based quantum technologies

Quantum nonlocality is one of the most striking predictions to emerge from quantum theory. Beyond their fundamental interest, loophole-free Bell tests enable powerful device-independent information protocols, guaranteed by the impossibility of faster-than-light communication. Bell tests and device-independent protocols employ space-like separation of measurements to guarantee the nonlocality of correlations and the monogamy of correlations under the no-signalling principle. In addition to closing the detection loophole, these experiments must also close two space-time loopholes, namely, that no basis choice may influence a distant particle (locality loophole), and that the entanglement generation must not influence the basis choices (freedom-of-choice loophole). In this chapter, we describe the random number generation technology that was employed by the first three experiments, closing, simultaneously, the detection and locality loopholes, and addressing the freedom-of-choice loophole. By combining the accelerated laser phase diffusion technology described in previous chapters with real-time randomness extraction and metrological assurances, the produced random digits satisfied the extremely stringent conditions of these experimental tests.

4.1 Design considerations: freshness and purity

Random numbers used to determine the basis choice in a Bell test have some special and very particular requirements when one is trying to close loopholes. The first one is the ability to place strict predictability bounds on the produced random digits. These bounds are extremely important when statistically evaluating the strength of the Bell inequality violation. The second types of requirements are related to space-time considerations. In particular, the random events that determine the basis choice have to be space-like separated from the distant detection station (locality loophole) and from the production of the pairs of particles (freedom-of-choice loophole), as illustrated in Fig. (4.1). This requires the generation of random digits in a time window strictly shorter than the light-time between the detectors. This is what we call the freshness property. The concept of freshness is very similar to the idea of latency, but with a subtle, yet very important, consideration. Latency typically accounts for the propagation or switch-on delay of a system. Freshness has a specific consideration in the generation of random digits. In particular, the freshness time is defined as the time difference between the occurrence of the relevant physical events influencing the value of the final bit, until such bit is used to select a measurement basis. In this section, we describe the proposed design for meeting all the relevant requirements mentioned above. This includes the analogue design, the analog-to-digital conversion, and the digital design for the randomness extraction stage in order to achieve low unpredictability values. Recent publications have reported progress towards the closure of the freedom of choice loophole by selecting the basis choice from cosmic sources (Handsteiner et al., 2017) and by using human choices from thousands of participants in the so-called Big Bell Test experiment (Abellan et al., 2018).

4.1.1 Analogue design

A single-mode laser diode (LD) is strongly current modulated, going above the threshold level for about 2 ns out of every 5 ns cycle, to produce a train of optical pulses with very similar waveforms, as seen in Fig. (4.4). In the time below the threshold, strong phase diffusion randomises the optical

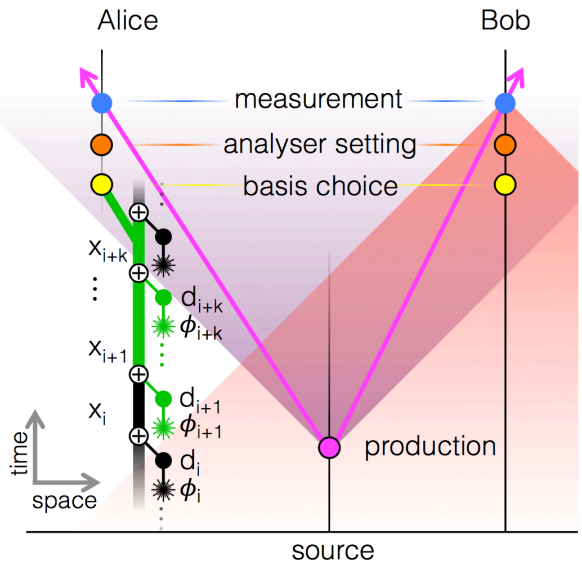
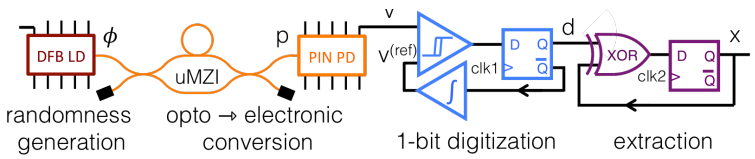


Figure 4.1: Space-time diagram for the production of random numbers in a loophole-free Bell scenario. As shown, up to k raw bits can be generated in a time window that is space-like separated from both (i) the pair generation and (ii) the distant measurement. Laser pulses with random phases ψ_i are converted into raw random bits d_i and extracted bits x_i by a running XOR ($\oplus$) calculation.

phase within the laser, and, therefore, the relative phase $\Delta\phi$ from one pulse to the next. At the point when a pulse leaves the laser, it is already a macroscopic ($\sim$mW) signal, with a phase that has been fully randomised by the microscopic process of spontaneous emission. See Fig. (4.3) for an estimation of the average phase diffusion as a function of time. For synchronisation with the experiments, all clock signals are generated from a central phase-locked-loop (PLL) device with a 10 MHz reference input. An unbalanced Mach-Zehnder interferometer (uMZI) converts the train of phase-random pulses into amplitude-random pulses - see Fig. (4.4b) - which are detected with a fast photodiode. The detected optical intensity is given by:



(a) Schematic

(b) Prototype

Figure 4.2: Random number generation scheme for loophole-free Bell test experiments. (a) Experimental schematic. Laser pulses with random phases ϕ_i from a semiconductor laser are converted into random powers by an unbalanced Mach Zehnder interferometer (uMZI) and detected with a linear photo-receiver (PIN PD) to give analogue voltages v_i. These are one-bit digitised with a comparator and D-type flip-flop to give raw bits d_i, and summed modulo 2 with an XOR gate to give extracted bits x_i. The output value x_{i+k} includes the parity of k raw bits, d_{i+1} to d_{i+k}, due to pulses space-like separated from the distant measurement and from the entanglement production. (b) One of the six prototypes delivered to the experimental groups. The prototypes have a general 10 MHz input clock for synchronisation, and generate the 200 MHz signals internally using a phase-locked-loop (PLL) chip.

$$p_I(t) = p_s(t) + p_l(t) + 2\sqrt{p_s(t)p_l(t)}\cos\Delta\phi(t), \tag{4.1}$$

being p_s and p_l the optical power from the short and long paths of the interferometer, respectively, and $\Delta\phi(t)$ the phase difference between the

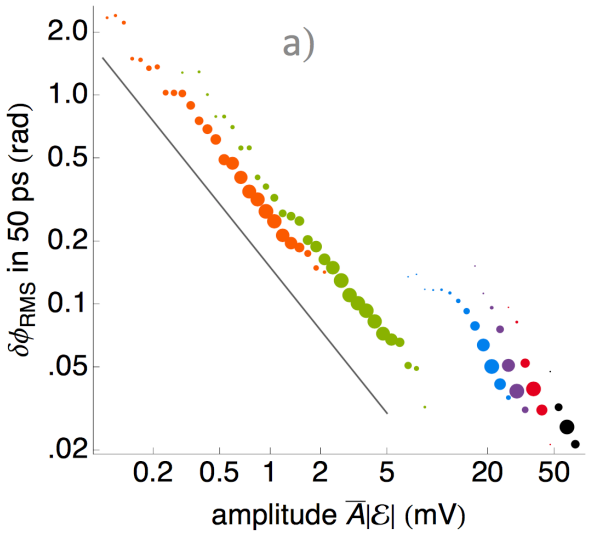
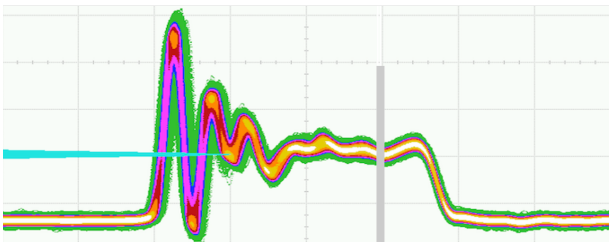
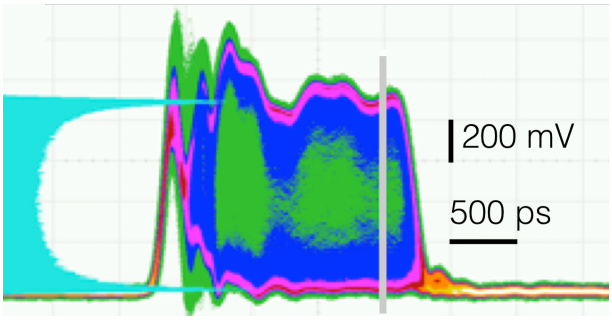


Figure 4.3: Observed frequencies (spot size) of field amplitude $|E|$ and resulting average phase diffusion $\langle \Delta\phi(\Delta T)^2 \rangle$ over $\Delta t = 50$ ps. These quantities are derived from a Kalman filtering reconstruction of heterodyne measurements of two lasers, one of them acting as a local oscillator with fixed current, and the other one as the test laser; see (Abellan et al., 2015b) for further experimental details. The test laser was operated with several currents (colors, left to right) 15, 16, 16.5, 17, 17.5 and 19 mA (colours left to right). Grey line shows $\langle \Delta\phi(50 \text{ ps})^2 \rangle \propto |E|^{-1}$ scaling of spontaneous-emission-driven phase diffusion, as theoretically expected. Because of the loss of coherence when biasing the test laser to low, the minimum current that could be tested using heterodyne measurements was 15 mA. In real operation, the gain-switched laser biasing current during the off-time of the pulse is much lower (implying a faster phase diffusion rate), and remains in the off-regime for around 3 ns rather than 50 ps (i.e. around 60 times longer).

fields in the two paths. The detected voltage can be written as the convolution $*$ of the detected intensity with the impulse response of the photodetector. If we let h be the impulse response, then the detected voltage



(a) Input pulses



(b) Interfering pulses

Figure 4.4: Persistence mode visualisation of pulse statistics after the photodetector. Warmer colours show greater frequency; teal histogram on the left axis describes the voltages sampled inside the time window indicated in grey. (a) Non-interfering pulses obtained by blocking the long interferometer path; (b) Interfering pulses.

reads as $v(t) = h * p_I(t)$. Because the bandwidth of the photoreceiver is much larger than the pulse repetition frequency, the signal mainly represents the optical energy received within the last $\tau_{PD} \sim 100$ ps, and, thus, from the present pulse. Nevertheless, we need to take account of "hangover error," i.e., delayed contributions from previous pulses. To model this behaviour, we define the impulse response as $h(t) = h_f(t) + h_s(t)$, where $h_f(t)$ represents the fast response of the detector and is non-zero for $0 \leq t \leq 5$ ns, and $h_s(t)$ accounts for the delayed response and is

non-zero for $t > 5$ ns only. Then, we can write the detected voltage as:

$$\begin{aligned} v(t) &= (h_f + h_s) * p_I(t) + v_{PD}(t) \\ &= h_f * p_I(t) + h_s * p_I(t) + v_{PD}(t) \\ &= v_s + v_l + v_\phi + v_H + v_{PD}, \end{aligned} \tag{4.2}$$

where $v_{s,l}(t) \equiv h_f * p_{s,l}(t)$, $v_\phi \equiv \mathcal{V}\sqrt{v_s v_l}\cos\Delta\phi \equiv h_f * (\sqrt{p_s p_l}\cos\Delta\phi)$, with $\mathcal{V}$ being the visibility of the interference, $v_H \equiv h_s * p_I(t)$, and $v_{PD}(t)$ the photodetector noise.

4.1.2 Digital design

A fast comparator and a D-type flip-flop digitise the signal (with one-bit resolution) at times t_i to give raw digital values $d_i = \theta[v(t_i) - v_{ref}(t_i)]$ at a rate of 200 Mb/s. Here, θ is the Heaviside step function and v_{ref} is the comparator reference level. In Eq. (4.2), the only term that contains space-like separated randomness comes from the phase diffusion process $v_\phi(t)$. By defining the sum of all the untrusted terms as $v_c \equiv v_s + v_l + v_H + v_{PD} - v_{ref}$, we can conveniently write the voltage signal as the sum of a trusted variable plus all the untrusted variables as

$$v(t) = v_\phi(t) + v_c(t) \tag{4.3}$$

and the value of every new digital bit as

$$d_i = \theta\big[v_\phi(t_i) - v_c(t_i)\big]. \tag{4.4}$$

Hence, we can now calculate the distribution function of the raw bits as

$$P(d_i = 0) = P\big(v_\phi(t_i) + v_c(t_i) \leq 0\big) = P\big(v_\phi(t_i) \leq -v_c(t_i)\big). \tag{4.5}$$

The expression on the right is, by definition, the cumulative distribution function of v_ϕ. As described in chapter 2, the distribution function of the cosine of a random variable is given by the arcsine distribution, which can be written as

$$P(v_\phi = x) = \frac{1}{\pi\sqrt{(\Delta v_\phi - x)(x - \Delta v_\phi)}}, \tag{4.6}$$

for $|x| \leq \Delta v_\phi$, with $\Delta v_\phi = 2\mathcal{V}\sqrt{v_s v_l}$ being the peak-to-peak range of v_ϕ. From Eq. (4.6) we can calculate the cumulative distribution function of v_ϕ as

$$P(v_\phi \leq x) \equiv \int_{-\infty}^{x} dx P(v_\phi) = \frac{2}{\pi} \arcsin \sqrt{\frac{1}{2} + \frac{x}{2\Delta v_\phi}}. \tag{4.7}$$

Finally, by using Eq. (4.7) in Eq. (4.5), we find that the probability of $d_i = 0$ is given by

$$P(d = 0) = \frac{2}{\pi} \arcsin \sqrt{\frac{1}{2} - \frac{v_c}{2\Delta v_\phi}}, \tag{4.8}$$

for $|v_c| \leq \Delta v_\phi$. Similarly, we can find the probability of $d_i = 1$ as $P(d_i = 1) = 1 - P(d_i = 0)$, namely

$$P(d = 1) = \frac{2}{\pi} \arcsin \sqrt{\frac{1}{2} + \frac{v_c}{2\Delta v_\phi}}, \tag{4.9}$$

In the experiments, the reference level for the comparator was set by feedback from the raw digital values via an integrator with a 1 ms time constant. Firstly, this slow feedback mechanism compensates for any possible laser drift in the long run, and also, it simplifies the integration and stability of the system in the experiments. We observed a raw-bit average of $\langle d \rangle = \frac{1}{2}[1 + 6.9(1) \times 10^{-4}]$.

