

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/301899096>

Quantum Random Number Generators

Article *in* Review of Modern Physics · April 2016

DOI: 10.1103/RevModPhys.89.015004

CITATIONS

170

READS

2,433

2 authors, including:



Juan Carlos Garcia-Escartin

Universidad de Valladolid

40 PUBLICATIONS 414 CITATIONS

SEE PROFILE

Quantum Random Number Generators

Miguel Herrero-Collantes*

*Instituto Nacional de Ciberseguridad,
Avenida José Aguado, 41, Edificio INCIBE 24005, León, Spain.*

*El Telecomunicación, Department of Signal Theory and Communications, University of Vigo,
Campus Universitario Lagoas-Marcosende, E-36310 Vigo,
Spain.*

Juan Carlos Garcia-Escartin†

*Universidad de Valladolid,
Dpto. Teoría de la Señal e Ing. Telemática,
Paseo Belén nº 15,
47011 Valladolid,
Spain.*

(Dated: October 24, 2016)

Random numbers are a fundamental resource in science and engineering with important applications in simulation and cryptography. The inherent randomness at the core of quantum mechanics makes quantum systems a perfect source of entropy. Quantum random number generation is one of the most mature quantum technologies with many alternative generation methods. We discuss the different technologies in quantum random number generation from the early devices based on radioactive decay to the multiple ways to use the quantum states of light to gather entropy from a quantum origin. We also discuss randomness extraction and amplification and the notable possibility of generating trusted random numbers even with untrusted hardware using device independent generation protocols.

CONTENTS

| | | | |
|---------------------------------------------------------------------|----|--------------------------------------------------------------------------------------|----|
| I. Motivation | 2 | G. Generators based on the phase noise of lasers | 21 |
| II. Random numbers and their applications | 2 | H. Generators based on amplified spontaneous emission | 23 |
| A. Pseudorandom number generators and true random number generators | 3 | I. Generators based on Raman scattering | 24 |
| B. Random numbers in simulation | 5 | J. Generators based on optical parametric oscillators | 27 |
| C. Random numbers in cryptography | 5 | VIII. Non-optical Quantum Random Number Generators | 28 |
| D. Random numbers in fundamental science | 7 | IX. Random numbers certified by quantum mechanics | 29 |
| III. Block description | 8 | A. Self-testing in quantum random number generators | 30 |
| IV. Entropy estimation | 9 | B. Device independent quantum random number generators | 31 |
| V. Quantum Random Number Generators based on radioactive decay | 10 | C. Other forms of quantum certification | 33 |
| A. The first quantum random number generators | 10 | X. Postprocessing | 34 |
| B. Evolution | 12 | A. Randomness extractors | 35 |
| C. Limitations | 12 | 1. Deterministic extractors | 35 |
| VI. Random Number Generators based on noise | 13 | 2. Seeded extractors | 36 |
| VII. Optical Quantum Random Number Generators | 14 | XI. Quantum randomness extractors: randomness expansion and randomness amplification | 37 |
| A. Quantum optics in random number generators | 14 | A. Quantum randomness expansion | 38 |
| B. Branching path generators | 15 | B. Quantum randomness amplification | 38 |
| C. Time of arrival generators | 17 | XII. Randomness testing | 39 |
| D. Photon counting generators | 19 | XIII. Discussion | 40 |
| E. Attenuated pulse generators | 20 | Acknowledgments | 40 |
| F. Generators based on quantum vacuum fluctuations | 20 | References | 40 |

* miguel.herrero@incibe.es

† juagar@tel.uva.es

I. MOTIVATION

Quantum mechanics offers interesting new protocols in the intersection between computer science, telecommunications, information theory and physics. Results like the protocols for quantum key distribution (Bennett and Brassard, 1984; Ekert, 1991) and efficient algorithms for problems that are thought or known to be hard for classical computers (Childs and van Dam, 2010; Ekert and Jozsa, 1996) show quantum physics can have a profound impact in the way we think about security, cryptography and computation.

Despite the impressive experimental achievements of the last decades, the current state of technology is still not advanced enough for a full-scale universal quantum computer. Quantum key distribution, on the other hand, has already become an established technology and the first commercial systems have been demonstrated in practical scenarios (Peev *et al.*, 2009; Sasaki *et al.*, 2011).

Another important well-established quantum technology is quantum random number generation. *Quantum random number generators*, *QRNGs*, are devices that use quantum mechanical effects to produce random numbers and have applications that range from simulation to cryptography. They are usually simpler than other quantum devices and are mature enough to be applied. QRNGs using different quantum phenomena have gone from the lab to the shelves with at least eight existing commercial products (ComScire, 2014; Hughes and Nordholt, 2016; ID Quantique, 2014; MPD, 2014; PicoQuant, 2014; QRB121, 2014; Quintessence Labs, 2014; Qutools, 2014) and online servers that provide quantum random numbers on demand (ANU, 2016; Humboldt-Universität, 2016; Stevanović *et al.*, 2008; University of Geneva, 2004; Walker, 1996), as well as many patents (Beausoleil *et al.*, 2008; Dultz *et al.*, 2002; Dultz and Hidlebrandt, 2002; Kim and Klass, 2001; Klass, 2003, 2005; Lutkenhaus *et al.*, 2007; Ribordy *et al.*, 2009; Sartor and Zimmermann, 2015; Trifonov and Vig, 2007; Vartsky *et al.*, 2011). In the last few years there has also been a large number of proposals, experiments, improvements and exciting theoretical results in randomness extraction and randomness certification.

The aim of this review is to collect the most important proposals for quantum random number generation and give an introduction to the new advanced protocols that use quantum physics to process, certify or otherwise deal with random strings. This paper complements previous surveys on the topics of physical and quantum random number generation (Stipčević, 2012; Stipčević and Koç, 2014) with a focus on QRNGs based on quantum optics.

Section II gives a brief description of the most important applications of randomness in science and computers. We review the differences between algorithmic methods to produce random looking numbers and physical methods to produce true random numbers and discuss

when each method is more appropriate. Due to their importance, we concentrate on applications to simulation and cryptography.

Section III describes the main functional elements of quantum random number generators and their roles. In Section IV, we present some mathematical measures of randomness which are particularly useful to analyse the amount of available random bits and the security of quantum random number generators.

Section V discusses QRNGs based on radioactive decay, which were the first proposed QRNGs and are still in use today. Section VI introduces random number generators based on electronic noise and analyses when they can be said to be quantum.

Section VII discusses how optics has modernized QRNGs. Most present-day QRNGs are based on quantum optics and we review the multiple implementations that work with the quantum states of light.

Section VIII covers alternative QRNGs based on non-optical quantum phenomena and Section IX is centered on those QRNGs whose randomness is backed by quantum mechanics.

Section X gives a brief tour on the available classical randomness extraction methods and Section XI introduces the quantum protocols for randomness expansion and amplification that allow to produce good-quality random outputs from weak randomness sources.

Section XII is an introduction to the statistical tests that are usually employed to assess the quality of the final random bit stream.

Finally, in Section XIII, we give an overview on the current state of quantum random number generation and the challenges and opportunities for the next generation of quantum devices in the field of randomness.

II. RANDOM NUMBERS AND THEIR APPLICATIONS

Random numbers are an essential resource in science, technology and many aspects of everyday life (Hayes, 2001). Randomness is required to different extents in applications like cryptography, simulation, coordination in computer networks or lotteries. Some applications require a small amount of random numbers and still use manual and mechanical methods to generate randomness, like tossing a coin, throwing a die, spinning a roulette wheel or a drawing a ball from a lottery machine. Here, we will concern ourselves with the generation of random numbers for computers.

Defining randomness is a deep philosophical problem and we will not attempt to solve it here. In this Section, we give common operational definitions of randomness that fit the different purposes the random numbers must fulfil. For instance, in simulation, a method that generates numbers simulating the statistics of the desired distribution can be considered to be “random enough”,

even if it produces a predictable sequence.

A. Pseudorandom number generators and true random number generators

In computing, it is important to distinguish between algorithmically generated numbers that mimic the statistics of random distributions and random numbers generated from unpredictable physical events.

Generating random numbers directly from a computer seems a particularly attractive idea. Methods that produce random numbers from a deterministic algorithm are called **pseudorandom number generators**, PRNGs. While it is clear that any algorithmically generated sequence cannot be truly random, for many applications the appearance of randomness is enough¹.

PRNGs normally start from a small string of bits called the *seed* that is used as the input of a procedure that outputs a long sequence of bits following the statistics of the uniform distribution. In principle, an RNG could produce numbers obeying any random distribution, but the standard practice is trying to provide a uniform distribution, from which we can obtain the most commonly used distributions using well-known transformations (Hörmann *et al.*, 2004). Knuth gives an excellent survey on PRNGs and how to transform uniform random numbers into other types of random quantities in his second book of the series “The Art of Computing Programming” (Knuth, 1997).

A large number of PRNGs are based on number theory. Linear congruential generators have been particularly popular since Lehmer introduced them in 1951 (Lehmer, 1951). Linear congruential generators produce random numbers from the recursive formula

$$X_{n+1} = (aX_n + c) \bmod m, \quad n \geq 0, \quad (1)$$

where X_i is the i th digit in the sequence of random numbers, $m > 0$ is the modulus, $0 \leq a < m$ is called the multiplier and $0 \leq c < m$ the increment. The properties of the output depend heavily on the correct choice of these parameters. A poor choice can create an output sequence with a short period.

Its period is one of the most important properties of any PRNG. The next number in a pseudorandom sequence is determined from the internal state of generator. For a finite memory, the internal state will at some point be the same and the output sequence will begin to repeat itself. PRNGs are chosen to have a large periods so

that the repetition does not appear during the intended operation time.

Apart from congruential linear generators, there is another large family of PRNGs based on linear shift feedback registers, LFSRs, and their generalizations. The most notable generator in this class is the Mersenne Twister (Matsumoto and Nishimura, 1998), which belongs to the family of twisted generalized linear shift feedback registers. The Mersenne Twister has a period which is a Mersenne prime of the form $2^n - 1$, for an integer n . The most widely used pseudorandom number generator is the MT19937, the standard implementation of the Mersenne Twister with a period $2^{19937} - 1$. It is the default generator in many programming languages and popular scientific software.

L’Ecuyer gives a good review of these and other alternative PRNGs based on different principles (L’Ecuyer, 2012).

Pseudorandom numbers have certain advantages that make them popular. They can be much faster than alternative random number generation methods and their results are reproducible. For instance, we can repeat the exact same simulation if we know the seed. However, for many applications, unpredictability is an important requisite. Clearly, a predictable lottery is not acceptable, even if all the resulting numbers are uniformly distributed. Some pseudorandom generators are designed to be unpredictable (see Section II.C), but, applications that need an output that cannot be guessed usually turn to **true random number generators**, TRNGs, if only to renew the seed of a PRNG.

True random number generators measure some unpredictable or, at least, difficult to predict physical process and use the results to create a sequence of random numbers. They either rely on unpredictable values that can be accessed from the software inside the computer or create the sequence in a special-purpose device that feeds it into the operating system.

The process of collecting unpredictable data is usually called *entropy gathering*. Some of the standard entropy sources the operating system can access include data from the sound card, disk access times, the timing of interrupts or user interaction data, like mouse motion or keystrokes, to name a few. The way the Linux operating systems collect entropy and convert it into random bits (Gutterman *et al.*, 2006) is an illustrative example of many of the most usual methods. Some authors call these generators that use non-deterministic events, non-physical non-deterministic RNGs (Killmann and Schindler, 2008) that stand in contrast to physical TRNGs based in non-deterministic physical effects in electronic circuits or in the result of some physical experiment. Alternatively, there are physical TRNGs based on different principles, such as chaotic systems (Stojanovski and Kocarev, 2001; Stojanovski *et al.*, 2001), thermal noise in electronic circuits (Murry, 1970; Petrie and Con-

¹ The famous quote from von Neumann “Any one who considers arithmetical methods of producing random numbers is, of course, in a state of sin” is just a way to acknowledge this fact, but also to admit it is an acceptable practice. In the same paper (von Neumann, 1951) he goes on to comment on some methods to produce pseudorandom sequences.

nelly, 2000), free running oscillators (Kohlbrenner and Gaj, 2004), or biometric parameters (Szczepanski *et al.*, 2004) as a few examples.

Some vendors include integrated physical random number generators in their processors. Intel has included in its recent processors a digital RNG based on a metastable latch that, due to thermal noise, suffers jumps in its state at around a 3 GHz rate. This integrated RNG can be directly accessed from a processor instruction, RdRand, (Hamburg *et al.*, 2012; Taylor and Cox, 2011). Similarly, the VIA Technologies Nehemiah processor core includes an on-chip random number generator which is based on a series of oscillators where thermal noise alters the jitter so that the combination of the oscillators' output is random (Cryptography Research Inc., 2003). These integrated RNG include conditioning circuits that process the output to remove biases.

With an integrated physical random number generator there is always an available source of entropy and we are not limited to resort to other sources of randomness that might not provide fresh entropy in a reliable and steady fashion. For instance, many servers are connected to a limited number of peripherals and do not have access to many random events like mouse motions. These servers can only gather entropy slowly and under severe constraints.

An integrated physical generator is a convenient addition, but it can also be complemented with the use of external RNGs. This can be a good solution if we do not trust the mechanism in the implementation, the vendor has not released it, or we suspect the chip might have a backdoor either by design or by sabotage (Becker *et al.*, 2014).

Quantum random number generators are a particular case of physical TRNGs in which the data is the result of a quantum event. As opposed to other physical systems where uncertainty is a result of an incomplete knowledge of the system, true randomness is an essential part of quantum mechanics as we know it.

On first sight, physical RNGs seem more desirable than deterministic methods. However, there are inconveniences that have impeded their wider adoption. Some of the problems in physical RNGs are

1. Limited generation rate. Physical RNG usually produce random numbers at a much smaller rate than software methods. In many cases, there is a fundamental limitation in the rate of change of the sampled physical parameter. If the system is sampled at a high rate, there is not enough time for the system to change and the random numbers are not independent.
2. It is difficult to give a convincing argument for the randomness of the data. There can be reasonable doubts about the randomness of the chosen physical phenomenon. Many physical random number

generators rely on our ignorance to describe a physical process rather than in its intrinsic randomness.

3. Adding an external device is usually inconvenient.
4. Failures are difficult to detect. If a hardware random number generator fails during operation, it can be difficult to notice. Official recommendations suggest introducing a startup test, a total failure test and an online test to check errors during operation (Killmann and Schindler, 2011; Schindler and Killmann, 2003).

The advanced Quantum Random Number Generators that have appeared with the impulse of quantum information research try to solve some of these shortcomings of traditional TRNGs. They offer a solution based on a trusted randomness source and many from the different implementations achieve fast generation rates, normally above the megabit per second, as we will see in the multiple optical implementations described in Section VII. This faster rate allows new applications for TRNGs, such as online casinos and Internet gambling, which require a constant stream of random data and cannot use the slower methods of traditional daily or weekly lotteries (ID Quantique, 2011; PokerStars, 2016).

An important distinction between pseudorandom number generators and physical random number generators is the focus on product or process randomness (Calude, 2015; Eagle, 2005). For pseudorandom number generators we can only evaluate the output strings. We focus on the product of the ultimately deterministic algorithm and we try to determine whether the string has all the properties of a random sequence. In order to determine if we have product randomness our options are limited to checking the output strings and submitting them to certain statistical test (see Section XII).

In physical random number generators we concentrate on process randomness. We look for a process that produces a random output and seek to obtain true random numbers from fundamentally random physical phenomena. Here, randomness is usually taken as unpredictability.

While, properly, classical phenomena can not be considered truly random, in common use, the terms physical and true random number generator are used interchangeably. Usually, it is fine to use an unpredictable physical system as a randomness source. However, there remains a doubt whether the backing physical process is truly random or, at least, presents serious difficulties to be predicted, like a chaotic system, or we simply have a poor model and a better one could destroy the illusion of randomness. Quantum random number generators excel in that aspect: they use very well defined inherently random processes as the source of their bits.

In the rest of this Section we will consider in some detail how algorithmic and physical random number gener-

ation methods are employed in two of the most important families of applications for RNGs, simulation and cryptography. We go through the particular requirements of randomness of each application and discuss the RNGs that are currently used in each case and the dangers of choosing a wrong randomness generation method. We then write about random number generation in fundamental science experiments.

B. Random numbers in simulation

Random numbers play an essential role in many scientific fields. They are fundamental ingredients in randomized algorithms, which have a wide range of applications in simulation, computing, number theory and other branches of science and engineering (Karp, 1991; Motwani and Raghavan, 1996).

Simplified models of the reality are indispensable tools when we want to predict the behaviour of complex systems that cannot be accurately described with a closed formula or when the computational needs for a full numerical analysis are too high. These models turn to random numbers to incorporate the combined effect of all that is left out. Thus, random number generation is needed in simulations in engineering, network, manufacturing, business and computer science problems (Bratley *et al.*, 1987; Fishman, 1978; Law and Kelton, 2000). The usual hypothesis is that we can obtain accurate results if we study enough cases chosen uniformly at random. These results, while probabilistic, are usually representative. We need, nevertheless, good random numbers. For instance, in the social sciences it is crucial to have a sound random sampling method to be confident that the study group is a faithful proxy for the whole population that we want to describe (Lohr, 2010).

A particularly important area is Monte Carlo and Quasi-Monte Carlo methods (Gentle, 2009; Metropolis and Ulam, 1949; Niederreiter, 1978) in which we can find the solution to a complex problem by averaging many random instances. These methods are very effective in solving problems in statistical physics and numerical integration, where they are extensively used. If we sample the state space really at random, the result is likely to be correct, but, due to the high volume of data they require, these algorithms usually get their random numbers from a PRNG. When correctly done, this is enough. In simulation we only need a generator following the right statistics. However, certain generators that seem reliable under the usual tests (see Section XII) have undetected long range correlations that can result in a wrong solution. This is a general problem for congruential generators. In “Random numbers fall mainly in the planes” (Marsaglia, 1968) Marsaglia showed that, choosing the right coordinates, consecutive random numbers from multiplicative congruential generators cluster into clear patterns. There

are ways to correct this bias (Bauke and Mertens, 2007), but there exist many examples of simulations using faulty PRNG that gave results that, when compared to a known solution, were proved to be wrong, while a different, better PRNG gave the correct answer. There are numerous recorded cases of such failures for the Ising model (Ferreberg *et al.*, 1992; Hoogland *et al.*, 1985; Kalle and Wansleben, 1984; Milchev *et al.*, 1986; Ossola and Sokal, 2004; Parisi and Rapuano, 1985; Schmid and Wilding, 1995) and related problems (Grassberger, 1993; Hongo *et al.*, 2010; Shchur *et al.*, 1997; Ziff, 1998). Choosing a bad seed during initialization can also result in a correlated output (Matsumoto *et al.*, 2007).

Because of these issues, there are authors that have proposed to test PRNGs with the practical problems they are going to solve in addition to the standard statistical tests (Coddington, 1994, 1996; Vattulainen *et al.*, 1994, 1995). For Monte Carlo methods it is also a generally good idea contrasting the results of the same algorithm with different PRNGs, which are unlikely to have the same kind of bias.

True RNG are seldom used for simulation apart from seeding the PRNG. They face several challenges. They are slow when compared to the fastest PRNGs and their results are not easy to reproduce. This is a problem during debugging and replication. The only way to repeat the results of a TRNG is storing the sequence, which can be extremely large for a Monte Carlo run. They also need a fast method to interface with the processor. Anyway, true random number generators are adequate for simulation. While the generation rates of present Quantum RNGs are still a few orders of magnitude below those of good quality PRNGs, they are growing and QRNGs have shown they can be used, at a speed disadvantage, in Monte Carlo simulation (Preez *et al.*, 2011). Improvements in the generation speed could make them a viable alternative in certain applications.

C. Random numbers in cryptography

Randomness is also a basic cryptographic primitive. Most of modern cryptography follows Kerckhoffs’s principle (Kerckhoffs, 1883) and assumes any cryptographic system can fall into the hands of the adversary and that all the details of the system are perfectly known. Cryptographic system are therefore open and all the security rests in the choice of a secret key. That way, if a channel is compromised, the users just need to change that key. This has many advantages and is generally considered good practice.

In that context, it is of the utmost importance to choose a random key, which usually means choosing an n -bit string uniformly at random from all the key space. Similarly, random numbers with sometimes more relaxed randomness requisites are needed in other cryptographic

protocols (Gennaro, 2006). Random numbers are required in nonces (numbers that must be used only once), in initialization vectors, in sequence numbers (Networking Working Group, 1996), in salt² to avoid dictionary attacks in hashed password lists and in digital signatures, as well as in many interactive protocols (Goldreich, 1999).

Quantum cryptography also needs a reliable randomness source. Quantum key distribution is open to attacks if the measurement bases and the states are not chosen in a truly random way, as has been shown for the BB84 protocol (Bouda *et al.*, 2012; Li *et al.*, 2015).

In cryptography it is not enough that the random numbers are uniform. They must also be unpredictable and the generator should limit the damage of any compromised key. There are, depending on authors, at least two new conditions for random numbers to be used in cryptography:

1. Unpredictability (forward security): an attacker that knows the whole sequence cannot guess the next bit with a probability better than one half.
2. Backward security: knowledge of a part of the sequence shall not permit an attacker to compute the previous values of the generator with better accuracy than guessing.

For practical purposes, both requisites of unpredictability can be reduced to polynomial-time unpredictability: that no algorithm can take a subsequence from the generator and guess efficiently (in polynomial time) any previous or following subsequences with better results than total random guessing. This concept is based on Yao's definition of indistinguishable sources (Yao, 1982).

Most PRNG are not up to the task of generating cryptographically secure random numbers. For instance, the internal state in the Mersenne Twister can be deduced from a long enough output sequence (Matsumoto and Nishimura, 1998) and the output of a large type of general congruential generators can be predicted without even knowing the parameters in the generator (Krawczyk, 1990).

² Passwords should not be stored directly as text to prevent further damage if the password file is compromised. The common practice is to store the cryptographic hash of the password string, which, ideally, is a fixed-length bit string that looks random and from which it is unfeasible to recover the original password. However, it is easy to compile a list of the most common passwords and create a list of their hashes. This is called a dictionary attack and it allows an adversary to find the original password from the hashed password list by comparison. One way to hamper this attack is to include a random sequence, called salt, that is hashed together with the password. The salt string is public, but different for every password in the list, making dictionary attacks computationally costly (precomputed universal tables are no longer a valid shortcut).

There are however, established ways to use pseudorandom number generators in cryptographic applications. Algorithmic generators that fulfil the additional criteria are called cryptographically secure pseudorandom number generators CSPRNGs. Two examples based on number theory are the Blum and Micali (Blum and Micali, 1984) and the Blum Blum Shub generators (Blum *et al.*, 1986). We can use Blum Blum Shub as an illustration. The output bits come from the recursive formula

$$X_{i+1} = X_i^2 \mod N \quad (2)$$

for $N = pq$ the product of two primes p and q congruent to 3 mod 4. X_i is the i th number used as the internal state. The algorithm has N and X_0 as inputs and the i th output bit is the parity of X_i (or, in some variations, a few least significant bits). The initial state X_0 should come from a TRNG. This generator has some desirable properties as long as certain common computational complexity assumptions hold. For instance, even if an attacker learnt the internal state X_i at stage i , we keep unpredictability to the left (the preceding bits of the binary string are not compromised). Guessing X_{i-1} from X_i is computationally hard unless the quadratic residuosity problem can be solved in polynomial time. Later work showed that breaking Blum Blum Shub is equivalent to factoring (Vazirani and Vazirani, 1985a). This is considered computationally secure in many cryptographic protocols. However, an attacker with a quantum computer that knows N could use Shor's algorithm for integer factorization to break the security of the generator (Shor, 1997).

There are also variations of the Mersenne Twister intended to make it secure for cryptographic use (Matsumoto *et al.*, 2005, 2008). Other approaches to CSPRNGs use cryptographic protocols such as DES or AES as blocks that transform a string of bits using as their secret key a processed seed from the computer's entropy pool. An example is the random number generation recommendation for banking in the ANSI X9.17 key management standard (American National Standards Institute, 1985).

There are different standards and recommendations for the cryptographic use of random number generators in key generation (Barker and Roginsky, 2012; National Institute of Standards and Technology, 2001) and in financial systems (American National Standards Institute, 2006), with instructions on how to treat the sources of entropy for seeding PRNGs (International Organization for Standardization, 2011; Turan *et al.*, 2016).

Cryptographical random number generators, as any critical part in a cryptographic protocol, can be subject to different cryptanalytic attacks (Kelsey *et al.*, 1998). There are also some quantum attacks that offer a moderate advantage with respect to classical strategies (Guedes *et al.*, 2013).

Certain generators are specifically designed for cryptography and are built to avoid common attacks. An example is the Fortuna pseudorandom number generator that uses multiple sources of entropy to reseed as frequently as possible so that, if the generator is compromised at some time, the previous output remains unguessable (Ferguson *et al.*, 2010). This and similar cryptographic generators are configurable and allow to replace the protocols inside their constituent blocks.

The design of cryptographically secure RNGs is far from trivial. There are multiple cases of faulty implementations of RNGs that have led to serious vulnerabilities. One common pitfall is the failure to properly seed the generator. Even if the transformation on the seed is secure and cannot be inverted, if there is not enough entropy an attacker can launch a brute force attack and try all the possible seeds. The outputs can then be compared to the output of the generator and the attacker can predict which keys the user has generated. This has happened many times since the early attacks on the SSL keys generated in the Netscape Browser, which used predictable sources like the time of the day or process numbers to seed its generator (Goldberg and Wagner, 1996; Shepherd, 1996). Similarly, a bug in the OpenSSL library resulted in a seed of limited entropy that used as its only randomness source process identifiers, PID, which have only 2^{15} possible values (Ahmad, 2008). The resulting possible keys could be generated by brute force in a few hours. Poor initialization can also weaken the random numbers in operating systems like Windows 2000 (Dorrendorf *et al.*, 2009). A few more examples of vulnerabilities due to initialization problems or other bad quality random number generators are weak RSA key generation in network devices (Heninger *et al.*, 2012; Lenstra *et al.*, 2012), repeated or guessable keys produced inside smart cards (Bernstein *et al.*, 2013; Courtois *et al.*, 2013; Nohl *et al.*, 2008) and the predictable random sequences that are used for cryptographic purposes in Android (Kim *et al.*, 2013; Michaelis *et al.*, 2013).

In this respect, physical RNGs, including QRNGs, can serve as way to seed CSPRNGs, preferably as an additional source of entropy. There are still some important precautions. Certain attacks specifically target TRNGs (Soucarros *et al.*, 2013; Zheng and Matsumoto, 1997) and they can be sensitive to environmental variables (Soucarros *et al.*, 2011). There are already some proposals to test QRNG (Walenta *et al.*, 2015) under the online test of the BSI AIS 20/31 standard (Killmann and Schindler, 2011) to make sure they do not fail during operation. As long as these aspects are taken into account, the relatively high rate of QRNGs makes them also a viable option to directly generate keys, probably after some kind of post-processing.

In fact quantum key distribution, QKD, (Bennett and Brassard, 1984; Ekert, 1991; Gisin *et al.*, 2002; Lo *et al.*, 2014; Scarani *et al.*, 2009) can be seen as nothing

more than a very sophisticated distributed secure random number generator that includes a physical method to generate entropy and a randomness amplification algorithm that weeds out the bits that could have been compromised (Owens *et al.*, 2008).

In that interpretation, many quantum hacking methods can be considered as attacks to an RNG or to the randomness generation block inside the QKD system (Stipčević, 2014). For instance, in detector blinding attacks (Gerhardt *et al.*, 2011; Lydersen *et al.*, 2010), an attacker can selectively disable the detectors in the receiver and eliminate any randomness in the measurement, determining the result. Similarly, time shift attacks take advantage of different detection efficiencies with time to make measurement in a chosen basis more or less likely introducing a bias (Zhao *et al.*, 2008) and attacks based on imperfect beam splitters perform a similar feat by introducing unbalances in the way the quantum states are directed to each measurement configuration (Li *et al.*, 2011).

QKD protocols assume they have access to true randomness and QRNGs are quite adequate for that purpose. We will see they are faster than alternative TRNGs, produce random numbers of good quality and suppose small deviations from the usual configuration of the equipment (they can be built with the same technology and their cost is only a small fraction of the total).

D. Random numbers in fundamental science

Finally, truly random numbers play a special role in experiments that try to determine the nature of the world. For philosophical reasons, in some proof of principle experiments we need to remove any possible bias when choosing a measurement or when making other decision. To this respect, quantum random number generators stand in a privileged position. Quantum mechanics is the only theory that, according to our understanding, offers true randomness.

This is particularly important in many experiments on the foundations of quantum mechanics, where many of the thought experiments that helped to shape our understanding of the quantum theory have entered the lab and can be tested experimentally (Shadbolt *et al.*, 2014). Quantum random numbers can also appear in any experiment where we want to be sure there is no hidden bias or that our decisions are independent from previous states of the system. Curiously, one of the early quantum random number generators based on radioactive decay, described in Section V, was designed as a way to remove bias in parapsychology experiments (Schmidt, 1970a,b). Later, QRNGs have become part in experiments where randomness is a philosophical necessity.

Quantum random number generators are a good solution in experiments that test the predictions of the quan-

tum theory. They can be built with equipment similar to that of the experiment or even be integrated into the experimental setup. While we must trust the inherent randomness of quantum effects, they can be instrumental in exploring other aspects of quantum mechanics like complementarity or nonlocality that are not directly dependent on the randomness of quantum measurement. Experimental tests of properties like the wave-particle duality usually require to take random decisions in a short time and quantum random number generators can fulfil that mission.

Experimental tests of Bell's Inequality (Brunner *et al.*, 2014) need a random choice of basis which can be done with an external QRNG connected to a switch like in the experiments of (Weihs *et al.*, 1998) and (Scheidl *et al.*, 2010) that used the QRNG in (Jennewein *et al.*, 2000) or with a passive choice, where the quantum randomness comes from separating the paths of the photons in the experiment in a balanced beam splitter (Tittel *et al.*, 1999), which can be equivalent in the right conditions (Gisin and Zbinden, 1999).

We also need true randomness for Wheeler's delayed choice experiment in which a photon inside an interferometer can behave like a wave or a particle depending on whether we close the interferometer or not (Wheeler, 1978). If the choice is delayed to after the photon is inside the interferometer, the photon must be able to behave both as a wave and a particle³ as the complete setup had not been decided when the photon entered it. From a fundamental point of view, it is crucial that the decision is made after the photon enters the interferometer. We need a fast and truly random number generator. The experiment in (Alley *et al.*, 1984) uses a single photon from a weak light source with a 50% probability of firing a detector connected to a switch and the experiments in (Jacques *et al.*, 2007, 2008) make this decision using a QRNG based on the measurement of the amplified shot noise of white light.

Other experiments include delayed-choice experiments based on entanglement swapping (Yurke and Stoler, 1992; Zukowski *et al.*, 1993) after Peres's proposal (Peres, 2000) in which whether two photons are entangled or not is decided *after* they have been measured (Ma *et al.*, 2012) and in quantum erasure experiments that erase path information (Ma *et al.*, 2013a), in both cases using the QRNG of (Jennewein *et al.*, 2000).

³ Indeed, the experiments show the photon can also behave as different combinations in between, with different degrees of visibility and distinguishability.

III. BLOCK DESCRIPTION

Physical random number generators can be divided into separate blocks with well-defined subtasks. The two most important blocks are the entropy source and the postprocessing stage. The *entropy source* consists of a physical system with some random physical quantity and the measurement equipment that reads these random variables. In digital random number generators we usually need to convert analog measurements into bit strings with the help of analog-to-digital converters. Measurement and quantization are noisy processes and there will be some contamination in what is called the *raw bit string* even if the measured quantity is truly random and free from correlations. The *postprocessing block* takes the raw bits and distills a shorter sequence without correlations.

The most important phase in postprocessing is randomness extraction. Randomness extractors are functions that transform the bits from the raw sequence into a uniform random sequence at the output with most or all of the randomness available in the input.

Figure 1 shows the block diagram of a typical physical random number generator. The exact parts vary from device to device. For instance, some physical random number generators are designed to produce raw sequences with negligible bias and forgo the postprocessing phase. There is a delicate balance in choosing an adequate postprocessing system. More involved randomness extraction methods usually allow to minimize the amount of random bits that are thrown away, but are slower. The overall bit rate depends on whether the increased production of bits compensates or not for the slower processing circuit or if it is justified to use a faster but more complex hardware to remove biases from the raw bit sequence.