4.1.3 Randomness extraction circuitry

A continuous parity calculation is performed as a randomness extractor. An XOR gate and a second flip-flop update the output x as $x_i = x_{i-1} \oplus d_i$, where $\oplus$ indicates an addition modulo 2. This describes a two-state machine, which changes state every time a new raw bit $d_i = 1$ and stays in the same state whenever $d_i = 0$, resulting, in principle, in a perfectly unbiased output distribution (see Box 6). Note that x accumulates the parity of all preceding raw bits, only k of which will be space-like separated from the distant measurement station. Therefore, only those k bits can be accounted for in the randomness analysis. As a result, when a bit $x_{i+k} = x_i \oplus d_{i+1} \oplus \cdots \oplus d_{i+k}$ is used for a basis setting, x_i contributes no space-like separated randomness, and the predictability of x_{i+k} will

be determined by $d_{i+1} \oplus \cdots \oplus d_{i+k} \equiv D_{i,k}$. Writing the predictability of d_i (i.e. the probability of the more likely value), as $\mathcal{P}(d_i) = \frac{1}{2}(1 + \epsilon_i)$, where $\epsilon_i \geq 0$ is the instantaneous excess predictability, we find (see Box 7) that if we can bound the instantaneous predictability of the raw bits $\epsilon_i \leq \epsilon_{max}$, then the predictability of the parity of k bits will be bounded as:

$$\mathcal{P}(D_{i,k}) \leq \frac{1}{2}(1 + \epsilon_{max}^k). \tag{4.10}$$

In other words, the RE output approaches ideal randomness exponentially in k (see Box 7).

Box 6. Distribution of the output of a two-state machine with arbitrary transition probabilities

If we take a two-state machine defined by $x_i = x_{i-1} \oplus d_i$, with x being the state of the system and d the input bit, the probability that the output is 1 in the next time step can be calculated as

$$\begin{aligned} P(x_i = 1) &= P(x_{i-1} = 0 \cap d_i = 1) + P(x_{i-1} = 1 \cap d_i = 0) \\ &= P(d_i = 1)P(x_{i-1} = 0) + P(d_i = 0)P(x_{i-1} = 1), \end{aligned} \tag{4.11}$$

where we used the independence property $P(a \cap b) = P(a)P(b)$. Now, by assuming the process to be stationary, i.e. not dependent on time, we use $P(x_i = 0) = P(x_{i-1} = 0)$, finding

$$P(x = 0) = P(d = 1)P(x = 0) + P(d = 0)P(x = 1), \tag{4.12}$$

or equivalently

$$P(x = 0) = \frac{P(d = 0)P(x = 1)}{1 - P(d = 1)} \tag{4.13}$$

From this last equation, by using the fact that $P(d = 0) = 1 - P(d = 1)$, we finally find

$$P(x = 0) = P(x = 1). \tag{4.14}$$

This means that the density function of the two state machine is totally unbiased, independently of the specific probability distribution function of the raw bits d.

Box 7. Predictability of the parity of k bits using a weak entropy source model

As shown in Eq. (4.3), our signal is composed of v_ϕ, a completely unpredictable term due to its physical origin, and v_c, a term containing the effect of other non-trustable processes. Here, we want to calculate the predictability of the parity of multiple partially-random bits. Let $a = \theta[v_\phi^{(a)} + v_c^{(a)}]$ and $b = \theta[v_\phi^{(b)} + v_c^{(b)}]$ be two bits obtained from our weak entropy source, where superscripts $^{(a)}$ and $^{(b)}$ represent each of those two realisations. Since $v_c^{(a)}$ and $v_c^{(b)}$ are not trusted to be independent, the joint probability distribution function $P(a, b)$ is not in general separable. However, because of the independence of the trustable term, the joint conditional probability separates as

$$P(a, b|v_c^{(a)} v_c^{(b)}) = P(a|v_c^{(a)}) P(b|v_c^{(b)}). \tag{4.15}$$

In general, for a partially-random bit d, the predictability is defined as $\mathcal{P}(d) \equiv \max[P(d = 0), P(d = 1)]$. A totally unpredictable source has predictability $1/2$, so writing $\mathcal{P}(d) \equiv \frac{1}{2}(1 + \epsilon_d)$, we define the predictability error as $\epsilon_d \equiv 2\mathcal{P}(d) - 1$. Considering now the two partially-random bits a and b with predictabilities $\mathcal{P}(a)$ and $\mathcal{P}(b)$ respectively, the predictability of $a \oplus b$ is the larger of

$$P(a \oplus b = 0) = P(a = 0)P(b = 0) + P(a = 1)P(b = 1) \tag{4.16}$$

or:

$$P(a \oplus b = 1) = P(a = 1)P(b = 0) + P(a = 0)P(b = 1), \tag{4.17}$$

We find that we can conveniently write this as

$$\mathcal{P}(a \oplus b) = \mathcal{P}(a)\mathcal{P}(b) + [1 - \mathcal{P}(a)][1 - \mathcal{P}(b)]. \tag{4.18}$$

By multiplying both terms by a factor of 2 and subtracting 1, we find

$$\begin{aligned} 2\mathcal{P}(a \oplus b) - 1 &= 2\mathcal{P}(a)\mathcal{P}(b) + 2[1 - \mathcal{P}(a)][1 - \mathcal{P}(b)] - 1 && (4.19)\\ &= 2\mathcal{P}(a)\mathcal{P}(b) + 2 - 2\mathcal{P}(a) - 2\mathcal{P}(b) + 2\mathcal{P}(a)\mathcal{P}(b) && (4.20)\\ &= 4\mathcal{P}(a)\mathcal{P}(b) - 2(\mathcal{P}(a) + \mathcal{P}(b)) + 2 && (4.21)\\ &= [2\mathcal{P}(a) - 1][2\mathcal{P}(b) - 1], && (4.22) \end{aligned}$$

and, using our definition of predictability error $\epsilon_x = 2\mathcal{P}(x) - 1$, we find

$$\epsilon_{a\oplus b} = \epsilon_a \epsilon_b. \tag{4.23}$$

If we now bound the predictability error of each bit as $\epsilon_x \leq \epsilon_{x,max}$, the error of the parity can be bounded as

$$\epsilon_{a\oplus b} \leq \epsilon_{a,max}\epsilon_{b,max}, \tag{4.24}$$

since $\epsilon_{a\oplus b}$ is monotonically increasing with ϵ_a and ϵ_b. Finally, if we combine the parity of k bits d_i for $i = 1, \cdots k$, i.e. $D(d_{i,k}) \equiv d_1 \oplus \cdots \oplus d_k$, and repeatedly apply Eq. (4.24), we find

$$\epsilon_{D_{i,k}} =\leq \prod_{i=1}^{k} \epsilon_{d_{i,max}} \tag{4.25}$$

showing an exponential approach to ideal randomness.

4.2 Measuring the age of the random bits

As illustrated in Fig. (4.1), the time window for randomness generation is bracketed on the early side by the requirement for space-like separation from the distant detection, and on the late side by the requirement for space-like separation from the pair generation. Ensuring that the random events fall within this window requires both upper and lower bounds on the freshness time. We measure the timing of relevant events using a differential probe and a 4 GHz real time oscilloscope (Agilent Infinitum MSO9404A). As shown in Fig. (4.5), we measure three delays in the circuit: (i) from the modulation of the laser, measured directly on the pins of the laser (conservative measurement), to the output of the photodetector (t_1), (ii) from the output of the photodetector to the input of the XOR gate (t_2), and (iii) from the input of the XOR gate to the CML output connector (t_3). We split these into three intervals to assist with the traceability of the signal while travelling through the electronics. All delays are quantified by capturing traces and using cursors to identify the zero-crossing times of the relevant edges. As shown in Fig. (4.6), for each transition we identify a best guess $t_i^{(best)}$ limited by the uncertainty of the interpolation between 50 ps samples. We find $t_1^{(best)} = 7.82$ ns, $t_2^{(best)} = 1.16$ ns, and

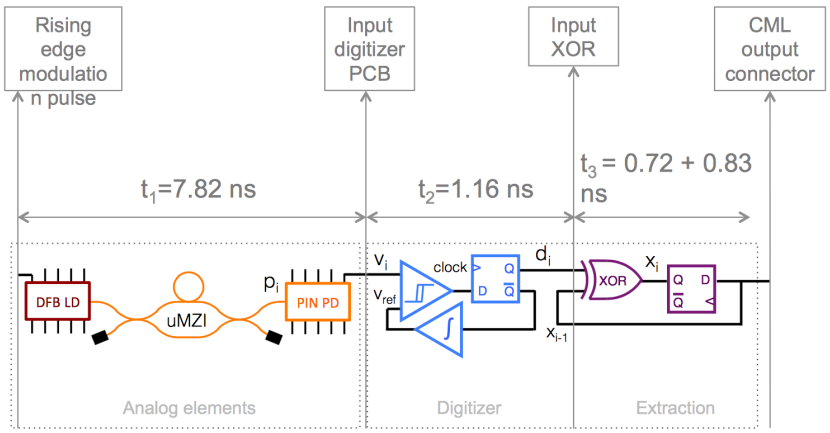


Figure 4.5: Schematic of the random number generator with timing information as directly measured by a 4 GHz real time oscilloscope. t_1 describes the time from the rising edge of the current pulse to the rising edge of the PIN PD output pulse, t_2 describes the time from the PIN PD pulse to the input of the XOR gate, and t_3 the time from the input of the XOR gate to the output SMA port.

$t_3^{(best)} = 1.55$ ns.

Measuring the intervals on the oscilloscope can cause a systematic error, which we now bound. In light of the $\sim 100-150$ps 10%-90% rise and fall times of the transitions, it is extremely improbable that we will misjudge the location of the edge by 100 ps or more, as this would mean placing the best guess outside of the transition region. As illustrated in Fig. (4.6), we calculate the upper and lower bounds for the transition times as $t_i^{(ub)} = t_i^{(best)} + 100$ ps and $t^{(lb)} = t_i^{(best)} - 100$ ps, respectively. By combining the three measured intervals we find $\tau^{(ub,sys)} = t_1^{(ub)} + t_2^{(ub)} + t_3^{(ub)} = 10.87$ ns and $\tau^{(lb,sys)} = t_1^{(lb)} + t_2^{(lb)} + t_3^{(lb)} = 10.21$ ns. Fig. (4.7) shows the sequence of measurements performed.

The jitter of the signal plus the jitter of the oscilloscope is quantified by accumulating 10^7 traces using the persistence mode of the oscilloscope. Measuring the rising edge of the signal at the photodiode output, we ob-

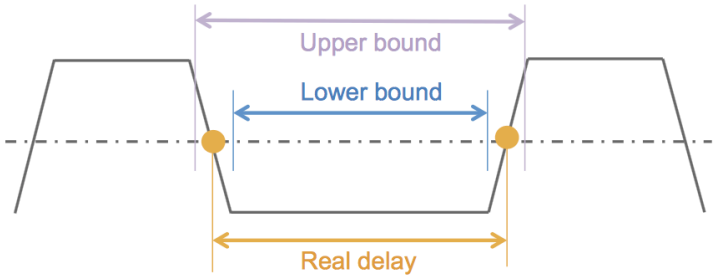


Figure 4.6: For a given captured trace, the best- guess estimate for the zero-crossing time is found by interpolation between the 50 ps samples of the 20 Gsps oscilloscope, with systematic uncertainty (orange circles). To obtain the upper bound (purple) and lower bound (blue) for the zero-crossing time, we add or subtract the half-width of the transition. Statistical uncertainty is accounted separately from the statistics of 10^7 traces collected in the oscilloscope's persistence mode.

serve that all of the traces fall within a 125 ps temporal window; there is no recorded value outside of this window. Making the hypothesis that events outside of this window will occur with probability of at least 1.4×10^{-6}, we can expect > 14 events on average outside of this window. A Poisson distribution with this mean predicts our observed zero events with probability 8×10^{-7}. We can, therefore, reject the hypothesis and assign a p-value $p < 1.4 \times 10^{-6}$ confidence to the 125 ps window for the measured zero-crossings. We note that this does not count the contribution of the oscilloscope to the jitter and is, thus, a conservative estimate. The freshness time combines intervals from three cascaded measurements. Adding three such windows, the conservatively estimated window for the full process is $3 \times 125 = 375$ ps. Half of this, i.e. 187.5 ps, can be assigned to the upper limit, and half to the lower. For simplicity, we use a conservative round number and define the jitter bound as $\tau_{jitt} = 200$ ps.

The lower and upper bounds for the freshness time of a single bit, including statistical and systematic errors, conservatively estimated, are

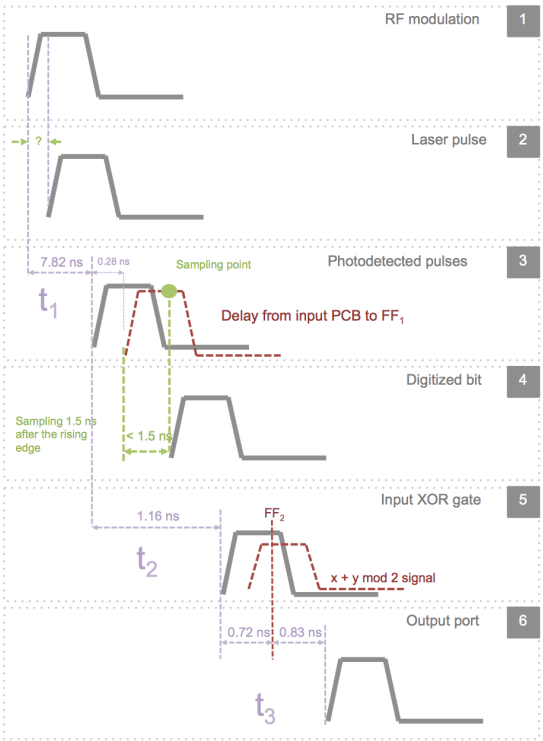


Figure 4.7: Details of the sequence of measurements used to obtain the freshness time. We start by measuring the modulation pulse directly at the laser diode pins (1). The LD generates an optical pulse sometime after the modulation pulse is applied (2). Then, the signal is photodetected and measured (3). The difference between (1) and (3) gives t_1. Next, the electrical pulse is digitised by a fast comparator and latched by a first flip-flop (4), and then propagates until the input of an XOR gate (5). At the input of the XOR gate we can tap the signal and measure the arrival time. The difference between (3) and (5) gives t_2. Finally, the signal goes into the randomness extraction circuitry, and propagates to the output, where we measure the arrival time again (6). The difference between (5) and (6) gives t_3.

then

$$\tau_f^{(lb,sys)} - \tau_{jitt} < \tau_f < \tau_f^{(ub,sys)} + \tau_{jitt}$$
$$10.01 \text{ ns} < \tau_f < 11.07 \text{ ns} \tag{4.26}$$

The clock of the RNG is derived from an external reference via a phase-locked loop, introducing a timing uncertainty that is nominally $<$ 1 ps and negligible on the scale of the other uncertainties. The freshness time for k events is therefore given by

$$\tau_f^{(k)} = \tau_f + (k-1) \times 5 \text{ ns}, \tag{4.27}$$

with 5 ns being the laser's modulation period.

4.3 Unpredictability bounds via randomness metrology

In order to upper bound the instantaneous predictability error, we follow a metrology approach based on the detection model in Eq. (4.2) and a characterisation of the involved noises. In particular, we quantify the noise in the detector and the long and short path of the interferometer, the noise in the analogue-to-digital conversion, and the memory effects due to bandwidth limitations. The measured and derived noises are summarised in Table (4.1). Below, we describe the experimental procedure.

4.3.1 Directly measurable noises

Statistics of the photodetection noise, and fluctuations in the long and the short paths of the interferometer, can be taken from the output of the photodetector. The statistics are measured with an AC-coupled oscilloscope (Agilent Infiniuum MSO9404A) with a 4 GHz input bandwidth and an 8-bit resolution, and are acquired as histograms of sampled voltages within a 50 ps window. For instance, to measure the photodetector noise, we connect the output of the detector to the oscilloscope, and we switch off the laser. The measured quantity thereby contains the fluctuations of the photodetector, plus the uncertainty introduced by the oscilloscope. To

Measured	RMS dev.	Derived	Mean	RMS dev.
v_O	1.7			
$v_D + v_O$	1.9	v_D		0.8
$v_s + v_D + v_O$	2.2	v_s	251	1.1
$v_l + v_D + v_O$	2.3	v_l	251	1.3
$v_l + v_H + v_D + v_O$	4.4	v_H		3.8
v'_O	3.4			
$v_{ref} + v'_O$	8.4	v_{ref}		7.7
v''_O	7			
$v_\phi + v_s + v_l + v_D + v_H + v''_O$	354	Δv_ϕ	483	

Table 4.1: Measured noise statistics. All voltages are in mV. v_O, v'_O and v''_O indicate the oscilloscope noise at gains of 50 mV/division, 100 mV/division and 200 mV/division, respectively. $v_l + v_H + v_D + v_O$ is measured using an interrupted pulse train, as in Section 4.3.3. $v_{ref} + v_O$ is measured using the x-y method of Sec. 4.3.2. Δv_ϕ is determined from the fit of Fig. 3.

retrieve the noise from the photodetector alone, we should subtract the noise in the scope. Similarly, to measure the fluctuations in the short and long arms of the photodetector, we can block the long and the short paths respectively. Importantly, the noise in the oscilloscope depends on the dynamic range setting. The larger the dynamic range, the larger the digitisation noise. Oscilloscope noises at different scales are also shown in Table (4.1)

4.3.2 A/D noise

In addition to a direct measurement of v_{ref}, the comparator reference voltage, we can also measure the input-output relation of the comparator chip. Note that while an ideal comparator converts each analogue input into an unambiguous digital output, a real comparator has noise and, therefore, the conversion of input values near the reference voltage is noisy. In order to quantify this “transition voltage” range, it is not sufficient to measure the reference noise, as any extra effect occurring inside the comparator itself or lack of knowledge of the performance of the device would be neglected. We emphasise that this measurement makes no assumptions at

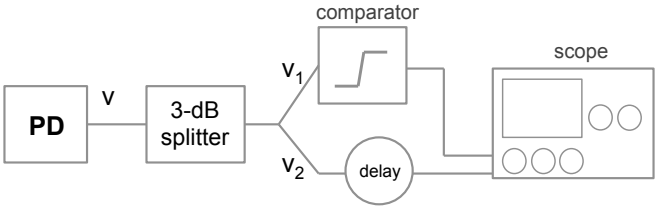
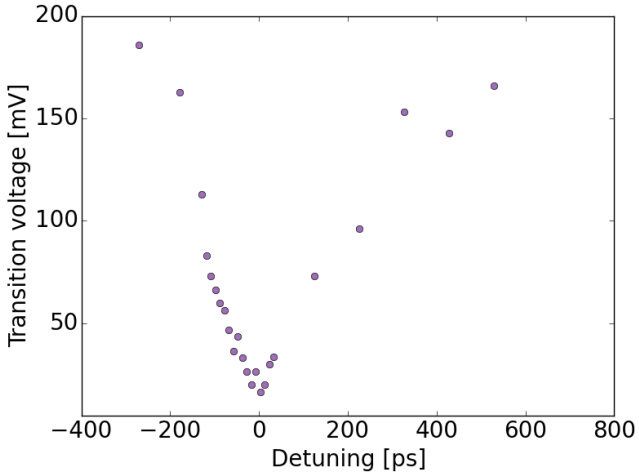


Figure 4.8: Schematic for the characterisation of the comparator chip. The signal from the photodetector (PD) is split in two by means of a 3-dB RF splitter. One of the signals is sent to the comparator and the other is sent to the scope. By comparing the digital value obtained with the chip and the input value measured with the scope, we can quantify the performance of the comparator. Note that this measurement assumes the oscilloscope as a reference device, but this equivalent to putting the scope's noise in the signal, making the measurement conservative.

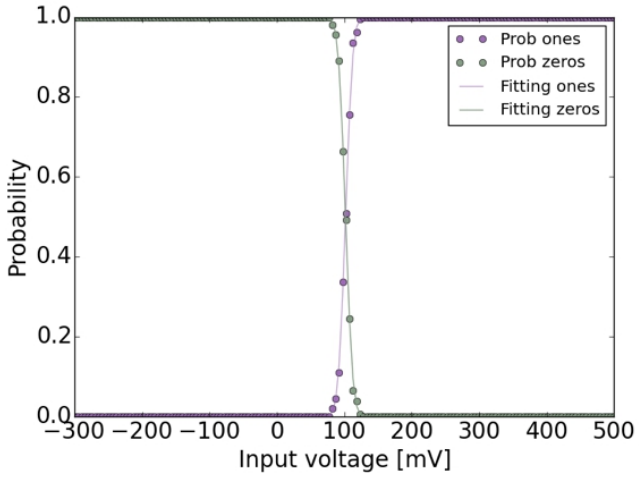
all about the circuit.

We now describe the measurement setup, as shown in Fig. 4.8. We use a 3 dB splitter (Mini-Circuits ZFRSC-183-S+) after the photodetector in order to get two copies of the output analogue random amplitude v_1 and v_2. We send v_1 to the comparator input and v_2 to the oscilloscope, which also records the output of the first flip-flop, i.e. the comparator output latched exactly at the same point the oscilloscope is sampling. In order to match the sampling points of the oscilloscope and the flip-flop, we sweep the scope's sampling point in steps of 10 ps until we find the best agreement - see Fig. 4.9(a). Note that having a mismatch in the sampling between the comparator and the scope leads to an incorrect characterisation of the digitisation errors. The closer the sampling points, the more accurate the result. Once the optimal sampling point is found, we can calculate which is the probability of obtaining a zero or a one, conditioned on the input value as measured by the scope - see Fig. (4.9(b)). We calculate $P(d = x|v_2)$ for $x \in \{0, 1\}$, finding a small but finite region in which near the threshold region, as expected, in which the same input analogue voltages give rise to different digital outputs.

Note that the characterisation of the digitisation noise suffers from



(a) Detuning



(b) Transition noise

Figure 4.9: (a) Probability of getting an output of zero or one for each input analogue voltage v_2, i.e. cumulative distribution function of the input signal. As observed, there is a small region near the threshold region in which input values can give zero or one with certain probabilities. The transition probability from $0 \to 1$ ($1 \to 0$) is in excellent agreement with the integral of a Gaussian variable with $\sigma_{v_{ref}} \leq 7.7$ mV. (b) Measured noise as a function of the detuning between the oscilloscope sampling time and the flip-flop sampling time. We emphasise that this measurement is conservative, as the measured error is necessarily larger than the real error.

some limitations. Ideally, we would need (i) the two outputs of the 3-dB splitter, as well as the impulse response of the comparator and the oscilloscope, to be identical, and (ii) as discussed above, the sampling point of the oscilloscope and flip-flop to be the same. In practice, unfortunately, (i) the two outputs of the 3-dB splitter are not identical (their difference is measured to be well described by a Gaussian distribution with zero mean and 1.32 mV RMS deviation), and (ii) the timing precision is limited to 10 ps. Note that the presence of both limitations are conservative from a measurement point of view, i.e., the real error will always be smaller than the measured error. The narrowest observed transition is depicted in Fig. (4.8), and shows an RMS width of 8.4 mV. Considering that the oscilloscope noise is 3.4 mV RMS, we can place an upper limit $v_{ref} \leq 7.7$ mV. In Fig. (4.9(b)), we depict the measured probabilities as well as the cumulative distribution function of a Gaussian variable with $\sigma = 7.7$ mV, showing excellent agreement with the observations.

4.3.3 Hangover noise

To measure the hangover errors, we periodically interrupt the modulation of the LD using an RF switch (Mini- Circuits ZASWA-2-50DR+) at 10 MHz. This generates a train of optical pulses at the output of the laser. Due to the relative path difference in the interferometer, three different types of pulses emerge: (i) the first output pulse, which contains only a short-path contribution and experiences no interference, (ii) the intermediate pulses, which contain both short and long-path contributions and show interference and (iii) the last pulse, which contains only a long-path contribution and, thus, shows no interference. This last pulse also contains any delayed response, i.e. “hangover” from previous pulses. By measuring the statistical behaviour of this last pulse, and comparing it with the long-path signal obtained by blocking the short-path, we can recover the contribution from hangover errors. This is illustrated in Fig. (4.10), which shows a train of nine optical pulses. In the experiment, trains of ten pulses were used.

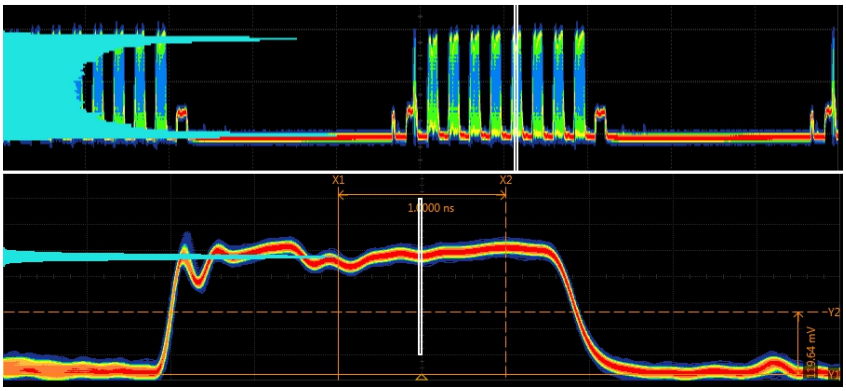


Figure 4.10: Measurement of "hangover error." Upper image shows persistence mode oscilloscope trace of trains of 9 optical pulses giving rise to 8 strongly interfering pulses followed by one pulse without interference, shown in higher resolution in the lower image. Pulse repetition period is 5 ns. Teal histograms on left vertical axis show data sampled in the region defined by the white cursors. "Hangover," i.e., remaining variation from previous pulses, is visible at the start of the lower trace, and decreases approaching the sampled point.