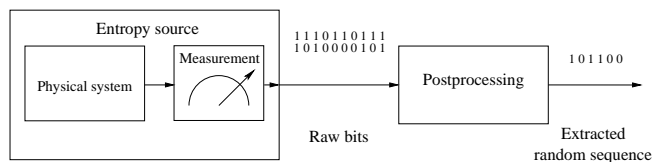


FIG. 1 Block diagram of a typical physical random number generator. A measurement system registers an unpredictable magnitude from a well-characterized physical system and converts the results into a binary raw bit sequence, which can still show some bias. The postprocessing stage extracts a smaller, ideally bias-free, random sequence assuming some bound to the amount of randomness of the raw sequence. The estimation usually comes from a thorough analysis of the original random physical system and the measurement errors.

In this review, we concentrate on the different quantum systems that can work as an entropy source. Section V describes measurements of radioactive decay. Section VII explains the many possible sources of entropy available in quantum optics. Section VIII discusses alternative quantum systems that do not use light.

Section X gives a brief review on some classical post-processing algorithms used to remove existing biases and Section XI introduces different quantum protocols that can be combined with imperfect randomness sources to obtain uniform output strings.

Before describing the particular systems from which quantum random number generators obtain randomness, in Section IV we comment the most common ways to measure entropy and the contexts in which each entropy measure can be applied. Different authors choose different criteria that will be mentioned when we describe the corresponding quantum random number generator.

In certain quantum random number generators, like device independent generators (Section IX.B), the physical measurement process and randomness estimation and extraction are intimately linked and we discuss them together.

IV. ENTROPY ESTIMATION

Entropy in its many forms offers a convenient way to measure randomness. The different entropies give a mathematical measure for surprise (how unexpected a value is). We express entropy in bits, in the information theory sense, which is closely related to the concept of thermodynamic entropy but takes it to a more natural formulation for information processing and communications.

A simple interesting measure is Shannon entropy (Shannon, 1948). For a random variable X with a probability distribution P_X so that $P_X(x)$ is the probability of getting the outcome x from a discrete set \mathcal{A} (an alphabet) with N possible values for x , the Shannon entropy of X , $H(X)$, is defined as

$$H(X) = - \sum_{x \in \mathcal{A}} P_X(x) \log_2 P_X(x). \quad (3)$$

Shannon entropy gives the average number of bits of information we can extract from a single outcome. For an alphabet of cardinality $N = |\mathcal{A}|$ and a uniform probability distribution, all the results are equally likely and we need $\log_2 N$ bits to describe them. We can imagine we place all the possible outcomes in a table and assign a $\log_2 N$ -bit string to each of them. In a uniform random process all the outcomes are equally “surprising” and we need to use all the bits. Less surprising distributions where some results are more likely than others would need, on average, less bits to be described. Table I shows an example of bit representations for the results of throwing a balanced and an unbalanced four-sided die (a tetrahedron).

Shannon entropy offers a rough estimation of randomness. Ideally, we would like to generate an almost uniform distribution with a Shannon entropy as close to $\log_2 N$ as possible. A higher Shannon entropy means we have

| Fair die | | | Loaded die | | |
|----------|--------|----------|------------|--------|----------|
| x | $P(x)$ | Sequence | x | $P(x)$ | Sequence |
| 1 | 1/4 | 00 | 1 | 1/2 | 0 |
| 2 | 1/4 | 01 | 2 | 1/4 | 10 |
| 3 | 1/4 | 10 | 3 | 1/8 | 110 |
| 4 | 1/4 | 11 | 4 | 1/8 | 111 |

TABLE I Entropy calculation example for a fair and a loaded four-sided die. For each possible outcome of a throw (first column) there is an associated probability shown in the second column. The third column shows a possible way to assign a bit sequence to each outcome. For a balanced die (left table) we have two bits of entropy $H(X) = -4(1/4) \log_2(1/4) = 2$. For a loaded die (right table), we have an entropy $H(X) = -(1/2) \log_2(1/2) - (1/4) \log_2(1/4) - 2(1/8) \log_2(1/8) = 1.75$. For the given encoding, we can check we need an average of $1(1/2) + 2(1/4) + 3(1/8) = 1.75$ bits to describe the result.

a distribution closer to uniform and that we can extract more random bits from the process, but there are other entropy measures that can give us a more useful figure when deciding how to use a randomness extractor to make the most efficient use of the available randomness, as described in Section X.

An interesting generalization of Shannon entropy is the family of Rényi entropies (Rényi, 1961). The Rényi entropy of order α is defined as

$$H_\alpha(X) = \frac{1}{1-\alpha} \log_2 \sum_{x \in \mathcal{A}} P_X(x)^\alpha. \quad (4)$$

Shannon entropy corresponds to the Rényi entropy in the limit $\alpha \rightarrow 1$. For any distribution, Rényi entropies obey the inequality

$$H_\alpha(X) \geq H_\beta(X) \quad (5)$$

for $\alpha \leq \beta$. Entropies of a different orders appear in many security proofs and randomness bounds (Cachin, 1997).

A particularly useful quantity is the min-entropy $H_\infty(X)$, which comes from taking the Rényi entropy when $\alpha \rightarrow \infty$. Alternatively, it can be defined as

$$H_\infty = -\log_2 \left(\max_{x \in \mathcal{A}} P_X(x) \right) \quad (6)$$

where we take the logarithm of the probability of the most likely outcome. The min-entropy gives a lower, worst-case bound to all the Rényi entropies. $2^{-H_\infty(X)}$ corresponds to the probability of guessing at the first attempt the outcome from measuring a random variable X with a known distribution. The optimal strategy is guessing the result is the most likely one. In the example given in Table I, for the uniform distribution the min-entropy is 2, but for the loaded die we have a value $-\log_2(1/2) = 1$. If we guess an outcome 1 we are right half of the time.

In a distribution with min-entropy k , every possible outcome x has a bounded probability $P_X(x) \leq 2^{-k}$. Any probability distribution of min-entropy k can be written as a convex combination of distributions that are uniform for k bits. This gives an important interpretation of min-entropy as the number of uniform bits that can be extracted from a given distribution. Intuitively, if no single string is too likely, for every random outcome we can extract about k bits of “surprise”, but no more (Chor and Goldreich, 1988; Zuckerman, 1990).

There are explicit constructions, like Trevisan’s extractor (Trevisan, 2001) and derived functions (Shaltiel, 2002), that can give almost k bits with a probability distribution as close to uniform as desired, provided there are some ancillary random bits of good quality. There are different kinds of randomness extractors (see Section X) in which min-entropy or derived quantities offer an upper bound on the number of available random bits.

Rényi entropies, including Shannon entropy and min-entropy, can be generalized to study joint distributions where part of the system is in the power of a legitimate user A and part of the system, which can be correlated to the first part, is in the possession of an eavesdropper B . In random number generation, the most useful quantity is conditional min-entropy. In the most general case, we can include distributions that come from quantum systems if we consider the density matrix ρ_{AB} of a state in the joint Hilbert space $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$ with a subspace that is restricted to A , \mathcal{H}_A , and a subspace only B can access, \mathcal{H}_B . The conditional min-entropy of ρ_{AB} related to a reduced density state σ_B in \mathcal{H}_B is defined as

$$H_\infty(A|B)_\rho = \sup_{\sigma_B} (-\log_2 \lambda), \quad (7)$$

where λ is the smallest real number for which

$$\lambda I_A \otimes \sigma_B - \rho_{AB} \quad (8)$$

is nonnegative (Renner, 2005) when I_A is the identity matrix corresponding to \mathcal{H}_A and we maximize over the density matrices σ_B with trace 1 describing the subsystem in \mathcal{H}_B . Conditional min-entropy gives how much information about the results of a measurement by A can be inferred from measurements on B alone. For classical distributions, $2^{-H_\infty(A|B)_\rho}$ gives the probability of guessing the outcomes of A from our knowledge of B using the optimal strategy (König *et al.*, 2009). If there is no side information (the systems of A and B are uncorrelated), we recover the definition and interpretation of the min-entropy in Equation (6).

When considering randomness extractors, it is also interesting to speak of the smooth min-entropy

$$H_\infty^\epsilon(A|B)_\rho = \sup_{\tilde{\rho}} H_\infty(A|B)_{\tilde{\rho}} \quad (9)$$

with a supremum taken over all the nonnegative operators $\tilde{\rho}_{AB}$ of trace 1 that are close to ρ_{AB} in the sense

that $\|\tilde{\rho}_{AB} - \rho_{AB}\| \leq \epsilon$ for the L_1 -norm $\|A\| = \text{tr} \sqrt{A^\dagger A}$ (König and Renner, 2011).

Instead of giving asymptotic parameters, like traditional entropies, smooth entropies give results valid for a single sample of a distribution. In random number generators, smooth min-entropy is useful as an estimator of the amount of random bits we can extract from a randomness source that might be correlated with an external attacker. Smooth min-entropy gives a tight bound on the length of the bits that a randomness extractor can produce from a given joint distribution and still give an output as close to uniform as desired and uncorrelated to any external system (König *et al.*, 2009; Renner, 2005).

For a general unknown source, estimating the min-entropy is far from trivial. The problem is intractable for any reasonable sampling circuit with limited size (Lyngsø and Pedersen, 2002; Watson, 2016). We can only determine min-entropy from measurement inefficiently. If our randomness source is stable and faraway bits are independent, this cost can be paid just once during characterization. Normally, physical random number generators use conservative, worst-case bounds for the min-entropy based on a deep analysis of the physical origin of the randomness and there are standardized methods for online estimation (Turan *et al.*, 2016). In that respect, quantum random number generators offer a clear advantage: their source of randomness is usually a very well defined quantum phenomenon. Quantum theory gives very accurate predictions. When compared to other random number generators that gather noise from complex processes like atmospheric noise, quantum random number generators have the virtue of a precise description of the randomness source which can be used to derive limits to the available min-entropy, even accounting for additional classical noise or the presence of eavesdroppers.

Nevertheless, even for these well-characterized quantum randomness sources, hidden correlations remain a challenge. There might be memory effects or correlations between consecutive runs of the quantum experiment that gives our random numbers and we must take due care to ensure independence and the lack of any experimental bias.

V. QUANTUM RANDOM NUMBER GENERATORS BASED ON RADIOACTIVE DECAY

A. The first quantum random number generators

With the rise of computer simulation during the second half of the 20th century, there was a growing need for electronic random number generators (Hull and Dobell, 1962). At that time, it was common to find tables of random numbers. The most famous of such compilations is probably the book “A million random digits with 100,000 normal deviates” from the RAND Corpo-

ration (RAND Corporation, 1955). The numbers in the book were generated using an electronic roulette wheel and were available in punched card format to allow easy interfacing with computers. There also appeared many electronic random number generators designed to be connected to computers or output devices like teleprinters (Sowey, 1972).

It was only natural for some researchers to turn to the intrinsic source of randomness of quantum phenomena (Isida and Ikeda, 1956; Manelis, 1961; Schmidt, 1970b; Vincent, 1970). Radioactive decay was a particularly accessible source of true randomness. Geiger-Müller tubes were already sensitive enough to capture and amplify α , β and γ radiation and reliable, well-characterized radioactive samples were available. For simplicity, most radioactivity-based quantum random number generators were based on the detection of β radiation (emitted electrons).

In a Geiger-Müller, GM, detector a single particle produces an ionization event that is amplified in a Townsend avalanche (Friedman, 1949). The result is a device that, when correctly configured, produces a pulse for each detected particle. The probability of any given atom to decay in a time interval $(t, t + dt)$ is given by an exponential random variable so that $P(t)dt = \lambda_m e^{-\lambda_m t} dt$ for a material with a decay constant λ_m . If the sample retains many of its original atoms (we are in times much smaller than the half-life) and the sample-detector system undergoes practically no change during our time interval (the position of the sample is constant, the gas in the GM tube does not become contaminated...), the time between detected pulses is also an exponential random variable. The times are independent from previous results and the number of pulses that arrive in a fixed time period follows a Poisson distribution. The exact rate depends on many factors, but it can be determined experimentally and we can be satisfied that the pulses arrive at independent times (Silverman *et al.*, 1999). The probability of finding m pulses in an observation period of T seconds is $P_m(T) = \frac{(\lambda T)^m}{m!} e^{-\lambda T}$, where λ gives the mean number of pulses we detect in one second for our source and corresponds to the parameter of the exponential distribution.

The QRNGs we describe in this Section are the fore-runners of the present day optical QRNGs we will see in Section VII that use similar concepts and circuits, but replace the radioactive source and the GM counter with photon sources and detectors.

The first QRNGs based on radioactive decay share many common elements. Most use digital counters to convert the pulses from the detector into random digits. A digital counter increases its output value by 1 when it receives a pulse at its input and can be reset to start the count from 0. Another key element is timing with a digital clock. These QRNGs can be best explained if we speak in terms of fast and slow clocks to describe clocks

with a frequency ν that is significantly greater or smaller than the mean rate of detection. A fast clock, with $\nu > \lambda$, generates many pulses between Geiger counts and when a slow clock, with $\nu < \lambda$, produces a pulse, there has been enough time to have registered many counts in the GM detector.

With these elements, the randomness in the time of arrival can be converted into random digits in a few different ways. The generators of Isida and Ikeda (Isida and Ikeda, 1956) and Vincent (Vincent, 1970) use a counter driven by a fast clock that is read and then reset to zero every time we get a count on the detector. The value of the counter at the moment of the detection is used to produce the random number. Figure 2 gives a graphical description of the method. The distribution of values is

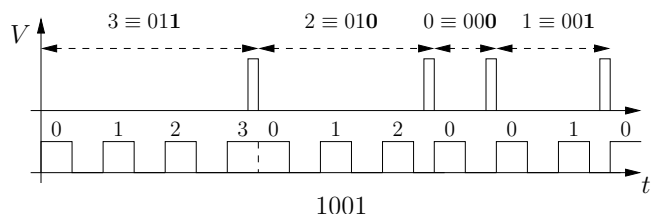


FIG. 2 Fast clock method: A fast clock (down) is used to increase a counter. Whenever a detection is made (up), the counter is read and reset, generating one random number.

not uniform and some correction is necessary. If we are producing decimal digits, we can take the least significant figure (Isida and Ikeda, 1956). The equivalent method for binary sequences is looking at the parity of the value of the counter, checking if the number of counted pulses is even or odd (Vincent, 1970). This kind of correction draws from previous results for true random number generators that face similar problems (Thomson, 1959).

A second option is to use a slow clock to determine when to read the counter. In the generator of Schmidt (Schmidt, 1970b), the pulses from the GM detector increase the value of a counter. When the slow clock produces a new pulse, the value of the counter is used as a random digit and the count starts again from 0. The output corresponds to the number of particle counts in each clock period. We restrict to a counter that generates values from 0 to $M - 1$, a modulo M counter. When $M = 2$ we have a binary random number generator. The distribution of the sampled digits is not uniform, but if we take the modulo M addition of multiple outputs, we can obtain a distribution with as small a bias as desired. This is called “contraction” and is discussed in detail in Schmidt’s paper (Schmidt, 1970b). Figure 3 shows an example of this generation method.

Radioactive decay has also been used to generate white noise for analog computers (Goodyear Aircraft Corporation, 1954; Howe, 1961; Manelis, 1961). Random noise generation was important, among others, in the analog calculations in airplane design simulations. It also has

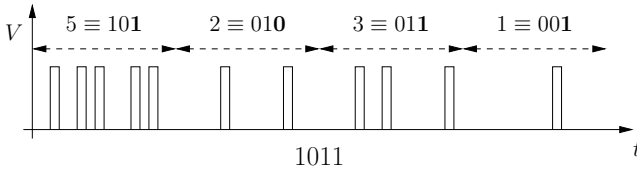


FIG. 3 Slow clock method: The Geiger detector is read at fixed intervals, generating a random number that equals to the number of detections during the period.

applications as a test signal and, generally, in communications and simulation problems where a broadband signal is necessary (Gupta, 1975). In this case, the pulses from the GM detector trigger a change of state in a voltage signal. Whenever a particle is detected the signal goes from high to low voltage or from low to high. The resulting random signal is called random telegraph noise (Rice, 1944). In this case we do not want a binary signal, but Gaussian noise. Instead of sampling, the signal is directed to a low pass filter to complete the noise generator.

B. Evolution

After the initial proposals, there have been different refinements to the basic concept. QRNGs based on radioactive decay are still popular. A good example is the web-based random number server HotBits (Walker, 1996) that has been working since 1996. In the HotBits generator, the random times of arrival of the radiation to the Geiger counter give pairs of intervals of random length. The time between two consecutive pulses is stored as t_1 and compared to the time between the next two pulses t_2 . The random bits come from comparing the times. If $t_1 > t_2$ we output a 0 bit and if $t_1 < t_2$ we output a 1. The generator reverses the criterion for 0 and 1 for every time pair in order to compensate for small systematic biases that might favour slightly unbalanced intervals. This provides a crude correction for small problems like, for instance, the loss of radioactive material due to radioactive disintegration that makes the second interval shorter on average by a very short time. Figure 4 gives a graphical description of the method.

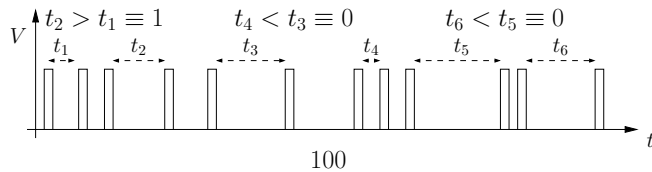


FIG. 4 Time difference method: This method compares the time between two events in the Geiger detector. If $t_i < t_{i+1}$ then a bit with value one is generated. Otherwise, the bit generated will be zero.

Some modern proposals replace Geiger counters with semiconductor detectors. Semiconductor devices such as PIN photodiodes can also capture the radiation from radioactive decay (Knoll, 2010; Lutz, 2007). Semiconductor detectors are convenient, as they do not require the same high voltage as Geiger tubes. The resulting signal is weaker than that of GM counters, but there are low noise amplifiers that can produce output pulses of a few volts of amplitude. While they can have different sensitivities and need calibration, for the generation of random numbers the important property is not as much determining the actual rate of the particles coming out of the source as it is registering random events.

Using off-the-shelf semiconductor devices can simplify the design of random number generators. One example of such generators is given by (Alkassar *et al.*, 2005) with a variation of the time interval method. Instead of comparing the time between pulses, the system reads a fast clock every time a pulse arrives. If the clock is in a high state (in the high voltage level of the clock cycle) at the moment of arrival the generator outputs a 1. If it is low it outputs a 0. For a good time resolution, the least significant bit of the digitized time should be random and there is no need for postcorrection.

Two other proposals for QRNGs that use semiconductor detectors with radioactive decay appear in (Duggirala *et al.*, 2010). The first proposal tries to address the problem that in QRNG we have access to an exponential random variable, the time of arrival, or a Poisson random variable, the number of pulses in a fixed time interval. But, in many occasions, RNGs are required to produce uniform random numbers. An exponential random variable of parameter λ can be converted to a uniform random variable if we compute:

$$U = e^{-\lambda E}, \quad (10)$$

where U is the uniform distribution and E the exponential distribution. The first proposal of (Duggirala *et al.*, 2010) addresses this with an RC circuit. They use a semiconductor detector whose output pulses trigger the fast discharge of a capacitor. The voltage at the RC circuit when a pulse arrives is the output variable. This approach has several limitations. It needs specialized hardware to transform the voltage to the output and has problems with noise. For that reason there is an alternative proposal with an approach similar to (Isida and Ikeda, 1956; Vincent, 1970), where a fast clock $\nu \gg \lambda$ drives an N -bit counter which is read when a pulse arrives. Here, the clock is supposed to be fast enough to guarantee the samples are uniform in the 2^N values.

C. Limitations

While QRNGs based on radioactive decay are a good way to obtain high quality true random numbers, they

have some drawbacks that limit their practical use. An important barrier is the low bit rate they can achieve, usually below a few hundred kilobits per second.

The first problem is the need for a radioactive source. In principle, all decay-based QRNGs could work on background radiation. Unless it is isolated, a detector will count stray cosmic rays, radiation from radium, thorium or other radioactive materials in the Earth's crust or particles from radon on air. However, natural activity rarely produces enough particles to cause more than a few counts per second. This poses a fundamental problem for the widespread use of radioactive decay QRNGs. In order to achieve a fast rate, the QRNG needs a highly radioactive source. The reviewed generators used Cobalt-60 (Isida and Ikeda, 1956), Strontium-90 (Schmidt, 1970b), Caesium-137 (Walker, 1996), Americium-241 (Alkassar *et al.*, 2005) or Nickel-63 (Duggirala *et al.*, 2010). This is highly inconvenient and requires improved safety measures. While α sources like Americium are easier to isolate and are common in smoke alarms, the additional precautions prevent straightforward computer integration and this approach works well only for dedicated isolated servers like HotBits (Walker, 1996).

A second limitation to the generated bit rate is the *dead time* of the detectors. In Geiger counters the avalanche that amplifies each count ionizes the gas inside the GM tube. The avalanche stops when the positive ions surround the cathode inside the tube. These ions prevent further avalanches until they have returned to their normal state (Friedman, 1949). The dead time is the minimum time for the GM tube to recover its full detection capability and can go from tens of nanoseconds to a few microseconds. This limits the count rate to the MHz range. Semiconductor detectors also need to replenish the carriers after each detection and have dead times in the microsecond range.

Dead time and other sources of non-uniformity need to be corrected when generating random bits. Vincent describes some important cautions in a follow-up paper (Vincent, 1971) to his original generator proposal. In general, the quality of the generated bits will be good and, when there is some residual bias, there exist simple postprocessing methods to recover a random output.

A final problem specific to semiconductor detectors is the damage they suffer from radiation. Geiger tubes also degrade with time, but the effect of radiation on them has been extensively studied, while semiconductors used specifically for radiation detection are relatively new. As long as the damage gives a progressive and slow reduction in efficiency, the output would retain randomness, but more studies on the long term behaviour of these detectors are needed.

Despite these constraints, radioactive decay is a suitable source of randomness for low speed applications. It can, for instance, be used to provide entropy for the seed of pseudorandom number generators. For more de-

manding systems that require high bit rates or when we would like to avoid radioactive sources, the recent optical QRNGs described in Section VII are good substitutes.

VI. RANDOM NUMBER GENERATORS BASED ON NOISE

Noise in electronic circuits is one of the preferred sources of entropy in classical physical random number generators. Noise appears as an unwanted effect in electronic systems of all kinds and it is readily available. A typical random number generator using noise is shown in Figure 5.

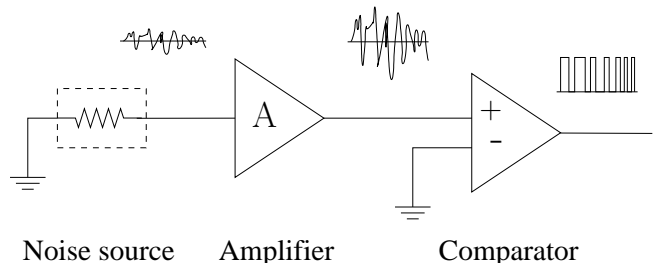


FIG. 5 Conceptual representation of a typical noise-based random number generator. The voltage coming from a source of white noise is amplified and compared to a threshold in a comparator to produce a digital signal with random transition times. This signal can be sampled or processed later to give a random bit sequence.

The noise source is represented as a resistor, but other elements can take its place. A Zener diode operated in the reverse breakdown region is another popular choice. In this scheme, voltage fluctuations due to noise are amplified and compared to a threshold to generate random bits. For a threshold of 0 volts, we can sample the amplified noise periodically and assign a 0 if we find a negative voltage and a 1 to a positive voltage.

If, instead of sampling, we generate a pulse every time the voltage from a white noise source crosses the threshold, the output will be a series of pulses with times of arrival that correspond to a Poisson distribution and we can use any of the methods described in Section V to produce random sequences. The electronic noise circuit replaces the Geiger counter in an otherwise unchanged system. In fact, many proposals for QRNG based on radioactive decay discuss both methods in parallel (Gude, 1985; Vincent, 1970).

There are multiple examples of true random number generators based on this electronic noise like those in (Holman *et al.*, 1997; Petrie and Connelly, 2000) to name a few.

Noise in those systems comes fundamentally from two sources, shot, or Schottky, noise (Schottky, 1918) and thermal, or Johnson-Nyquist, noise (Johnson, 1928; Nyquist, 1928), with flicker noise contributing sometimes

at low frequencies. Shot noise generates from quantum effects due to the granularity of the current. Currents are formed by discrete carriers and show quantum fluctuations. Thermal noise comes from thermal agitation of the carriers and is produced by statistical motion that depends on the temperature. In practice, both noises tend to appear side by side and are difficult to isolate. In many cases the frontier between shot and thermal fluctuations is blurry (Landauer, 1993).

In this review, we will not discuss in detail random number generators based on electronic noise. While electronic noise coming from shot fluctuations can be rightfully said to be quantum (Reznikov *et al.*, 1998), it is usually not well characterized and separated from thermal noise, it is subject to many environmental fluctuations and can show memory effects (Stipčević, 2012). Somewhat arbitrarily, we choose to concentrate on generators where the quantum effects are well isolated and we have a higher degree of control. Unless there is some interesting effect, we will not discuss true random number generators where quantum noise is only an unquantified part of the total available randomness.

There are a few interesting exceptions. Certain commercial quantum random number generators use electronic noise in semiconductors. For ComScire's QRNG there is a detailed estimation of the quantum entropy gathered from shot noise in MOS transistors (ComScire, 2014). Likewise, under the right conditions, Zener diodes can be operated in a regime where quantum shot noise dominates (Somlo, 1975; Stipčević, 2004).

VII. OPTICAL QUANTUM RANDOM NUMBER GENERATORS

Most of the existing QRNGs are based on quantum optics. The inherent randomness in many parameters of the quantum states of light allows for a rich choice of implementations. Light from lasers, light emitting diodes or single photon sources is a convenient and affordable substitute for radioactive material as a source of quantum randomness and there are many available detectors. In this section, we study some of the most common ways to harness quantum light to produce random bits.

First, we give an overview of the concepts of quantum optics that appear in the generators. Then, we propose a classification of optical quantum random number generators, OQRNGs, based on the generation mechanism. Table II gives a summary of the covered optical generators with some representative examples, the typical bit rates and the limitations of each kind of generator.

A. Quantum optics in random number generators

The optical field can be described at the quantum level in terms of photons (Klauder and Sudarshan, 1968; Loudon, 2001). From the many possible families of quantum states, Fock states and coherent states give the most relevant description of the quantum states of light in random number generators. Fock states, or number states, are described as states $|n\rangle$ that contain n photons sharing a mode (they have the same frequency, polarization, temporal profile and a common path). Coherent states, which share many properties with classical light, can be written as a superposition of number states

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \quad (11)$$

where α is a complex number. The amplitude $|\alpha|^2$ corresponds to the mean photon number of the state. Weak laser light is an excellent approximation to a coherent state. We can also use the coherent states from a laser to produce a proxy for single photon states by choosing a low enough intensity, as it usual, for instance, in quantum key distribution with typical values of α around 0.1.

In many applications we are only interested in producing uncorrelated single photons. In that case, attenuated light from a light emitting diode, LED, can be valid as long as we generate photons with a separation larger than the coherence time of the source.

There are many different technologies that can generate single photons and detect them (Buller and Collins, 2009; Eisaman *et al.*, 2011). Photomultiplier tubes (PMTs), single photon avalanche photodiodes (SPADs) operating in the Geiger mode or superconducting nanowire detectors are some of the most popular detectors, but there is a growing number of alternatives (Hadfield, 2009). For instance, there have been important advances in silicon detectors (Ghioni *et al.*, 2007) that open the door to integration in electronic circuits and in superconducting nanowire single-photon detectors that extend the high-efficiency detection wavelengths to the near infrared (Marsili *et al.*, 2013).

Traditionally, while binary decisions between no photons and one or more photons are relatively easy to take, single photon detectors have limited photon counting capabilities. There are new improved detectors, but their cost is still high and most applications use a binary approach to photon detection. Another limitation to most single photon detectors is the time they need to recover after a detection, known as dead time. We will later see how these limitations affect our quantum random number generators.

| Type (Section) | Physical principle | Representative examples | Rate (order) | Challenges |
|----------------------------------------------|-----------------------------------------------|-------------------------------------------------------------------------------------------------|--------------|-------------------------------------------------------------------|
| Branching path (VII.B) | Path superposition + measurement | (Jennewein <i>et al.</i> , 2000) | Mbps | - Unbalanced detectors. - Detector dead time. |
| Time of arrival (VII.C) | Time of arrival statistics | (Stipčević <i>et al.</i> , 2007) (Wayne <i>et al.</i> , 2009) (Wahl <i>et al.</i> , 2011) | Mbps | - Time precision. - Detector dead time. |
| Photon counting (VII.D) | Photon number statistics | (Fürst <i>et al.</i> , 2010) (Ren <i>et al.</i> , 2011) | Mbps | - Photon resolving capability. - Detector dead time. |
| Attenuated pulse (VII.E) | Binary measurement of coherent states | (Wei and Guo, 2009a) | Mbps | - Source instability. - Detector dead time. |
| Vacuum fluctuations (VII.F) | Shot noise measurement | (Gabriel <i>et al.</i> , 2010) (Shen <i>et al.</i> , 2010) (Symul <i>et al.</i> , 2011) | Mbps-Gbps | - Classical noise. - Postprocessing. |
| Phase noise (VII.G) | Laser phase noise | (Guo <i>et al.</i> , 2010) (Qi <i>et al.</i> , 2010) (Jofre <i>et al.</i> , 2011) | Gbps | - Phase drift. - Pulse repetition rate. |
| Amplified Spontaneous Emission, ASE (VII.H) | Amplitude fluctuations in ASE noise | (Williams <i>et al.</i> , 2010) (Argyris <i>et al.</i> , 2012) | Gbps | - Sampling/digitization. - Postprocessing. |
| Raman Scattering (VII.I) | Interaction with phonon fluctuations | (Bustard <i>et al.</i> , 2011) (Collins <i>et al.</i> , 2015) | kbits-Mbps | - Raman gain. (Stimulated) - Detector dead time. (Spontaneous) |
| Optical Parametric Oscillators, OPOs (VII.J) | Bistability in optical parametric oscillators | (Marandi <i>et al.</i> , 2011) (Marandi <i>et al.</i> , 2012b) | kbits | - Cavity decay time. - Pump repetition rate. |

TABLE II Summary of the optical methods for quantum random number generation. The table gives the section where we describe the details of each implementation, the principle of operation, a few representative examples, the order of magnitude of the typical bit rates of each generator and a list of the most important limitations.

B. Branching path generators

OQRNGs take advantage of the random nature of quantum measurement. In a large number of quantum random number generators this measurement is taken over photons in a superposition of two or more paths. For instance, if we define a state $|1\rangle_1|0\rangle_2$ which represents one photon in the first of two possible paths and a state $|0\rangle_1|1\rangle_2$ with the photon in the second path, we can prepare a superposition

$$\frac{|1\rangle_1|0\rangle_2 + |0\rangle_1|1\rangle_2}{\sqrt{2}}. \quad (12)$$

Measuring that state with a detector at the end of each path will result in a click in just one of the detectors with a probability one half for each path. There are many quantum optics experiments that generate similar states in Mach-Zehnder interferometers and related optical setups. Figure 6 shows the archetypal QRNG that uses quantum measurement with detectors in different positions as proposed for the choice of basis in QKD⁴ (Rarity

et al., 1994). In this configuration, we have a balanced

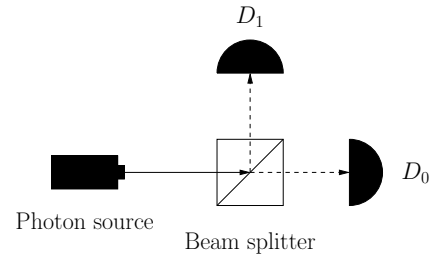


FIG. 6 A weak light source sends a state with one photon to a balanced beam splitter. The path the photon takes at the output is random and there will be a detection with the same probability at each detector. We can consider that a click on detector D_0 is recorded as a 0 bit and a detection in D_1 is a 1.

beam splitter with equal transmissivity and reflectivity

SARG04 (Scarani *et al.*, 2004), the receiver must choose its measurement basis at random. We can imagine a switch connected to an RNG that directs the incoming photons to one of two alternative measurement setups depending on the result. In practice, the implementation might be different.