4.3.4 Deriving the bounds from the observed noises

By using Eq. (4.10) we can estimate the predictability of the source after combining the parity of k bits. However, an upper bound on the predictability of the raw bits, ϵ_{max}, is required. In order to estimate ϵ_{max}, which accounts for the worst-case instantaneous effect that can be observed at a single-bit level (i.e. the worst-case predictability of a single bit), we take the largest of Eqs. (4.8-4.9) based on the metrological measurements obtained in the previous section. This can be written simply as

$$\epsilon_{max} = \frac{2}{\pi} \max_{\{|v_c|, \Delta v_\phi\}} \arcsin \sqrt{\frac{1}{2} + \frac{|v_c|}{2\Delta v_\phi}}, \tag{4.28}$$

and corresponds to finding the largest possible value of the untrusted noises $\max |v_c|$ and the smallest value of $\Delta v_\phi = 2\mathcal{V}\sqrt{v_s v_l}$.

Maximising $|v_c|$

In order to maximise the instantaneous effect, we will replace $|v_c|$ in Eq. (4.28) with $\langle|v_c|\rangle + \kappa\sigma_{v_c}$, where $\langle|v_c|\rangle$ is the average value of the untrusted noises, σ_{v_c} is the combined standard deviation, and κ, a free parameter, specifies the frequency of events that will fall outside of the defined range. For $\kappa = 6$, for instance, it represents a 6σ confidence level on the derived estimate, or equivalently that 1 out of every ~ 500000000 events will be outside of the range. We calculate $\langle v_c\rangle$ from Eq. (4.9), finding

$$\langle v_c \rangle = 2\Delta v_\phi[\langle \sin^2 \pi P(d=1)/2\rangle - 1/2] \tag{4.29}$$

$$\approx 2\Delta v_\phi[\sin^2 \pi\langle P(d=1)\rangle/2 - 1/2], \tag{4.30}$$

where the approximation of $\langle \sin^2(P(d=1)\pi/2)$ is justified in light of the fact that $|v_c| << \Delta v_\phi$. We measure $\langle P(d=1)\rangle = 0.50035$, and therefore find directly $\langle v_c\rangle = 3.0$ mV. For the RMS deviation σ_{v_c}, since we cannot measure it directly, we consider three levels of distrust of the equipment, which we name as "ordinary," "digitiser paranoid" and "fully paranoid." In all cases, the noises are individually described by the measured statistics in Table 4.1, but their assumed correlations vary. In ordinary distrust, we make the physically reasonable assumption that the noise sources are uncorrelated. In digitiser paranoid distrust, we assume that the comparator, the only nonlinear element of the signal chain, chooses v_{ref} in function of the other noises in order to maximise the predictability. In fully paranoid distrust, we assume that all noise sources are collaborating to maximise predictability. We can write these different scenarios as,

$$\text{(ordinary)} \qquad \sigma_{v_c} = \sqrt{\sum_i \sigma_i^2} \tag{4.31}$$

$$\text{(digitiser paranoid)} \qquad \sigma_{v_c} = \sigma_{v_{ref}} + \sqrt{\sum_{i\,\notin v_{ref}} \sigma_i^2} \tag{4.32}$$

$$\text{(fully paranoid)} \qquad \sigma_{v_c} = \sum_i \sigma_i \tag{4.33}$$

where the summation is performed over all the untrusted noises and σ_i represents the RMS deviation of each independently characterised noise.

Distrust level	Noise σ_{v_c}	ϵ^4_{max} (26 ns)	ϵ^6_{max} (36 ns)
Ordinary	8.6 mV	2.5×10^{-5}	1.3×10^{-7}
Dig. par.	11.7 mV	8.6×10^{-5}	8.0×10^{-7}
Fully par.	14.5 mV	2.0×10^{-4}	2.9×10^{-6}

Table 4.2: Noise and predictability for different trust scenarios. All predictabilities are given for a 6σ confidence level. Times in parentheses indicate freshness time $\tau_f^{(k)}$. See text for details.

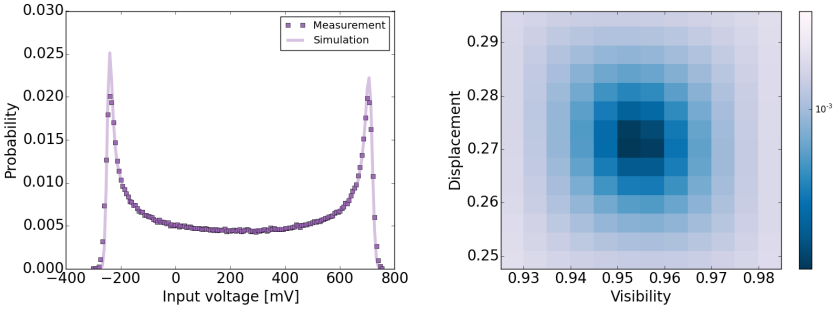
These assumptions lead to normally-distributed v_c with RMS deviations shown in Table 4.2. Fluctuations in v_c are, in principle, unbounded but rarely exceed a few standard deviations, a situation that is captured by assigning confidence bounds, in this case to $\mathcal{P}(d)$ and $\mathcal{P}(x)$. In the case of the numbers depicted in Table 4.2, $\kappa = 6$ is used. Noise fluctuations will produce a fraction $P_{6\sigma}$ of the raw bits with $\epsilon > \epsilon_{max}$, where $P_{6\sigma} \approx 2 \times 10^{-9}$. The excess predictability of the extracted bit exceeds ϵ^k_{max} at most this often, even assuming maximally correlated raw-bit excess predictability.

Minimising $\Delta v_\phi = 2\mathcal{V}\sqrt{v_s v_l}$

To minimise this expression, we first need to estimate $\mathcal{V}$. We do so by following a Monte Carlo approach based on Eq. (4.2). By using the knowledge acquired during the characterisation of our equipment, we can write the interference process as a function of the interference visibility $\mathcal{V}$ only, i.e. we can write Eq. (4.2) as

$$f(\mathcal{V}) = v_s + v_l + \mathcal{V}\sqrt{v_s v_l}\cos\Delta\phi + v_H + v_{PD}, \tag{4.34}$$

where $v_s(t)$ and $v_l(t)$ represent the long and short path signals of the interferometer, respectively, $\Delta\phi$ the phase difference between subsequent optical pulses, v_H the hangover errors, and v_{PD} the photodetector noise signal. From the metrological characterisation, we find that all the variables described in this equation, except for $\mathcal{V}$ and $\Delta\phi$, can be described by normal distributions with measurable parameters. We run a Monte Carlo numerical simulation sweeping the unknown value of $\mathcal{V}$ from $0.8 \cdots 1$ in steps of 0.05, while setting the rest of the noise variables to normal distributions with the parameters given in Table 4.1. In the case of $\Delta\phi$, we use



(a) Histogram **(b)** LSQ error

Figure 4.11: Measured and simulated distributions for the accelerated phase diffusion process. (a) Measured histogram with the least square error Monte Carlo simulation in shaded points. (b) Least square error calculated after sweeping the visibility parameter. A secondary free parameter is introduced in the fitting procedure to account for mean value displacement along the voltage axis.

a normal random process also with a standard deviation $\gg 3$, in agreement with the phase diffusion measurements depicted in Fig. (4.3). In every Monte Carlo step, we accumulate 10 Mb of data. We then calculate the resulting histogram, and, finally, we calculate the deviation between the simulated histogram and the measured histogram. The result with the best fit is obtained for $\mathcal{V}^{(LSE)} = 0.955$. The least-square-error for the sweeping step and the resulting histogram can be seen in Fig. (4.11).

Finally, in the term $\sqrt{v_s v_l}$ in Eq. (4.34) we use $v_s \to \langle v_s \rangle$ and $v_l \to \langle v_l \rangle$. To correct for fluctuations in these two terms with a confidence of $\kappa = 6$ we multiply by the correction factor, finding

$$\sqrt{1 - 6\sigma_{v_s}/\langle v_s \rangle}\sqrt{1 - 6\sigma_{v_l}/\langle v_l \rangle} \approx 0.971$$

4.4 Statistical analysis

Although no output test of the output can assure randomness, tests can, nonetheless, detect failures. In this section, we follow two strategies for

such testing. First, we compute the autocorrelation of the data. Second, we apply standard batteries of statistical tests. Several statistical batteries are used to test the quality of the output, including the TestU01 Alphabit battery (L'Ecuyer et al., 2007), the NIST SP800-22 battery (Rukhin et al., 2010), and the Dieharder battery (Brown, 2016; Marsaglia, 1985). The results are consistent with ideal randomness for k = 3 and above. Due to the high output rate of the RNG, testing is limited by computation speed for the various tests. In this respect, Alphabit has a significant advantage, as it was designed for testing physical RNGs, without the more computationally-intensive tests used for pseudo random number generators. For example, testing a 1.5 Gb sequence with the NIST battery takes more than 3 hours on a desktop computer whereas the Alphabit battery takes one minute.

Autocorrelation

Because of the low computational capacity of physical RNGs, imperfections are expected mostly in low-order correlations, as shown in Fig (4.12). We use the unbiased estimator for the autocorrelation of the extracted output

$$\Gamma_x(k) = \langle x_i x_{i+k} \rangle - \langle x_i \rangle^2. \tag{4.35}$$

Considering the output of the RE, with $x_i = x_{i-1} \oplus d_i$, where d_i are raw bits, we note that x can be described as a symmetric two-state machine that changes state whenever $d = 1$. By using this property, and as detailed in Box 8, we find a closed upper bound form for the correlation, given by

$$\Gamma_x(k) \leq \frac{1}{4} \epsilon_{max}^k, \tag{4.36}$$

and, therefore, the next-bit correlation coefficients decay to expected behaviour exponentially in k. Also, note that the values of the correlation coefficients are directly related to the bias; the larger the bias, the larger the correlation. In Fig. (4.13a) we show the next-bit correlation coefficient ($d = 1$) for a dataset using different values of extraction depth k, clearly showing the exponential decay for increasing k. Then, in Fig. (4.13b), we show the autocorrelation for a data set of 1 Tb for $k = 4$, showing calculated values within the statistical sensitivity up to a correlation distance of

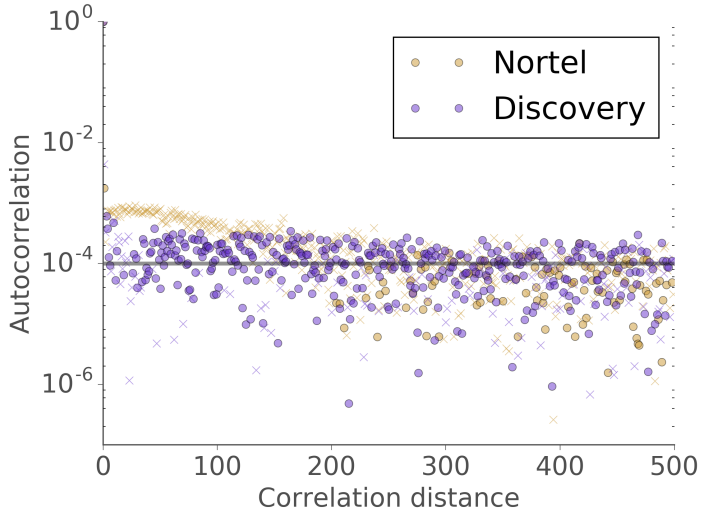
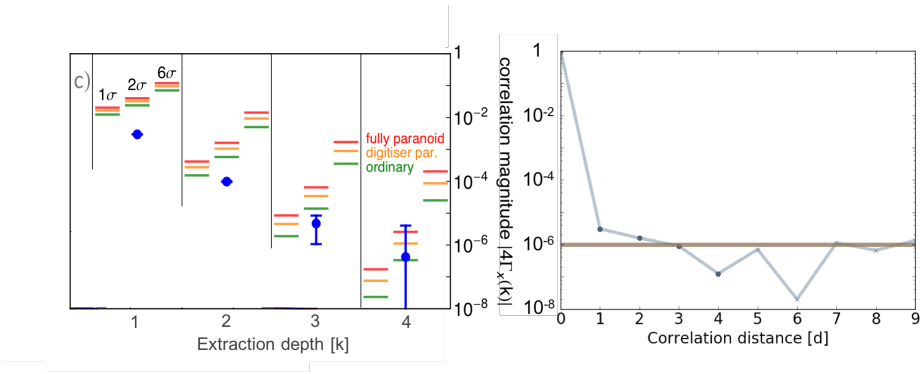


Figure 4.12: Autocorrelation of the raw data for two high-bandwidth photodetectors. As observed, for exactly the same input signal, the Nortel photodetector (orange dots) shows a relatively long positive correlation coefficient that vanishes to the statistical noise level after $d = 200$. In contrast, for exactly the same input signal, the discovery photodetector (purple dots) falls within the statistical level much quicker. Thus, the correlation is not on the optical signal, but, rather, it is a memory effect of the photodetector. We attribute the larger correlation in the Nortel photodetector to long-lived states. A sample size of 100 Mb is used for both measurements, leading to a statistical noise level of 10^{-4}. The noise level is shown as a grey line.