⁴ In the most popular quantum key distribution protocols, like BB84 (Bennett and Brassard, 1984), E91 (Ekert, 1991) or

$T = R = \frac{1}{2}$ so that classical light entering any of the two input ports would be divided into two streams of the same optical power, half going through and half reflecting. If we have a single photon in one input and the vacuum in the second, we cannot divide the power and we have the desired path superposition. Conceptually, the simplest way to produce random numbers from this path division is placing two detectors D_0 and D_1 , one for each output, and generate a bit every time we detect a photon. Clicks in D_0 would produce a 0 bit and clicks in D_1 would produce a 1. Optical QRNGs using spatial superpositions usually apply variations on this basic scheme. In fact, in the original QKD application (Rarity *et al.*, 1994) the random number generator was not fully implemented as a separate device controlling the measurement basis in the receiver. Instead, they used a passive implementation where the beam splitter took the input state and sent it with equal probability to one of two measurement setups, one for each possible basis. A complete implementation with a beam splitter and two photomultiplier tubes as detectors was first deployed as a subsystem in the experimental implementation of a Bell test (Weihs *et al.*, 1998) and later developed as a standalone device (Jennewein *et al.*, 2000) with some modifications. The most important difference is the way the random sequence is created, with a random digital signal as an intermediate step. In the modified model, detections in D_1 take a digital signal to a high level and detections in D_0 to a low level. The result is a random signal with changes in a time scale of the order of the inverse of the mean photon detection rate. If we sample this signal with a clock with a frequency sufficiently below the photon detection rate, assigning a binary 0 when the state is low and a 1 for high state, we obtain a constant stream of random bits. The same procedure was tested with polarized photons in a linear 45° state and a polarizing beam splitter with essentially the same results. In (Wang *et al.*, 2006) there is an alternative take on polarization to path conversion with a weak laser source with linear polarization attenuated to the single photon level and a Fresnel prism that separates the positive and negative circular polarization components and directs them to two avalanche photodiodes. This kind of polarization generator can be modified to provide adjustable probabilities for each bit value if we include an electronically controlled polarizer at the source, like in the fiber-based QRNG of (Xu *et al.*, 2015) or the decision making system in (Naruse *et al.*, 2015), which adapts the probability to previous results.

Other generators are implemented in optical fiber systems where a weak light pulse is directed to a balanced fiber coupler connected to two detectors. Two examples are the generators in (Soubusta *et al.*, 2001, 2003), which use a pulsed laser source that produces, after a tunable attenuation circuit, a coherent state with an amplitude greater than 1 that maximizes the random bit generation

rate⁵.

There are also implementations based on polarization inside optical fiber, with sources that are either single photon states or polarization entangled states

$$\frac{|H\rangle_1 |V\rangle_2 - |V\rangle_1 |H\rangle_2}{\sqrt{2}} \quad (13)$$

that are a superposition of horizontally polarized photon states $|H\rangle$ and vertically polarized photons $|V\rangle$ (Bronner *et al.*, 2009; Fiorentino, 2006; Fiorentino *et al.*, 2006, 2007). The generators with entangled states produce the photons in nonlinear crystals and use coincidence detectors. One of the photons can be used as a herald or we can watch for anticorrelated polarization measurements in the different paths.

QRNGs with optical path branching can show a few problems. All types of photodetectors have some kind of dead time after a click. This can generate anticorrelation of neighbouring bits. A detection at some time makes it less likely to find a photon immediately after due to the “blunted” sensitivity of the detector before full recovery. Also, for real detectors and beam splitters we will find slightly different detection efficiencies and coupling ratios that can introduce some bias. There are a few other concerns: afterpulsing can create correlated bits, pulses with multiple photons can produce simultaneous detections and the presence of dark counts means there will be occasional clicks when there are no photons. In practice, these effects, particularly dead time, limit the maximum generation rate to a few Mbps, which could be improved with detectors with a smaller recovery time.

There are many ways to counteract these problems. For instance, the generator in (Jennewein *et al.*, 2000) includes a setup phase in which the tube voltage and the detection threshold of the photodetectors can be adjusted to compensate detection efficiency and path coupling differences. Another popular method is applying an unbiasing algorithm that distils a random sequence at the cost of losing some bits. We discuss unbiasing in more detail in Section X.

If we convert path superpositions into time superpositions we can use one detector instead of two, or more, detectors, and avoid problems caused by having different detection efficiencies and dark count numbers. That is the approach in (Stefanov *et al.*, 2000) where weak light from a timed pulsed laser inside an optical fiber is coupled into two fibers of different length connected to the

⁵ Ideally, we should choose the amplitude of the coherent state α so as to maximize the probability of only one detector clicking either due to one or more photons. For the coherent state at the input of the beam splitter, this amplitude should be $\alpha = \sqrt{2 \ln 2}$, but the final configuration uses a higher level due to additional losses.

same detector. The additional delay in one path permits to distinguish the route of the photon. The whole attenuation is designed to make each path equally likely.

The random bit generation rates can improve if the generator measures more than two possible paths. Each measurement then gives more than one random bit. W-states of the form

$$|W_n\rangle = \frac{|10\dots 00\rangle + |01\dots 00\rangle + \dots + |00\dots 01\rangle}{\sqrt{n}} \quad (14)$$

can be created by branching the photon path many times and give the desired statistics. This approach takes more complex devices, but integrated optical circuits inside silicon chips can offer an economical and scalable alternative. Integrated circuits show less variability and the optical couplers that replace the beam splitters show smaller deviations from a perfectly balanced device. There have been experimental demonstrations of integrated generators with 8 outputs that can produce 3 bits per each measurement, with potential for straightforward extension to 16 outputs (Gräfe *et al.*, 2014).

Another important point is the choice of photon sources. In many of the reviewed generators, the photons come from LEDs. In order to guarantee independent photons, the rate is limited to be much smaller than the coherence time, which is usually not a problem as the limiting factor tends to be the dead time of the detectors. A common alternative is using weak laser light. However, it can be interesting to study other photon sources. The effect of a beam splitter on the different quantum states of light is well known (Fearn and Loudon, 1987; Ou *et al.*, 1987; Prasad *et al.*, 1987) and the resulting counting statistics can be used in a variety of generation schemes. There are results that suggest that true single photon sources, which show photon antibunching, can increase the rate of random bits when compared to coherent light from lasers. Brighter sources have a faster photon rate and, in those conditions and once all the effects are considered, single photon sources offer the best overall random bit rates (Oberreiter and Gerhardt, 2015).

Finally, there are QRNGs that give up beam splitters altogether. These generators use the natural spatial uncertainty in the generation process. For instance, the commercial Quantis RNG has two integrated detectors placed in positions where the spatial profile of a light source has an equal amplitude (Ribordy *et al.*, 2009).

A detector array allows a higher generation rate with more of one bit per detection. In that case, there must be some compensation for the non-uniform spatial profile of most photon sources. An early incarnation of this concept was the optical random number generator of (Martino and Morris, 1991) that used photon counting detectors with levels around the thousands of photons and needed involved calibration procedures. More recent OQRNG use detectors with single photon precision. One

of such generators uses a micro channel plate detector and a wedge and strip anode to assign two coordinates to the place where a photon from an attenuated LED reaches a photocathode (Qiurong *et al.*, 2014). Then, the random bit sequence is extracted from the position using Huffman coding to compensate for non-uniformities.

Other implementations use an integrated array of single-photon avalanche photodiodes, SPADs, combined with postprocessing (Burri *et al.*, 2014; Burri and Stucki, 2013; Stucki *et al.*, 2013). A weak light source produces clicks in random positions of the array. We can assign a 1 to the pixels that find a photon and a 0 to the pixels that do not click. Even if the distribution of bits in the discrete 2D grid of the detectors is not uniform, we can extract a random sequence if we compare two neighbouring pixels, which should have almost the same probability of detecting a photon, and then take the logical XOR of the bits as their output. Alternatively, we can use the whole string from the array as the input of a randomness extraction algorithm. In these generators, apart from the usual dead time, afterpulsing and dark counts concerns, we have to contemplate the possibility of crosstalk between detectors. However, the effects of crosstalk can be minimized with a proper design.

C. Time of arrival generators

There are also multiple ways to use the randomness in photon detection times to generate random bits. The OQRNGs in this and the following section are usually based on the same principles as the QRNGs that detect radioactive decay we discussed in Section V. In fact, one of the earliest proposals for this kind of quantum random number generator was a random pulser that tried to simulate the arrival of radioactive counts in order to calibrate nuclear instruments (Takeuchi and Nagai, 1983). Some methods are essentially the same than their Geiger counter predecessors but replace radioactive materials with light sources, which can achieve much higher bit rates. Photon production is faster and less problematic and the maximum bit rate is now limited by the capabilities of the detectors instead of the generation speed.

The basic QRNG using time has a weak source of photons, a detector and timing circuitry that registers either the precise time of each detection or the number of clicks in a fixed period of time. In short time periods with one or only a few photons on average, both the photons coming from LED incoherent light and from the coherent states from a laser arrive at the detector following an exponentially distributed time $\lambda e^{-\lambda t}$ for an average number of photons per second λ . The time between two photodetections is the difference of two exponential random variables, which is also exponential. In that case, we can compare the time differences between the arrival of consecutive pulses and compare two time differences

t_1 and t_2 . We can assign a 1 if $t_2 > t_1$ and a 0 if $t_1 > t_2$. This gives a uniform random bit.

In time of arrival generation, precise time tagging becomes important. Measurement will always have a limited precision and the effects of digitizing the time intervals can be noticeable. Instead of having real times t_1 and t_2 , we have integers with the number of the counted clock periods n_1 and n_2 . For instance, the possibility $t_1 = t_2$, with a negligible probability for an ideal continuous time measurement, must be taken into account. Now we can find two consecutive measures for which we read the same time, $n_1 = n_2$. In our basic scheme that generates a 0 or a 1 depending on whether the second interval is shorter than the first one or not, the output is not defined and we must discard these results. Considering the equality as a valid result would require a different analysis of the probabilities of each outcome and how we assign them to a binary bit.

Figure 7 shows two potential approaches to timing with resettable and non-resettable clocks.

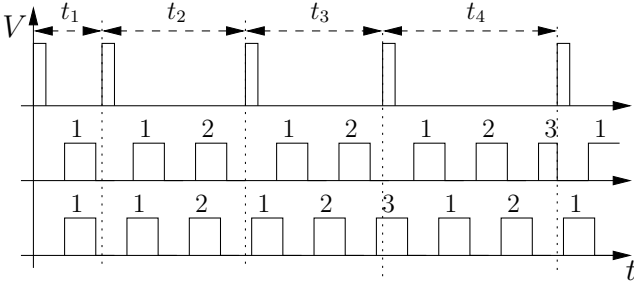


FIG. 7 Generation scheme where the arrival of the rising edge of a detection pulse (up) starts a count of the rising edges of a clock. The clock can be independent from the pulses (bottom) or be reset with every incoming pulse (middle). In the example, $t_2 > t_1$ and $t_4 > t_3$ and the output should be 11. Using a resettable clock we find discrete times $n_1 = 1$, $n_2 = 2$, $n_3 = 2$ and $n_4 = 3$ that produce the sequence 11 ($n_2 > n_1$ and $n_4 > n_3$), while for a fixed clock we read $n_1 = 1$, $n_2 = 2$, $n_3 = 3$ and $n_4 = 2$ and the output is 10.

The fine details are explained at length in (Stipčević *et al.*, 2007), which gives one of the first optical quantum random number generators that uses time detection. This generator takes the photons from an LED arriving at a PMT and compares the times of arrivals, in a scheme similar to the method that compares the time of arrival of two particles at a Geiger counter shown in Figure 4. As expected, a fast clock with many ticks per click gives better results as we have a higher resolution. A second conclusion is that using a resettable clock eliminates many biases coming from imprecise time measurement.

A similar generator where the source of the photons, an LED, and the detector, an SPAD, are integrated side by side in the same chip is described in (Khanmohammadi *et al.*, 2015).

The random time of arrival can also be used as a sig-

nal that chooses a time bin from a clock, following the template of the radioactive decay generators summarized in Figure 2. The generator of (Dynes *et al.*, 2008) uses a gated APD detector and outputs a 1 if a photon is found in an even clock cycle and a 0 if it is found in an odd cycle. The scheme also adds a self-differentiating circuit to avoid biases from the capacitive response of the detector. An interesting variation on the even-odd generation method is given in (Ma *et al.*, 2005), where a pulsed laser produces attenuated states with a small probability of having one or more photons in each time bin. The bins are grouped into pairs and output 0 is assigned to an empty bin with no detection followed by a detection and output 1 to a detection followed by an empty bin. This is basically equivalent to using the parity of the time bin where a photon is found, but discards occasional consecutive counts and can be extended to different ways of grouping the time bins (Yu *et al.*, 2010).

There are many other proposals that try to generate random bits from time measurements. In principle, each time difference t_i is a real number and it would seem we can extract an infinite amount of entropy from two pulses. However, time precision limits how many usable bits we have. If our timing information has p bits of precision, the time bin in which we find a photon is a random variable with $N = 2^p$ possible values and we can compute the probability of a photon arrival in each bin. We can then compute the relevant entropy measure (Section IV) for our discrete probability distribution to see how many bits of randomness are available.

Certain OQRNGs use digitized time differences with k bits and distill the available entropy into a random bit string with a mathematical function. In (Wayne *et al.*, 2009) the photons from a laser diode are detected with an avalanche photodiode and then the least significant bits of the measured time are collected until they reach 432 bits that are then whitened with the SHA-256 algorithm (National Institute of Standards and Technology, 2012). Similarly, in (Wahl *et al.*, 2014, 2011) an attenuated LED sends photons to a photomultiplier tube and the bits from the time of arrival are processed with a resilient function (Bose and Ray-Chaudhuri, 1960; Sunar *et al.*, 2007) chosen to take the maximum advantage of the available entropy while doing the processing with a function that can be efficiently implemented in hardware. The generator of (Kravtsov *et al.*, 2015) also tries to optimize extraction from quantized time differences with hardware designed to work with minimal computation that includes a lookup table that implements Elias' deterministic randomness extraction algorithm (see Section X.A.1 and (Elias, 1972)).

All these processing algorithms try to convert most of the randomness available in the exponential distribution into a uniform bit sequence and require additional hardware and processing effort.

There are also ways to generate photons with a more

uniform time of arrival. The counting statistics at a detector are a function of the photon flux variation at the source (Klauder and Sudarshan, 1968). For a laser diode with a non-uniform current, we have an inhomogeneous Poisson process and the waiting time at the detector can be adjusted. The generator in (Wayne and Kwiat, 2010) has circuit that reshapes the exponential time of arrival distribution into an almost uniform one. For a variable photon flux $\lambda(t)$, the time of arrival is a distribution

$$\lambda(t)e^{-\int_a^b \lambda(t')dt'}. \quad (15)$$

Ideally, we would want a uniform distribution, which can be approximated by driving a laser with a current that repeats periodically a finite approximation to the function

$$\frac{1}{T-t} \quad (16)$$

where T is a reset parameter that determines when to restart the pulse cycle at the source. The current goes back to the initial value when T finishes or when a pulse is detected, whichever happens first.

An alternative way to “flatten” the exponential distribution is taking short time bins from an external time reference and consider the time of arrival within those bins (Nie *et al.*, 2014). The time when the photon arrives with respect to the origin of a particular bin is a random variable in a short, almost flat, part of the exponential time distribution, which gives a distribution closer to that of a uniform random variable.

There are also mixed generators that use both time and space uncertainty. For instance, the generator in (Li *et al.*, 2013) uses detectors in two paths to start and stop a timer, in a method similar to the intermediate signal generator in (Jennewein *et al.*, 2000), and uses the resulting time to generate random numbers. In order to have a uniform probability, the scheme assigns a binary string to non-uniform ranges of time measurements that have the same probability. The generator in (Thamrin *et al.*, 2008) works with the same kind of intermediate signal. It uses polarized photons combined with a fast clock sampling method (Fig. 2). The value of a counter is measured with the falling edge of a signal with its transitions controlled by two spatially separated detectors, although there seems to be no post-processing to avoid correlation in the most significant bits. The generator in (Stipčević and Bowers, 2015) combines a branching path configuration at a beam splitter with the time difference method. There is one random bit associated to the detector that finds the photon and a bit associated to the difference between times of arrival at the detectors. The generator combines both bits to provide a random stream without the biases of the two independent generation methods.

D. Photon counting generators

Another large group of generators based on time effects use the number of registered detections in a fixed time T . For an exponential time random variable, the number of photons that arrive in a fixed time T follows a Poisson distribution. The probability of finding n photons in that interval is

$$P(n) = \frac{(\lambda T)^n}{n!} e^{-\lambda T}. \quad (17)$$

For instance, the generator in (Fürst *et al.*, 2010) follows an approach similar to the radioactive decay generator of (Schmidt, 1970b) (see Figure 3) and generates bits from the parity of the total counts registered in a fixed period. The source of light is an LED and, as in many other time-based QRNG, the authors turn to PMTs for faster detection. Interestingly, the generator takes advantage of the dead time of the detector. For the parity method, the random variable that describes the true rate of photocounts when the detector has a small dead time gives a smaller final bias when compared to a pure Poisson process. This approach of taking the least significant bit of the photon count is also followed in (Lopes Soares *et al.*, 2014), where thermal and weak coherent state sources are compared.

Certain generators use an approach similar to the time difference comparisons of the previous section. If the first measurement gives n_1 photons and there are n_2 photons in the next time bin, we can generate a 1 when $n_1 > n_2$ and a 0 if $n_1 < n_2$ (Ren *et al.*, 2011).

With these methods we are generating just one bit for each measurement. But, depending on λT , our measurements can have a higher entropy. There are some ways to take a fuller advantage of the data we already have.

Certain generators assign more than one bit per detection depending on the counted photon number. The possible results are grouped into sets with equal total probability, which usually requires adjusting the mean photon level of the source to make sure all the sets are really equally, or almost equally, likely (Jian *et al.*, 2011).

Depending on the exact photon rate λT in the observed period T , the second, third or further least significant bits of the number of counted photons might also be uniform. This is taken into account dynamically in the generator of (Tisa *et al.*, 2015) which has an array of integrated CMOS SPAD detectors that receive light from an LED to generate random numbers in parallel in a 32×32 detector matrix. This is the principle behind the commercial generator of Micro Photon Devices (MPD, 2014). In this approach it is important to properly characterize the dead time, as the rate that registers at the detector λ_{det} is affected by dead time. The corrected rate

$$\lambda_{det} = \frac{\lambda}{1 + \lambda \frac{t_{dead}}{T}} \quad (18)$$

helps to adjust the choice of how many bits from the counted number of photons should be used.

There are also generators that use everyday devices. Certain commercial cameras that are not designed for quantum detection can, nevertheless, offer good enough precision for quantum random number generation. There have been demonstrations of random numbers generated on a mobile phone (Sanguinetti *et al.*, 2014) from the variations in the count statistic of a state with around 410 photons. In that implementation, the results are taken to a randomness extractor to eliminate correlations and noise effects. This approach is related to the shot noise generators of Section VII.F.

Other photon counting methods take bins of length T , subdivide them into smaller bins where we are likely to have zero or one photons and then use more involved procedures to convert the non-uniform Poisson statistics of the large bin into a uniform random variable (Wang *et al.*, 2015a,b; Yan *et al.*, 2015).

E. Attenuated pulse generators

Certain generators are based on a simplified version of the previous methods with more relaxed requirements for the detectors. Most current single photon detectors have a limited photon number resolving capability and have a binary response of click (one or more photons are detected) or no click (no photon has been found). Photon counting methods usually rely on multiple clicks in a long time period that is divided into a concatenation of smaller bins in the time resolution of the detector. These methods assume a weak source that produces zero or one photons in that bin and that there is a small or ideally negligible probability of generating two or more photons in that shorter time period.

We call an attenuated pulse generator to the OQRNG with a weak source that has the same probability of generating a photon or not. More precisely, we require the complete system to give a detection probability of one half. We can imagine a superposition of the empty and single photon states in the same spatio-temporal mode (the path that goes to a certain detector in a certain time) so that the quantum state of our photon pulse is

$$\frac{|0\rangle_1 + |1\rangle_1}{\sqrt{2}}. \quad (19)$$

We can associate a 0 to a no-detection event and a 1 to a click. The occupied state does not need to have exactly one photon. Any superposition

$$\frac{1}{\sqrt{2}}|0\rangle_1 + \sum_{k=1}^{\infty} \alpha_k |k\rangle_1 \quad (20)$$

with $\sum_{k=1}^{\infty} |\alpha_k|^2 = \frac{1}{2}$ is valid. Externally, we just take the 1s from clicks and do not care if they are triggered by one or more photons.

Coherent states provide such a superposition and are easy to produce. For a coherent state of amplitude α the probability of finding zero photons is

$$p(n=0) = e^{-|\alpha|^2} \quad (21)$$

and the complementary probability of finding one or more photons (and finding a click in the detector) is

$$p(n \geq 1) = (1 - e^{-|\alpha|^2}), \quad (22)$$

as can be seen from Eq. (11). The simplest idea would be to find the α for which $p(n=0) = p(n \geq 1)$, which happens for $\alpha = \sqrt{\ln 2}$. Eq. (17) shows any Poissonian source with $\lambda T = \ln 2 \approx 0.693$ also gives the desired detector probability.

In practice, the generator works with an effective mean photon number at the detector $\eta\lambda T$, with an efficiency η that depends on many factors such as detector efficiency or path losses. The OQRNG can be adjusted by fine tuning of a variable attenuator. This is the model of the generator in (Wei and Guo, 2009a). Alternatively, the generator can act on the light source. The OQRNG in (Bisadi *et al.*, 2015a,b) adjusts the current of an LED in order to have the desired balance. The OQRNG of (Stipčević and Ursin, 2015) also has an adjustable source to guarantee a 50% probability of detection, this time inside an on-demand circuit that produces the photon pulses after a trigger signal has arrived.

Even after tuning, there can be residual bias and the system can drift out of the tuned state during operation. The generator in (Wei and Guo, 2009b) uses von Neumann extraction to address the problem (see Section X). For two detections with photon numbers n_1 and n_2 , it outputs a 1 if $n_1 > 0$ and $n_2 = 0$ (a click followed by an empty pulse) and a 0 if $n_1 = 0$ and $n_2 > 1$ (no click followed by a detection). The results with two successive empty pulses or two successive clicks are discarded. For a Poissonian source, both bit values are equally likely with a probability $P(n > 0)P(n = 0) = e^{-\eta\lambda T}(1 - e^{-\eta\lambda T})$. The resulting bit rate is at least four times slower, but free from bias. Greater biases result in smaller rates, but the bits still present balanced probabilities.

F. Generators based on quantum vacuum fluctuations

Another group of quantum generators exploits the fluctuations in the quantum vacuum state. The vacuum state can be written as a superposition of amplitude quadrature states $|x\rangle$

$$|0\rangle = \int_{-\infty}^{\infty} \psi(x) |x\rangle dx, \quad (23)$$

where $\psi(x)$ is the ground-state wavefunction. The wavefunction is a Gaussian around $x = 0$ so that

$$|\psi(x)|^2 = \frac{1}{\sqrt{\pi}} e^{-x^2}. \quad (24)$$

Homodyne measurement (Collett *et al.*, 1987) offers a simple way to measure the X quadrature. The balanced homodyne detection scheme of Fig. 8 has an output proportional to the quadrature amplitude of the vacuum field and gives an amplified reading of the basic uncertainty in the vacuum state.

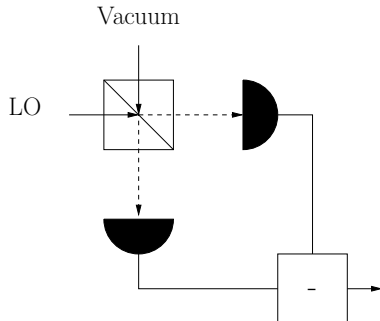


FIG. 8 Homodyne measurement of the vacuum: A laser acting as a local oscillator, LO, is mixed with the vacuum state in a balanced beam splitter. The readings of two detectors at the output of the beam splitter are subtracted and processed to give a current output proportional to the X quadrature of the vacuum field. The proportionality constant is a function of the reference field in the local oscillator.

The homodyne detector mixes the vacuum state with a reference laser field from a local oscillator and subtracts the current measurements of two amplitude detectors. The resulting signal can then be processed and digitized to produce the random numbers. Depending on the digitizer that receives the values from the optical detectors, the choice of the local oscillator, the detectors' bandwidth, noise factors and other problems, we might have a different amount of available random bits. With an adequate treatment, the uncertainty in the final measurement can be mostly attributed to the intrinsic quantum fluctuations of the observed vacuum state and not to the shot noise from the local oscillator or other noise sources (Yuen and Chan, 1983). This random signal can be digitized and sent to a comparator or an entropy extraction circuit to produce random sequences (Trifonov and Vig, 2007). The generator in (Shen *et al.*, 2010) implements this method by sampling the filtered shot-noise signal periodically and taking the last bit of its digitized amplitude.

We can also take the quadrature measurement, divide the range of possible values of x into boxes from x_i to x_{i+1} and then assign to each box different random bit values. The continuous quadrature value x is in box i with a probability

$$\int_{x_i}^{x_{i+1}} |\psi(x)|^2 dx. \quad (25)$$

The QRNG of (Gabriel *et al.*, 2010) implements this method. It takes 5 bits per measurement (32 bins) and

hashes the resulting sequence to remove residual correlations.

QRNGs that measure the vacuum fluctuations can go beyond the Mbps rates of single photon detection methods and reach rates in the Gbps range. They can use fast classical detectors and we can optimize the speed of the electronic part of the generator and concentrate on reducing the technical noise, like the generator of (Symul *et al.*, 2011), which discards the least significant bits as a fast method of randomness extraction after noticing that the most significant bits of the digitized homodyne measurement carry most of the quantum noise.

The method can also be used with the squeezed vacuum state. The generator of (Zhu *et al.*, 2012) uses second harmonic generation in a parametric oscillator with no input signal to produce a squeezed vacuum state that presents a larger uncertainty in the measured quadrature. In the squeezed vacuum state, the Gaussian wavefunction

$$|\psi(x)|^2 = \sqrt{\frac{s}{\pi}} e^{-sx^2} \quad (26)$$

is wider by a squeezing parameter $0 < s < 1$. Homodyne measurement produces a larger range of voltages and makes conversion to digital strings easier. We can define more voltage ranges and reduce the effects of classical noise. With more squeezing (a smaller s) the entropy due to quantum noise increases and the bit rate after randomness extraction can be higher. The generation of squeezed vacuum states is described in more detail in Section VII.J in relation to QRNGs with optical parametric oscillators.

G. Generators based on the phase noise of lasers

The output of a laser has a random phase of quantum origin that can be used to produce random bits. Inside the cavity of a single-mode semiconductor laser, spontaneous emission causes fluctuations in the output field (Henry, 1982). This phase noise, also known as phase diffusion, comes from a combination of different quantum effects⁶. Direct phase measurement is not technologically feasible for optical signals, but an unbalanced Mach-Zehnder interferometer, MZI, (see Fig. 9) can translate phase differences into amplitude variations.

⁶ There are many opposing views on the exact role of the vacuum fluctuations and spontaneous emission in laser phase noise and whether spontaneous emission is a direct manifestation of vacuum fluctuations or not (Fain, 1982; Gea-Banacloche *et al.*, 1988; Ginzburg, 1983; Henry and Kazarinov, 1996; Scully and Stenholm, 1988). As far as quantum random number generators are concerned, the exact nature of phase noise is not relevant as long as it is a quantum effect that can produce an observable with a known distribution.

In an unbalanced MZI one of the arms introduces a delay τ with respect to the other arm. Assuming a constant or slowly varying amplitude in each arm, the output has a constant level and a variation proportional to $\cos(\phi(t) - \phi(t + \tau))$ for a random phase difference $\Delta\phi(t) = \phi(t) - \phi(t + \tau)$. The amplitude at the output ports of the interferometer can be measured with high speed standard optical detectors.

If the introduced delay is far above the coherence time of the laser⁷, $\tau \gg \tau_{coh}$, the phase difference $\Delta\phi(t)$ is a Gaussian random variable of a mean that tends to 0 (Lax, 1967). If we sample the amplitude of the detector with a time difference between samples $\Delta t \gg \tau + \tau_{coh}$, the resulting amplitudes are independent (Guo *et al.*, 2010; Qi *et al.*, 2010). These amplitudes are the random variable in many OQRNGs. While the voltages at the detectors carry many classical sources of noise, the quantum phase noise is known to be inversely proportional to the laser output power (Henry, 1982) and, if we operate the laser at a low intensity close the lasing threshold, we can make the quantum uncertainty the dominant noise.

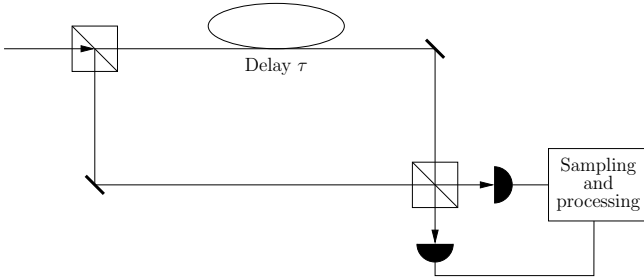


FIG. 9 If we divide the light coming from a laser in a beam splitter and make it interfere with a delayed version of itself, the quantum phase noise will produce a random amplitude at the output. Choosing an adequate delay and sampling rate, we can process these amplitudes to generate random numbers.

The generators in (Guo *et al.*, 2010; Qi *et al.*, 2010) use the basic configuration in Fig. 9 and sample at a fixed period the voltage in one of the detectors. After processing, the voltages V_k measured at times $t_k = t_0 + k\Delta t$ are independent Gaussian random variables.

To generate the random bits, the OQRNG of (Guo *et al.*, 2010) takes the least significant bit of the voltage measurement or the least significant bit from the difference $V_{k+1} - V_k$ between two results if we want to remove biases from the digitization of the voltage amplitudes.

The generator in (Qi *et al.*, 2010) adds a phase compensation system in the interferometer to avoid classical phase drift effects that might mask the quantum signal. Its random bits come from comparing each measured

voltage with a threshold at the mean voltage value 0. For the Gaussian voltage signal of interest, we can produce random bits if we choose an output 1 for $V_k > 0$ and a 0 for $V_k < 0$.

The voltage distribution is Gaussian and we cannot directly use all the digitized bits, which are correlated. However, we can feed them to a randomness extraction algorithm to generate uncorrelated bits. This is the approach of the generators of (Liu *et al.*, 2010b) and (Xu *et al.*, 2012) which use the same optical delay circuit as the previous implementations and the generator of (Nie *et al.*, 2015), which uses a modified interferometer with advanced phase drift correction to achieve rates of tens of Gbps. We can also use Faraday mirrors to correct phase jitter (Zhu *et al.*, 2011).

For all these generators, we can try to maximize the rate either by increasing the sampling rate or the number of bits we take. However, faster sampling means higher correlations and digitizers have a limited precision. For any given system the randomness rate can be optimized by acting on the sampling rate (Zhou *et al.*, 2015). Increasing the sampling rate increases the generated random bit rate until $\Delta t = \tau$. After that point, the bits we read have a higher correlation. The additional samples produce a smaller number of uniform bits and the overall speed decreases. We should choose a delay that maximizes the final bit rate

$$R_s = -\frac{1}{\tau} \log_2 \left[2\Phi \left(\frac{\lambda}{\sqrt{\tau}} \right) - 1 \right], \quad (27)$$

for a parameter λ that depends on the laser power, the length of the measured voltage interval and other constants of our system. $\Phi(x)$ is the cumulative distribution function of the standard Gaussian distribution.

An interesting alternative implementation of phase noise quantum random number generators uses pulsed lasers to avoid phase correlations in the optical field. In the generator demonstrated in (Jofre *et al.*, 2011), a laser is driven by short pulses that take it rapidly from below the threshold to lasing levels. The time the laser is below the threshold, any previous coherence is attenuated and amplified spontaneous emission introduces a new random field. When the laser is suddenly taken above threshold, it amplifies the cavity field to a classical level. After the short amplification stage, the resulting field has a known amplitude due to gain saturation, but the phase is random.

The resulting output has a series of pulses with a random phase. The phase is converted into amplitude with the usual unbalanced Mach Zehnder interferometer, this time with a delay τ that matches the repetition rate at the laser so that two consecutive pulses interfere at the output beam splitter (Fig. 10).

The phase of each pulse ϕ_i is uniformly random in $[-\pi, \pi)$ and so is the phase different between neighbouring pulses. The interferometer converts the phase into

⁷ For semiconductor laser with a linewidth $\Delta\nu_{las}$ we can determine a coherence time $\tau_{coh} = \frac{1}{\pi\Delta\nu_{las}}$ (Henry, 1982).

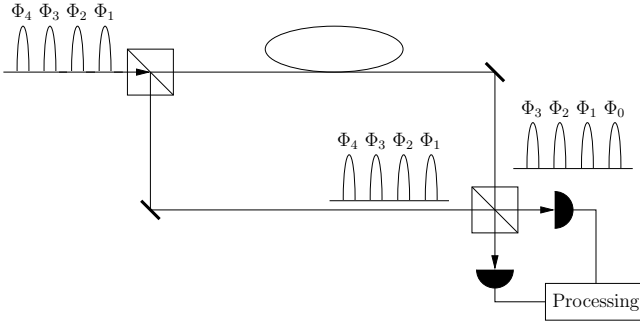


FIG. 10 Using a pulsed laser we can generate individual pulses with a random phase due to quantum phase noise. If we introduce a delay in one arm of an interferometer, we have the interference of two pulses with independent phases and the output will have a random amplitude.

an amplitude variation that, after detection and filtering, provides energy measurements that are almost uniformly distributed in a restricted range.

The same configuration with a pulsed laser has been refined later adding passive phase compensation to reduce classical phase drift (Tang *et al.*, 2013) and tuning the system to achieve a faster rate up to 43 Gbps (Abellán *et al.*, 2014).

Quantum noise inside semiconductor lasers plays also a role in classical random number generators based on chaos. There have appeared many random number generators that have one or more semiconductor lasers with optical feedback. The lasers produce a chaotic signal with pulses of a random amplitude and time position (Hirano *et al.*, 2010; Kanter *et al.*, 2010; Reidler *et al.*, 2009; Uchida *et al.*, 2008). Quantum noise in the laser is the origin of a random variation in the cavity that is then amplified in a chaotic process. While these generators have some entropy due to quantum effects, most of the unpredictability of the final sequence rests on chaotic evolution, which is deterministic. In a sense, they work as physical pseudorandom number generators that take a random quantum seed and expand these small fluctuations at the quantum level into a fast changing physical process to achieve generation rates up to hundreds of Gbps.

H. Generators based on amplified spontaneous emission

Fiber communication systems owe their fast long range data rates to optical amplification. There are different technologies for optical amplification, like erbium-doped fiber amplifiers, EDFAs, and semiconductor optical amplifiers, SOAs, both popular alternatives in optical communication systems. These optical amplifiers work on variations of the same principle: the light is directed into a medium with population inversion so that the photons in the signal stimulate the coherent emission of new pho-

tons that increase the signal's power. However, any excited medium capable of stimulated emission also shows spontaneous emission. That means there appear spontaneously emitted photons inside the gain medium that are amplified by stimulated emission just like the signal is. The random quantum phenomenon of spontaneous emission is thus amplified to a measurable signal with a random amplitude.

This noise, known as amplified spontaneous emission, ASE, noise is a major limitation to optical gain in communication systems. Larger gains introduce larger noise powers and there is a maximum amplification that can be obtained without degrading the signal-to-noise ratio. Amplified spontaneous emission, either alone or in its beats with the signal or itself, is a strong source of noise that dominates over thermal noise in the detector or the optical shot noise. ASE noise is a first rate challenge in optical communication systems, but can be turned into a good source of entropy in quantum random number generators. Amplified spontaneous emission gives a readily available strong signal with a quantum origin that can be measured with existing optical equipment at fast rates. Sampling random amplitudes of the ASE field in different frequency bands gives statistically independent random variables, even at high sampling rates. The rate of change is usually much faster than the detection mechanism and the speed of the detectors is the limiting factor to the rate in most QRNGs that sample ASE noise. These devices can achieve generation rates of Gbps.

The first proposed quantum random number generators using amplified spontaneous emission work with commercial equipment from optical fiber communications. The generator of (Williams *et al.*, 2010) uses as a source of random light a pumped erbium/ytterbium co-doped fiber with no input that generates photons by spontaneous emission and amplifies them on their way to a processing stage with a bandpass filter and a second low noise amplifier. The filter limits the signal in the detector to help it work correctly. The signal is then split into its two polarization components, which are independent, and sent to two square-law photodetectors. The resulting voltage signal is mostly what is known as ASE-ASE beat noise, a signal of a random amplitude, with some residual noise from other sources. These voltages have a known distribution that depends on the shape of the filter. The difference of the voltages is a random variable of mean 0. The random bits come from comparing the voltages after each detector $v_1(t)$ and $v_2(t)$, generating a 1 when $v_1(t_i) > v_2(t_i)$ at the sampling time t_i and a 0 otherwise. The resulting sequence still has some small correlation between bits. To correct that, the generator outputs the exclusive OR of the raw bit sequence with a delayed version of itself.

The generator in (Martin *et al.*, 2015) also uses a filtered ASE source, a back-pumped erbium doped fiber, but, instead of two detectors, it works with direct de-

tection in a single avalanche photodiode. For the chosen filter, the spectral bandwidth of the optical signal is larger than the detector bandwidth by a factor of m . In that case, the intensity distribution that gives the probability of finding n photons for a source with an average of λ photons in the time of detection (the inverse of the detection bandwidth) is (Wong *et al.*, 1998)

$$p_{BE}(n, \lambda, m) = \frac{\Gamma(n+m)}{\Gamma(n+1)\Gamma(m)} \left(1 + \frac{1}{\lambda}\right)^{-n} (1+\lambda)^{-m}. \quad (28)$$

For a high enough value of n and m , the distribution has a large standard deviation and most of the uncertainty in the measured voltage comes from the ASE noise and not from electrical noise. We can generate random numbers comparing the results to a threshold value that gives equal probabilities for values below and above it (0 for values below the threshold, 1 for values above). The necessary threshold can vary during operation due to power changes in the source or a drift in environmental conditions during the time of generation. The resulting bias can be corrected with a randomness extractor.

Each measurement can give more than one random bit. The quantum random number generator in (Argyris *et al.*, 2012) also uses a single detector but extracts the random bits from a statistical analysis of the random distribution of the detected voltage. The device generates amplified spontaneous emission in two different implementations, one with an erbium-doped fiber amplifier and another with a semiconductor optical amplifier. In both cases, the signal is directed to an optical attenuator. The whole unfiltered noise signal reaches the photodetector where the noise beats give a Gaussian voltage distribution that is digitized. Discarding the few first most significant bits gives a good quality random signal.

Another group of QRNGs uses superluminescent LEDs as the light source. Superluminescent light diodes are incoherent semiconductor sources with internal optical gain that offer an alternative broadband source of ASE. Their output shows a flat spectrum in a wide frequency range. The noise in separate parts of the spectrum is independent and can be used to increase the random bit rate. The generator of (Li *et al.*, 2011) can generate multiple bit streams using a wavelength multiplexed configuration where the light from the superluminescent diode is divided into many channels with bandpass filters for different frequency bands. Each channel ends in a single detector whose output is compared to a threshold to generate the random bits. Each output is then processed by taking the XOR of the bit sequence with a delayed version of itself. The experiment in the paper is for a two channel system, but the method can be extended to multiple parallel streams.

The QRNG in (Li *et al.*, 2014) also uses a superluminescent diode in a refined version of the comparison method in (Williams *et al.*, 2010). The filtered ASE noise

from the diode is amplified in an EDFA and taken to a balanced detection scheme where the optical output is split in two parts and sent to two detectors, one of which receives a delayed signal. This self-differencing takes part of the processing to the optical signal and gives a more symmetric voltage distribution for which it is easier to define a threshold at voltage 0.

As in other generators, we can also try and use all the samples of the digitized voltage and then use postprocessing with delayed versions of the signal to remove residual correlations (Yamazaki and Uchida, 2013). In that case, the final bit rate can be improved by over-sampling. If we use a sampling rate above the spectrum linewidth of the detected noise, which is limited by the detector, the resulting bits are correlated, but adequate postprocessing can restore a good quality sequence (Liu *et al.*, 2013).

A curious alternative is the RNG of (Wei *et al.*, 2010) that uses the spontaneous emission from a regular light emitting diode without amplification. With no amplifier, the random directions of emission of an LED makes detection difficult. In order to collect enough light, the light source and the detector are placed in the focal points of an ellipsoidal cavity so that the emitted light is collected into the photodiode's sensitive area. The amplitude fluctuations due to the randomness in the emission times come from many independent events and tend to a Gaussian distribution. The voltage at the detector is then sampled and the bits from the digitizer are unbiased to give a random bit string at the output.

I. Generators based on Raman scattering

The interaction between photons and the quantum vibrational states of certain materials is also a good source of randomness. Some quantum RNG resort to Raman scattering phenomena to obtain the entropy for random bit generation.

There are two important Raman scattering effects. The first is spontaneous Raman scattering. In spontaneous Raman scattering, SpRS, a photon is scattered when it interacts with a molecular lattice that absorbs or creates a phonon to produce a new photon of a higher or lower frequency. If the scattered photon has a larger wavelength and the energy difference is converted into a phonon we speak of a Stokes photon and when there is an energy gain and an incoming photon and an existing phonon produce a scattered photon of a smaller wavelength we speak of an anti-Stokes photon. Anti-Stokes transitions usually produce a smaller field, as they need an established phonon population of the right excited levels of the medium, which in thermal equilibrium is smaller than the population of the ground state (Boyd, 2008).

Another Raman effect is stimulated Raman scattering, SRS. In stimulated Raman scattering a photon of

the frequency ω_S corresponding to the energy difference between a pump photon and the matching phonon in a spontaneous Raman scattering event stimulates the production of a new photon of the same frequency ω_S . This process can be used to obtain optical amplification. If we have a strong optical pump and a signal at the frequency ω_S , the photons of the signal stimulate the emission of new photons that join the signal pulse consuming phonons and the photons from the pump. This mechanism is used in many photonic devices for amplification and wavelength conversion (Islam, 2002; Jalali *et al.*, 2006) as well as in multiple applications in spectroscopy (Colthup *et al.*, 1990). While SpRS is almost isotropic and happens at many frequencies, the resulting field in stimulated Raman scattering is mostly contained in a narrow spatial direction and consists primarily of Stokes photons (Boyd, 2008).

Some of the QRNGs based on Raman scattering work on principles similar to those of the amplified spontaneous emission noise generators of Section VII.H, but, instead of employing quantum spontaneous emission events that are amplified through stimulated emission, they have a strong pump with no input signal so that the spontaneous Raman scattering photons that are produced at random from quantum noise are amplified in a stimulated Raman scattering process (Penzkofer *et al.*, 1979). The process starts from spontaneous emission to the Stokes field that comes from the fluctuations of the phonon field (Raymer and Walmsley, 1990). The spontaneously generated photons induce new Raman scattering processes and the field is amplified to a macroscopic level in what is known as spontaneously initiated stimulated Raman scattering, SISRS. The quantum fluctuations at the initiating process show at the output field as an uncertainty in the optical phase (Belsley *et al.*, 1993; Kuo *et al.*, 1991; Smithey *et al.*, 1991) and amplitude (photon number) (Raymer *et al.*, 1982; Walmsley and Raymer, 1983).

The first proposal for random number generation with stimulated Raman scattering (Bustard *et al.*, 2011) is based on measurement of the random phase in the field out of an optically pumped diamond (Figure 11). Diamonds are a good material for Raman experiments due to their high Raman gain and their transparency at a wide range of wavelengths. A pulsed laser signal is focused into the diamond and produces a Stokes field with a random phase that is uniformly random in the $[0, 2\pi)$ range. An optical bandpass filter takes away the pump, which is in a different frequency band than the Stokes field. The random phases are converted into interference patterns at a CCD camera by combining the Stokes field and a reference pulse in a beam splitter. The beam splitter is tilted so that there appear intensity fringes at the detector. The random phase is recovered by fitting the interference pattern to a cosine model and then it is assigned to a bin out of 64 possible phase ranges. The resulting 6 bits are then taken to a bit extraction algorithm

to remove any remaining bias.

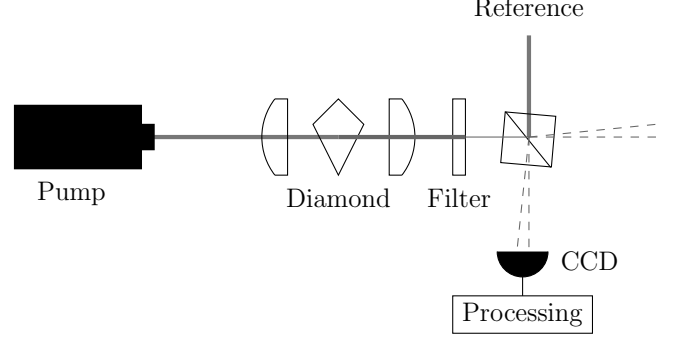


FIG. 11 Generation of random numbers based on Raman scattering by measuring the phase in the field out of a pumped diamond. In this method, the phase is measured using the interference pattern of the scattered field and a reference. The pattern comes from a tilted beam splitter.

The random fluctuations in the amplitude of the field permit a simpler detection scheme without phase to amplitude conversion. Direct detection gives a straightforward amplitude measurement. There is, however, a new problem. Power fluctuations in the pump pulses can mask the quantum effect we want to measure. The generator in (Bustard *et al.*, 2013) monitors the pump power to solve this problem (see Figure 11). The basic setup is essentially the same as in the phase Raman random number generator we have just covered. The pump starts an SIRS process in a diamond and the Stokes field is filtered from the pump background. Now we can directly use a detector with the output field. During normal operation, the amplitude fluctuations can reach up to multiple times the mean energy. The exact amplitude distribution has no known analytic expression and depends on the Raman gain, the focusing geometry and the effects of phonon decay, among others (Raymer *et al.*, 1985). The output field has also small contributions due to pump coupling to more than one spatial mode and other masking effects. The amount of available entropy can be estimated deconvolving the Stokes energy distribution from the detection noise, as measured without a signal. The results show only a small effect of electrical detection in the total noise. In order to extract the entropy, the measured intensity values are corrected with the power values of the monitored reference and the compensated amplitude measurements are binned into intensity ranges that are assigned a bit string. As a last step, the sequence is applied Toeplitz hashing to remove bias and classical noise.

In both cases we have described, Raman interaction has a potential for fast generation rates. The system dephases in times of the order of a few picoseconds, resetting the vacuum phonon state before the new random field is generated. The pulses come with a period much longer than the dephasing time for the phonons in the diamond. In these random number generators, the rate

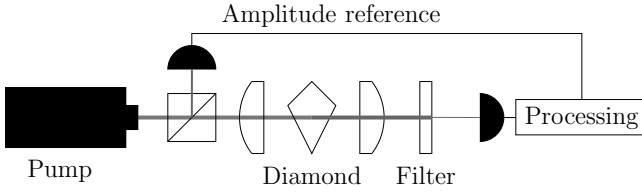


FIG. 12 We can use the amplitude fluctuations in Raman scattering as a randomness source. In order to correct for the fluctuations of the pump, which do not have a quantum origin, we must include an amplitude correction method.

limit comes from the repetition rate of the laser. Stimulated Raman scattering requires large powers in order to produce a strong output signal. In the free-space configuration of the discussed generators the available lasers limited the rate to the range of kbps. These rates can be improved with faster lasers.

An alternative way to measure phase differences with a higher rate is given in (England *et al.*, 2014), where Raman interaction happens inside a highly nonlinear Potassium Titanyl Phosphate, KTiOPO_4 , waveguide. Waveguides offer tight confinement and the guided pump field has a stronger interaction with the medium that allows us to use power levels in the range of faster repetition lasers, like the titanium:sapphire oscillator with a repetition rate of 80 MHz of this generator. The random numbers come from converting the random phase into an amplitude variation in an interferometer with a delayed arm, like in the schemes for quantum random number generators based on phase noise we discussed in Section VII.G.

The quantum effects in spontaneous Raman scattering, SpRS, can also serve as a randomness source in schemes without amplification at the cost of adding single photon detectors. By improving the detector, we can have a continuous wave laser pump of relatively low power. If we only observe the scattered photons with large frequency shifts, this interaction is mostly between the input photons and the vacuum noise phonon fluctuations instead of interactions with the thermal phonon field. The quantum randomness from phonon vacuum fluctuations is the principle behind the QRNG of (Collins *et al.*, 2015, 2014) where a strong pump inside a highly nonlinear As_2S_3 fiber generates spontaneous Raman photons in different frequency bands. The pump photons interact with phonons of different energies. The scattered photons occupy the spectrum following a known probability distribution with two separate regions. One part of the spectrum is associated to thermal phonons and, in a time T , it has an expected scattered photon detection rate (Collins *et al.*, 2015; Kobliska and Solin, 1973; Lin *et al.*, 2007)

$$R(\nu, T) = C\eta\Delta\nu PL(1 + n_{BE}(\nu, T))g(\nu) \quad (29)$$

that depends on different experimental parameters like

the Raman coupling efficiency C , the experimental loss factor η , the measurement bandwidth $\Delta\nu$, the laser power P or the effective scattering length of the device L . Two particularly interesting factors are the gain profile of the medium with frequency $g(\nu)$, which includes both polarizations, and the thermal phonon occupation number

$$n_{BE}(\nu, T) = \frac{1}{e^{\frac{h\nu}{k_B T}} - 1} \quad (30)$$

that gives the Bose-Einstein distribution of the population of phonons with energy $h\nu$ for a thermal energy $k_B T$. This distribution is close to the smaller detunings with respect to the pump. The photon distribution in frequency is concentrated a few THz above the pump frequency.

The spectrum has a second peak at higher detunings due to the quantum vacuum fluctuations of the phonon field. In the discussed As_2S_3 fiber, the distribution peaks around 10.4 THz above the pump (Collins *et al.*, 2012). At room temperature, the distributions of quantum and thermal origin are centered around different parts of the spectrum. While both distributions are random, the thermal component shows the same problems as the thermal noise generators we discussed in Section VI and we prefer the more stable random distribution from the quantum part of the spectrum. There is still some contribution from thermal scattering events, but this and other biases can be corrected with postprocessing.

Once we have selected the most adequate frequencies, we can use a coarse wavelength division multiplexer to measure two slices of the spectrum with an equal probability of having a spontaneously scattered photon. The multiplexer converts the spectrum distribution into a spatial separation. The rest of the scheme basically follows the model of the spatial separation generators we discussed in Section VII.B. In the discussed experiments, two detectors D_0 and D_1 measure the photons in the paths of the two spectrum slices during a time T . The output bit is a 0 if there is a click only in D_0 and a 1 if only D_1 clicks. Two simultaneous detections and empty time bins are discarded. The differences in the collection efficiencies of the two detector channels and the non-flat shape of the Raman spectrum introduces biases in the sequence. In order to correct the bias, there is a post-processing stage that XORs the sequence with a 16-bit delayed version of itself.

The experiment gave raw generation rates of 1 Mbps, 650 kbps after postprocessing. The ultimate limit for the random bit generation rate depends on the decay time of the Raman response function. Spontaneous Raman scattering photons that are generated with a time separation less than the Raman response time can have frequency correlations. The photon generation rate can be controlled with the power of the pump laser to avoid correlations. In the studied fiber, the medium reacts in less than 100 fs (Asobe *et al.*, 1995). Generation rates up

to 1 GHz would still show a small two photon probability of the order of 5×10^{-3} in that response interval.

In the experiment, the generation rate is limited by the detectors. The detector limitations are the same as in the generators based on single photon detection we discussed in Sections VII.B and VII.C. Most single photon detectors are limited to a MHz rate, but more advanced detector technologies can bring the rate closer to the Raman physical limit. Additionally, the rates can be improved by dividing the spectrum into more than two channels. A wavelength division multiplexer can take the photons into multiple paths that allow to extract more than one bit per measurement.

J. Generators based on optical parametric oscillators

Binary phase selection in degenerate optical parametric oscillators offers a further way to amplify quantum randomness from the microscopic level to a macroscopic optical field. In an optical parametric oscillator, OPO, the photons that appear from spontaneous parametric down conversion of the light from a pump start an oscillation inside a cavity, even without any input at the resonant lower frequencies (Harris *et al.*, 1967; Louisell *et al.*, 1961). The zero-point fluctuations alone can initiate the gain in the cavity. The principle is similar to the amplification of quantum noise inside a laser we have discussed in Section VII.G.

In spontaneous parametric down conversion, the non-linear response of a medium converts the photons from a pump at a frequency ω_p into two photons: a signal photon with frequency ω_s and an idler photon at ω_i so that $\omega_p = \omega_s + \omega_i$. This phenomenon has applications in entanglement generation and in parametric amplifiers. In a medium with type I degenerate down conversion each photon from the pump produces two photons with the same frequency and polarization. Different pump photons give different polarizations, but all the generated photons have the same frequency. In these conditions, an optical parametric oscillator with no input but the pump amplifies the uncertainty in the vacuum fluctuations and the output is a squeezed vacuum state where the uncertainty at the quantum level can be measured from a macroscopic optical signal (Wu *et al.*, 1986, 1987).

The cavity of an optical parametric oscillator has losses and there is a gain threshold below which spontaneous parametric down conversion cannot be amplified to the macroscopic level (Yariv and Yeh, 2007). In a continuous wave type I degenerate OPO where both the signal and the idler fields are indistinguishable, the gain mechanism is phase dependent and has a period of π for the signal phase (Marandi *et al.*, 2012a; Nabors *et al.*, 1990). For an adequate pumping power, there are only two stable oscillation states where the gain is greater than the oscillator losses. These states show a phase with respect to

the pump around $\theta_s = 0$ in one state and around $\theta_s = \pi$ in the other.

The optical parametric oscillator quantum random number generators of (Marandi *et al.*, 2011, 2012b) use as their randomness source the phase of the macroscopic field inside the cavity, which is inherited from the vacuum fluctuations. In this process, classical noise effects are negligible and do not change the phase state. In order to convert the phase variations into a binary random number, we can take two independent cavities of the same output power and make their output fields interfere at a beam splitter. If both cavities have a state around the same phase, there will be a constructive interference and the signal will have close to double the original power. If the phase states are around opposite values there is a destructive interference and the output power is close to 0.

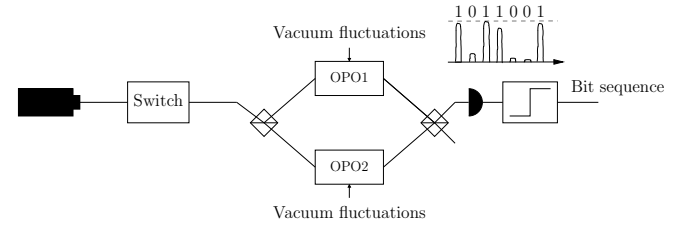


FIG. 13 Quantum random number generation with two optical parametric oscillators. A pulsed laser creates an oscillation in each OPO in one out of two possible stable states with a phase centered around 0 or π with respect to the pump. The final stable phase depends on the initial conditions of the quantum fluctuations in the cavity and when the pulses from both OPOs interfere we will have close to totally destructive or close to totally constructive interference. The resulting amplitudes can be easily distinguished and be assigned to the 0 and 1 bit values.

For the right cavity parameters, the phase distribution can be quite narrow around the central values $\theta_s = 0$ and $\theta_s = \pi$ and the output power of the interferometer has two clearly distinguishable optical power values that can be told apart using a threshold in the middle of the expected detector voltages corresponding to a totally constructive interference and a totally destructive one. The value of the comparison can be used to generate random bits. A low voltage state (destructive interference) can be interpreted as a 0 and a high voltage state (constructive interference) as 1.

The bit rate depends on the time it takes for the cavity to generate a new random phase. Once a stable state is established inside the cavity, it will feed itself. We need to restart the oscillation to generate a new random value. In the generator of (Marandi *et al.*, 2011, 2012b) the cavity is detuned by blocking and unblocking the pump.

There is a minimum time before we have a fresh source of randomness. We must first allow the field inside the cavity to decay to the quantum noise level before a new oscillation builds up. Otherwise, when we establish the

oscillation, the residual field dominates over quantum fluctuations and the new phase state is correlated to the previous phase value. This is the limiting factor in the speed of OPO-based QRNGs. The exact time for regeneration depends on the cavity and the pump power. If we pump well above threshold, like in the described generators, it can take from 10 to 20 times the $1/e$ decay time of the cavity to go back to the quantum noise level (Marandi *et al.*, 2012b). The intensity decay time can be estimated from the oscillator parameters as

$$\tau_{off} = \frac{T}{2\delta_E - 2\delta_E \sqrt{\frac{P_{off}}{P_{th}}}} \quad (31)$$

for a cavity with an electric field fractional roundtrip loss δ_E , a cavity roundtrip time T and pump powers at the threshold and “off” levels of P_{th} and P_{off} respectively (Marandi *et al.*, 2012b).

In the described QRNGs the bit rate is in the order of tens of kbps before serious correlation problems appear. Shorter cavities can have lower build-up times and, when combined with pumps at higher repetition rates, would allow rates in the Gbps range (Lecomte *et al.*, 2005).

There are also interesting variations of the method with other parametric processes. This generation method is not necessarily restricted to second-order nonlinear materials. Instead, we could use $\chi^{(3)}$ effects in integrated optical parametric oscillators (Liu *et al.*, 2010a; Razzari *et al.*, 2010).

Apart from optical parametric oscillators, there are other bistable optical systems where quantum effects can produce jumps between stable states. For instance, the quantum random number generator in (Sunada *et al.*, 2011) uses a semiconductor ring laser that is driven from a monostable to a bistable state. The amplified spontaneous emission noise in the counter-propagating laser modes that appears during switching defines the final stable state from the two possible options and gives a random macroscopic bit that has a quantum origin.

Competition between optical modes is also the source of randomness in the generator proposal of (Shenoy *et al.*, 2013), in which spontaneously emitted photons in two possible competing modes are amplified in a laser setup so that there is a macroscopic winning mode that amplifies the quantum uncertainty at the single photon level.

VIII. NON-OPTICAL QUANTUM RANDOM NUMBER GENERATORS

While quantum light offers a simple source of quantum randomness, there have also been proposals for quantum random number generators based on other physical systems.

For historical reasons, we have already discussed in their own section the quantum random number genera-

tors based on the random behaviour of radioactive decay (Section V). They were the first quantum random number generators well before the explosion of quantum information theory and remain in use. While they are based on the detection of particles, they are in many aspects equivalent to the optical schemes based on photon counting, time of arrival and position (in fact, in the case of γ radiation we can say we have an optical system, just with photons of a very high frequency).

A second family of non-optical random number generators with a quantum contribution is the group of electronic RNGs we have covered in Section VI. In general, their source of randomness is not so clearly defined as in the rest of quantum random number generators described in this paper, but noise generation with Zener diodes, when implemented properly, can be taken to an almost purely quantum regime (Stipčević, 2004) and electronic shot noise is the source of randomness in certain commercial quantum random number generator of ComScire (ComScire, 2014).

In a reverse-biased Zener diode with a low breakdown voltage, the dominant source for the current that appears is the completely quantum tunnel effect (Pierret, 1996). The p-n junction of the diode presents a potential energy barrier that is thin enough to allow random quantum tunneling of some of the electrons from the valence band of the p-side to the conduction band of the n-side of the junction. This creates a random reverse current that is the basis for many electronic noise physical random number generators.

Similarly, the tunnel effect at the p-n junctions in MOS transistors creates a leakage current formed by the electrons that tunnel through the insulating layer under the gate. This tunneling introduces a varying current that suffers from shot noise due to the discrete nature of the electrons. These changes can be converted into a variable jitter in ring oscillators and processed to produce random numbers (ComScire, 2014). The origin of the noise is similar to that of the optical random number generators discussed in Section VII.F, but replacing discrete elements of light (photons) with discrete elements of current (electrons).

The shot noise in p-n junctions of different semiconductor devices is a usual source of randomness in home-made electronic random number generators. An example is the random number generator based on reversed-biased p-n junctions in transistors of (Platt and Logue, 2015).

Quantum tunneling is the basic principle behind these and many additional non-optical random number generators. Apart from shot noise in p-n junctions, tunneling explains, among others, cold emission of electrons from metallic surfaces or alpha decay (Razavy, 2014). From that point of view, we can say a QRNG based on radioactive alpha decay is also based on tunneling. Similarly, the random number generator that amplifies the electrons coming from nano-size emitters under an elec-

tric field in (Vartsky *et al.*, 2011) is a QRNG based on tunneling.

Other quantum random number generators measure the state of atomic quantum systems, like trapped ions. QRNGs based on measurements on trapped ions, while slower than their optical counterparts, have an interesting application to device independent quantum random number generation (Pironio *et al.*, 2010) and other certified generators that are based on experimental tests of quantum mechanics (Um *et al.*, 2013). Trapped ions systems are more complex to implement than most optical measurement setups, but they offer almost perfect detection efficiencies, which is paramount in certification. Due to the special interest of this generation method, we give a more detailed description in Section IX.B.

There are also more exotic proposals related to the certification of the produced random bits, like generating random numbers with Majorana fermions (Deng and Duan, 2013). A Majorana fermion is a particle predicted in 1937 (Majorana, 1937) for which there is convincing experimental support (Nadj-Perge *et al.*, 2014) and which would have desirable properties against noise and imperfections in certain implementations of quantum information protocols.

Another curious proposal is the QRNG of (Katsoprinakis *et al.*, 2008) that measures the quantum fluctuations of the collective spin of an alkali-metal vapor. Spin noise is a random magnetic moment that appears when we have a collection of atoms, even in the absence of an external magnetic field, and is proportional to the number of involved atoms. Spin noise allows to probe the properties of the system efficiently with experiments imitating magnetic resonance methods and its measurement has applications, among others, to spectroscopy in semiconductors (Hübner *et al.*, 2014; Katsoprinakis *et al.*, 2007).

Spin noise is an Ornstein-Uhlenbeck stochastic process that appears from the quantum uncertainty of the spin degrees of freedom combined with measurement-induced noise coming from atomic collisions. The spin state can be probed optically due to optical selection rules that permit to map the varying spin polarization onto the intensity of a probe light beam. With a proper setup, the fluctuations in the optical power due to spin noise dominate over the electronic noise and the photon shot noise and the optical power gives a precise measurement of the global magnetic field.

The QRNG in (Katsoprinakis *et al.*, 2008) measures the spin noise by analyzing the polarization of a probe beam after traversing an alkali-metal vapor under a magnetic field. Spin noise produces a random change in the polarization that can be monitored by measuring the amplitude in the horizontal and vertical component of the light after a polarizing beam splitter. Comparing the level in one branch to a threshold that includes the presence of background noise, we can generate a random bi-

nary sequence assigning a 0 or a 1 depending on whether the stay below the threshold or not.

The generation rate reaches the kbps range and is limited by the relaxation time of the system. In this case, it is desirable that the coherence of the system is short-lived so that a new random state can be created as fast as possible. Samples below the relaxation time would be correlated. Nevertheless, there are systems with lower relaxation times, particularly solid state systems like GaAs structures, which could allow dephasing rates in the order of 1 GHz (Oestreich *et al.*, 2005; Stich *et al.*, 2007).

IX. RANDOM NUMBERS CERTIFIED BY QUANTUM MECHANICS

Cryptographic random number generators face a problem of trust. Users must ultimately trust the algorithm of a pseudorandom number generator or the device that implements a true random number generation method. The alternative, which is devising a random number generation from scratch, is highly undesirable. The cryptographic maxim “Don’t roll your own crypto” sums up the collected experience of the security community and warns against non-tested systems. Trusted algorithms and devices have resisted years of cryptanalysis and attempted attacks and public inspection vouches for their robustness.

Unfortunately, this means that, at some point, users must trust the device or the algorithm they are given. The question, which might seem academic or for the paranoid-minded, is not trivial. The events in the last years have shown RNGs are a tempting target for hidden attacks. For instance, the pseudo-random number generation algorithm DUAL_EC_DRBG, which was proposed as a NIST standard (Barker and Kelsey, 2007), allows backdoors that permit an attacker to recover the whole random sequence with minimal information (Bernstein *et al.*, 2015; Checkoway *et al.*, 2014; Hales, 2014; Shumow and Ferguson, 2007), which has had practical consequences in the Juniper network attack (CVE7755, 2015). At the hardware level, there are demonstrations of how a rogue manufacturer or any attacker with access to the device can insert very hard to detect errors in real world RNGs by introducing dopants in certain parts of the circuit (Becker *et al.*, 2014). This is an example of the more general threat of hardware trojans, which are different kinds of malicious modifications that are inserted at the hardware level (Tehranipoor and Koushanfar, 2010).