$d = 9$. The statistical sensitivity for such a large dataset is $\sim 10^{-6}$. Finally, in Fig. (4.14), we take the same 1 Tb dataset but instead of computing the correlation for the whole sequence, we split it into $1,000$ sequences of 1 Gb each, and study the distribution function of the correlation coefficients. For an ideal random sequence, we expect all these distributions to be normally distributed with zero mean and standard deviation given by the statistical sensitivity (3.16×10^{-5} for 1 Gb sequences). All corre-



b) Correlation and derived bounds

a) 1 Tb correlation for k=4

Figure 4.13: Autocorrelation data obtained from the output of the prototypes. (a) Comparison between derived correlation bounds from the metrological characterisation and the calculated correlation coefficients for several extraction depths. As observed, the calculated correlations are below the derived bounds, showing the very conservative nature of the randomness metrology procedure. (b) Autocorrelation calculated with a long dataset of 1 Tb for extraction depth $k = 4$. All coefficients are within the statistical sensitivity.

lation coefficients pass the normality test from the SciPy library (Python), based on the D'Agostino and Pearson tests (R. B. D'Agostino, 1971; R. D'Agostino et al., 1973).

Box 8. Autocorrelation of a two-state machine

By using the correlation estimator

$$\Gamma_x(k) = \langle x_i x_{i+k} \rangle - \langle x_i \rangle^2 \tag{4.37}$$

and letting $x_i = x_{i-1} \oplus d_i$ be the output of a two-state machine, with d_i being the new input value at time i, we will calculate here an expression for the correlation based on the predictability of the raw data $\max[P(d=0), P(d=1)] < \frac{1}{2}(1+\epsilon_{max})$.

From Eq. (4.37), we note that the term $\langle x_i x_{i+k} \rangle$ is only different from zero for $x_i = 1$ and $x_{i+k} = 1$. In the case of our two-state machine, this

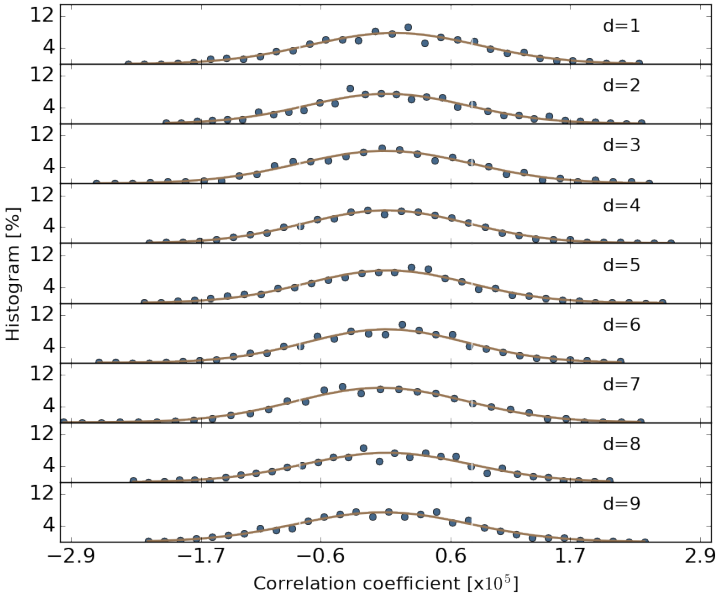


Figure 4.14: Distribution function of the autocorrelation coefficients evaluated from the computation of 1000 datasets of 1 Gb each. All coefficients are distributed according to normal statistics, as expected from a random sequence. All correlation coefficients pass normality tests.

situation corresponds to having an even number of transitions between i and $i+k$, or equivalently, and even number of input values equal to 1, i.e:

$$P(x_i = 1 \cap x_{i+k} = 1) = P(x_i = 1 | x_{i+k} = 1) P(x_{i+k} = 1)$$
$$= \frac{1}{2} \sum_{j=0}^{\lfloor k/2 \rfloor} \binom{k}{2j} P(d=1)^{2j} P(d=0)^{k-2j}.$$

Let us assume that the predictability of the raw data is $P(d=0) = \frac{1}{2}(1+$

ϵ_{max}). We find:

$$P(x_i = 1 \cap x_{i+k} = 1) \leq \frac{1}{2} \sum_{j=0}^{\lfloor k/2 \rfloor} \binom{k}{2j} (\frac{1}{2} - \epsilon_{max})^{2j} (\frac{1}{2} + \epsilon_{max})^{k-2j}$$

Then, by using the fact that:

$$\sum_{j=0}^{\lfloor k/2 \rfloor} \binom{k}{2j} p^{2j} (1-p)^{k-2j} = \frac{1}{2}\Big(1 + (1-2p)^k\Big), \tag{4.38}$$

and using that $p = \frac{1}{2}(1 - \epsilon_{max})$, we get to

$$P(x_i = 1 \cap x_{i+k} = 1) \leq \frac{1}{4}(1 + \epsilon_{max}^k).$$

Finally, if we substitute this into Eq. (4.37), using also the fact that $\langle x_i \rangle^2 = 1/4$ by definition (the two-state machine is unbiased), we get the simple expression for the autocorrelation

$$\Gamma_x(k) \leq \frac{1}{4} \epsilon_{max}^k \tag{4.39}$$

4.4.1 NIST SP800-22 battery of statistical tests

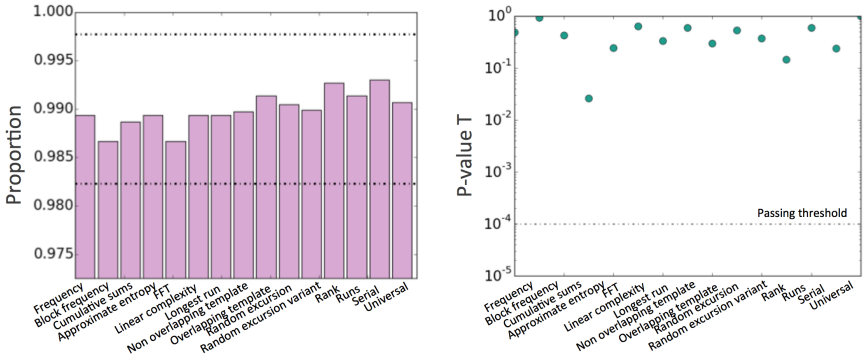
As per NIST recommendations (Rukhin et al., 2010), we use 1500 sequences of 1 Mb each to assess the random numbers generated by the device. The tested sequences pass both the proportion and uniformity of the p-values assessments - see Fig. (4.15).

4.4.2 Dieharder battery of statistical tests

We run the Dieharder test with default settings. Results are shown in Table 4.3.

Test name	N tuple	t samples	p samples	p-value	Res.
diehard birthdays	0	100	100	0.869	P
diehard operm5	0	1000000	100	0.627	P
diehard rank 32x32	0	40000	100	0.491	P
diehard rank 6x8	0	100000	100	0.469	P
diehard bitstream	0	2097152	100	0.949	P
diehard opso	0	2097152	100	0.412	P
diehard oqso	0	2097152	100	0.491	P
diehard dna	0	2097152	100	0.782	P
diehard count 1sstr	0	256000	100	0.595	P
diehard count 1sbyt	0	256000	100	0.441	P
diehard parking lot	0	12000	100	0.996	W
diehard 2dsphere	2	8000	100	0.936	P
diehard 3dsphere	3	4000	100	0.941	P
diehard squeeze	0	100000	100	0.587	P
diehard sums	0	100	100	0.761	P
diehard runs	0	100000	100	0.120	P
diehard runs	0	100000	100	0.517	P
diehard craps	0	200000	100	0.862	P
diehard craps	0	200000	100	0.970	P
Marsag. tsang gcd	0	10000000	100	0.681	P
Marsag. tsang gcd	0	10000000	100	0.208	P
sts monobit	1	100000	100	0.153	P
sts runs	2	100000	100	0.800	P
sts serial	1 . . . 16	100000	100	0.120 − −0.987	P
rgb bitdist	1 . . . 12	100000	100	0.076 − −0.960	P
rgb minimum dist.	2	10000	1000	0.194	P
rgb minimum dist.	3	10000	1000	0.459	P
rgb minimum dist.	4	10000	1000	0.540	P
rgb minimum dist.	5	10000	1000	0.829	P
rgb permutations	2	100000	100	0.592	P
rgb permutations	3	100000	100	0.773	P
rgb permutations	4	100000	100	0.985	P
rgb permutations	5	100000	100	0.478	P
rgb lagged sum	0 . . . 32	1000000	100	0.114 − −0.993	P
rgb kstest test	0	10000	1000	0.814	P
dab bytedistrib	0	51200000	1	0.459	P
dab dct	256	50000	1	0.805	P
dab filltree	32	15000000	1	0.227	P
dab filltree	32	15000000	1	0.612	P
dab filltree2	0	5000000	1	0.188	P
dab filltree2	1	5000000	1	0.490	P
dab monobit2	12	65000000	1	0.437	P

Table 4.3: Summary of results for the entire Dieharder battery for k=3. In column `n tuple`, the notation $1 \ldots x$ indicates that the test was repeated with the `n tuple` setting covering this range. As shown, the parking lot test showed a weak value, i.e., an inconclusive result, in the initial run. For an ideal source, it is expected that $\sim$ one weak value will appear in any given full test run of the suite. As recommended, we re-ran the weak test with the option `-Y`, which increases `p samples` until a clear result (passed or failed) emerged. The test was passed. In the table we rounded the p-values to the third digit precision. Also P=Passed and W=Weak.



(a) Proportion test **(b)** Uniformity of p-values test

Figure 4.15: Summary of results for the NIST SP800-22 battery. (a) Results for the proportion test, i.e. evaluating how many times each test passes or fails (note that even a perfect random number generator is supposed to fail some tests from time to time). Dot-dash lines indicate limits of acceptable behaviour as recommended by NIST SP800-22. (b) Uniformity of the p-values assessment, which mainly quantifies how the outcomes of each statistic (p-values) are distributed along the (0,1) range. Both quantities satisfy the statistics for a perfect random number generator.

4.4.3 Alphabit battery of statistical tests (TestU01)

We use the Alphabit battery following two testing strategies: (i) test many different sequences of a relatively small size, e.g. 300 files of 1 Gb each, and (ii) testing very long sequences, e.g. one file containing 1 Tb. Using (i), we can quantify how often the generator fails the Alphabit battery. This is important because an ideal random number generator should fail with around 0.2% probability for a significance level of 10^{-3}. With (ii) we can test for weaker correlations/anomalies, below the statistical uncertainty of strategy (i). For each test, a p-value p is computed and its deviation from zero or one $\Delta(p) = \min 1-p, p$ is measured. If $\Delta(p) \geq 10^{-2}$ the test is considered to pass that statistic. In contrast, a test is considered inconclusive or weak when its deviation is $10^{-2} > \Delta(p) \geq 10^{-6}$, failed when $10^{-6} > \Delta(p) \geq 10^{-15}$, "eps," (which implies catastrophic failure),

when $10^{-15} > \Delta(p) \geq 10^{-300}$, and "eps2" when $\Delta(p) < 10^{-300}$.

Results for strategy (i) are depicted in Fig. (4.16) and Fig. (4.17). We tested 1 Mb for $k = 1$, 120 Mb for $k = 2$, 500 Mb for $k = 3$, and 1 Gb for $k = 4$. In each case, we tested 300 sequences. For strategy (ii) we tested a single 1 Tb file, two 500 Gb files, one 80 Gb file, and two 64 Gb file for $k = 3$ and all tests were passed. For evaluating the results, we followed the same criteria for evaluating the results as in (Jakobsson, 2014), in which regularities in commercial RNG systems were found for 64 Gb and above.

4.5 Conclusion

In this chapter, we have reported the design and prototyping of a random number generation device to meet the stringent requirements of so-called loophole-free Bell test experiments. We combined an ultrafast phase diffusion source of raw bit generation with randomness metrology and real-time parity bit randomness extraction directly on board with basic electronic components. By doing so, we were able to demonstrate the generation of random numbers with unpredictability bounds below 10^{-5} in less than 30 ns, even when being extremely paranoid about the untrusted noises. The devices reported in this chapter played a fundamental role in the strongest refutation to date of a local realistic worldview, thereby confirming the nonlocal and unpredictable nature of the universe, in agreement with the predictions of quantum mechanics.

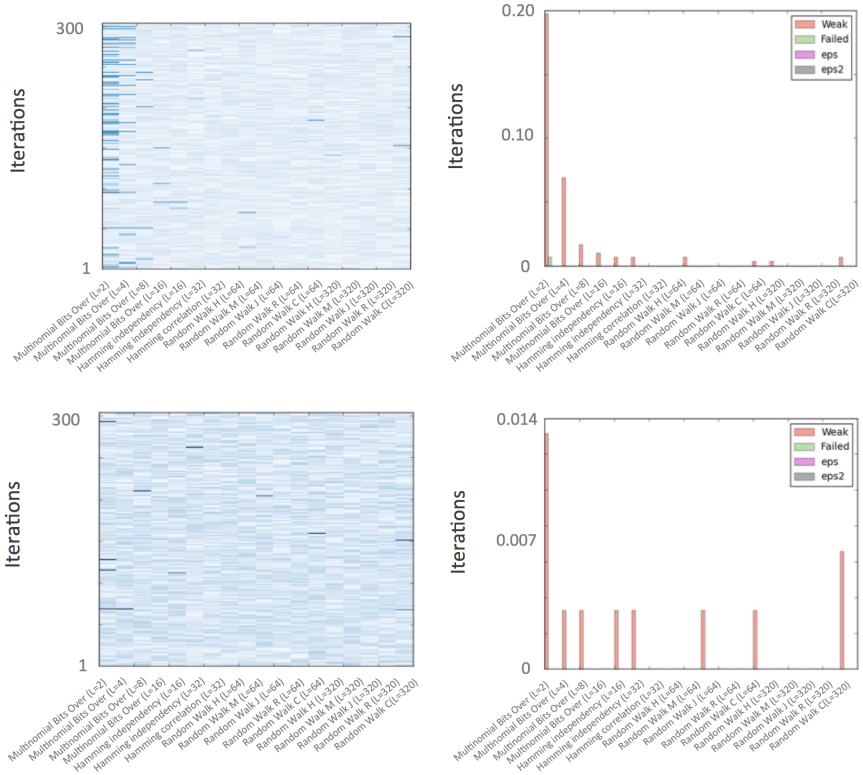


Figure 4.16: Alphabit battery of statistical tests for $k = 1$ (top) and $k = 2$ (bottom). Left: Results for each of the 17 tests (horizontal axis) in the Alphabit battery for 300 iterations (vertical axis). A dark blue square representing a weak value is observed for that particular iteration and test. Right: Frequency of obtaining weak, failed, eps, and eps2 p-values for each of the 17 tests of the Alphabit battery. As shown, for $k = 1$ the Alphabit battery is able to find statistically significant anomalies, indicating the need for randomness extraction.