For physical random number generators there is also the possibility of spontaneous failure. If a component from the device stops working or degrades, the quality of the output bits might suffer. Subtle hardware failures can be hard to notice, especially if the device still produces an output. For that reason, security recommendations like the AIS 31 standard of the German *Bundesamt*

für Sicherheit in der Informationstechnik (Killmann and Schindler, 2011) or the draft of NIST SP 800-90B (Turan *et al.*, 2016) ask for some kind of self testing inside true random number generators. A subsystem should monitor the state of the device at all times (Bucci and Luzzi, 2005; Fischer, 2012).

In this Section, we review three quantum-inspired ways of working with untrusted devices. The first method is using some properties associated to quantum phenomena to observe the quality of the produced bits. The second subsection gathers the proposals collectively known as device independent quantum random number generators, which are based on the clever realization that there are quantum correlations that guarantee certain statistical independence unless some trusted physical principles, like causality, are wrong. The third part describes quantumness certification methods that are inspired by device independent generators, but use less stringent experimental tests of different aspects of the quantum theory and provide a limited certification under more relaxed security assumptions.

A. Self-testing in quantum random number generators

Most quantum random number generators do not fully characterize their source of randomness. For instance, while a photon at a beam splitter (Figure 6) should produce perfectly random bits, there can be problems with detector efficiency, unbalances in the splitting process, imperfections in the source and many unsuspected sources of correlation. For that reason, there have appeared different methods to check the quality of the random numbers produced in physical random number generators. This is not exclusive to quantum random number generators. In classical physical random number generators there are different ways to check the output to detect failures, like including hardware versions of the NIST and Diehard randomness tests we describe in Section XII (Hotoleanu *et al.*, 2010; Santoro *et al.*, 2009a,b; Suresh *et al.*, 2013; Vaskova *et al.*, 2010, 2011; Yang *et al.*, 2015). Here, we discuss only the self-testing approaches that are directly related to the quantum properties of the random number generator.

There are also self-testing methods that can work both with classical noise and quantum sources of entropy. The self-testing circuit described in (Saito *et al.*, 2010) compares the time of arrival of random pulses coming either from thermal noise or from the detection of radioactive decay with a Geiger counter (Section V) and tests the resulting distribution against the expected Poisson time of arrival. Only the random numbers passing the tests are put forward to the output, filtering out obvious failures.

While there is still a risk from a malicious attacker that modifies the output to produce predictable sequences that will pass the tests, these self-checking systems can

detect spontaneous failures and less sophisticated attacks and they are a good addition to security. Tests can serve as a canary to detect operation errors and alert that something is wrong.

Testing must be done with due care. Accurate entropy estimation is a hard problem and a system that evaluates the available entropy with a poor implementation can be vulnerable to attacks (Dodis *et al.*, 2013).

The first mention to self-testing in a quantum setting was presented in the optical QRNG of (Fiorentino *et al.*, 2007) that is designed to work with either a single photon in a polarization superposition

$$|\psi\rangle = \frac{|H\rangle + |V\rangle}{\sqrt{2}} \quad (32)$$

or with an entangled state

$$|\psi\rangle = \frac{|H\rangle_1 |V\rangle_2 + |V\rangle_1 |H\rangle_2}{\sqrt{2}}. \quad (33)$$

The quantum random number generator works on the principles of path branching discussed in Section VII.B.

The device includes a testing phase in which it performs full tomography of the input state (James *et al.*, 2001) from a set of measurements in order to determine the 2×2 matrix that describes the photonic two level system for a single photon or the effective two-dimensional Hilbert space of interest in the case of the photon pair. From the measurement results, the generator estimates the minimum possible min-entropy $H_\infty(\hat{\rho})$ for the joint state of the user and an eavesdropper, $\hat{\rho}$, for the worst case over all the possible decompositions. Then, the raw bits are fed to a randomness extractor (Barak *et al.*, 2003) that, for the estimated bound on the available entropy, produces a shorter unbiased random string.

This method offers protection against an adversary that can control the quantum state from which we obtain the entropy as long as we can take repeated measurements on the same state. In order to perform state tomography correctly, we need to assume the measured state is the preserved throughout the process. This can be interesting when the attacker can only alter the photon source or when there is a physical problem with the generator. While this kind of self-testing offers a limited protection against advanced attackers, it is an effective way to detect accidental errors in the device.

Tomography offers a reasonable entropy estimation in models where we assume honest errors in implementation or failures during operation instead of a collection of components from untrusted colluding manufactures. Such a model is put forward in the self-testing QRNG of (Lunghi *et al.*, 2015) where randomness from a quantum origin is separated from technical noise using the

dimension witness of (Bowles *et al.*, 2014) defined as

$$W = \begin{vmatrix} p(1|0,0) - p(1|1,0) & p(1|2,0) - p(1|3,0) \\ p(1|0,1) - p(1|1,1) & p(1|2,1) - p(1|3,1) \end{vmatrix} \quad (34)$$

where $p(b|x,y)$ gives the conditional probability of finding an outcome b (from ± 1) for a state prepared in one out of four $x = 0, 1, 2, 3$ possibilities in a measurement setting y that can be 0 or 1. In the discussed generator, the four states correspond to the circular right and left polarizations or the diagonal and antidiagonal polarizations of the second photon from an entangled pair, which is measured in the diagonal or the circular polarization basis. The first photon acts as a herald.

W gives an idea of “how quantum” is the combination of preparation and measurement. Any $W > 0$ shows that some measurements are incompatible and there is some quantum randomness that allows to give a bound on the guessing probability. The result can be used to decide the level of compression in a randomness extractor. For smaller values of W (a more classical behaviour) the raw input bits produce a smaller number of clean random bits. The experimental test of this method in (Lunghi *et al.*, 2015) gave a final bit rate around tens of bits per second and showed a correct response to environmental changes, like the alignment problems resulting from turning off the air conditioning in the lab.

A similar approach to self-testing with a Faraday-Michelson quantum key distribution system (Mo *et al.*, 2005) is given in (Song *et al.*, 2015).

An alternative is to take advantage of the uncertainty principle to ensure any adversary has a limited amount of information. As in the previous methods, our goal is not only to generate random bits, but to be sure they are private (no external attacker can learn our sequence). For instance, if we measure the polarization of the first photon in the entangled state of Eq. (33) in the horizontal-vertical basis, we would get perfectly random numbers, but an adversary that captures the second half would know the exact sequence we obtain by taking the same measurement. This can be acceptable in applications like simulation, but in cryptography we need to avoid any information leakage. The certification method in (Valone *et al.*, 2014) is designed to ensure privacy without full tomography by switching between two mutually unbiased bases (Bandyopadhyay *et al.*, 2002; Durt *et al.*, 2010). Instead of a full tomographic measurement, two bases are enough. The conditional min-entropy with respect to an eavesdropper (Section IV) gives a bound to the amount of randomness we can safely extract from a measurement (De *et al.*, 2012; König *et al.*, 2009). The uncertainty principle guarantees there is a limited correlation with the environment for any possible input state (we can prove a bound on the conditional min-entropy from our measurement results). This implementation requires a small random seed to choose between the bases.

The original randomness in the seed is expanded after the measurements into a reliable private bit string. The seed needs to be uniform and cannot be taken from the same weak randomness source as the rest of the bits (see Section X for a more detailed description of randomness extraction and the role of uniform seeds). The method was demonstrated with entangled photon pairs generated from parametric down-conversion and measurement in the diagonal/antidiagonal and the horizontal/vertical polarization bases.

We can also follow the methods of precision measurement (Bloom *et al.*, 2014; Maddaloni *et al.*, 2013) and propose a complete model of the generator where all the sources of uncertainty are rigorously characterized and all the experimental imperfections are taken into account in the most conservative way. The experimental standards followed in precision measurement have been put to test in atomic clocks with impressive results and can be adapted to quantum random number generation. This characterization based on metrology has been followed by (Mitchell *et al.*, 2015) to vouch for the randomness in a phase noise QRNG. The chosen device, described in (Abellán *et al.*, 2014), is based in the random phase in a laser, as explained in Section VII.G. A physical model can give a strict bound for the average min-entropy, which is used to choose a randomness extractor. The method works with theoretical considerations alone, but also gives room to introduce constraints based on auxiliary measurements or on the data that has been generated. This kind of estimation has also been done in (Haw *et al.*, 2015) for the initial configuration of the QRNG based on the measurement of vacuum fluctuations of (Symul *et al.*, 2011) (see Section VII.F).

B. Device independent quantum random number generators

A second approach to certifying random numbers is ignoring the details inside the quantum random number generator and judge the results based only on the output. In particular, we want to prove that the output must be random or otherwise some physical law must be broken. This is the basic model behind device independent quantum information processing, which started in the context of quantum key distribution with (Mayers and Yao, 1998) and (Barrett *et al.*, 2005) with multiple further developments (Acín *et al.*, 2007; Colbeck, 2007; Colbeck and Kent, 2011; Magniez *et al.*, 2006).

In the case of random number generation, it tries to address the worst imaginable case where an adversary has generated genuinely random numbers, for instance with a quantum random number generator, and then has hidden them inside a manipulated device. If we check the output of that device, the sequence will pass all randomness tests and we will trust the results. This problem is difficult to

avoid, but has a quantum solution.

Device independent quantum random number generators solve the problem of trusting the device with schemes based on Bell tests. The ideas of Bell violation stem from the discussion of an apparent discordance of quantum theory and relativity known as the Einstein-Podolsky-Rosen paradox (Einstein *et al.*, 1935). In an entangled state, measurement of one of the particles immediately sets the state of the other particle. This seems to contradict the no-signalling principle than forbids faster than light communication. John Bell showed that the contradiction could be settled experimentally (Bell, 1964). The statistics of measurement on space-like separated entangled particles would be different in a realistic local world with no interaction faster than light and in a world where the laws of quantum mechanics hold. Both alternatives are incompatible. Aspect's experiment (Aspect *et al.*, 1982) showed support for the quantum description. There are, however, experimental loopholes that could still allow a hidden variable theory that is local or realistic. A series of ever more sophisticated experiments is closing alternative explanations and confirm the predictions of quantum theory (Giustina *et al.*, 2015; Hensen *et al.*, 2015; Shalm *et al.*, 2015). A detailed description of Bell inequalities and nonlocality can be found in (Brunner *et al.*, 2014).

In the experimental QRNG of (Pironio *et al.*, 2010) the chosen version of the Bell's inequalities is the Clauser-Horne-Shimony-Holt, CHSH, formulation (Clauser *et al.*, 1969), which is particularly elegant, simple and intuitive. We study the correlations in measurements from two devices and define two variables x and y , one for each device. The variables can take two values, 0 and 1, that correspond to a choice between two binary measurements. Both measurement devices are identical. The measurement in the x configuration gives a binary output a and the measurement defined by y gives an outcome b . We are interested in the correlation function

$$I = \sum_{x,y} (-1)^{xy} [P(a = b | xy) - P(a \neq b | xy)] \quad (35)$$

where $P(a = b | xy)$ and $P(a \neq b | xy)$ are the probabilities that $a = b$ or $a \neq b$ when the settings are x and y . For a realistic local theory we should always find $I \leq 2$. Any value above 2 indicates non-locality.

The function I can be experimentally approximated by estimating the probabilities after taking a series of measurements. As long as the systems are separated and do not interact, if the laws of quantum mechanics hold and the inputs x_i and y_i at any stage i are generated by independent random processes, the estimation of I , \tilde{I} , gives, after some work, a lower bound to the min-entropy of the outputs. The original derivation of the bound on min-entropy in (Pironio *et al.*, 2010) had a technical error, but in (Pironio and Massar, 2013) and (Fehr *et al.*, 2013) there are restored correct proofs of the main results, as

well as demonstrations of some additional properties of the protocol, like its composability⁸ and its fitness to generate random bits for their use in cryptography.

If the system admits a classical description, $\tilde{I} \leq 2$, the bound is zero and the system could be deterministic. If the measurements are done on states showing some entanglement the produced random bits are guaranteed to have some randomness. The resulting bit sequence is not necessarily uniformly random, but the bound in its min-entropy means it can be converted into a random uniform string with an appropriate randomness extractor (see Section X).

For quantum devices with spacelike separated parts with access to independent random sources, there are no additional constraints on the devices or the input states as long as $\tilde{I} > 2$. The only additional requisite is that the chosen measurement settings x_i and y_i at each stage of the protocol have some randomness (are not perfectly predictable). In that respect, the described generator is a randomness expansion scheme, much similarly to what happens in Ekert's proposal for quantum key distribution (Ekert, 1991; Vazirani and Vidick, 2014). Starting from a random seed, the protocol gives a longer output random string whose randomness is certified by quantum mechanics. The protocol in (Pironio *et al.*, 2010) is quadratic: in order to produce n certified random bits it consumes a previously existing random sequence of the order of \sqrt{n} bits. The protocol of (Vazirani and Vidick, 2011) creates strings with n random bits certified to be secure against quantum adversaries starting from a seed of a length of the order of $\log_2^3 n$ bits, offering an exponential expansion.

Physically, the QRNG in (Pironio *et al.*, 2010) was implemented with trapped ion qubits (Olmschenk *et al.*, 2007) in order to close the detection loophole. Ion systems result in slower generation when compared to optical implementations, but offer almost perfect detection efficiency. Each atom first emits a photon with which it is entangled and then interference between the photons entangles the ions. This is a probabilistic heralded process. Experimental violation of Bell's inequality is a delicate task and the generation process was excruciatingly slow, giving only 42 certified random bits with a 99% confidence level⁹ after around a month of continuous running.

⁸ In cryptography, proofs of security are limited to the particular conditions of the protocol and might fail when the results are put forward to a second cryptographic protocol. Putting together the information leaked from the first and the second protocol can compromise the data in a way neither protocol alone does. We say a protocol is composable if we can prove its output can be safely used as the input of another protocol, maybe under some restrictions. A composable protocol can be used as a part of a larger system and is still secure (Barak *et al.*, 2004; Canetti, 2001).

⁹ The statistical nature of the device independent generation pro-

Later proposals relax some of the requisites to allow for optical implementations and faster generation rates. Most optical detectors have a low efficiency, but transition-edge-sensor detectors (Lita *et al.*, 2008) have been shown to offer a high enough efficiency to close the detection loophole in some modified versions of Bell’s inequality (Giustina *et al.*, 2013) and have been used to generate certified quantum random numbers at a rate of about half a bit per second (Christensen *et al.*, 2013).

The QRNG of (Cañas *et al.*, 2014) takes an alternative model that permits lower detection efficiencies with a semi-device-independent approach (Pawłowski and Brunner, 2011) where we still do not trust the device but suppose we work with a quantum system with a bounded dimension. The experiment encodes the quantum data in the linear transverse momentum of single photons using spatial light modulators. While in the mentioned demonstration there are only two paths available, including spatial light modulators permits to control the spatial profile of single photons to encode higher dimensional quantum states. This optical system reaches bit rates of 0.28 certified bits per second.

Other optical implementations focus on optimizing device independent random bit generation in experiments with entangled photon pairs. This is the approach in (Mátar *et al.*, 2015) and (Vivoli *et al.*, 2015) and in the NIST randomness beacon (NIST, 2011).

The ideas of device independent quantum random number generators can be extended to an even more general model where quantum mechanics needs not to be true, following the example of the device independent quantum key distribution protocols (Barrett *et al.*, 2012, 2005) that only require the no-signalling principle to hold. The no-signalling principle forbids the transmission of *information* faster than the speed of light. A faster than light communication device would allow sending messages to the past and produces a conflict with causality (Tolman, 1917), as exemplified by the grandfather paradox¹⁰. The no-signalling principle is subtle. In entangled states, while there is non-locality and there are correlations that seem to travel faster than the speed of light, it is in fact impossible to use them to send information (Bussey, 1982; Dieks, 1982; Jordan, 1983).

In the device independent quantum random number generators of (Pironio *et al.*, 2010) and (Vazirani and

Vidick, 2011) the bounds are also given for the non-signalling restriction. The exact bound on the conditional min-entropy changes, but the general results hold. In this new model, the protocols still work as randomness amplification schemes that need a uniform random seed.

All the commented device independent random number generators, quantum and non-signalling alike, are, in fact, implementations of protocols that use the results from physical experiments to expand randomness. They start from a small random seed and produce a longer bit sequence guaranteed to be random. We give a more detailed description of this quantum randomness expansion in Section XI.

C. Other forms of quantum certification

Instead of testing locality with Bell inequalities, we can try to design certified quantum random number generators based on other experimental tests of the basic features of quantum theory. The Kochen-Specker theorem shows that there are states for which no non-contextual hidden variable model can reproduce the predictions of quantum mechanics (Kochen and Specker, 1967). Contextuality in quantum mechanics is related to the existence of non-commutable observables where the order of measurement is important and there is no predefined model that can give the outcomes of two successive incompatible measurements. Contextuality implies nonlocality (Einstein, 1948).

Quantum random number generators based on test of contextuality are designed to make sure we are accessing quantum randomness and not classical noise. In this model, we still work with untrusted devices but in a less adversarial setting. We assume the manufacturer of the random number generator is not actively trying to fool us, but we admit the device can be faulty or poorly designed. A test of contextuality shows whether we are truly reading bits from a quantum source or not. One of the advantages of quantum random number generators is that we can clearly trace the origin of our random bits to a defined quantum phenomenon. These certified generators can help to detect the randomness due to classical noise, imperfections or failures in the device and take only the randomness from quantum origin. Contextuality tests can work without spacelike separation of the devices. This is both the merit and the disadvantage of the method. These tests do not required complex non-local entangled states, but we cannot count on causality to guarantee the bits must be random. Unlike in device independent protocols, a rogue manufacturer can feed us pregenerated bits without being detected.

The quantum random number generators of (Deng *et al.*, 2013) and (Um *et al.*, 2013) produce certified random bits based on contextuality tests through the violation of the Klyachko-Can-Binicioglu-Shumovsky, KCBS,

cess can only certify a violation of Bell’s inequality with a certain confidence level. We can ask for more certainty by taking more measurements (and thus reducing the generation speed).

¹⁰ In the grandfather paradox, a time traveller, somewhat cruelly, decides to prevent the journey by killing his grandfather (Nahin, 1999). While it is still open whether General Relativity allows time travel, we can consider causality a fundamental principle. Even if it is not completely impossible, the no-signalling restriction is equivalent to asking an attacker for the highly nontrivial feat of time travel.

inequality (Klyachko *et al.*, 2008), which doesn't require entangled states. The basic principle follows the model of (Pironio *et al.*, 2010). A violation of the KCBS inequality guarantees a lower bound in the entropy of the output string, which can then be fed to a randomness extractor. The results serve as a certificate of quantumness, with a minimum amount of randomness that can be safely said to be of quantum origin.

The physical implementation can be optical (Deng *et al.*, 2013), with a qutrit¹¹ encoded in a photon in a superposition of three possible paths, or use a three-level trapped ion (Um *et al.*, 2013), which permits to close the detection efficiency loophole and avoids the problems of obtaining a single photon on demand. In the ion system, the random bits come from registering or not fluorescence during a measurement that takes around 10 ms. In both cases, under the tested experimental conditions, the devices could only provide a net gain in randomness, i.e. generate more random bits than they consumed, when using non-uniform measurement settings.

Along the same lines, there are also theoretical proposals for random number generators based on contextuality tests in settings similar to the previous experiment (Abbott *et al.*, 2012) and with entangled states (Abbott *et al.*, 2014) that highlight the relationship of randomness and incomputability (Calude and Svozil, 2008).

X. POSTPROCESSING

Standard random number generators are designed to produce a random uniform string. The postprocessing stage takes care of converting the raw bit sequence into a good quality output as close as possible to a uniform bit distribution. Postprocessing can include tasks like buffering to accumulate samples before generating the output strings or health tests that check the generator is working properly (Schindler and Killmann, 2003). For instance, the commercial quantum random number generator based on path branching Quantis includes hardware to check for inconsistencies following the AIS31 standard (ID Quantique, 2014).

Apart from these tasks, which vary from generator to generator, the main purpose of postprocessing is randomness extraction. Most physical RNGs include one form or another of randomness extraction to correct for biases and correlations that appear due to imperfections in the measurement and generation devices even for good randomness sources with a high entropy.

A high entropy is not enough to guarantee the generated random sequence is fit for any purpose. While there

are methods that can fix weak sources for their use in randomized algorithms (Zuckerman, 1996), where randomness brings efficiency, not all protocols can work with imperfect randomness. In particular, many cryptographic protocols for tasks like bit commitment, encryption, zero knowledge or secret sharing are not secure unless they use an almost uniform random sequence (Dodis *et al.*, 2004).

Some hardware random number generators mix different randomness sources by taking the logical XOR of their bits or feed the strings to a cryptographic hash function (Networking Working Group, 2005). Von Neumann proposed a simple debiasing method in which, for every pair of generated bits, we discard the results 00 and 11 and assign a 0 to 01 and a 1 to 10 (von Neumann, 1951). If we have a systematic bias this method will remove it at the cost of throwing away at least half of our bits and reducing our bit rate at least by one fourth (discarding more bits the more biased our original sequence was). The basic method can be refined to improve its efficiency (Elias, 1972; Peres, 1992).

Before going on describing randomness extraction in more detail, it is important to define what is considered as an “acceptably” uniform output. A useful concept is that of distance between distributions. For two probability distributions X and Y defined in the same support (they can take the same values in a finite alphabet \mathcal{A}), we can define a statistical distance

$$d(X, Y) = \max_{a \in \mathcal{A}} |P_X(a) - P_Y(a)|. \quad (36)$$

This metric gives the maximum difference in the probability of getting a particular result in the compared distributions. We say two distributions X and Y are ϵ -close if

$$d(X, Y) \leq \epsilon. \quad (37)$$

In randomness extraction the goal is to produce an output sequence which is as close to uniform as possible. That usually means taking the n bits of the raw output and transforming them into strings of m bits with a distribution which is ϵ -close to U_m (a distribution uniform in $\{0, 1\}^m$) for a small ϵ that depends on our requisites.

Ideally, we would like extractors that give as many output bits as possible with the smallest use of additional resources like computation time or additional randomness. In that respect, the randomness measures we have discussed in Section IV serve as a design guide. In particular, the min-entropy of the distribution of the raw sequence gives a limit on how many bits we can extract. If we take n -bit strings from the raw sequence with a distribution X of min-entropy $H_\infty(X) = k$, we can extract at most k random bits that are close to uniform, irrespective of the original length. A random process is called an (n, k) -source if it produces n bits with a distribution X of min-entropy $H_\infty(X) \geq k$.

¹¹ The Kochen-Specker theorem works for any quantum system of dimension $d \geq 3$.

In the following section we will discuss different methods to generate bit sequences as close to uniform as desired for rates close to the min-entropy limit and the advantages and limitations of different randomness extraction approaches.

A. Randomness extractors

Randomness extractors are functions that convert a weak source of entropy into a uniform bit generator. They were originally introduced in the study of randomized algorithms, but have become a basic tool in many areas of theoretical computer science. Randomness extractors and related concepts like dispersers, condensers and expander graphs have multiple applications and appear in the fields of pseudorandom number generators, error-correcting codes, samplers, expander graphs and hardness amplifiers, among others (Vadhan, 2007).

In this Section, we discuss only the few concepts about extractors most relevant to QRNGs and refer the interested reader to the extensive literature on the subject, ranging from introductory tutorials (Shaltiel, 2011) to detailed surveys (Nisan, 1996; Nisan and Ta-Shma, 1999; Shaltiel, 2002). There are many available options for randomness extraction and the final choice is usually influenced by the speed and hardware requirements of each method. Here, we just comment on some particularly interesting extractors.

In order to have an efficient method and preserve as many bits as necessary, we need to have a good estimation of our available entropy and then choose an adequate randomness extractor (Ma *et al.*, 2013b). Otherwise, the output of the extraction function will not have the desired properties.

In the following, we assume we have a well-characterized randomness source. The relevant entropy measures were discussed in Section IV. The raw sequence is assumed to have a known min-entropy or, in some cases, at least some known properties such as independence between bits or that it comes from a Markov process.

In the next Sections, we also assume by default that we want an (n, m, k, ϵ) -extractor: a function that convert n bits of an (n, k) -source into m output bits with a distribution that is ϵ -close to uniform, with m as close to k as possible.

1. Deterministic extractors

Deterministic extractors are functions

$$\text{Ext} : \{0, 1\}^n \rightarrow \{0, 1\}^m \quad (38)$$

that take input strings of n bits $\{0, 1\}^n$ into m output bits. They are particularly attractive as they are deterministic algorithms that only need an input sequence to

work. However, they have some limitations that prevent their use with certain randomness sources.

As in all extractors, we can only produce an output close to uniform if the input sequence already has enough intrinsic entropy. If the input sequence is an (n, k) -source, a necessary condition for the output sequence to be close to uniform is that $m \geq k$. Unfortunately, the necessary condition is not sufficient and we can only find deterministic extractors for certain limited input distributions.

An elementary argument shows the impossibility of general deterministic extractors. Imagine a function from $\{0, 1\}^n$ to $\{0, 1\}^m$. We can divide all possible inputs into one set of all the input n -bit strings that give a 0, $\text{Ext}^{-1}(0)$, and another set that is taken to 1, $\text{Ext}^{-1}(1)$, and at least one of them has a size 2^{n-1} or larger. An input that is a uniform distribution in the larger set has at least min-entropy $n - 1$ but produces always the same output showing there is no one-size-fits-all extractor valid for any input distribution (Chor and Goldreich, 1988).

There are, however, valid extractors for input distributions belonging to certain families of processes that describe reasonable sources. Among others, there are practical deterministic extractors for samplable distributions (Trevisan and Vadhan, 2000), for bit-fixing sources where an adversary can set part of the bits (Gabizon *et al.*, 2006; Kamp and Zuckerman, 2007) and generalizations for affine sources (Bourgain, 2007; Gabizon and Raz, 2005) or sources with an output that is distributed uniformly over an unknown algebraic variety (Dvir, 2012).

Variable length deterministic extractors form another group of interesting deterministic extractors which deviate slightly from the description of Equation (38). They are exemplified in the von Neumann algorithm: a deterministic method that works for an unknown distribution and gives an output of a length that is not known before the extraction. In the von Neumann randomness extractor described at the beginning of this section the only requisite is that each input bit is independent from the previous and following bits. Refined versions of von Neumann's method reduce the discarded entropy and give efficiencies close the information theory limit given by the Shannon entropy of the source (Elias, 1972; Peres, 1992). Further modifications give algorithms that produce unbiased sequences on the more general condition that the input sequence comes from a Markov chain (Blum, 1986; Zhou and Bruck, 2012).

The main appeal of the original method is its simplicity. It requires minimal computing power, it can be implemented with just basic hardware and the distribution at the source needs not to be perfectly known. However, it has some important limitations. If we have an external attacker that can alter the bias from bit to bit, even slightly, the von Neumann extractor no longer works. In fact, there is no deterministic algorithm that can give a uniform output for a random variable

$X = (X_1, X_2, \dots, X_n)$ with n bits if the bias of the input bits can vary so that the probability of finding a 1 for the n th bit conditioned on the measured string for the previous bit values s is

$$\delta \leq P_{X_i}(1|x_1x_2\dots x_{n-1} = s) \leq 1 - \delta \quad (39)$$

for a $0 < \delta \leq \frac{1}{2}$. This is called a Santha-Vazirani source and was described as a model for weak randomness sources in (Santha and Vazirani, 1986) together with an impossibility proof for a deterministic extractor.

Despite this limitation, there are deterministic algorithms that permit to use a weak Santha-Vazirani source to simulate randomized algorithms (Andreev *et al.*, 1999; Vazirani and Vazirani, 1985b). The requisites for randomization are less stringent than for other applications, like cryptography, and weak sources that fail to produce nearly uniform outputs are sometimes valid.

Even if we use a deterministic extractor, a single weak source is not good enough for many cryptographic protocols. While weak randomness can be used securely with signature schemes, encryption and other related protocols need a high quality key or they become vulnerable (Austrin *et al.*, 2014; Dodis *et al.*, 2004; Dodis and Spencer, 2002; McInnes and Pinkas, 1991).

For applications where we need an output close to uniform, (Santha and Vazirani, 1986) offer a simple solution: combining the output of two independent Santha-Vazirani weak sources we can produce output sequences that cannot be distinguished by any polynomial-time algorithm from a uniform distribution. As long as we have access to a physical method that produces *some* randomness, we can generate bit strings that cannot be distinguished from a random string with any efficient algorithm. This is just as good as true randomness for the vast majority of applications of randomness, including cryptography.

Multiple source extractors follow this model and take the output of two or more weak sources and process them to generate a sequence that is close to uniform. There are many methods that depend on the concrete input distributions, the number of sources we have and the desired properties of the output sequence.

A simple extractor valid for two n -bit blocks from two independent weak sources, both with min-entropy at least $n/2$, is taking the $GF(2)$ inner product of the n -bit blocks, which reduces to computing the parity of the bitwise AND of the two sequences (Chor and Goldreich, 1988; Vazirani, 1987a,b).

Other representative methods to combine different randomness sources can be found in (Barak *et al.*, 2006; Bourgain, 2005; Dodis *et al.*, 2004; Rao, 2009; Raz, 2005; Shaltiel, 2008).

The idea of combining sources is also behind the second main group of randomness extractors, seeded extractors. We can consider them a special case of multiple source

extractors with one weak source and a perfectly uniform source that only produces a small amount of bits.

2. Seeded extractors

As we have seen, for many raw bit distributions, we can only achieve an output close to uniform with the help of some additional randomness. In seeded extractors we have a function

$$\text{Ext} : \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m \quad (40)$$

that takes as its input n bits from the raw sequence and a uniform random seed of d bits to produce m output bits. We assume d is much smaller than m . With the addition of the seed, which plays a role similar to the seed in pseudorandom number generators, we can guarantee that there exist extractors that produce an almost uniform output close to the maximum possible length. We call a (k, ϵ) extractor to a function that, for any input k source (a raw sequence of, at least, min-entropy k), produces an output sequence that is ϵ close to uniform. The seed acts as a catalyst that permits to find general methods that will always work.

Seeded randomness extractors were first defined in (Nisan and Zuckerman, 1996) in the context of randomized algorithms. Using the probabilistic method (Alon and Spencer, 2016), (Radhakrishnan and Ta-Shma, 2000) showed there always exist extractors with an output that contains almost all of the available hidden entropy in an input raw sequence coming from any k -source. For input blocks of n bits from a k -source, we can build extractors with an output of a size $m \approx k + d$ that is ϵ -close to uniform using only a seed of a length d of the order of $\log_2(n)$. There are different explicit constructions for these seeded extractors, like the ones in (Lu *et al.*, 2003; Ta-Shma, 1996).

The need for a uniform seed seems a contradiction: we require the resource we are trying to produce. However, the requisites on the seed are less restrictive than it seems. In many explicit extractors the seed has a length logarithmic in the size of the input string. For a small enough d , we can even replace the requisite of randomness by an exhaustive enumeration of all the 2^d possible sequences. In randomized algorithms, enumeration followed by majority voting permits to simulate a good uniform source (Goldreich and Wigderson, 2002). However, this approach is clearly not valid for cryptography, where we need unpredictability.

In quantum random number generators, seeded extractors provide protection against external attackers. There are constructions for which there exist proofs of security against quantum attackers of different power (Ben-Aroya and Ta-Shma, 2012).

A first notable result is the Trevisan extractor (Trevisan, 2001), an explicit construction which has some

nice properties like its resistance against quantum adversaries (De *et al.*, 2012; De and Vidick, 2010; Ta-Shma, 2011) and the way it preserves the randomness of its seed (Mauerer *et al.*, 2012). The Trevisan extractor is built on the Nisan-Wigderson pseudorandom number generator (Nisan and Wigderson, 1994). It can be seen as a random function whose truth table is given by the bits from the weak source. The random function expands the d bits of a uniform random seed, both in the PRNG and the extractor sense. Different variations of the Trevisan extractor have been implemented for their use with quantum random number generators and in quantum key distribution (Ma *et al.*, 2013b; Mauerer *et al.*, 2012). Their main advantage is that the size of the random uniform seed is only poly-logarithmic in the size of the input blocks. However, practical implementations can slow down the bit generation process due to the involved calculations required during the extraction.

A second general method of particular interest is two-universal hashing. The Leftover Hash Lemma (Håstad *et al.*, 1999; Impagliazzo *et al.*, 1989) shows that the output of a two-universal hash function with an input with high enough entropy is almost uniformly random. Two-universal hash functions, such as the families introduced in (Carter and Wegman, 1979; Wegman and Carter, 1981), can extract the randomness in a weak source in a secure way in the presence of an eavesdropper. If we have a good estimation or a conservative bound on the correlation of our weak random source with the eavesdropper, using the conditional entropies described in Section IV, it is possible to use a generalization of the Leftover Hash Lemma with side information (Tomamichel *et al.*, 2011). In the most general case, the side information can also be quantum. In a quantum random number generator with technical noise, we can assume that all the randomness that comes from imperfections or otherwise does not adjust to our model of the quantum system that produces the raw bits is due to an eavesdropper. In those conditions it is still possible to design a seeded extractor that gives an almost uniform output that is independent from external systems (König and Renner, 2011; König and Terhal, 2008). These methods are also applied in privacy amplification in Quantum Key Distribution (Bennett *et al.*, 1995, 1988; König *et al.*, 2005; Renner and König, 2005).

Randomness extraction with two-universal or, more generally, l -universal hashing forces us to use a relatively long seed, comparable to the size of the block n , but it can be recycled. A randomly chosen public uniform seed can be reused and permits a secure seeded extractor in the presence of an imperfect randomness source under partial influence of an attacker (Barak *et al.*, 2003; Skorski, 2015).

When compared to implementations of the Trevisan extractor, this method offers a fast extractor function that takes less computational resources at the cost of

a larger seed (Ma *et al.*, 2013b). Some implementations, like hashing with Toeplitz random binary matrices (Krawczyk, 1994; Mansour *et al.*, 1990), are particularly efficient. We can define one such extractor where the seed is used as a rectangular matrix that is multiplied to n -vectors from the source to produce an output of almost independent bits (Frauchiger *et al.*, 2013). This approach is used in some commercial devices which include the extraction function as a precomputed random matrix that acts as the seed and is distributed coded into the device (Troyer and Renner, 2012). While ensuring the seed is uniformly random to a high degree is a painstaking task, it only needs to be done once. Long unsophisticated methods, like repeatedly taking the XOR of multiple independent generators, are acceptable.

XI. QUANTUM RANDOMNESS EXTRACTORS: RANDOMNESS EXPANSION AND RANDOMNESS AMPLIFICATION

Quantum mechanics does not only offer new sources of entropy for random number generators, but also new protocols related to randomness extraction. We will consider physical randomness extractors which use untrusted ancillary systems either to expand the random output of a uniform source or to turn a weak randomness source into strong one (Chung *et al.*, 2014).

There are two interesting families of protocols: quantum randomness expansion and quantum randomness amplification. In quantum randomness expansion, we start from small random seed and, with the help of a quantum protocol, we produce a longer bit sequence with strong guarantees of randomness. In randomness amplification we take a weak source, either classical or quantum, and use a quantum system to amplify the randomness in the weak source and give an arbitrarily close to uniform output.

Related to these ideas is also privacy amplification, where we take a bit string which is partially known to an adversary and produce a smaller sequence for which no external attacker can have any statistically significant information. There are known classical (Bennett *et al.*, 1995, 1988) and quantum (Deutsch *et al.*, 1996) algorithms for this task, but we can also use methods related to randomness extraction protocols that can guarantee the output is uncorrelated to any causally preceding events and, therefore, must be private.

In this Section, we give an overview of the main ideas behind these concepts. The reader can also find a good review of all the mathematics involved in (Pivoluska *et al.*, 2014).

A. Quantum randomness expansion

Quantum randomness expansion protocols follow the model of seeded randomness extractors (see Section X.A.2): assisted by a random seed, we process the bits from a weak randomness source and give an output that is as close to uniform as desired.

All the device independent generators discussed in Section IX.B are, indeed, implementations of some kind of randomness expansion protocol working on the weak randomness produced in the nonlocality experiments of different Bell tests. The quantum system serves both as a weak source of randomness and as a way to guarantee the privacy of the results. The random seed serves as a starting point to take the randomness in the quantum devices into a uniform output.

Randomness expansion protocols can be concatenated using a limited number of devices (Miller and Shi, 2014). By repetition of simple protocols with a finite number of quantum devices, we can increase the size of the output arbitrarily to produce sequences certified against quantum adversaries (Coudron and Yuen, 2014).

If we relax our requirements and trust part of the system, we can also find semi-device independent randomness expansion protocols. For instance, for untrusted devices but a trusted quantum state with a bounded dimension, the protocol in (Bouda *et al.*, 2014) gives an expansion scheme that does not require entanglement, which makes it easier to implement in practice. If we consider an adversary which does not directly control our device, but can characterize it better than us and has a complete model of its inner workings, we can also produce a private output string if we make full use of all the data taken from a series of Bell tests instead of restricting to the usual inequalities (Bancal *et al.*, 2014).

A different kind of extractor without Bell tests is the source-independent seeded extractor in (Cao *et al.*, 2016), which is designed to work with imperfect quantum sources and addresses many problems of optical quantum random number generators like losses, multiphoton pulses or unbalanced beam splitters.

Similarly, there are also quantum-to-classical randomness extractors that give a procedure to measure a quantum state from a source that can be correlated to an eavesdropper so that we maximize the amount of random bits we get without giving away information to the adversary (Berta *et al.*, 2014).

Finally, the concepts of randomness expansion can also be formulated as a privacy amplification problem in which we want to extend the length of a private string while keeping it secret under the usual assumptions of the device independence scenario with untrusted equipment (Colbeck and Kent, 2011). The task is possible and efficient against quantum attackers, but, unlike other protocols, there are severe limitations if we consider attackers that are only restricted by nonsignalling constraints

(Arnon-Friedman and Ta-Shma, 2012). Anyway, while considering nonsignalling attackers gives quite general security results, quantum mechanics seems to be the non-local theory that best describes the physical world and a quantum secure protocol can be safely considered as valid.

B. Quantum randomness amplification

The need for a uniform seed in device-independent protocols comes from two parts of the procedure. First, in Bell tests we assume we have uniform random bits to choose the measurement settings. Second, the generated bit sequence is only guaranteed to have a lower bound on min-entropy, but we need to use some seeded randomness extractor to obtain a uniform output bit string.

Quantum randomness amplification protocols eliminate these previous uniform randomness requisites and give a way to use a weak source in combination with quantum devices to produce uniform random bits. In Section X.A.1 we have seen it is impossible to find a general deterministic method to extract randomness from any limited min-entropy source, even from restricted weak origins of entropy like Santha-Vazirani sources. With the help of quantum mechanics, we can solve this problem and find methods to extract almost uniform randomness in those situations. From a certain point of view, these protocols are not so much deterministic randomness extractors as multiple source extractors where we prove how to combine the randomness in the quantum devices with the randomness of a weak source to produce a good quality output. While the exact details vary from protocol to protocol, the quantum part is usually limited to simple measurements on the different subsystems of an entangled state. From an experimental point of view, the hardest requisite to satisfy is making sure the quantum devices are independent, which can be a problem in protocols that require multiple devices.

A remarkable contribution to quantum randomness amplification is the randomness amplification protocol of (Colbeck and Renner, 2012), which shows there are deterministic protocols that can amplify the randomness in Santha-Vazirani sources using ancillary physical systems. The result rests only on nonlocality and is robust against attackers that can go beyond quantum mechanics. This protocol needs a large supply of imperfect randomness. One natural application would be using quantum randomness amplification only to provide the random seed for the quantum randomness expansion protocols of the previous Section and then use the less involved quantum randomness expansion protocols to generate the final random bit stream.

While the original protocol works only for small biases δ in the definition of the source, see Eq. (39), (Gallego *et al.*, 2013) give a quantum randomness amplification

protocol that is valid for arbitrarily weak sources of entropy. Further protocols can take any input weak source with a bounded nonzero min-entropy (Bouda *et al.*, 2014; Chung *et al.*, 2014; Plesch and Pivoluska, 2014) and give practical ways to use Santha-Vazirani sources, requiring only a limited number of independent devices (Brandão *et al.*, 2016).

There are also interesting ramifications for fundamental science experiments. Many of the concepts of quantum randomness amplification can be traced back to the study of randomness in Bell inequalities. These results are interesting in themselves as they determine which random number generators can be used in the foundational experiments on nonlocality in Bell tests. In Bell experiments there is a “free will” loophole: if the settings in the measurement are correlated, the violation of a Bell inequality cannot be used as a guarantee against an eavesdropper (Koh *et al.*, 2012). Fortunately, even in the usual experiments, there is a certain tolerance for small correlations (Hall, 2010), but general min-entropy sources are not valid for the selection of the settings in Bell experiments (Thinh *et al.*, 2013).

XII. RANDOMNESS TESTING

Once we have generated a raw random sequence, we need to do some quality checks to be sure the device is working correctly. Unfortunately, there is no way to check a finite sequence is truly random. Taken to its most absurd extreme, it is like asking whether a 0 bit is fundamentally more random than a 1. Apart from the uncomputable Kolmogorov complexity (Li and Vitányi, 2008), there is no way to deduce that a random string is really random, but there are methods to detect suspicious sequences. While the bit string 1111111111 is just as likely as 0100110111, if we have a generator that consistently outputs more ones than zeros we have reason to suspect it is not acting randomly.

The customary approach to randomness testing is using a series of statistical tests. Knuth covers some of the most usual ones in (Knuth, 1997). The main suites available to perform these statistical tests are the NIST (Rukhin *et al.*, 2010), TestU01 (L’Ecuyer and Simard, 2007) and the DieHard and DieHarder (Brown, 2016; Marsaglia, 1996) suites. There are also special-purpose randomness testing batteries, like the one included with the SPRNG software (Srinivasan *et al.*, 2003), which is designed to check for problems in parallel implementations of pseudorandom number generators.

These suites include different tests. In the following list, we present some of the most relevant tests to give a feeling of the kind of hidden correlations that can appear.

1. The *frequency (monobit)* test, which calculates the proportion between ones and zeroes and how close

that proportion is to $\frac{1}{2}$, and frequency tests within a block, similar to the previous one, but testing for the expected probabilities for the specified block sizes.

2. The *runs* test, which checks if the number of *runs*¹² in a bit string corresponds to that in a random sequence and if the oscillation between zeroes and ones is too fast or too slow.
3. The *spectral* test, which tries to detect periodic features in the sequence that would indicate a deviation from the assumption of randomness.
4. Maurer’s *Universal Statistical* test (Maurer, 1992), which detects whether or not the sequence can be significantly compressed without loss of information.
5. *Autocorrelation* tests which check the correlation of the sequence with shifted versions of itself.

Most tests apply statistical analyses similar to the standard chi-squared test. The result is a *p-value* that indicates how likely it is for a purely random number generator to produce the tested sequence. Each test suite has different threshold values to determine if a given *p-value* is compatible with randomness or not.

These tests, while useful to detect faulty generators, cannot prove a generator produces truly random outputs. Deterministic pseudorandom number generators like the Mersenne Twister can pass the tests but are predictable. Likewise, there can be false positives for correlations and the tests should be run multiple times for each generator. Statistically, even a perfect random number generator would fail a test from time to time.

Testing is also vulnerable to an active attacker that feeds us pregenerated random sequences that pass the tests. In Section IX.B we have described some quantum protocols to solve this issue.

Apart from that, the tests are usually designed with pseudorandom number generators in mind and do not include physical models into account. Some correlations due to implementation-related problems, like afterpulsing in photon detectors, are not specifically checked.

All these problems notwithstanding, any good quantum random number generator should be able to pass all the tests in any given suite and using some form of randomness testing during operation can help to detect sudden failures or faulty components.

¹² A *run* is defined as an uninterrupted sequence of identical bits bounded by a bit of the opposite value before and after the same-bit sequence.

XIII. DISCUSSION

Quantum random number generation is probably the most mature quantum technology. We have seen the multiple ways we can harness the randomness in quantum mechanics to produce random bit strings. Physical phenomena such as radioactive decay, photon splitting, noise in Raman amplification, laser phase noise or amplified spontaneous emission can serve as reliable entropy sources.

We have reached a point where optical quantum random number generators routinely reach generation rates in the order of megabits per second with promises of gigabit rates and new generation methods are still being suggested every year. While there is a race to announce the highest possible generation rates, in many cases, the actual implementation is limited by practical hurdles in the speed of the electronic systems and the postprocessing methods.

Many proposals focus on the generation principle, on making sure the quantum phenomenon of interest produces fresh entropy at a fast rate, but do not deal with making full use of the available bits and give random bit rates which are only true as an extrapolation. In the research phase, it is perfectly acceptable to leave all the processing details for later and work on a limited collection of stored samples, but, at this point of development, there is a need for better and faster production of the final, usable random bits.

Commercial devices, by necessity, have these aspects covered but they still offer bit rates with a gap around two orders of magnitude with respect to the fastest possible lab rates. In some applications, like simulation, this is important, as quantum random number generators have to compete against fast pseudorandom number generators that work essentially at the speed of the available processor.

Concerning the bit rate, there are two relevant issues. One is the communication bottleneck. External devices will always need a communication channel with the computer that uses the random bits. The fastest USB protocols (USB 3.0 and 3.1) and PCI Express components can reach communication rates in the order of tens of Gbps that is enough for many generators. Alternatively, many optical implementations can be adapted or have been demonstrated to work in integrated silicon setups that could be included as part of future processors.

Communication at those rates is challenging, but it is an engineering problem that can be solved with current technology with the right systems. A second more interesting limitation is randomness extraction. In Section X, we have described different ways to turn the raw bits coming from measurement and the first simple conditioning into good quality random bits. While some quantum random number generators are claimed to directly produce random enough raw sequences, in some applications

like cryptography, less than perfect uniformity can pose serious problems. In general, quantum random number generators should include a well-designed postprocessing phase.

Seeded extractors like Trevisan's or two-universal hashing have good security properties against quantum attackers. That should be the standard that postprocessing methods should aspire to. At the moment, postprocessing is relatively slow when compared to the potential generation rates of the fastest optical generators. The most efficient implementations use postprocessing based on two-universal hashing with binary matrix multiplication. There is a large open area of research on identifying and constructing new extractors that are resistant against quantum attacks and can be fast enough to sustain output bit rates in the order of Gbps.

Self-testing is another area for future improvement. Physical random number generators can fail due to component degradation or even external attacks. In Section IX we have described many possible approaches to quality control. In particular, device independent protocols offer reliable random numbers even if we don't trust our hardware. Device independent randomness generation and quantum randomness expansion and amplification are quite active areas of research and the last years have seen many interesting results, including new protocols based on nonlocality that can perform classically impossible tasks, like physically-assisted deterministic randomness extraction from weak sources.

Device independent quantum random number generators are still experimentally challenging and produce bits at sluggish rates. In Section IX we have also commented on more relaxed approaches to certification, but this is likely to be an active area for the next years, both in technological development research to make better device independent QRNGs and in the theoretical search for simpler paths to certification.

At the moment of writing, both pure and applied research have reached an interesting point where there are new fundamental results and, at the same time, there appear different quantum random number generators in the market.

With this review, we hope we have introduced the reader to the existing technologies and hinted at some future directions.

ACKNOWLEDGMENTS

This work has been funded by Project TEC2015-69665-R (MINECO/FEDER, UE).

REFERENCES

Abbott, A.A., C.S. Calude, J. Conder, and K. Svozil (2012), "Strong Kochen-Specker theorem and incomputability of

- quantum randomness,” *Physical Review A* **86** (6), 062109.
- Abbott, A.A., C.S. Calude, and K. Svozil (2014), “A quantum random number generator certified by value indefiniteness,” *Mathematical Structures in Computer Science* **24** (03), e240303.
- Abellán, C., W. Amaya, M. Jofre, M. Curty, A. Acín, J. Capmany, V. Pruneri, and M.W. Mitchell (2014), “Ultrafast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode,” *Optics Express* **22** (2), 1645..
- Acín, A., N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani (2007), “Device-independent security of quantum cryptography against collective attacks,” *Physical Review Letters* **98** (23), 1–4..
- Ahmad, D. (2008), “Two Years of Broken Crypto: Debian’s Dress Rehearsal for a Global PKI Compromise,” *IEEE Security Privacy Magazine* **6** (5), 70–73.
- Alkassar, A., T. Nicolay, and M. Rohe (2005), “Obtaining true-random binary numbers from a weak radioactive source,” *Computational Science and Its Applications - Icscs 2005*, Pt 2 **3480**, 634–646.
- Alley, C.O., O.G. Jakubowicz, and W.C. Wickes (1984), “Results of the delayed-random-choice quantum mechanics experiment with light quanta,” in *Proceedings of the 2nd International Symposium on Foundations of Quantum Mechanics, Tokyo*, pp. 158–164.
- Alon, N., and J.H. Spencer (2016), *The Probabilistic Method*, 4th ed., Wiley Series in Discrete Mathematics and Optimization (Wiley).
- American National Standards Institute, (1985), *ANSI X9.17-Financial Institution Key Management (Wholesale) standard*, Tech. Rep.
- American National Standards Institute, (2006), *ANSI X9.82 (Parts 1 to 4)- Random Number Generation*, Tech. Rep.
- Andreev, A.E., A.E.F. Clementi, J.D.P. Rolim, and L. Trevisan (1999), “Weak random sources, hitting sets, and BPP simulations,” *SIAM Journal on Computing* **28** (6), 2103–2116.
- ANU, (2016), <https://qrng.anu.edu.au/> “ANU Quantum Random Numbers Server,” Australian National University.
- Argyris, A., E. Pikasis, S. Deligiannidis, and D. Syvridis (2012), “Sub-Tb/s Physical Random Bit Generators Based on Direct Detection of Amplified Spontaneous Emission Signals,” *Journal of Lightwave Technology* **30** (9), 1329–1334.
- Arnon-Friedman, R., and A. Ta-Shma (2012), “Limits of privacy amplification against nonsignalling memory attacks,” *Physical Review A* **86**, 062333.
- Asobe, M., T. Kanamori, K. Naganuma, H. Itoh, and T. Kaino (1995), “Third-order nonlinear spectroscopy in As₂S₃ chalcogenide glass fibers,” *Journal of Applied Physics* **77** (11), 5518–5523.
- Aspect, A., P. Grangier, and G. R. (1982), “Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment : A New Violation of Bell’s Inequalities,” *Physical Review Letters* **49** (2), 91–94.
- Austrin, P., K.-M. Chung, M. Mahmoody, R. Pass, and K. Seth (2014), “On the impossibility of cryptography with tamperable randomness,” in *Advances in Cryptology – CRYPTO 2014, Part I*, (Springer, Berlin, Heidelberg) pp. 462–479.
- Bancal, J.-D., L. Sheridan, and V. Scarani (2014), “More randomness from the same data,” *New Journal of Physics* **16** (3), 033011.
- Bandyopadhyay, S., P.O. Boykin, V. Roychowdhury, and F. Vatan (2002), “A New Proof for the Existence of Mutually Unbiased Bases,” *Algorithmica* **34** (4), 512–528.
- Barak, B., R. Canetti, J.B. Nielsen, and R. Pass (2004), “Universally composable protocols with relaxed set-up assumptions,” in *Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science, FOCS ’04* (IEEE Computer Society, Washington, DC, USA) pp. 186–195.
- Barak, B., R. Impagliazzo, and A. Wigderson (2006), “Extracting randomness using few independent sources,” *SIAM Journal on Computing* **36** (4), 1095–1118.
- Barak, B., R. Shaltiel, and E. Tromer (2003), “True Random Number Generators Secure in a Changing Environment,” *Cryptographic Hardware and Embedded Systems - CHES 2003* **2779**, 166–180.
- Barker, E., and A. Roginsky (2012), “Recommendation for Cryptographic Key Generation,” NIST Special publication **800-133** (March), 90.
- Barker, E., and J. Kelsey (2007), “Recommendation for random number generation using deterministic random bit generators (revised),” NIST Special publication **800-90A** (March), 90.
- Barrett, J., R. Colbeck, and A. Kent (2012), “Unconditionally secure device-independent quantum key distribution with only two devices,” *Physical Review A* **86**, 062326.
- Barrett, J., L. Hardy, and A. Kent (2005), “No signalling and quantum key distribution,” *Physical Review Letters* **95**, 010503.
- Bauke, H., and S. Mertens (2007), “Random numbers for large-scale distributed Monte Carlo simulations,” *Physical Review E* **75**, 1–14.
- Beausoleil, R.G., W.J. Munro, and T.P. Spiller (2008), “Self-authenticating quantum random number generator,” Patent US 7428562 B2.
- Becker, G.T., F. Regazzoni, C. Paar, and W.P. Burleson (2014), “Stealthy dopant-level hardware Trojans: Extended version,” *Journal of Cryptographic Engineering* **4** (1), 19–31.
- Bell, J.S. (1964), “On th Einstein-Podolsky-Rosen paradox,” *Physics*, no. 1, 1968 **1**, 195.
- Belsley, M., D.T. Smithey, K. Wedding, and M.G. Raymer (1993), “Observation of extreme sensitivity to induced molecular coherence in stimulated Raman scattering,” *Physical Review A* **48** (2), 1514–1525.
- Ben-Aroya, A., and A. Ta-Shma (2012), “Better short-seed quantum-proof extractors,” *Theoretical Computer Science* **419**, 17 – 25.
- Bennett, C.H., and G. Brassard (1984), “Quantum cryptography: Public key distribution and coin tossing,” *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India*, 175.
- Bennett, C.H., G. Brassard, C. Crepeau, and U. M. Maurer (1995), “Generalized privacy amplification,” *IEEE Transactions on Information Theory* **41** (6), 1915–1923.
- Bennett, C.H., G. Brassard, and J.-M. Robert (1988), “Privacy amplification by public discussion,” *SIAM Journal on Computing* **17** (2), 210–229.
- Bernstein, D.J., Y.A. Chang, C.M. Cheng, L.P. Chou, N. Heninger, T. Lange, and N. van Someren (2013), “Factoring RSA keys from certified smart cards: Coppersmith in the wild,” *Lecture Notes in Computer Science* **8270 LNCS** (PART 2), 341–360.
- Bernstein, D.J., T. Lange, and R. Niederhagen (2015), “Dual

- EC: A Standardized Back Door,” IACR Cryptology ePrint Archive, eprint-2015-26238 **2015**, 767.
- Berta, M., O. Fawzi, and S. Wehner (2014), “Quantum to classical randomness extractors,” *IEEE Transactions on Information Theory* **60** (2), 1168–1192.
- Bisadi, Z., M. Mancinelli, S. Manna, S. Tondini, M. Bernard, A. Samusenko, M. Ghulinyan, G. Fontana, P. Bettotti, F. Ramiro-Manzano, G. Pucker, and L. Pavesi (2015a), “Silicon nanocrystals for nonlinear optics and secure communications,” *physica status solidi (a)* **212** (12), 2659–2671.
- Bisadi, Z., A. Meneghetti, G. Fontana, G. Pucker, P. Bettotti, and L. Pavesi (2015b), “Quantum random number generator based on silicon nanocrystals LED,” in *Proc. SPIE*, Vol. 9520, edited by Jean-Marc Fédéli, p. 952004.
- Bloom, B.J., T.L. Nicholson, J.R. W.s, S.L. Campbell, M. Bishof, X. Zhang, W. Zhang, S.L. Bromley, and J. Ye (2014), “An optical lattice clock with accuracy and stability at the 10^{-18} level.” *Nature* **506** (7486), 71–75.
- Blum, M. (1986), “Independent unbiased coin flips from a correlated biased source—a finite state Markov chain,” *Combinatorica* **6** (2), 97–108.
- Blum, L., M. Blum, and M. Shub (1986), “A Simple Unpredictable Pseudo-Random Number Generator,” *SIAM Journal on Computing* **15** (2), 364–383.
- Blum, M., and S. Micali (1984), “How to Generate Cryptographically Strong Sequences of Pseudorandom Bits,” *SIAM Journal on Computing* **13** (4), 850–864.
- Bose, R.C., and D.K. Ray-Chaudhuri (1960), “On a class of error correcting binary group codes,” *Information and Control* **3** (1), 68–79.
- Bouda, J., M. Pawłowski, M. Pivoluska, and M. Plesch (2014), “Device-independent randomness extraction from an arbitrarily weak min-entropy source,” *Physical Review A* **90**, 032313.
- Bouda, J., M. Pivoluska, M. Plesch, and C. Wilmott (2012), “Weak randomness seriously limits the security of quantum key distribution,” *Physical Review A* **86** (6), 062308.
- Bourgain, J. (2005), “More on the sum-product phenomenon in prime fields and its applications,” *International Journal of Number Theory* **01** (01), 1–32.
- Bourgain, J. (2007), “On the construction of affine extractors,” *GAFA Geometric And Functional Analysis* **17** (1), 33–57.
- Bowles, J., M.T. Quintino, and N. Brunner (2014), “Certifying the dimension of classical and quantum systems in a prepare-and-measure scenario with independent devices,” *Physical review letters* **112** (14), 140407..
- Boyd, R.W. (2008), “Chapter 9 - Stimulated Brillouin and Stimulated Rayleigh Scattering,” in *Nonlinear Optics*, third ed. (Academic Press, Burlington) pp. 429–471.
- Brandão, F.G.S.L., R. Ramanathan, A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, T. Szarek, and H. Wojewódka (2016), “Realistic noise-tolerant randomness amplification using finite number of devices,” *Nature communications* **7**, 11345.
- Bratley, P., B.L. Fox, and L.E. Schrage (1987), “A Guide to Simulation,” (Springer-Verlag, New York).
- Bronner, P., A. Strunz, C. Silberhorn, and J.-P. Meyn (2009), “Demonstrating quantum random with single photons,” *European Journal of Physics* **30** (5), 1189–1200.
- Brown, R.G. (2016), “Dieharder: A random number test suite” <https://www.phy.duke.edu/~rgb/General/dieharder.php>.
- Brunner, N., D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner (2014), “Bell nonlocality,” *Reviews of Modern Physics* **86** (2), 419–478.
- Bucci, M., and R. Luzzi (2005), “Design of Testable Random Bit Generators,” *Cryptographic Hardware and Embedded Systems* **3659**, 147–156.
- Buller, G.S., and R.J. Collins (2009), “Single-photon generation and detection,” *Measurement Science and Technology* **21** (1), 012002.
- Burri, S., D. Stucki, Y. Maruyama, C. Bruschini, E. Charbon, and F. Regazzoni (2014), “SPADs for quantum random number generators and beyond,” in *Design Automation Conference (ASP-DAC), 2014 19th Asia and South Pacific* (IEEE) pp. 788–794.
- Burri, S., and D. Stucki (2013), “Jailbreak imagers: Transforming a single-photon image sensor into a true random number generator,” in *Image Sensor*, EPFL-CONF-191217, pp. 5–8.
- Bussey, P.J. (1982), ““Super-luminal communication” in Einstein-Podolsky-Rosen experiments,” *Physics Letters A* **90** (1-2), 9–12.
- Bustard, P.J., D.G. England, J. Nunn, D. Moffatt, M. Spanner, R. Lausten, and B.J. Sussman (2013), “Quantum random bit generation using energy fluctuations in stimulated Raman scattering,” *Optics Express* **21** (24), 29350.
- Bustard, P.J., D. Moffatt, R. Lausten, G. Wu, I.A. Walmsley, and B.J. Sussman (2011), “Quantum random bit generation using stimulated Raman scattering,” *Optics Express* **19** (25), 25173–25180.
- Cachin, C. (1997), “Entropy Measures and Unconditional Security in Cryptography,” PhD Thesis, ETH Zürich, <http://dx.doi.org/10.3929/ethz-a-001806220>.
- Calude, C.S. (2015), “Indeterminism and Randomness”, CDMTCS Research Reports CDMTCS-485 <http://hdl.handle.net/2292/27854>.
- Calude, C.S., and K. Svozil (2008), “Quantum Randomness and Value Indefiniteness,” *Advanced Science Letters* **1** (2), 165–168.
- Canetti, R. (2001), “Universally composable security: A new paradigm for cryptographic protocols,” in *Proceedings of the 42Nd IEEE Symposium on Foundations of Computer Science*, FOCS ’01 (IEEE Computer Society, Washington, DC, USA) p. 136. Updated version available at <https://eprint.iacr.org/2000/067.pdf>.
- Cañas, G., J. Carriñe, E.S. Gómez, J.F. Barra, A. Cabello, G.B. Xavier, G. Lima, and M. Pawłowski (2014), “Experimental quantum randomness generation invulnerable to the detection loophole,” *arXiv:1410.3443*.
- Cao, Z., H. Zhou, X. Yuan, and X. Ma (2016), “Source-independent quantum random number generation,” *Physical Review X* **6**, 011020.
- Carter, J.L., and M.N. Wegman (1979), “Universal classes of hash functions,” *Journal of Computer and System Sciences* **18** (2), 143 – 154.
- Checkoway, S., M. Fredrikson, W. Madison, and R. Niederhagen (2014), “On the Practical Exploitability of Dual EC in TLS Implementations,” *USENIX Security* 2014.
- Childs, A.M., and W. van Dam (2010), “Quantum algorithms for algebraic problems,” *Reviews of Modern Physics* **82** (1), 1–52.
- Chor, B., and O. Goldreich (1988), “Unbiased bits from sources of weak randomness and probabilistic communication complexity,” *SIAM Journal on Computing* **17** (2), 230–261.