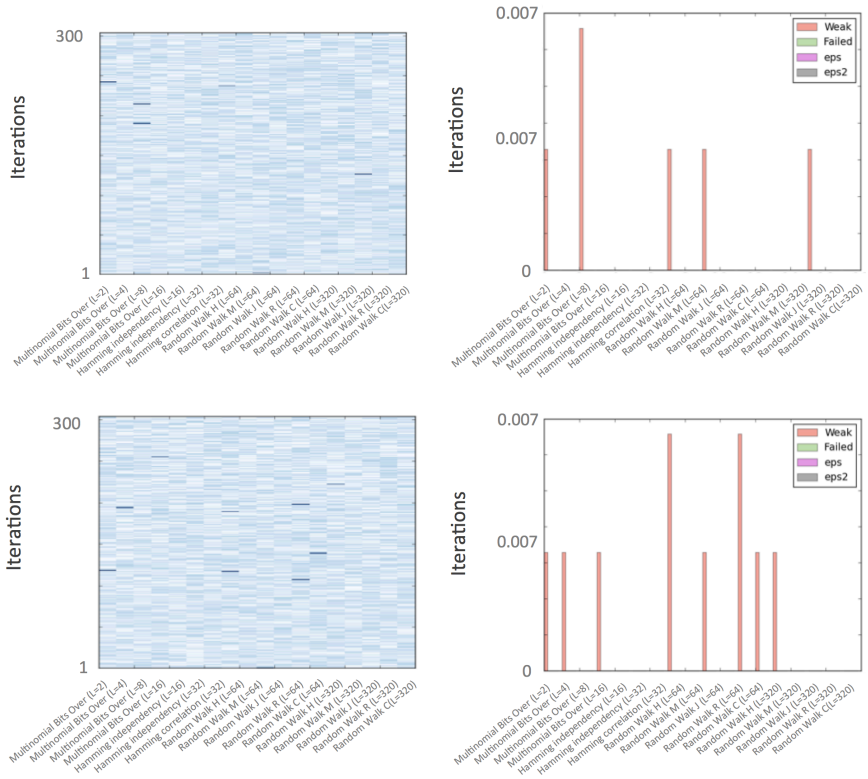


Figure 4.17: Alphabit battery of statistical tests tests for $k = 3$ (top) and $k = 4$ (bottom). Left: Results for each of the 17 tests (horizontal axis) in the Alphabit battery for 300 iterations (vertical axis). A dark blue square representing a weak value is observed for that particular iteration and test. Right: Frequency of obtaining weak, failed, eps, and eps2 p-values for each of the 17 tests of the Alphabit battery. As shown, for $k = 1$ (Fig. 4.16), the Alphabit battery is able to find statistically significant anomalies, indicating the need for randomness extraction.

Chapter 5

Conclusions and Outlook

Random numbers are a key ingredient to keep the wheel of the information era turning. They are used in randomised algorithms, in Monte Carlo methods, in data transmission protocols, in gambling, and in cryptography, among many other applications. While, strictly speaking, random numbers can only be obtained by measuring a quantum mechanical process, multiple workarounds have been developed over the years due to the unavailability of high-speed and scalable quantum technologies. In this thesis, we have reported progress towards the development of a miniature and scalable quantum random number generation technology for high-speed operation and with high-quality guarantees.

We have, firstly, thoroughly studied the accelerated phase diffusion dynamics in pulsed semiconductor lasers in connection with quantum random number generation. By using components from the telecommunications industry, we have demonstrated the validity of the process at bit rates exceeding 40 Gb/s. Besides being a record speed in quantum random number generation at the time of publication, the most important finding is that the dynamics of the intracavity field in a pulsed commercial laser are capable of achieving full phase randomisation in the order of the 100 ps timescale.

We then dedicated a significant effort towards the implementation and miniaturisation of the technology, firstly, on the development of prototypes for use in supercomputation and research. Up to eight different prototypes were built, one of them being tested and validated by supercomputer nu-

merical simulation researchers in the field of nuclear fission science. The other prototypes were designed to meet the stringent requirements of the so-called loophole-free Bell test experiments of local realism. In addition to building technologies and validating them in real environments, we also showed progress towards chip-level integration using photonic integrated circuits, paving the way for mass scale production of quantum devices. Initially, we demonstrated an all optically integrated quantum entropy source on an Indium Phosphide chip. Then, the integration of the critical interferometric and detection steps of the phase diffusion scheme on a Silicon-based Photonic platform, the most advanced semiconductor industry.

Last but not least, we also introduced the randomness metrology methodology, a set of techniques to characterise and derive quantitative estimates on the unpredictability of physical random number generators. Starting from a theoretical model of the process, and following this with a careful characterisation of the hardware components, we have proved that pure randomness can be extracted even under paranoid considerations about the untrusted noises. The randomness metrology has the potential to become a useful tool for random number generation designers, as well as for the development of new regulations and certifications required to validate the next generation of random number generators.

5.1 Outlook

Randomness is a fascinating topic, and a great deal of research and development is constantly ongoing at both the academia and the industrial levels. Following on strictly from the results of this thesis, there are some interesting research lines to pursue in the future. Examples include the exploration of the average phase diffusion rate when going down to the tenths of picoseconds scale (or even below), and the development of a general framework for the randomness metrology methodology and its application in multiple generators. Another example is the packaging of the integrated chips reported in chapter 3, which, in the case of Silicon, requires the development of an hybrid packaging or hybrid fabrication technique for integrating the laser source.

More generally, the field of quantum randomness generation now has

two well differentiated dynamics. One of them is more industrially oriented, and is focused on developing tiny devices that can be mass-produced and integrated into general-purpose communication and computation devices. Quantum random number generation has the potential to become the first mass-market application of the so-called second quantum revolution, and lots of efforts is being made in this direction. The other principle research line, which is more present in academia, is the development of so-called device-independent (DI) and self-testing (ST) random number generation technologies. In these schemes, entangled states and the nonlocal properties of certain quantum states are used to produce and certify quantum digits. DI-RNGs allows for the generation of random digits even in extremely paranoid scenarios. This is achieved through a loophole-free violation of a Bell inequality, and has significant interest for fundamental research. Alternatively, ST-RNG technology allows for a new generation of devices in which entropy estimates can be derived directly from the observation of a so-called witness, i.e. a property of the quantum system that prove the quantum mechanical nature of the process. In these circumstances, entropy estimates can be derived without a full characterisation of the device, making the process arguably simpler. However, the functioning of the device needs to be trusted, and as a result, ST-RNG technology offers similar security guarantees to a trusted and characterised device. In addition, both DI-RNGs and ST-RNGs necessitate raw randomness in order to select the measurement or state preparation basis, thus requiring a random number generator with such metrological assurances as the ones proposed in this thesis.

Bibliography

Abellan, C.: “Quantum random number generation based on vacuum field fluctuations” (Sept. 2013). url: http://hdl.handle.net/2099.1/19148

Abellan, C., W. Amaya, D. Domenech, P. Muñoz, J. Capmany, S. Longhi, M. Mitchell, and V. Pruneri: “Quantum entropy source on an InP photonic integrated circuit for random number generation”. *Optica* **3**, 9, 989–994 (2016). doi: 10.1364/OPTICA.3.000989

Abellan, C., W. Amaya, M. Jofre, M. Curty, A. Acin, J. Capmany, V. Pruneri, and M. W. Mitchell: “Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode”. *Optics express* **22**, 2, 1645–1654 (2014). doi: 10.1364/OE.22.001645

Abellan, C., W. Amaya, M. Jofre, M. Curty, A. Acin, V. Capmany J. Pruneri, and M. W. Mitchell: “Ultrafast quantum random number generation using off-the-shelf components”. *2014 Conference on Lasers and Electro-Optics (CLEO) - Laser Science to Photonic Applications*. June 2014, 1–2. doi: 10.1364/CLEO_AT.2014.AW3P.2

Abellan, C., W. Amaya, and M. W. Mitchell: “Un test de Bell sin escapatorias”. *Investigacón y Ciencia* **472**. Panorama (Jan. 2016)

Abellan, C., W. Amaya, M. W. Mitchell, and V. Pruneri: “Toward an Optically-Integrated Quantum Random Number Generator”. *2015 European Conference on Lasers and Electro-Optics - European Quantum Electronics Conference*. Optical Society of America, 2015, url: http://www.osapublishing.org/abstract.cfm?URI=CLEO_Europe-2015-JSV_4_3

Abellan, C., W. Amaya, D. Mitrani, V. Pruneri, and M. W. Mitchell: “Generation of fresh and pure random numbers for loophole-free Bell tests”.

Phys. Rev. Lett. **115**, 25, 250403 (2015). doi: 10.1103/PhysRevLett.115.250403

Abellan, C., J. Tura, M. Garcia, F. Beduini, A. Hirschmann, V. Pruneri, A. Acin, M. Marti, and M. W. Mitchell: "Game, cloud architecture and outreach for The BIG Bell Test." Vol. Volume 62, Number 4. American Physical Society, Mar. 2017. url: http://meetings.aps.org/Meeting/MAR17/Session/V27.7

Abellan, C. et al.: "Challenging local realism with human choices". *Nature* **557**, 212–216 (2018). doi: 10.1038/s41586-018-0085-3

Adler, R.: "A study of locking phenomena in oscillators". *Proceedings of the IRE*. Vol. 34. IEEE, 1946, 351–357. doi: 10.1109/JRPROC.1946.229930

Agrawal, G. P. and R. Roy: "Effect of injection-current fluctuations on the spectral linewidth of semiconductor lasers". *Phys. Rev. A* **37**, 7, 2495–2501 (1988). doi: 10.1103/PhysRevA.37.2495

Ahmad, D.: "Two Years of Broken Crypto: Debian's Dress Rehearsal for a Global PKI Compromise". *IEEE Security & Privacy* **6**, 5, 70–73 (2008). doi: 10.1109/MSP.2008.131

Alduino, A., L. Liao, R. Jones, M. Morse, B. Kim, W.-Z. Lo, J. Basak, B. Koch, H.-F. Liu, H. Rong, M. Sysak, C. Krause, R. Saba, D. Lazar, L. Horwitz, R. Bar, S. Litski, A. Liu, K. Sullivan, O. Dosunmu, N. Na, T. Yin, F. Haubensack, I.-w. Hsieh, J. Heck, R. Beatty, H. Park, J. Bovington, S. Lee, H. Nguyen, H. Au, K. Nguyen, P. Merani, M. Hakami, and M. Paniccia: "Demonstration of a High Speed 4-Channel Integrated Silicon Photonics WDM Link with Hybrid Silicon Lasers". *Integrated Photonics Research, Silicon and Nanophotonics and Photonics in Switching*. Optical Society of America, 2010, PDIWI5. doi: 10.1364/IPRSN.2010.PDIWI5

Balle, S., N. B. Abraham, P. Colet, and M. San Miguel: "Parametric dependence of stochastic frequency variations in the gain switching of a single-mode laser diode". *IEEE Journal of Quantum Electronics* **29**, 1, 33–41 (Jan. 1993). issn: 0018-9197. doi: 10.1109/3.199242

Balle, S., R. Banerjee, and M. San Miguel: "Effects of an intensity-dependent linewidth enhancement factor on the transient spectral properties of a gain-switched single-mode semiconductor laser". *IEEE Photonics*

Technology Letters **5**, 5, 503–506 (May 1993). issn: 1041-1135. doi: 10.1109/68.215262

Balle, S., P. Colet, and M. San Miguel: "Statistics for the transient response of single-mode semiconductor laser gain switching". *Phys. Rev. A* **43**, 498–506 (1 Jan. 1991). doi: 10.1103/PhysRevA.43.498

Bernstein, D. J., J. Buchmann, and E. Dahmen: *Post-quantum cryptography*. Berlin, Heidelberg, 2009. doi: 10.1007/978-3-540-88702-7

Blum, M.: "Independent Unbiased Coin Flips From A Correlated Biased Source: A Finite State Markov Chain". *25th Annual Symposium on-Foundations of Computer Science, 1984.* Oct. 1984, 425–433. doi: 10.1109/SFCS.1984.715944

Blum, M. and S. Micali: "How to generate cryptographically strong sequences of pseudo random bits". *23rd Annual Symposium on Foundations of Computer Science (sfcs 1982)*. Nov. 1982, 112–117. doi: 10.1109/SFCS.1982.72

Brown, R. G.: "Dieharder: A random number test suite" (2016). url: https://webhome.phy.duke.edu/~rgb/General/dieharder.php