- Christensen, B.G., K.T. McCusker, J.B. Altepeter, B. Calkins, T. Gerrits, A.E. Lita, A.J. Miller, L.K. Shalm, Y. Zhang, S.W. Nam, N. Brunner, C.C.W. Lim, N. Gisin, and P.G. Kwiat (2013), “Detection-Loophole-Free Test of Quantum Nonlocality, and Applications,” *Physical Review Letters* **111** (13), 130406.
- Chung, K.-M., Y. Shi, and X. Wu (2014), “Physical Randomness Extractors: Generating Random Numbers with Minimal Assumptions,” arXiv:1402.4797v3.
- Clauser, J.F., M.A. Horne, A. Shimony, and R.A. Holt (1969), “Proposed Experiment to Test Local Hidden-Variable Theories,” *Physical Review Letters* **23** (15), 880–884.
- Coddington, P.D. (1994), “Analysis of random number generators using Monte Carlos simulation,” *International Journal of Modern Physics C* **05** (03), 547–560.
- Coddington, P.D. (1996), “Tests of random number generators using Ising model simulations,” *International Journal of Modern Physics C* **7**, 295–303.
- Colbeck, R. (2007), “Quantum And Relativistic Protocols For Secure Multi-Party Computation,” PhD Thesis, arXiv:0911.3814.
- Colbeck, R., and A. Kent (2011), “Private randomness expansion with untrusted devices,” *Journal of Physics A* **44** (9), 95305.
- Colbeck, R., and R. Renner (2012), “Free randomness can be amplified,” *Nature Physics* **8** (6), 450–453.
- Collett, M.J., R. Loudon, and C.W. Gardiner (1987), “Quantum Theory of Optical Homodyne and Heterodyne Detection,” *Journal of Modern Optics* **34** (6), 881–902.
- Collins, M.J., A.S. Clark, C. Xiong, E. Mägi, M.J. Steel, and B.J. Eggleton (2015), “Random number generation from spontaneous Raman scattering,” *Applied Physics Letters* **107** (14), 141112.
- Collins, M.J., A.C. Judge, A.S. Clark, S. Shahnia, E.C. Magi, M.J. Steel, C. Xiong, and B.J. Eggleton (2012), “Broadband photon-counting Raman spectroscopy in short optical waveguides,” *Applied Physics Letters* **101** (21), 211110.
- Collins, M.J., A. Clark, Z. Yan, C. Xiong, M.J. Steel, and B.J. Eggleton (2014), “Quantum Random Number Generation using Spontaneous Raman Scattering,” in *CLEO: 2014* (OSA, Washington, D.C.) p. JTh2A.123.
- Colthup, N.B., L.H. Daly, and S.E. Wiberley, (1990), *Introduction to Infrared and Raman Spectroscopy*, Third Ed. (Elsevier, San Diego).
- ComScire, (2014), https://comscire.com/files/whitepaper/Pure_Quantum_White_Paper.pdf, “Entropy Analysis and System Design for Quantum Random Number Generators in CMOS Integrated Circuits”.
- Coudron, M., and H. Yuen (2014), “Infinite Randomness Expansion with a Constant Number of Devices,” in *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, STOC ’14 (ACM, New York, NY, USA) pp. 427–436.
- Courtois, N.T., D. Hulme, K. Hussain, J.A. Gawinecki, and M. Grajek (2013), “On Bad Randomness and Cloning of Contactless Payment and Building Smart Cards,” 2013 IEEE Security and Privacy Workshops (242497), 105–110.
- Common Vulnerabilities and Exposures, (2015), <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7755>, “Vulnerability report CVE-2015-7755”.
- Cryptography Research Inc., (2003), *Evaluation of VIA C3 Nehemiah Random Number Generator*, Tech. Rep. Available at <https://www.rambus.com/via-technologies-random-number-generator/>
- De, A., C. Portmann, T. Vidick, and R. Renner (2012), “Trevisan’s Extractor in the Presence of Quantum Side Information,” *SIAM Journal on Computing* **41** (4), 915–940.
- De, A., and T. Vidick (2010), “Near-optimal extractors against quantum storage,” in *Proceedings of the Forty-second ACM Symposium on Theory of Computing*, STOC ’10 (ACM, New York, NY, USA) pp. 161–170.
- Deng, D.-L., C. Zu, X.-Y. Chang, P.-Y. Hou, H.-X. Yang, Y.-X. Wang, and L.-M. Duan (2013), “Exploring Quantum Contextuality to Generate True Random Numbers,” arXiv:1301.5364.
- Deng, D.-L., and L.-M. Duan (2013), “Fault-tolerant quantum random-number generator certified by Majorana fermions,” *Physical Review A* **88** (1), 12323.
- Deutsch, D., A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera (1996), “Quantum privacy amplification and the security of quantum cryptography over noisy channels,” *Physical Review Letters* **77**, 2818–2821.
- Dieks, D. (1982), “Communication by EPR devices,” *Physics Letters A* **92** (6), 271–272.
- Dodis, Y., A. Elbaz, R. Oliveira, and R. Raz (2004), “Improved randomness extraction from two independent sources,” in *Proceedings RANDOM 2004*, pp. 334–344.
- Dodis, Y., S. J. Ong, M. Prabhakaran, and A. Sahai (2004), “On the (im)possibility of cryptography with imperfect randomness,” in *Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science, 2004*, pp. 196–205.
- Dodis, Y., D. Pointcheval, S. Ruhault, D. Vergnaud, and D. Wichs (2013), “Security analysis of pseudo-random number generators with input: /dev/random is not robust,” 2013 ACM SIGSAC Conference on Computer and Communications Security, CCS’13, Berlin, Germany, November 4–8, 2013, 647–658.
- Dodis, Y., and J. Spencer (2002), “On the (non)universality of the one-time pad,” in *Foundations of Computer Science, 2002*, pp. 376–385.
- Dorrendorf, L., Z. Gutterman, and B. Pinkas (2009), “Cryptanalysis of the random number generator of the Windows operating system,” *ACM Transactions on Information and System Security* **13** (1), 1–32.
- Duggirala, R., A. Lal, and S. Radhakrishnan (2010), “Radioisotope Decay Rate Based Counting Clock,” in *MEMS Reference shelf 6* (Springer-Verlag, New York) pp. 127–170.
- Dultz, W., G. Dultz, E. Hildebrandt, and H. Schmitzer (inventors), and Deutsche Telekom Ag (assignee) (2002), “Method for generating a random number on a quantum-mechanics basis and random generator,” Patents EP 1029394 B1 and WO 1999/066641 A1.
- Dultz, W., and E. Hildebrandt (inventors), and Deutsche Telekom Ag (assignee) (2002), “Optical random-number generator based on single-photon statistics at the optical beam splitter,” Patents US 6393448 B1 and EP 0940010 B1.
- Durt, T., B.-G. Englert, I. Bengtsson, and K. Życzkowski (2010), “On mutually unbiased bases,” *International Journal of Quantum Information* **08** (04), 535–640.
- Dvir, Z. (2012), “Extractors for varieties,” *computational complexity* **21** (4), 515–572.
- Dynes, J.F., Z.L. Yuan, A.W. Sharpe, and A.J. Shields (2008), “A high speed, postprocessing free, quantum random number generator,” *Applied Physics Letters* **93** (3), 031109.

- Eagle, A. (2005), “Randomness is unpredictability,” *The British Journal for the Philosophy of Science* **56** (4), 749–790.
- Einstein, A. (1948), “Quanten-Mechanik und Wirklichkeit,” *Dialectica* **2** (3-4), 320–324.
- Einstein, A., B. Podolsky, and N. Rosen (1935), “Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?” *Physical Review* **47** (10), 777–780.
- Eisaman, M.D., J. Fan, A.L. Migdall, and S.V. Polyakov (2011), “Single-photon sources and detectors,” *Review of Scientific Instruments* **82** (7), 071101.
- Ekert, A.K. (1991), “Quantum cryptography based on Bell’s theorem,” *Physical Review Letters* **67** (6), 661–663.
- Ekert, A.K., and R. Jozsa (1996), “Quantum computation and Shor’s factoring algorithm,” *Reviews of Modern Physics* **68** (3), 733–753.
- Elias, P. (1972), “The efficient construction of an unbiased random sequence,” *The Annals of Mathematical Statistics* **43** (3), 865–870.
- England, D.G., P.J. Bustard, D.J. Moffatt, J. Nunn, R. Lausten, and B.J. Sussman (2014), “Efficient Raman generation in a waveguide: A route to ultrafast quantum random number generation,” *Applied Physics Letters* **104** (5), 051117.
- Fain, B. (1982), “Spontaneous emission vs. vacuum fluctuations,” *Il Nuovo Cimento B* **68** (1), 73–78.
- Fearn, H., and R. Loudon (1987), “Quantum theory of the lossless beam splitter,” *Optics Communications* **64** (6), 485–490.
- Fehr, S., R. Gelles, and C. Schaffner (2013), “Security and composability of randomness expansion from Bell inequalities,” *Physical Review A* **87**, 012335.
- Ferguson, N., B. Schneier, and T. Kohno (2010), “Generating Randomness,” in *Cryptography Engineering : Design Principles and Practical Applications* (Wiley Publishing, Inc., Indianapolis) pp. 137–161.
- Ferrenberg, A.M., D.P. Landau, and Y.J. Wong (1992), “Monte Carlo simulations: Hidden errors from “good” random number generators,” *Physical Review Letters* **69** (23), 3382–3384.
- Fiorentino, M. (2006), “A quantum random bit generator for secure communication,” *SPIE Newsroom* **3**, 1–2.
- Fiorentino, M., W.J. Munro, C.M. Santori, S.M. Spillane, and R. G. Beausoleil (2006), “All-fiber-optic quantum random number generator,” in *2006 Conference on Lasers and Electro-Optics and 2006 Quantum Electronics and Laser Science Conference* (IEEE) pp. 1–2.
- Fiorentino, M., C.M. Santori, S.M. Spillane, R.G. Beausoleil, and W.J. Munro (2007), “Secure self-calibrating quantum random-bit generator,” *Physical Review A* **75** (3), 032334.
- Fischer, V. (2012), “A closer look at security in random number generators design,” *Lecture Notes in Computer Science* **7275 LNCS**, 167–182.
- Fishman, G.S. (1978), *Principles of Discrete Event Simulation* (J. Wiley & Sons, Inc., New York, NY, USA).
- Friedman, H. (1949), “Geiger Counter Tubes,” *Proceedings of the IRE* **37** (7), 791–808.
- Frauchiger, D., R. Renner, and M. Troyer (2013), “True randomness from realistic quantum devices,” arXiv:1311.4547.
- Fürst, M., H. Weier, S. Nauwerth, D.G. Marangon, C. Kurt-siefer, and H. Weinfurter (2010), “High speed optical quantum random number generation,” *Optics Express* **18** (12), 13029–13037.
- Gabizon, A., and R. Raz (2005), “Deterministic extractors for affine sources over large fields,” in *46th Annual IEEE Symposium on Foundations of Computer Science (FOCS’05)*, pp. 407–416.
- Gabizon, A., R. Raz, and R. Shaltiel (2006), “Deterministic extractors for bit-fixing sources by obtaining an independent seed,” *SIAM Journal on Computing* **36** (4), 1072–1094.
- Gabriel, C., C. Wittmann, D. Sych, R. Dong, W. Mauerner, U.L. Andersen, C. Marquardt, and G. Leuchs (2010), “A generator for unique quantum random numbers based on vacuum states,” *Nature Photonics* **4** (October), 711–715.
- Gallego, R., L. Masanes, G. de la Torre, C. Dhara, L. Aolita, and A. Acín (2013), “Full randomness from arbitrarily deterministic events,” *Nature Communications* **4**, 2654.
- Gea-Banacloche, J., M.O. Scully, and M.S. Zubairy (1988), “Vacuum Fluctuations and Spontaneous Emission in Quantum Optics,” *Physica Scripta* **T21**, 81–85.
- Gennaro, R. (2006), “Randomness in cryptography,” *IEEE Security and Privacy* **4** (2), 64–67.
- Gentle, J.E. (2009), *Computational Statistics*, 1st ed. (Springer Publishing Company, New York).
- Gerhardt, I., Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurt-siefer, and V. Makarov (2011), “Full-field implementation of a perfect eavesdropper on a quantum cryptography system,” *Nature Communications* **2** (2027), 349.
- Ghioni, M., A. Gulinatti, I. Rech, F. Zappa, and S.D. Cova (2007), “Progress in Silicon Single-Photon Avalanche Diodes,” *IEEE Journal of Selected Topics in Quantum Electronics* **13** (4), 852–862.
- Ginzburg, V.L. (1983), “The nature of spontaneous radiation,” *Soviet Physics Uspekhi* **26** (8), 713–719.
- Gisin, N., and H. Zbinden (1999), “Bell inequality and the locality loophole: Active versus passive switches,” *Physics Letters A* **264** (2-3), 103–107.
- Gisin, N., G. Ribordy, W. Tittel, and H. Zbinden (2002), “Quantum cryptography,” *Reviews of Modern Physics* **74** (1), 145–195.
- Giustina, M., A. Mech, S. Ramelow, B. Wittmann, J. Kofler, J. Beyer, A.E. Lita, B. Calkins, T. Gerrits, S.W. Nam, R. Ursin, and A. Zeilinger (2013), “Bell violation using entangled photons without the fair-sampling assumption,” *Nature* **497** (7448), 227–230.
- 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 (2015), “Significant-Loophole-Free Test of Bell’s Theorem with Entangled Photons,” *Physical Review Letters* **115** (25), 1–7.
- Goldberg, I., and D. Wagner (1996), “Randomness and the Netscape Browser,” *Dr. Dobbs’s Journal* **January**, 66–70.
- Goldreich, O. (1999), *Modern Cryptography, Probabilistic Proofs and Pseudorandomness*, Algorithms and Combinatorics, Vol. 17 (Springer-Verlag, Berlin, Heidelberg).
- Goldreich, O., and A. Wigderson (2002), “Derandomization that is rarely wrong from short advice that is typically good,” in *Proceedings of RANDOM 2002* (Springer, Berlin, Heidelberg) pp. 209–223.
- Goodyear Aircraft Corporation, (1954), “Random Noise Generator for Simulation Studies,” Report GER-6436 , 791–808.
- Gräfe, M., R. Heilmann, A. Perez-Leija, R. Keil, F.

- Dreisow, M. Heinrich, H. Moya-Cessa, S. Nolte, D.N. Christodoulides, and A. Szameit (2014), “On-chip generation of high-order single-photon W-states,” *Nature Photonics* **8** (10), 791–795.
- Grassberger, P. (1993), “On correlations in “good” random number generators,” *Physics Letters A* **Vol. 181** (No. 1), 43–46.
- Gude, M. (1985), “Concept for a High Performance Random Number Generator Based on Physical Random Phenomena,” *Frequenz* **39** (7–8).
- Guedes, E.B., F.M. de Assis, and B. Lula (2013), “Quantum attacks on pseudorandom generators,” *Mathematical Structures in Computer Science* **23** (3), 608–634.
- Guo, H., W. Tang, Y. Liu, and W. Wei (2010), “Truly random number generation based on measurement of phase noise of a laser,” *Physical Review E* **81** (5), 051137.
- Gupta, M.S. (1975), “Applications of electrical noise,” *Proceedings of the IEEE* **63** (7), 996–1010.
- Guterman, Z., B. Pinkas, and T. Reinman (2006), “Analysis of the Linux Random Number Generator,” 2006 IEEE Symposium on Security and Privacy (S&P’06), 370–385.
- Hadfield, R.H. (2009), “Single-photon detectors for optical quantum information applications,” *Nature Photonics* **3** (12), 696–705.
- Hales, T.C. (2014), “The NSA Back Door to NIST,” *Notices of the American Mathematical Society* **61** (02), 1.
- Hall, M.J.W. (2010), “Local deterministic model of singlet state correlations based on relaxing measurement independence,” *Physical Review Letters* **105**, 250404 (see also erratum: PRL 116, 219902, 2016).
- Hamburg, M., P. Kocher, and M.E. Marson (2012), “Analysis of Intel’s Ivy Bridge digital random number generator,” white paper by Cryptography Research Inc., available at <https://www.rambus.com/intel-ivy-bridge-random-number-generator/>.
- Harris, S.E., M.K. Oshman, and R.L. Byer (1967), “Observation of Tunable Optical Parametric Fluorescence,” *Physical Review Letters* **18** (18), 732–734.
- Håstad, J., R. Impagliazzo, L. A. Levin, and M. Luby (1999), “A pseudorandom generator from any one-way function,” *SIAM Journal on Computing* **28** (4), 1364–1396.
- Haw, J.Y., S.M. Assad, A.M. Lance, N.H.Y. Ng, V. Sharma, P.K. Lam, and T. Symul (2015), “Maximization of Extractable Randomness in a Quantum Random-Number Generator,” **054004**, 1–12.
- Hayes, B. (2001), “Randomness as a resource,” *American Scientist* **89** (4), 300–304.
- Heninger, N., Z. Durumeric, E. Wustrow, and J.A. Halderman (2012), “Mining your Ps and Qs: detection of widespread weak keys in network devices,” *Proceedings of the 21st USENIX Security Symposium*, 35.
- Henry, C. (1982), “Theory of the linewidth of semiconductor lasers,” *IEEE Journal of Quantum Electronics* **18** (2), 259–264.
- Henry, C., and R.F. Kazarinov (1996), “Quantum noise in photonics,” *Reviews of Modern Physics* **68** (3), 801–853.
- Hensen, B., H. Bernien, A.E. Dreau, A. Reiserer, N. Kalb, M.S. Blok, J. Ruitenber, R.F.L. Vermeulen, R.N. Schouten, C. Abellan, W. Amaya, V. Pruneri, M.W. Mitchell, M. Markham, D.J. Twitchen, D. Elkouss, S. Wehner, T.H. Taminiau, and R. Hanson (2015), “Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres,” *Nature* **526** (7575), 682–686.
- Hirano, K., T. Yamazaki, S. Morikatsu, H. Okumura, H. Aida, A. Uchida, S. Yoshimori, K. Yoshimura, T. Harayama, and P. Davis (2010), “Fast random bit generation with bandwidth-enhanced chaos in semiconductor lasers,” *Optics Express* **18** (6), 5512.
- Holman, W.T., J.A. Connelly, and A.B. Dowlatabadi (1997), “An integrated analog/digital random noise source,” *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications* **44** (6), 521–528.
- Hongo, K., R. Maezono, and K. Miura (2010), “Random number generators tested on quantum Monte Carlo simulations,” *Journal of Computational Chemistry* **31** (11), 2186–2194.
- Hoogland, A., A. Compagner, and H.W.J. Blöte (1985), “Smooth finite-size behaviour of the three-dimensional Ising model,” *Physica A* **132** (2–3), 593–596.
- Hörmann, W., J. Leydold, and G. Derflinger (2004), *Automatic Nonuniform Random Variate Generation*, Statistics and Computing No. 1 (Springer, Berlin, Heidelberg).
- Hotoleanu, D., O. Cret, A. Suci, T. Györfi, and L. Vacariu (2010), “Real-Time Testing of True Random Number Generators Through Dynamic Reconfiguration,” 2010 13th Euromicro Conference on Digital System Design: Architectures, Methods and Tools, 247–250.
- Howe, R.M. (1961), *Design fundamentals of analog computer components* (Van Nostrand, Princeton, New Jersey).
- Hübner, J., F. Berski, R. Dahbashi, and M. Oestreich (2014), “The rise of spin noise spectroscopy in semiconductors: From acoustic to GHz frequencies,” *Physica Status Solidi B* **251** (9), 1824–1838.
- Hughes, R., and J. Nordholt (2016), “Strengthening the Security Foundation of Cryptography With Whitewood’s Quantum-Powered Entropy Engine,” Retrieved from <http://www.whitewoodencryption.com>.
- Hull, T.E., and A.R. Dobell (1962), “Random Number Generators,” *SIAM Review* **4** (3), 230–254.
- Humboldt-Universität, (2016), <https://qrng.physik.hu-berlin.de/> “High Bit Rate Quantum Random Number Generator Service.”
- ID Quantique, (2011), *User Case White Paper, Loterie Romande*, Tech. Rep. retrieved from <http://www.idquantique.com>
- ID Quantique, (2014), <http://www.idquantique.com/random-number-generation> “QUANTIS random number generator”.
- Impagliazzo, R., L. A. Levin, and M. Luby (1989), “Pseudorandom generation from one-way functions,” in *Proceedings of the Twenty-first Annual ACM Symposium on Theory of Computing*, STOC ’89 (ACM, New York, NY, USA) pp. 12–24.
- Isida, M., and H. Ikeda (1956), “Random number generator,” *Annals of the Institute of Statistical Mathematics* **8** (2), 119–126.
- Islam, M.N. (2002), “Raman amplifiers for telecommunications,” *IEEE Journal of Selected Topics in Quantum Electronics* **8** (3), 548–559.
- Jacques, V., E. Wu, F. Grosshans, F. Treussart, P. Grangier, A. Aspect, and J.-F. Roch (2007), “Experimental Realization of Wheeler’s Delayed-Choice Gedanken Experiment,” *Science* **315** (5814), 966–968.
- International Organization for Standardization, (2011), *Random bit generation*, ISO/IEC 18031.
- Jacques, V., E. Wu, F. Grosshans, F. Treussart, P. Grangier, A. Aspect, and J.-F. Roch (2008), “Delayed-Choice Test of Quantum Complementarity with Interfering Single

- Photons,” *Physical Review Letters* **100** (22), 220402.
- Jalali, B., V. Raghunathan, D. Dimitropoulos, and O. Boyraz (2006), “Raman-based silicon photonics,” *IEEE Journal of Selected Topics in Quantum Electronics* **12** (3), 412–421.
- James, D.F.V., P.G. Kwiat, W.J. Munro, and A.G. White (2001), “Measurement of qubits,” *Physical Review A* **64**, 052312.
- Jennewein, T., U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger (2000), “A Fast and Compact Quantum Random Number Generator,” *Review of Scientific Instruments* **71** (4), 1675–1680.
- Jian, Y., M. Ren, E. Wu, G. Wu, and H. Zeng (2011), “Two-bit quantum random number generator based on photon-number-resolving detection,” *Review of Scientific Instruments* **82** (7), 073109.
- Jofre, M., M. Curty, F. Steinlechner, G. Anzolin, J.P. Torres, M.W. Mitchell, and V. Pruneri (2011), “True random numbers from amplified quantum vacuum,” *Optics Express* **19** (21), 20665–20672.
- Johnson, J.B. (1928), “Thermal agitation of electricity in conductors,” *Physical Review* **32**, 97.
- Jordan, T.F. (1983), “Quantum correlations do not transmit signals,” *Physics Letters A* **94** (6-7), 264.
- Kalle, C., and S. Wansleben (1984), “Problems with the random number generator RANF implemented on the CDC Cyber 205,” *Computer Physics Communications* **33** (4), 343–346.
- Kamp, J., and D. Zuckerman (2007), “Deterministic extractors for bit-fixing sources and exposure-resilient cryptography,” *SIAM Journal on Computing* **36** (5), 1231–1247.
- Kanter, I., Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh (2010), “An optical ultrafast random bit generator,” *Nature Photonics* **4** (1), 58–61.
- Karp, R.M. (1991), “An introduction to randomized algorithms,” *Discrete Applied Mathematics* **34** (1-3), 165–201.
- Katsoprinakis, G.E., A.T. Dellis, and I.K. Kominis (2007), “Measurement of transverse spin-relaxation rates in a rubidium vapor by use of spin-noise spectroscopy,” *Physical Review A* **75**, 042502.
- Katsoprinakis, G.E., M. Polis, A. Tavernarakis, A.T. Dellis, and I.K. Kominis (2008), “Quantum random number generator based on spin noise,” *Physical Review A* **77** (5), 054101.
- Kelsey, J., B. Schneier, D. Wagner, and C. Hall (1998), “Cryptanalytic Attacks on Pseudorandom Number Generators,” in *Fast Software Encryption, Lecture Notes in Computer Science* **Vol. 1372**, 168–18.
- Kerckhoffs, A. (1883), “La cryptographie militaire,” *Journal des sciences militaires* **IX**, 5–83.
- Khanmohammadi, A., R. Enne, M. Hofbauer, and H. Zimmermann (2015), “A Monolithic Silicon Quantum Random Number Generator Based on Measurement of Photon Detection Time,” *IEEE Photonics Journal* **7** (5), 1–13.
- Killmann, W., and W. Schindler (2008), “A design for a physical RNG with robust entropy estimators,” in *Lecture Notes in Computer Science* **5154 LNCS**, 146–163.
- Killmann, W., and W. Schindler (2011), “A proposal for : Functionality classes for random number generators,” *AIS 20 / AIS 31 standard*, available from <https://www.bsi.bund.de>.
- Kim, S.H., D. Han, and D.H. Lee (2013), “Predictability of Android OpenSSL’s pseudo random number generator,” *Proceedings of the 2013 ACM SIGSAC conference on Computer & Communications Security - CCS ’13*, 659–668.
- Kim, H.J., and M.J. Klass (2001), “Random number generator,” Patent US 6249009 B1.
- Klass, M.J. (2003), “Random number generator,” Patent US 6539410 B1.
- Klass, M.J. (2005), “Apparatus for generating random numbers,” Patent US 6965907 B2.
- Klauder, J.R., and E.C.G. Sudarshan (1968), *Fundamentals of Quantum Optics*, The Mathematical Physics Monographs Series (Benjamin, New York).
- Klyachko, A.A., M.A. Can, S. Binicioğlu, and A.S. Shumovsky (2008), “Simple Test for Hidden Variables in Spin-1 Systems,” *Physical Review Letters* **101** (2), 020403.
- Knoll, G.F. (2010), *Radiation Detection and Measurement*, 4th ed. (John Wiley & Sons Inc).
- Knuth, D.E. (1997), *The Art of Computer Programming, Volume 2 (3rd Ed.): Seminumerical Algorithms* (Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA).
- Kobliska, R.J., and S.A. Solin (1973), “Temperature Dependence of the Raman Spectrum and the Depolarization Spectrum of Amorphous As₂S₃,” *Physical Review B* **8** (2), 756.
- Kochen, S., and E.P. Specker (1967), “The Problem of Hidden Variables in Quantum Mechanics,” *Journal of Mathematics and Mechanics* **17** (1), 59–87.
- Koh, D.E., M.J.W. Hall, Setiawan, J.E. Pope, C. Marletto, A. Kay, V. Scarani, and A. Ekert (2012), “Effects of reduced measurement independence on Bell-based randomness expansion,” *Physical Review Letters* **109**, 160404.
- Kohlbrenner, P., and K. Gaj (2004), “An Embedded True Random Number Generator for FPGAs,” in *Proceedings of the 2004 ACM/SIGDA 12th International Symposium on Field Programmable Gate Arrays, FPGA ’04* (ACM, New York, NY, USA) pp. 71–78.
- König, R., U. Maurer, and R. Renner (2005), “On the power of quantum memory,” *IEEE Transactions on Information Theory* **51** (7), 2391–2401.
- König, R., R. Renner, and C. Schaffner (2009), “The Operational Meaning of Min- and Max-Entropy,” *IEEE Transactions on Information Theory* **55** (9), 4337–4347.
- König, R., and R. Renner (2011), “Sampling of Min-Entropy Relative to Quantum Knowledge,” *IEEE Transactions on Information Theory* **57** (7), 4760–4787.
- König, R.T., and B.M. Terhal (2008), “The bounded-storage model in the presence of a quantum adversary,” *IEEE Transactions on Information Theory* **54** (2), 749–762.
- Kravtsov, K.S., I.V. Radchenko, S.P. Kulik, and S.N. Molotov (2015), “Minimalist design of a robust real-time quantum random number generator,” *Journal of the Optical Society of America B* **32** (8), 1743–1747.
- Krawczyk, H. (1990), *How to Predict Congruential Generators*, in *Advances in Cryptology, Lecture Notes in Computer Science*, **Vol. 435**, 138–153.
- Krawczyk, H. (1994), *LFSR-based hashing and authentication*, in *Advances in Cryptology, CRYPTO ’94, Lecture Notes in Computer Science*, **Vol. 839**, 129–139.
- Kuo, S.J., D.T. Smithey, and M.G. Raymer (1991), “Spatial interference of macroscopic light fields from independent Raman sources,” *Physical Review A* **43** (7), 4083–4086.
- Landauer, R. (1993), “Solid-state shot noise,” *Physical Review B* **47** (24), 16427–16432.
- Law, A.M., and D.W. Kelton (2000), *Simulation modeling and analysis*, 3rd ed., McGraw Hill Series in Industrial Engineering and Management Science (McGraw-Hill, New York, NY).
- Lax, M. (1967), “Classical Noise. V. Noise in Self-Sustained

- Oscillators,” *Physical Review* **160** (2), 290–307.
- Lecomte, S., R. Paschotta, S. Pawlik, B. Schmidt, K. Furusawa, A. Malinowski, D.J. Richardson, and U. Keller (2005), “Synchronously pumped optical parametric oscillator with a repetition rate of 81.8 GHz,” *IEEE Photonics Technology Letters* **17** (2), 483–485.
- L’Ecuyer, P., and R. Simard (2007), “A C Library for Empirical Testing of Random Number Generators,” *ACM Transactions on Mathematical Software* **33** (4), 22.
- L’Ecuyer, P. (2012), “Random Number Generation,” in *Handbook of Computational Statistics*, edited by J.E. Gentle, W.K. Härdle, and Y. Mori (Springer, Berlin, Heidelberg) pp. 35–71.
- Lehmer, D.H. (1951), “Mathematical Methods in Large-scale Computing Units,” *Annals of the Computation Laboratory of Harvard University* **26**, 141–146.
- Lenstra, A.K., J.P. Hughes, M. Augier, J.W. Bos, T. Kleinjung, and C. Wachter (2012), “Public Keys,” in *Crypto 2012, Lecture Notes in Computer Science* **Vol. 7417**, pp. 626–642.
- Li, H.-W., Z.-Q. Yin, S. Wang, Y.-J. Qian, W. Chen, G.-C. Guo, and Z.-F. Han (2015), “Randomness determines practical security of BB84 quantum key distribution,” *Scientific Reports* **5**, 16200.
- Li, H.-W., S. Wang, J.-Z. Huang, W. Chen, Z.-Q. Yin, F.-Y. Li, Z. Zhou, D. Liu, Y. Zhang, G.-C. Guo, W.-S. Bao, and Z.-F. Han (2011), “Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources,” *Physical Review A* **84**, 062308.
- Li, L., A. Wang, P. Li, H. Xu, L. Wang, and Y. Wang (2014), “Random Bit Generator Using Delayed Self-Difference of Filtered Amplified Spontaneous Emission,” *IEEE Photonics Journal* **6** (1), 1–9.
- Li, M., and P.M.B. Vitányi (2008), *An Introduction to Kolmogorov Complexity and Its Applications*, 3rd ed. (Springer, New York).
- Li, S., L. Wang, L.-A. Wu, H.-Q. Ma, and G.-J. Zhai (2013), “True random number generator based on discretized encoding of the time interval between photons,” *Journal of the Optical Society of America A* **30** (1), 124.
- Li, X., A.B. Cohen, T.E. Murphy, and R. Roy (2011), “Scalable parallel physical random number generator based on a superluminescent LED,” *Optics Letters* **36** (6), 1020.
- Lin, Q, F. Yaman, and G.P. Agrawal (2007), “Photon-pair generation in optical fibers through four-wave mixing: Role of Raman scattering and pump polarization,” *Physical Review A* **75** (2), 023803.
- Lita, A.E., A.J. Miller, and S.W. Nam (2008), “Counting near-infrared single-photons with 95% efficiency,” *Optics Express* **16** (5), 3032.
- Liu, X., R.M. Osgood, Y. Vlasov, and W.M.J. Green (2010a), “Mid-infrared optical parametric amplifier using silicon nanophotonic waveguides,” *Nature Photonics* **4** (8), 557–560.
- Liu, Y., M.-Y. Zhu, B. Luo, J.-W. Zhang, and H. Guo (2013), “Implementation of 1.6 Tb s^{-1} truly random number generation based on a super-luminescent emitting diode,” *Laser Physics Letters* **10** (4), 045001.
- Liu, Y., M. Zhu, and H. Guo (2010b), “Truly random number generation via entropy amplification,” *arXiv:1006.3512*.
- Lo, H.-K., M. Curty, and K. Tamaki (2014), “Secure quantum key distribution,” *Nature Photonics* **8** (8), 595–604.
- Lohr, S.L. (2010), *Sampling: Design and Analysis*, 2nd ed., (Duxbury Press).
- Lopes Soares, E. de J., F.A. Mendonça, and R.V. Ramos (2014), “Quantum Random Number Generator Using Only One Single-Photon Detector,” *IEEE Photonics Technology Letters* **26** (9), 851–853.
- Loudon, R. (2001), *The Quantum Theory of Light*, 3rd ed. (Oxford University Press, Oxford, UK).
- Louisell, W.H., A. Yariv, and A.E. Siegman (1961), “Quantum Fluctuations and Noise in Parametric Processes. I.” *Physical Review* **124** (6), 1646–1654.
- Lu, C.-J., O. Reingold, S. Vadhan, and A. Wigderson (2003), “Extractors: Optimal up to constant factors,” in *Proceedings of the Thirty-fifth Annual ACM Symposium on Theory of Computing*, STOC ’03 (ACM, New York, NY, USA) pp. 602–611.
- Lunghi, T., J.B. Brask, C.C.W. Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, and N. Brunner (2015), “Self-Testing Quantum Random Number Generator,” *Physical Review Letters* **114** (15), 150501.
- Lutkenhaus, N., J.L. Cohen, and H.-K. Lo (inventors), and Magiq Technologies, Inc. (assignee) (2007), “Efficient use of detectors for random number generation,” Patent US 7197523 B2.
- Lutz, G. (2007), *Semiconductor Radiation Detectors* (Springer-Verlag, Berlin, Heidelberg).
- Lydersen, L., C. Wiechers, C. Wittmann, Dominique Elser, J. Skaar, and V. Makarov (2010), “Hacking commercial quantum cryptography systems by tailored bright illumination,” *Nature Photon* **4** (686), 5.
- Lyngsø, R.B., and C.N.S. Pedersen (2002), “The consensus string problem and the complexity of comparing hidden Markov models,” *Journal of Computer and System Sciences* **65** (3), 545 – 569.
- Ma, H.-Q., Y. Xie, and L.-A. Wu (2005), “Random number generation based on the time of arrival of single photons,” *Applied Optics* **44** (36), 7760.
- Ma, X.-S., J. Kofler, A. Qarry, N. Tetik, T. Scheidl, R. Ursin, S. Ramelow, T. Herbst, L. Ratschbacher, A. Fedrizzi, T. Jennewein, and A. Zeilinger (2013a), “Quantum erasure with causally disconnected choice,” *Proceedings of the National Academy of Sciences* **110** (4), 1221–1226.
- Ma, X.-S., S. Zotter, J. Kofler, R. Ursin, T. Jennewein, Č. Brukner, and A. Zeilinger (2012), “Experimental delayed-choice entanglement swapping,” *Nature Physics* **8** (6), 480–485.
- Ma, X., F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo (2013b), “Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction,” *Physical Review A* **87** (6), 062327.
- Maddaloni, P., M. Bellini, and P. De Natale (2013), *Laser-based Measurements for Time and Frequency Domain Applications: A Handbook* (CRC Press).
- Magniez, F., D. Mayers, H. Ollivier, and M. Mosca (2006), “Self-testing of quantum circuits,” in *Automata, Languages and Programming, Lecture Notes in Computer Science* **Vol. 4051**, 72–83.
- Majorana, E. (1937), “Teoria simmetrica dell’elettrone e del positrone,” *Il Nuovo Cimento* **14** (4), 171–184.
- Manelis, B. (1961), “Generating random noise,” *Electronics* **8 Sep.**, 66–69.
- Mansour, Y., N. Nisan, and P. Tiwari (1990), “The computational complexity of universal hashing,” in *Proceedings of the Twenty-second Annual ACM Symposium on Theory of Computing*, STOC ’90 (ACM, New York, NY, USA) pp.