Chaitin, G. J.: "On the Simplicity and Speed of Programs for Computing Infinite Sets of Natural Numbers". *J. ACM* **16**, 3, 407–422 (July 1969). issn: 0004-5411. doi: 10.1145/321526.321530

Chambers, R. P.: "Random-number generation on digital computers". *IEEE Spectrum* **4**, 2, 48–56 (Feb. 1967). issn: 0018-9235. doi: 10.1109/MSPEC.1967.5216203

Chor, B. and O. Goldreich: "Unbiased bits from sources of weak randomness and probabilistic communication complexity". *SIAM J. Comput.* **17**, 2, 230–261 (Apr. 1988). doi: 10.1137/0217015

Church, A.: "On the concept of a random sequence". *Bull. Amer. Math. Soc.* **46**, 2, 130–135 (Feb. 1940). url: https://projecteuclid.org:443/euclid.bams/1183502434

Click, T. H., A. Liu, and G. A. Kaminski: "Quality of random number generators significantly affects results of Monte Carlo simulations for organic and biological systems". *Journal of Computational Chemistry* **32**, 3, 513–524 (2011). issn: 1096-987X. doi: 10.1002/jcc.21638

D'Agostino, R. B.: "An omnibus test of normality for moderate and large size samples". *Biometrika* **58**, 2, 341–348 (1971). doi: 10.1093/biomet/58.2.341

D'Agostino, R. and E. S. Pearson: "Tests for departure from normality. Empirical results for the distributions of b2 and √b1". *Biometrika* **60**, 3, 613–622 (1973). doi: 10.1093/biomet/60.3.613

Devos, F., P. Chavel, and P. Garda: "Optical generation of random-number arrays for on-chip massively parallel Monte Carlo cellular processors". *Opt. Lett.* **12**, 3, 152–154 (Mar. 1987). doi: 10.1364/OL.12.000152

Dynes, J. F., Z. L. Yuan, A. W. Sharpe, and A. J. Shields: "A high speed, postprocessing free, quantum random number generator". *Applied Physics Letters* **93**, 3, 031109 (2008). doi: 10.1063/1.2961000

Eckhardt, R.: "**Stan Ulam, John von Neumann, and the Monte Carlo Method**". *Stanislaw Ulam*. Los Alamos Science, 1987. url: http://la-science.lanl.gov/lascience15.shtml

Ferrenberg, A. M., D. P. Landau, and Y. Wong: "Monte Carlo simulations: Hidden errors from "good" random number generators". *Phys. Rev. Lett.* **69**, 3382–3384 (23 Dec. 1992). doi: 10.1103/PhysRevLett.69.3382

Fisher, R. A. and F. Yates: *Statistical tables for biological, agricultural and medical research*. Edinburgh: Oliver and Boyd, 1938. doi: 10.1002/bimj.19650070219

Fleming, M. W. and A. Mooradian: "Fundamental line broadening of single□mode (GaAl)As diode lasers". *Applied Physics Letters* **38**, 7, 511–513 (1981). doi: 10.1063/1.92434

Frauchiger, D., R. Renner, and M. Troyer: "True randomness from realistic quantum devices". *arxiv quant-ph* **1311.4547** (Nov. 2013). url: https://arxiv.org/abs/1311.4547

Fürst, H., H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer, and H. Weinfurter: "High speed optical quantum random number generation". *Opt. Express* **18**, 12, 13029–13037 (June 2010). doi: 10.1364/OE.18.013029

Gabriel, C., C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs: "A generator for unique quantum random numbers based on vacuum states". *Nature Photonics* **4**, 711–715 (Aug. 2010). doi: 10.1038/nphoton.2010.197

George, J., M. J, and S. B: "Dice game having truly random number generation". US Patent 3,592,473. 1971. url: http://www.google.com/patents/US3592473

Gisin, N., G. Ribordy, W. Tittel, and H. Zbinden: "Quantum cryptography". *Rev. Mod. Phys.* **74**, 145–195 (1 Mar. 2002). doi: 10.1103/RevModPhys.74.145

Giustina, M., M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-Å. Larsson, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin, B. Wittmann, and A. Zeilinger: "Significant-Loophole-Free Test of Bell's Theorem with Entangled Photons". *Phys. Rev. Lett.* **115**, 250401 (25 Dec. 2015). doi: 10.1103/PhysRevLett.115.250401

Goldberg, I. and D. Wagner: "Randomness and the Netscape browser". *Dr. Dobb's Journal*, 66–70 (1996)

Guo, H., W. Tang, Y. Liu, and W. Wei: "Truly random number generation based on measurement of phase noise of a laser". *Phys. Rev. E* **81**, 051137 (5 May 2010). doi: 10.1103/PhysRevE.81.051137

Handsteiner, J., A. S. Friedman, D. Rauch, J. Gallicchio, B. Liu, H. Hosp, J. Kofler, D. Bricher, M. Fink, C. Leung, A. Mark, H. T. Nguyen, I. Sanders, F. Steinlechner, R. Ursin, S. Wengerowsky, A. H. Guth, D. I. Kaiser, T. Scheidl, and A. Zeilinger: "Cosmic Bell Test: Measurement Settings from Milky Way Stars". *Phys. Rev. Lett.* **118**, 060401 (6 Feb. 2017). doi: 10.1103/PhysRevLett.118.060401

Haw, J. Y., S. M. Assad, A. M. Lance, N. H. Y. Ng, V. Sharma, P. K. Lam, and T. Symul: "Maximization of Extractable Randomness in a Quantum Random-Number Generator". *Physical Review Applied* **3**, 054004 (2015). doi: 10.1103/PhysRevApplied.3.054004

Heck, M., J. F. Bauters, M. L. Davenport, J. K. Doylend, S. Jain, G. Kurczveil, S. Srinivasan, Y. Tang, and J. E. Bowers: "Hybrid Silicon Photonic Integrated Circuit Technology". *IEEE Journal of Selected Topics in Quantum Electronics* **19**, 4, 6100117–6100117 (July 2013). issn: 1077-260X. doi: 10.1109/JSTQE.2012.2235413

Henry, C.: "Theory of the linewidth of semiconductor lasers". *IEEE Journal of Quantum Electronics* **18**, 2, 259–264 (Feb. 1982). issn: 0018-9197. doi: 10.1109/JQE.1982.1071522

Henry, C.: "Theory of the phase noise and power spectrum of a single mode injection laser". *IEEE Journal of Quantum Electronics* **19**, 9,

1391–1397 (Sept. 1983). issn: 0018-9197. doi: 10.1109/JQE.1983.1072058

Hensen, B., H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson: "Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres". *Nature* **526**, 682–686 (2015). doi: 10.1038/nature15759

Herrero-Collantes, M. and J. C. Garcia-Escartin: "Quantum random number generators". *Rev. Mod. Phys.* **89**, 015004 (1 Feb. 2017). doi: 10.1103/RevModPhys.89.015004

Hull, T. E. and A. R. Dobell: "Random Number Generators". *SIAM Review* **4**, 3, 230–254 (1962). doi: 10.1137/1004061

Inoue, H., H. Kumahora, Y. Yoshizawa, M. Ichimura, and O. Miyatake: "Random Numbers Generated by a Physical Device". *Journal of the Royal Statistical Society. Series C (Applied Statistics)* **32**, 2, 115–120 (1983). issn: 00359254, 14679876. url: http://www.jstor.org/stable/2347290

Isaksson, H.: "A Generator of Random Numbers". *Off-print of Teleteknik, Englesk Edition* **III**, 2 (1959)

Isida Masatuguand Ikeda, H.: "Random number generator". *Annals of the Institute of Statistical Mathematics* **8**, 1, 119–126 (Dec. 1956). issn: 1572-9052. doi: 10.1007/BF02863577

Jakobsson, K. S.: "Theory, Methods and Tools for Statistical Testing of Pseudo and Quantum Random Number Generators". Dissertation (2014). url: http://www.diva-portal.org/smash/record.jsf?pid=diva2:740158

Jennewein, T., U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger: "A fast and compact quantum random number generator". *Review of Scientific Instruments* **71**, 4, 1675–1680 (2000). doi: 10.1063/1.1150518

Jofre, M., M. Curty, F. Steinlechner, G. Anzolin, J. P. Torres, M. W. Mitchell, and V. Pruneri: "True random numbers from amplified quantum vacuum". *Opt. Express* **19**, 21, 20665–20672 (Oct. 2011). doi: 10.1364/OE.19.020665

Kendall, M. G.: "A theory of randomness". *Biometrika* **32**, 1, 1–15 (1941). doi: 10.1093/biomet/32.1.1

Kendall, M. G. and B. Babington-Smith: “Second Paper on Random Sampling Numbers”. *Supplement to the Journal of the Royal Statistical Society* **6**, 1, 51–61 (1939). issn: 14666162. url: http://www.jstor.org/stable/2983623

Kendall, M. G. and B. Babington Smith: *Tables of random sampling numbers*. English. On cover: Department of Statistics. University of London, University College. Cambridge : Cambridge University Press, 1939

Khanmohammadi, A., R. Enne, M. Hofbauer, and H. Zimmermanna: “A Monolithic Silicon Quantum Random Number Generator Based on Measurement of Photon Detection Time”. *IEEE Photonics Journal* **7**, 5, 1–13 (Oct. 2015). issn: 1943-0655. doi: 10.1109/JPHOT.2015.2479411

Killmann, W. and W. Schindler: “A proposal for : Functionality classes for random number generators ”. *AIS standard* (2011). url: https://www.bsi.bund.de

Knuth, D. E.: *The Art of Computer Programming*. Addison-Wesley, 1997. isbn: 0-201-89684-2

Kolmogorov, A. N.: “Three approaches to the quantitative definition ofinformation’”. *Probl. Peredachi Inf.* **1**, 1, 3–11 (1965)

Lalanne, P., H. Richard, J. Rodier, P. Chavel, J. Taboury, K. Madani, P. Garda, and F. Devos: “2-D generation of random numbers by multimode fiber speckle for silicon arrays of processing elements”. *Optics Communications* **76**, 5, 387–394 (1990). doi: 10.1016/0030-4018(90)90272-U

Lancaster, D.: “Spots before your eyes”. *Popular Electronics*, 29–34 (Sept. 1967). url: http://swtpc.com/mholley/PopularElectronics/Sep1967/PE_Sep1967.htm

Lang, R. and K. Kobayashi: “External optical feedback effects on semiconductor injection laser properties”. *IEEE Journal of Quantum Electronics* **16**, 3, 347–355 (Mar. 1980). issn: 0018-9197. doi: 10.1109/JQE.1980.1070479

Lax, M.: “Classical Noise. V. Noise in Self-Sustained Oscillators”. *Phys. Rev.* **160**, 290–307 (2 Aug. 1967). doi: 10.1103/PhysRev.160.290

L'Ecuyer, P. and R. Simard: "TestU01: A C Library for Empirical Testing of Random Number Generators". *ACM Trans. Math. Softw.* **33**, 4, 22:1–22:40 (Aug. 2007). issn: 0098-3500. doi: 10.1145/1268776.1268777

Lehmer, D. H.: "Mathematical methods in large-scale computing units". *Proceedings of a Second Symposium on Large-Scale Digital Calculating Machinery*. Harvard University Press, Cambridge, Mass., Nov. 1949, 141–146. doi: 10.1109/SFCS.1982.72

Lenstra, A. K., J. P. Hughes, M. Augier, J. W. Bos, T. Kleinjung, and C. Wachter: "Ron was wrong, Whit is right". **64** (2012). url: http://eprint.iacr.org/2012/064

Li, X., A. B. Cohen, T. E. Murphy, and R. Roy: "Scalable parallel physical random number generator based on a superluminescent LED". *Opt. Lett.* **36**, 6, 1020–1022 (Mar. 2011). doi: 10.1364/OL.36.001020

Lin, Y., F. Wang, X. Zheng, H. Gao, and L. Zhang: "Monte Carlo simulation of the Ising model on FPGA". *Journal of Computational Physics* **237**, 224–234 (2013). issn: 0021-9991. doi: 10.1016/j.jcp.2012.12.005

Lunghi, T., J. B. Brask, C. C. W. Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, and N. Brunner: "Self-Testing Quantum Random Number Generator". *Phys. Rev. Lett.* **114**, 150501 (15 Apr. 2015). doi: 10.1103/PhysRevLett.114.150501

Ma, H.-Q., Y. Xie, and L.-A. Wu: "Random number generation based on the time of arrival of single photons". *Appl. Opt.* **44**, 36, 7760–7763 (Dec. 2005). doi: 10.1364/AO.44.007760

Ma, X., F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo: "Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction". *Phys. Rev. A* **87**, 062327 (6 June 2013). doi: 10.1103/PhysRevA.87.062327

Maddocks, R. S., S. Matthews, E. W. Walker, and C. H. Vincent: "A compact and accurate generator for truly random binary digits". *Journal of Physics E: Scientific Instruments* **5**, 6, 542 (1972). url: http://stacks.iop.org/0022-3735/5/i=6/a=018

Mahalanobis, P. C., S. S. Bose, P. R. Ray, and S. Kumar Banerji: "Tables of Random Samples from a Normal Population". *Sankhyā: The Indian Journal of Statistics (1933-1960)* **1**, 2/3, 289–328 (1934). issn: 00364452. url: http://www.jstor.org/stable/40383681

Manelis, J.: “Generating random noise with radioactive sources”. *Electronics (U.S.)* **34**, 36 (Sept. 1961). url: https://www.osti.gov/scitech/biblio/4837260

Marron, J., A. J. Martino, and G. M. Morris: “Generation of random arrays using clipped laser speckle”. *Appl. Opt.* **25**, 1, 26–30 (Jan. 1986). doi: 10.1364/AO.25.000026

Marsaglia, G.: *The Marsaglia random number CDROM including the diehard battery of tests of randomness*. Florida State University, 1985. url: www.stat.fsu.edu/pub/diehard

Marsaglia, G.: “Random numbers fall mainly in the planes”. *Proceedings of the National Academy of Sciences of the United States of America* **61**, 1, 25–28 (Sept. 1968). url: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC285899/

Martin-Löf, P.: “The definition of random sequences”. *Information and control* **9**, 6, 602–619 (1966). doi: 10.1016/S0019-9958(66)80018-9

Martino, A. J. and M. G. Morris: “Optical random number generator based on photoevent locations”. *Appl. Opt.* **30**, 8, 981–989 (Mar. 1991). doi: 10.1364/AO.30.000981

Matsumoto, M. and T. Nishimura: “Mersenne Twister: A 623-dimensionally Equidistributed Uniform Pseudo-random Number Generator”. *ACM Trans. Model. Comput. Simul.* **8**, 1, 3–30 (Jan. 1998). issn: 1049-3301. doi: 10.1145/272991.272995

Matthews, J. C. F., A. Politi, A. Stefanov, and J. L. O’Brien: “Manipulation of multiphoton entanglement in waveguide quantum circuits”. *Nature Photonics* **3**, 6, 346–350 (2009). doi: 10.1038/nphoton.2009.93

Mitchell, M. W., C. Abellan, and W. Amaya: “Strong experimental guarantees in ultrafast quantum random number generation”. *Phys. Rev. A* **91**, 012314 (1 Jan. 2015). doi: 10.1103/PhysRevA.91.012314

Morris, G. M.: “Opto-electronic random number generating system and computing systems based thereon”. 1989. url: http://www.google.com/patents/US4833633

Morris, G. M.: “Optical Computing By Monte Carlo Methods”. *Optical Engineering* **24**, 24 (1985). doi: 10.1117/12.7973430

Nakamoto, S.: “Bitcoin: A peer-to-peer electronic cash system” (2008). url: http://www.academia.edu/download/32413652/BitCoin_P2P_electronic_cash_system.pdf

Nisan, N. and D. Zuckerman: “Randomness is linear in space”. *Journal of Computer and System Sciences* **52**, 1, 43–52 (1996). doi: 10.1006/jcss.1996.0004

Oksendal, B.: *Stochastic differential equations: an introduction with applications*. 2003. doi: 10.1007/978-3-642-14394-6

Pawlak, Z.: “Flip-flop as generator of random binary digits”. *Math. Comp.* **10**, 53, 28–30 (1956). doi: 10.1090/S0025-5718-1956-0076466-8

Pironio, S., A. Acín, S. Massar, A. Boyer de La Giroday, D. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. Manning, and C. Monroe: “Random numbers certified by Bell’s theorem”. *Nature* **464**, 1021–1024 (2010). doi: 10.1038/nature09008

Qi, B., 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.* **35**, 3, 312–314 (Feb. 2010). doi: 10.1364/OL.35.000312

Rand Corporation: *A Million Random Digits With 100,000 Normal Deviates*. Glencoe Free Press. 1955

Rarity, J., P. Owens, and P. Tapster: “Quantum Random-number Generation and Key Sharing”. *Journal of Modern Optics* **41**, 12, 2435–2444 (1994). doi: 10.1080/09500349414552281

Rude, M., C. Abellán, A. Capdevila, D. Domenech, M. W. Mitchell, W. Amaya, and V. Pruneri: “Quantum random number generation on a Si Chip”. *Submitted* (2017)

Rukhin, A., J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo: “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications” (2010). doi: 10.6028/NIST.SP.800-22r1a

Santha, M. and U. V. Vazirani: “Generating Quasi-Random Sequences From Slightly-Random Sources”. *25th Annual Symposium on Foundations of Computer Science, 1984.* Oct. 1984, 434–440. doi: 10.1109/SFCS.1984.715945

Schawlow, A. L. and C. H. Townes: “Infrared and Optical Masers”. *Phys. Rev.* **112**, 1940–1949 (6 Dec. 1958). doi: 10.1103/PhysRev.112.1940

Schmidt, H.: “Quantum□Mechanical Random□Number Generator”. *Journal of Applied Physics* **41**, 2, 462–468 (1970). doi: 10.1063/1.1658698

Shalm, L. K., E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman, K. J. Coakley, S. D. Dyer, C. Hodge, A. E. Lita, V. B. Verma, C. Lambrocco, E. Tortorici, A. L. Migdall, Y. Zhang, D. R. Kumor, W. H. Farr, F. Marsili, M. D. Shaw, J. A. Stern, C. Abellán, W. Amaya, V. Pruneri, T. Jennewein, M. W. Mitchell, P. G. Kwiat, J. C. Bienfang, R. P. Mirin, E. Knill, and S. W. Nam: "Strong Loophole-Free Test of Local Realism". *Phys. Rev. Lett.* **115**, 250402 (25 Dec. 2015). doi: 10.1103/PhysRevLett.115.250402

Shaltiel, R.: "Recent Developments in Explicit Constructions of Extractors". *Bulletin of the EATCS* **77**, 67–95 (2002)

Shamir, A.: "On the generation of cryptographically strong pseudo-random sequences". *Automata, Languages and Programming: Eighth Colloquium Acre (Akko), Israel July 13–17, 1981*. Ed. by S. Even and O. Kariv. Berlin, Heidelberg: Springer Berlin Heidelberg, 1981, 544–550. isbn: 978-3-540-38745-9. doi: 10.1007/3-540-10843-2_43

Shannon, C. E.: "Communication theory of secrecy systems". *The Bell System Technical Journal* **28**, 4, 656–715 (Oct. 1949). issn: 0005-8580. doi: 10.1002/j.1538-7305.1949.tb00928.x

Shepherd, S. J.: "Lessons learned from security weaknesses in the Netscape World Wide Web browser". *IEE Colloquium on Public Uses of Cryptography*. Apr. 1996, 7/1–7/6. doi: 10.1049/ic:19960524

Shor, P. W.: "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". *SIAM Review* **41**, 2, 303–332 (1999). doi: 10.1137/S0036144598347011

Sibson, P., M. Godfrey, C. Erven, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan, R. H. Hadfield, J. O'Brien, and M. G. Thompson: "Integrated Photonic Devices for Quantum Key Distribution". *CLEO: 2015*. Optical Society of America, 2015, FF1A.6. doi: 10.1364/CLEO_QELS.2015.FF1A.6

Smit, M., X. Leijtens, H. Ambrosius, E. Bente, J. van der Tol, B. Smalbrugge, T. de Vries, E.-J. Geluk, J. Bolk, R. van Veldhoven, L. Augustin, P. Thijs, D. D'Agostino, H. Rabbani, K. Lawniczuk, S. Stopinski, S. Tahvili, A. Corradi, E. Kleijn, D. Dzibrou, M. Felicetti, E. Bitincka, V. Moskalenko, J. Zhao, R. Santos, G. Gilardi, W. Yao, K. Williams, P. Stabile, P. Kuindersma, J. Pello, S. Bhat, Y. Jiao, D. Heiss, G.

Roelkens, M. Wale, P. Firth, F. Soares, N. Grote, M. Schell, H. Debregeas, M. Achouche, J.-L. Gentner, A. Bakker, T. Korthorst, D. Gallagher, A. Dabbs, A. Melloni, F. Morichetti, D. Melati, A. Wonfor, R. Penty, R. Broeke, B. Musk, and D. Robbins: "An introduction to InP-based generic integration technology". *Semiconductor Science and Technology* **29**, 8, 083001 (2014). doi: 10.1088/0268-1242/29/8/083001

Soldano, L. B. and E. C. M. Pennings: "Optical multi-mode interference devices based on self-imaging: principles and applications". *Journal of Lightwave Technology* **13**, 4, 615–627 (Apr. 1995). issn: 0733-8724. doi: 10.1109/50.372474

Solomonoff, R.: "A formal theory of inductive inference. Part I". *Information and Control* **7**, 1, 1–22 (1964). issn: 0019-9958. doi: 10.1016/S0019-9958(64)90223-2

Solomonoff, R. J.: "A formal theory of inductive inference. Part II". *Information and control* **7**, 2, 224–254 (1964). doi: 10.1016/S0019-9958(64)90131-7

Sowey, E. R.: "A Chronological and Classified Bibliography on Random Number Generation and Testing". *International Statistical Review / Revue Internationale de Statistique* **40**, 3, 355–371 (1972). issn: 03067734, 17515823. url: http://www.jstor.org/stable/1402472

Sowey, E. R.: "A Second Classified Bibliography on Random Number Generation and Testing". *International Statistical Review / Revue Internationale de Statistique* **46**, 1, 89–102 (1978). issn: 03067734, 17515823. url: http://www.jstor.org/stable/1402512

Sowey, E. R.: "A Third Classified Bibliography on Random Number Generation and Testing". *Journal of the Royal Statistical Society. Series A (General)* **149**, 1, 83–107 (1986). issn: 00359238. url: http://www.jstor.org/stable/2981887

Stefanov, A., N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden: "Optical quantum random number generator". *Journal of Modern Optics* **47**, 4, 595–598 (2000). doi: 10.1080/09500340008233380

Sterzer, F.: "Parametric oscillator random number generator". 1962. url: http://www.google.com/patents/US3069632

Sterzer, F.: “Random Number Generator Using Subharmonic Oscillators”. *Review of Scientific Instruments* **30**, 4, 241–243 (1959). doi: 10.1063/1.1716525

Stipcevic, M. and B. M. Rogina: “Quantum random number generator based on photonic emission in semiconductors”. *Review of Scientific Instruments* **78**, 4, 045104 (2007). doi: 10.1063/1.2720728

Symul, T., S. M. Assad, and P. K. Lam: “Real time demonstration of high bitrate quantum random number generation with coherent laser light”. *Applied Physics Letters* **98**, 23, 231103 (2011). doi: 10.1063/1.3597793

Ticknor, A. J. and H. H. Barrett: “Optical Implementations In Boltzmann Machines”. *Optical Engineering* **26**, 26 (1987). doi: 10.1117/12.7974015

Tillmann, M., B. Dakić, R. Heilmann, S. Nolte, A. Szameit, and P. Walther: “Experimental boson sampling”. *Nature Photonics* **7**, 7, 540–544 (May 2013). doi: 10.1038/nphoton.2013.102

Tippett, L. H.: “Random Sampling Numbers”. *Tracts for Computers* **15** (1927)

Vadhan, S. P.: “Pseudorandomness”. *Foundations and Trends® in Theoretical Computer Science*. Vol. 7. 1–3. 2012, 1–336. doi: 10.1561/0400000010

Vallone, G., D. G. Marangon, M. Tomasin, and P. Villoresi: “Quantum randomness certified by the uncertainty principle”. *Phys. Rev. A* **90**, 052327 (5 Nov. 2014). doi: 10.1103/PhysRevA.90.052327

Vincent, C. H.: “The generation of truly random binary numbers”. *Journal of Physics E: Scientific Instruments* **3**, 8, 594 (1970). url: http://stacks.iop.org/0022-3735/3/i=8/a=303

Von Neumann, J.: “Various Techniques Used in Connection With Random Digits”. *Monte Carlo Methods, Appl. Math. Series*. Vol. 12. (Summary written by George E. Forsythe); reprinted in John von Neumann, Collected Works. Vol. 5, Pergamon Press; Macmillan, New York, 1963, pp. 768-770. MR 28 1104. U. S. Nat. Bureau of Standards, 1951, 36–38

Wahl, M., 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 **98**, 17, 171105 (2011). doi: 10.1063/1.3578456

Walmsley, I. A.: "Quantum optics: Science and technology in a new light". *Science* **348**, 6234, 525–530 (2015). issn: 0036-8075. doi: 10.1126/science.aab0097 eprint: http://science.sciencemag.org/content/348/6234/525.full.pdf

Wayne, M. A. and P. G. Kwiat: "Low-bias high-speed quantum random number generator via shaped optical pulses". *Opt. Express* **18**, 9, 9351–9357 (Apr. 2010). doi: 10.1364/OE.18.009351

Whitaker, S. and E. Kelsey: "Binary random number generator using switching tree and wide-band noise source". US Patent 3,423,683. 1967. url: http://www.google.sr/patents/US3423683

Williams, C. R. S., J. C. Salevan, X. Li, R. Roy, and T. E. Murphy: "Fast physical random number generator using amplified spontaneous emission". *Optics express* **18**, 23, 23584–23597 (Nov. 2010). doi: 10.1364/OE.18.023584

Xu, F., B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo: "Ultrafast quantum random number generation based on quantum phase fluctuations". *Opt. Express* **20**, 11, 12366–12377 (May 2012). doi: 10.1364/OE.20.012366

Yule, G. U.: "A test of Tippett's random numbers". *Journal of the royal Statistical Society* **101**, 1, 167–172 (1938). issn: 09528385. url: http://www.jstor.org/stable/2980656

Zadok, A., H. Shalom, M. Tur, W. D. Cornwell, and I. Andonovic: "Spectral shift and broadening of DFB lasers under direct modulation". *IEEE Photonics Technology Letters* **10**, 12, 1709–1711 (Dec. 1998). issn: 1041-1135. doi: 10.1109/68.730477