- 235–243.
- Marandi, A., N.C. Leindecker, V. Pervak, R.L. Byer, and K.L. Vodopyanov (2012a), “Coherence properties of a broadband femtosecond mid-IR optical parametric oscillator operating at degeneracy,” *Optics Express* **20** (7), 7255.
- Marandi, A., N.C. Leindecker, K.L. Vodopyanov, and R.L. Byer (2011), “Twin Degenerate OPO for Quantum Random Bit Generation,” in *Nonlinear Optics* (Optical Society of America), paper NME4.
- Marandi, A., N.C. Leindecker, K.L. Vodopyanov, and R.L. Byer (2012b), “All-optical quantum random bit generation from intrinsically binary phase of parametric oscillators,” *Optics Express* **20** (17), 19322–19330.
- Marsaglia, G. (1968), “Random numbers fall mainly in the planes,” *Proceedings of the National Academy of Sciences of the United States of America* **61** (1), 25–28.
- Marsaglia, G. (1996), <http://stat.fsu.edu/pub/diehard/>, “DIEHARD: a battery of tests of randomness”.
- Marsili, F., V.B. Verma, J.A. Stern, S. Harrington, A.E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M.D. Shaw, R.P. Mirin, and S.W. Nam (2013), “Detecting single infrared photons with 93% system efficiency,” *Nature Photonics* **7**.
- Martin, A., B. Sanguinetti, C.C.W. Lim, R. Houlmann, and H. Zbinden (2015), “Quantum Random Number Generation for 1.25-GHz Quantum Key Distribution Systems,” *Journal of Lightwave Technology* **33** (13), 2855–2859.
- Martino, A.J., and G.M. Morris (1991), “Optical random number generator based on photoevent locations,” *Applied optics* **30** (8), 981–9.
- Matsumoto, M., and T. Nishimura (1998), “Mersenne Twister: a 623-dimensionally equidistributed uniform pseudo-random number generator,” *ACM Transactions on Modeling and Computer Simulation* **8** (1), 3–30.
- Matsumoto, M., T. Nishimura, M. Hagita, and M. Saito (2005), “Cryptographic Mersenne Twister and Fubuki stream/block cipher,” *Cryptographic ePrint* <http://eprint.iacr.org/2005/165>.
- Matsumoto, M., Mutsuo Saito, T. Nishimura, and M. Hagita (2008), “CryptMT3 Stream Cipher,” in *New Stream Cipher Designs, Lecture Notes in Computer Science*, **Vol. 4986** (Springer, Berlin, Heidelberg) pp. 7–19.
- Matsumoto, M., I. Wada, A. Kuramoto, and H. Ashihara (2007), “Common defects in initialization of pseudorandom number generators,” *ACM Transactions on Modeling and Computer Simulation* **17** (4), article 15.
- Mátar, A., P. Skrzypczyk, J.B. Brask, D. Cavalcanti, and A. Acín (2015), “Optimal randomness generation from optical Bell experiments,” *New Journal of Physics* **17** (17), 22003.
- Maurer, W., C. Portmann, and V.B. Scholz (2012), “A modular framework for randomness extraction based on Trevisan’s construction,” *arXiv:1212.0520*.
- Maurer, U. (1992), “A Universal Statistical Test for Random Bit Generators,” *Journal of Cryptology* **5** (2), 89–105.
- Mayers, D., and A. Yao (1998), “Quantum cryptography with imperfect apparatus,” in *Proceedings of the 39th Annual Symposium on Foundations of Computer Science*, FOCS ’98 (IEEE Computer Society, Washington, DC, USA) pp. 503–509.
- McInnes, J.L., and B. Pinkas (1991), “On the impossibility of private key cryptography with weakly random keys,” in *Advances in Cryptology-CRYPTO’90*, (Springer, Berlin, Heidelberg) pp. 421–435.
- Metropolis, N., and S. Ulam (1949), “The Monte Carlo Method,” *Journal of the American Statistical Association* **44** (247), 335–341.
- Michaelis, K., C. Meyer, and J. Schwenk (2013), “Randomly Failed! The State of Randomness in Current Java Implementations,” in *Topics in Cryptology CT-RSA 2013, Lecture Notes in Computer Science*, **Vol. 7779** (Springer, Berlin, Heidelberg) pp. 129–144.
- Milchev, A., K. Binder, and D.W. Heermann (1986), “Fluctuations and lack of self-averaging in the kinetics of domain growth,” *Zeitschrift für Physik B Condensed Matter* **535**, 521–535.
- Miller, C.A., and Y. Shi (2014), “Universal security for randomness expansion,” *arXiv:1411.6608*.
- Mitchell, M.W., C. Abellán, and W. Amaya (2015), “Strong experimental guarantees in ultrafast quantum random number generation,” *Physical Review A* **91**, 012314.
- Mo, X.-F., B. Zhu, Z.-F. Han, Y.-Z. Gui, and G.-C. Guo (2005), “Faraday-Michelson system for quantum cryptography,” *Optics letters* **30** (19), 2632–2634.
- Motwani, R., and P. Raghavan (1996), “Randomized algorithms,” *ACM Computing Surveys* **28** (1), 33–37.
- Micro Photon Devices (2014), “Quantum random number generator,” <http://www.micro-photon-devices.com/Products/Instrumentation/Quantum-Random-Number>.
- Murry, H.F. (1970), “A General Approach for Generating Natural Random Variables,” *IEEE Transactions on Computers* **C-19** (12), 1210–1213.
- Nabors, C.D., S.T. Yang, T. Day, and R.L. Byer (1990), “Coherence properties of a doubly resonant monolithic optical parametric oscillator,” *Journal of the Optical Society of America B* **7** (5), 815.
- Nadj-Perge, S., I.K. Drozdov, J. Li, H. Chen, S. Jeon, J. Seo, A.H. MacDonald, B.A. Bernevig, and A. Yazdani (2014), “Observation of Majorana fermions in ferromagnetic atomic chains on a superconductor,” *Science* **346** (6209), 602–607.
- Nahin, P.J. (1999), *Time Machines* (Springer, New York).
- Naruse, M., M. Berthel, A. Drezet, S. Huant, M. Aono, H. Hori, and S.-J. Kim (2015), “Single-photon decision maker,” *Scientific Reports* **5**, 13253.
- National Institute of Standards and Technology, (2001), *Security Requirements for Cryptographic Modules*, Federal Information Processing Standards Publication FIPS PUB 140-2.
- National Institute of Standards and Technology, (2012), *FIPS PUB 180-4. Secure Hash Standard*.
- Networking Working Group, (1996), *RFC 1948. Defending Against Sequence Number Attacks*.
- Networking Working Group, (2005), *RFC 4086. Randomness Requirements for Security*.
- von Neumann, J. (1951), “Various techniques used in connection with random digits,” republished in *Collected works. Vol.5 Design of computers, theory of automata and numerical analysis* (Pergamon Press, Oxford).
- Nie, Y.-Q., L. Huang, Y. Liu, F. Payne, J. Zhang, and J.-W. Pan (2015), “The generation of 68 Gbps quantum random number by measuring laser phase fluctuations,” *Review of Scientific Instruments* **86** (6), 063105.
- Nie, Y.-Q., H.-F. Zhang, Z. Zhang, J. Wang, X. Ma, J. Zhang, and J.-W. Pan (2014), “Practical and fast quantum random number generation based on photon arrival time relative to external reference,” *Applied Physics Letters* **104** (5), 051110.
- Niederreiter, H. (1978), “Quasi-Monte Carlo methods and pseudo-random numbers,” *Bulletin of the American Math-*

- ematical Society **84** (6), 957–1041.
- Nisan, N. (1996), “Extracting randomness: how and why. A survey,” in *Proceedings of Computational Complexity* (IEEE Computer Society Press) pp. 44–58.
- Nisan, N., and A. Ta-Shma (1999), “Extracting Randomness: A Survey and New Constructions,” *Journal of Computer and System Sciences* **58** (1), 148–173.
- Nisan, N., and A. Wigderson (1994), “Hardness vs randomness,” *Journal of Computer and System Sciences* **49** (2), 149 – 167.
- Nisan, N., and D. Zuckerman (1996), “Randomness is linear in space,” *Journal of Computer and System Sciences* **52** (1), 43 – 52.
- NIST, (2011), “NIST Randomness Beacon,” http://www.nist.gov/itl/csd/ct/nist_beacon.cfm.
- Nohl, K., D. Evans, Starbug, and H. Plötz (2008), “Reverse-engineering a Cryptographic RFID Tag,” in *Proceedings of the 17th Conference on Security Symposium*, SS’08 No. July (USENIX Association, Berkeley, CA, USA) pp. 185–193.
- Nyquist, H. (1928), “Thermal Agitation of Electric Charge in Conductors,” *Physical Review* **32** (1), 110–113.
- Oberreiter, L., and I. Gerhardt (2015), “Light on a beam splitter: More randomness with single photons,” *Laser & Photonics Reviews* **8**.
- Oestreich, M., M. Römer, R.J. Haug, and D. Hägele (2005), “Spin noise spectroscopy in GaAs,” *Physical Review Letters* **95**, 216603.
- Olmschenk, S., K.C. Younge, D.L. Moehring, D.N. Matsukevich, P. Maunz, and C. Monroe (2007), “Manipulation and detection of a trapped Yb^+ hyperfine qubit,” *Physical Review A* **76** (5), 1–9.
- Ossola, G., and A.D. Sokal (2004), “Systematic errors due to linear congruential random-number generators with the Swendsen-Wang algorithm: A warning,” *Physical Review E* **70** (2), 27701.
- Ou, Z.Y., C.K. Hong, and L. Mandel (1987), “Relation between input and output states for a beam splitter,” *Optics Communications* **63** (2), 118–122.
- Owens, I.J., R.J. Hughes, and J.E. Nordholt (2008), “Entangled quantum-key-distribution randomness,” *Physical Review A* **78** (2), 022307.
- Parisi, G., and F. Rapuano (1985), “Effects of the random number generator on computer simulations,” *Physics Letters B* **157** (4), 301–302.
- Pawlowski, M., and N. Brunner (2011), “Semi-device-independent security of one-way quantum key distribution,” *Physical Review A* **84** (1), 010302.
- Peev, M., C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J.F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A.W. Sharpe, A.J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouiri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z.L. Yuan, H. Zbinden, and A. Zeilinger (2009), “The SECOQC quantum key distribution network in Vienna,” *New Journal of Physics* **11**, 1–37.
- Penzkofer, A., A. Laubereau, and W. Kaiser (1979), “High intensity Raman interactions,” *Progress in Quantum Electronics* **6** (2), 55–140.
- Peres, A. (2000), “Delayed choice for entanglement swapping,” *Journal of Modern Optics* **47** (2-3), 139–143.
- Peres, Y. (1992), “Iterating von Neumann’s Procedure for Extracting Random Bits,” *The Annals of Statistics* **20** (1), 590–597.
- Petrie, C.S., and J.A. Connelly (2000), “A noise-based IC random number generator for applications in cryptography,” *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications* **47** (5), 615–621.
- PicoQuant, (2014), “PQRNG 150 Quantum Random Number Generator,” <http://www.picoquant.com/products/category/quantum-random-number-generator/pqrng-150-quantum-random-number-generator>.
- Pierret, R.F. (1996), *Semiconductor device fundamentals*, 2nd ed. (Addison-Wesley, Reading, Massachusetts).
- Pironio, S., A. Acín, S. Massar, A. Boyer de la Giroday, D.N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T.A. Manning, and C. Monroe (2010), “Random numbers certified by Bell’s theorem,” *Nature* **464** (7291), 1021–1024.
- Pironio, S., and S. Massar (2013), “Security of practical private randomness generation,” *Physical Review A* **87**, 012336.
- Pivoluska, M., M. Plesch, M. Pivoluskaa, and M. Plesch (2014), “Device Independent Random Number Generation,” *Acta Physica Slovaca* **64** (6), 601–664.
- Platt, C., and A. Logue (2015), “Really, really random number generator,” *Make*: **45**, 78–81.
- Plesch, M., and M. Pivoluska (2014), “Device-independent randomness amplification with a single device,” *Physics Letters A* **378** (40), 2938 – 2944.
- PokerStars, (2016), *Data Privacy for our Software*, Description of the shuffling method retrieved from <https://www.pokerstars.com/poker/room/features/security/> (19th of August 2016).
- Prasad, S., M.O. Scully, and W. Marthienssen (1987), “A quantum description of the beam splitter,” *Optics Communications* **62** (3), 139–145.
- du Preez, V., M.G.B. Johnson, A. Leist, and K.A. Hawick (2011), “Performance and Quality of Random Number Generators,” in *International Conference on Foundations of Computer Science (FCS’11)*, FCS4818, pp. 16–21.
- Qi, B., Y.-M. Chi, H.-K. Lo, and L. Qian (2010), “High-speed quantum random number generation by measuring phase noise of a single-mode laser,” *Optics Letters* **35** (3), 312.
- Qiurong, Y., Z. Baosheng, L. Qinghong, and Z. Nanrun (2014), “Multi-bit quantum random number generation by measuring positions of arrival photons,” *Review of Scientific Instruments* **85** (10), 103116.
- QRB121, (2014), “QRBG121 Quantum Random Number Generator,” <http://qrbg.irb.hr>.
- Quintessence Labs, (2014), “Fast Quantum Random Number Generation,” <http://www.quintessencelabs.com/our-technology/?tab=random-number>.
- Qutools, (2014), “quRNG - Quantum Random Number Generator,” <http://www.qutools.com/products/quRNG/index.php>.
- Radhakrishnan, J., and A. Ta-Shma (2000), “Bounds for dispersers, extractors, and depth-two superconcentrators,” *SIAM Journal on Discrete Mathematics* **13** (1), 2–24.
- RAND Corporation, (1955), “A million random digits with 100,000 normal deviates,” http://www.rand.org/pubs/monograph_reports/MR1418.html.
- Rao, A. (2009), “Extractors for a constant number of poly-

- nomially small min-entropy independent sources,” *SIAM Journal on Computing* **39** (1), 168–194.
- Rarity, J.G., P.C.M. Owens, and P.R. Tapster (1994), “Quantum Random-number Generation and Key Sharing,” *Journal of Modern Optics* **41** (12), 2435–2444.
- Raymer, M.G., K. Rzačzewski, and J. Mostowski (1982), “Pulse-energy statistics in stimulated Raman scattering,” *Optics letters* **7** (2), 71–73.
- Raymer, M.G., I.A. Walmsley, J. Mostowski, and B. Sobolewska (1985), “Quantum theory of spatial and temporal coherence properties of stimulated Raman scattering,” *Physical Review A* **32** (1), 332.
- Raymer, M.G., and I.A. Walmsley (1990), “The Quantum Coherence Properties of Stimulated Raman Scattering,” in *Progress in Optics XXVIII*, edited by E. Wolf, pp. 181–270, (North-Holland Publishing Company, Amsterdam, London).
- Raz, R. (2005), “Extractors with weak random seeds,” in *Proceedings of the Thirty-seventh Annual ACM Symposium on Theory of Computing*, STOC ’05 (ACM, New York, NY, USA), pp. 11–20.
- Razavy, M. (2014), *Quantum theory of tunneling*, 2nd ed. (World Scientific, Singapore).
- Razzari, L., D. Duchesne, M. Ferrera, R. Morandotti, S. Chu, B.E. Little, and D.J. Moss (2010), “CMOS-compatible integrated optical hyper-parametric oscillator,” *Nature Photonics* **4** (1), 41–45.
- Reidler, I., Y. Aviad, M. Rosenbluh, and I. Kanter (2009), “Ultrahigh-speed random number generation based on a chaotic semiconductor laser,” *Physical Review Letters* **103** (July), 1–4.
- Ren, M., E. Wu, Y. Liang, Y. Jian, G. Wu, and H. Zeng (2011), “Quantum random-number generator based on a photon-number-resolving detector,” *Physical Review A* **83** (2), 023820.
- Renner, R. (2005), “Security of quantum key distribution,” PhD Thesis, ETH Zürich, <http://dx.doi.org/10.3929/ethz-a-005115027>.
- Renner, R., and R. König (2005), “Universally composable privacy amplification against quantum adversaries,” in *Theory of Cryptography, TCC 2005. Lecture Notes in Computer Science*, Vol. 3378 (Springer, Berlin, Heidelberg) pp. 407–425.
- Rényi, A. (1961), “On Measures of Entropy and Information,” in *Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability, Volume 1: Contributions to the Theory of Statistics*, University of California Press, pp. 547–561.
- Reznikov, M., R. de Picciotto, M. Heiblum, D.C. Glattli, A. Kumar, and L. Saminadayar (1998), “Quantum shot noise,” *Superlattices and Microstructures* **23** (3-4), 901–915.
- Ribordy, G., and O. Guinnard (inventors), and ID Quantique (assignee) (2009), “Method and apparatus for generating true random numbers by way of a quantum optics process,” Patent US7519641.
- Rice, S.O. (1944), “Mathematical Analysis of Random Noise,” *Bell System Technical Journal* **23** (3), 282–332.
- Rukhin, A., J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo, and L.E. Bassham III (2010), *A statistical test suite for random and pseudorandom number generators for cryptographic applications*, NIST Special Publication 800-22, Revision 1.a.
- Saito, T., K. Ishii, I. Tatsuno, S. Sukagawa, and T. Yanagita (2010), “Randomness and Genuine Random Number Generator With Self-testing Functions,” in *Joint International Conference on Supercomputing in Nuclear Applications and Monte Carlo 2010 (SNA + MC2010)*.
- Sanguinetti, B., A. Martin, H. Zbinden, and N. Gisin (2014), “Quantum Random Number Generation on a Mobile Phone,” *Physical Review X* **4** (3), 031056.
- Santha, M., and U.V. Vazirani (1986), “Generating quasi-random sequences from semi-random sources,” *Journal of Computer and System Sciences* **33** (1), 75–87.
- Santoro, R., O. Sentieys, and S. Roy (2009a), “On-line monitoring of Random Number Generators for embedded security,” in *2009 IEEE International Symposium on Circuits and Systems (IEEE)* pp. 3050–3053.
- Santoro, R., O. Sentieys, and S. Roy (2009b), “On-the-Fly Evaluation of FPGA-Based True Random Number Generator,” in *2009 IEEE Computer Society Annual Symposium on VLSI (IEEE)* pp. 55–60.
- Sartor, P., and K. Zimmermann (inventors), and Sony Corporation (assignee) (2015), “Optical random number generator and method for generating a random number,” Patent US 2015/0261502 A1.
- Sasaki, M., M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K.-I. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J.F. Dynes, A.R. Dixon, A.W. Sharpe, Z.L. Yuan, A.J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger (2011), “Field test of quantum key distribution in the Tokyo QKD Network,” *Optics Express* **19** (11), 10387.
- Scarani, V., A. Acín, G. Ribordy, and N. Gisin (2004), “Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations,” *Physical Review Letters* **92**, 057901.
- Scarani, V., H. Bechmann-Pasquinucci, N.J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev (2009), “The security of practical quantum key distribution,” *Reviews of Modern Physics* **81**, 1301–1350.
- Scheidt, T., R. Ursin, J. Kofler, S. Ramelow, X.-S. Ma, T. Herbst, L. Ratschbacher, A. Fedrizzi, N.K. Langford, T. Jennewein, and A. Zeilinger (2010), “Violation of local realism with freedom of choice,” *Proceedings of the National Academy of Sciences* **107** (46), 19708–19713.
- Schindler, W., and W. Killmann (2003), “Evaluation Criteria for True (Physical) Random Number Generators Used in Cryptographic Applications,” in *Cryptographic Hardware and Embedded Systems – CHES 2002, Lecture Notes in Computer Science*, Vol. **2523**, 431–449.
- Schmid, F., and N.B. Wilding (1995), “Errors in Monte Carlo simulations using shift register random number generators,” *International Journal of Modern Physics C* **6**, 781.
- Schmidt, H. (1970a), “A PK test with electronic equipment,” *Journal of Parapsychology* **34** (3), 175–181.
- Schmidt, H. (1970b), “Quantum Mechanical Random Number Generator,” *Journal of Applied Physics* **41** (2), 462–468.
- Schottky, W. (1918), “Über spontane Stromschwankungen in verschiedenen Elektrizitätsleitern,” *Annalen der Physik* **362** (23), 541–567.

- Scully, M.O., and S. Stenholm (1988), “The Role of Vacuum Fluctuations and Spontaneous Emission in the Laser Linewidth,” *Physica Scripta* **T21**, 119.
- Shadbolt, P., J.C.F. Mathews, A. Laing, and J.L. O’Brien (2014), “Testing foundations of quantum mechanics with photons,” *Nature Physics* **10** (4), 278–286.
- Shalm, L.K., E. Meyer-Scott, B.G. Christensen, P. Bierhorst, M.A. W., 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 (2015), “Strong Loophole-Free Test of Local Realism,” *Physical Review Letters* **115** (25), 250402.
- Shaltiel, R. (2002), “Recent developments in explicit constructions of extractors,” *Bulletin of the EATCS* **77** (67-95), 10.
- Shaltiel, R. (2008), “How to get more mileage from randomness extractors,” *Random Structures & Algorithms* **33** (2), 157–186.
- Shaltiel, R. (2011), “An Introduction to Randomness Extractors,” in *Automata, languages and programming*, Lecture Notes in Computer Science, **Vol. 6756**, 21–41.
- Shannon, C.E. (1948), “A Mathematical Theory of Communication,” *The Bell System’s Technical Journal* **27** (1), 379–423.
- Shchur, L.N., J.R. Heringa, and H.W.J. Blöte (1997), “Simulation of a directed random-walk model The effect of pseudo-random-number correlations,” *Physica A* **241**, 579–592.
- Shen, Y., L. Tian, and H. Zou (2010), “Practical quantum random number generator based on measuring the shot noise of vacuum states,” *Physical Review A* **81** (6), 63814.
- Shenoy, H.A., R. Srikanth, and T. Sriniva (2013), “Efficient quantum random number generation using quantum indistinguishability,” *Fluctuation and Noise Letters* **12** (04), 1350020.
- Shepherd, S.J. (1996), “Lessons learned from security weaknesses in the Netscape World Wide Web browser,” in *IEE Colloquium on Public Uses of Cryptography*, Vol. 1996 (IEE) pp. 7(1)–7(6).
- Shor, P.W. (1997), “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,” *SIAM Journal on Computing* **26** (5), 1484.
- Shumow, D., and N. Ferguson (2007), “On the possibility of a back door in the NIST SP800-90 Dual EC PRNG,” in *Proc. Crypto*, Vol. 7.
- Silverman, M.P., W. Strange, C.R. Silverman, and T.C. Lipscombe (1999), “Tests of alpha-, beta-, and electron capture decays for randomness,” *Physics Letters A* **262** (4-5), 265–73.
- Skorski, M. (2015), “True random number generators secure in a changing environment: Improved security bounds,” in *SOFSEM 2015: Theory and Practice of Computer Science, Lecture Notes in Computer Science*, **Vol. 8939**, pp. 590–602 (Springer, Berlin, Heidelberg).
- Smithey, D.T., M. Belsley, K. Wedding, and M.G. Raymer (1991), “Near quantum-limited phase memory in a Raman amplifier,” *Physical Review Letters* **67** (18), 2446–2449.
- Stich, D., J. Zhou, T. Korn, R. Schulz, D. Schuh, W. Wegscheider, M. W. Wu, and C. Schüller (2007), “Effect of initial spin polarization on spin dephasing and the electron g factor in a high-mobility two-dimensional electron system,” *Physical Review Letters* **98**, 176401.
- Somlo, P.I. (1975), “Zener-diode noise generators,” *Electronics Letters* **4** (14), 72.
- Song, X.-T., H.-W. Li, Z.-Q. Yin, W.-Y. Liang, C.-M. Zhang, Y.-G. Han, W. Chen, and Z.-F. Han (2015), “Phase-Coding Self-Testing Quantum Random Number Generator,” *Chinese Physics Letters* **32** (8), 080302.
- Soubusta, J., O. Haderka, and M. Hendrych (2001), “Quantum random number generator,” in *Proc. SPIE 4356, 12th Czech-Slovak-Polish Optical Conference on Wave and Quantum Aspects of Contemporary Optics*, pp. 54–60.
- Soubusta, J., O. Haderka, M. Hendrych, and P. Pavlicek (2003), “Experimental realization of Quantum random number generator,” in *Proc. SPIE 5259, 13th Czech-Slovak-Polish Optical Conference on Wave and Quantum Aspects of Contemporary Optics*, pp. 7–13.
- Soucarros, M., C. Canovas-Dumas, J. Clédière, P. Elbaz-Vincent, and D. Réal (2011), “Influence of the temperature on true random number generators,” in *Hardware-Oriented Security and Trust (HOST), 2011 IEEE International Symposium on*, pp. 24–27.
- Soucarros, M., J. Clédière, C. Dumas, and P. Elbaz-Vincent (2013), “Fault Analysis and Evaluation of a True Random Number Generator Embedded in a Processor,” *Journal of Electronic Testing* **29** (3), 367–381.
- Sowey, E.R. (1972), “A Chronological and Classified Bibliography on Random Number Generation and Testing,” *International Statistical Review / Revue Internationale de Statistique* **40** (3), 355–371.
- Srinivasan, A., M. Mascagni, and D. Ceperley (2003), “Testing parallel random number generators,” *Parallel Computing* **29** (1), 69 – 94.
- Srinivasan, A., and D. Zuckerman (1999), “Computing with very weak random sources,” *SIAM Journal on Computing* **28** (4), 1433–1459.
- Stefanov, A., N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden (2000), “Optical quantum random number generator,” *Journal of Modern Optics* **47** (4), 595–598.
- Stevanović, R., G. Topić, K. Skala, M. Stipčević, and B.M. Rogina (2008), “Quantum Random Bit Generator Service for Monte Carlo and Other Stochastic Simulations,” in *Large-Scale Scientific Computing, Lecture Notes in Computer Science*, **Vol. 4818**, pp. 508–515.
- Stipčević, M. (2004), “Fast nondeterministic random bit generator based on weakly correlated physical events,” *Review of Scientific Instruments* **75** (11), 4442.
- Stipčević, M. (2012), “Quantum random number generators and their applications in cryptography,” in *Proc. SPIE 8375, Advanced Photon Counting Techniques VI, 837504 (May 1, 2012)*, pp. 837504.
- Stipčević, M. (2014), “Preventing detector blinding attack and other random number generator attacks on quantum cryptography by use of an explicit random number generator,” arXiv:1403.0143.
- Stipčević, M., and J.E. Bowers (2015), “Spatio-temporal optical random number generator,” *Optics Express* **23** (9), 11619.
- Stipčević, M., and B.M. Rogina (2007), “Quantum random number generator based on photonic emission in semiconductors,” *Review of Scientific Instruments* **78** (4), 45104.
- Stipčević, M., and Ç.K. Koç (2014), “True Random Number Generators,” *Open Problems in Mathematics and Computational Science* (Springer International Publishing, Switzerland), pp. 275–315.

- Stipčević, M., and R. Ursin (2015), “An On-Demand Optical Quantum Random Number Generator with In-Future Action and Ultra-Fast Response,” Nature Publishing Group (August 2014), 1–8.
- Stojanovski, T., and L. Kocarev (2001), “Chaos-based random number generators-part I: analysis,” *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, **48** (3), 281–288.
- Stojanovski, T., J. Pihl, and L. Kocarev (2001), “Chaos-based random number generators. Part II: practical realization,” *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, **48** (3), 382–385.
- Stucki, D., S. Burri, E. Charbon, C. Chunnillall, A. Meneghetti, and F. Regazzoni (2013), “Towards a high-speed quantum random number generator,” in *Proc. SPIE 8899, Emerging Technologies in Security and Defence; and Quantum Security II; and Unmanned Sensor Systems X, 88990R (October 29, 2013)*, pp. 837504.
- Sunada, S., T. Harayama, K. Arai, K. Yoshimura, K. Tsuzuki, A. Uchida, and P. Davis (2011), “Random optical pulse generation with bistable semiconductor ring lasers,” *Optics Express* **19** (8), 7439.
- Sunar, B., W.J. Martin, and D.R. Stinson (2007), “A Provably Secure True Random Number Generator with Built-In Tolerance to Active Attacks,” *IEEE Transactions on Computers* **56** (1), 109–119.
- Suresh, V.B., D. Antonioli, and W.P. Burleson (2013), “On-chip lightweight implementation of reduced NIST randomness test suite,” in *Proceedings of the 2013 IEEE International Symposium on Hardware-Oriented Security and Trust, HOST 2013*, pp. 93–98.
- Symul, T., S.M. Assad, and P.K. Lam (2011), “Real time demonstration of high bitrate quantum random number generation with coherent laser light,” *Applied Physics Letters* **98** (23), 231103.
- Szczepanski, J., E. Wajnryb, J.M. Amigó, M.V. Sanchez-Vives, and M. Slater (2004), “Biometric random number generators,” *Computers & Security* **23** (1), 77–84.
- Takeuchi, S., and T. Nagai (1983), “Random pulser based on photon counting,” *Nuclear Instruments and Methods in Physics Research* **215** (1–2), 199–202.
- Tang, G.-Z., M.-S. Jiang, S.-H. Sun, X.-C. Ma, C.-Y. Li, and L.-M. Liang (2013), “Quantum Random Number Generation Based on Quantum Phase Noise,” *Chinese Physics Letters* **30** (11), 114207.
- Ta-Shma, A. (1996), “On extracting randomness from weak random sources (extended abstract),” in *Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing*, STOC ’96 (ACM, New York, NY, USA) pp. 276–285.
- Ta-Shma, A. (2011), “Short seed extractors against quantum storage,” *SIAM Journal on Computing* **40** (3), 664–677.
- Taylor, G., and G. Cox (2011), “Digital randomness,” *IEEE Spectrum* **48** (9), 32–58.
- Tehraniipoor, M., and F. Koushanfar (2010), “A Survey of Hardware Trojan Taxonomy and Detection,” *IEEE Design and Test of Computers* **27** (1), 10–25.
- Thamrin, N.M., G. Witjaksono, A. Nuruddin, and M.S. Abdullah (2008), “A Photonic-based Random Number Generator for Cryptographic Application,” in *2008 Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing* (IEEE) pp. 356–361.
- Thinh, L.P., L. Sheridan, and V. Scarani (2013), “Bell tests with min-entropy sources,” *Physical Review A* **87**, 062121.
- Thomson, W.E. (1959), “ERNIE—A Mathematical and Statistical Analysis,” *Journal of the Royal Statistical Society. Series A (General)* **122** (3), 301–333.
- Tisa, S., F. Villa, A. Giudice, G. Simmerle, and F. Zappa (2015), “High-Speed Quantum Random Number Generation Using CMOS Photon Counting Detectors,” *IEEE Journal of Selected Topics in Quantum Electronics* **21** (3), 23–29.
- Tittel, W., J. Brendel, N. Gisin, and H. Zbinden (1999), “Long-distance Bell-type tests using energy-time entangled photons,” *Physical Review A* **59** (6), 4150–4163.
- Tolman, R.C. (1917), *The Theory of the Relativity of Motion* (University of California Press, Berkeley, CA).
- Tomamichel, M., C. Schaffner, A. Smith, and R. Renner (2011), “Leftover hashing against quantum side information,” *IEEE Transactions on Information Theory* **57** (8), 5524–5535.
- Trevisan, L. (2001), “Extractors and pseudorandom generators,” *Journal of the ACM* **48** (4), 860–879.
- Trevisan, L., and S. Vadhan (2000), “Extracting randomness from samplable distributions,” in *Proceedings of the 41st Annual Symposium on Foundations of Computer Science, 2000*, pp. 32–42.
- Trifonov, A., and H. Vig (inventors), and Magiq Technologies, Inc. (assignee) (2007), “Quantum noise random number generator,” Patent US7284024.
- Troyer, M., and R. Renner (2012), “A randomness extractor for the quantis device,” ID Quantique Technical Report <http://www.idquantique.com/wordpress/wp-content/uploads/quantis-rndextract-techpaper.pdf>.
- Turan, M.S., E. Barker, J. Kelsey, K.A. McKay, M.L. Baish, and M. Boyle (2016), “Recommendation for the Entropy Sources Used for Random Bit Generation,” (Second DRAFT) NIST Special Publication 800–90B.
- Uchida, A., K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kurashige, M. Shiki, S. Yoshimori, K. Yoshimura, and P. Davis (2008), “Fast physical random bit generation with chaotic semiconductor lasers,” *Nature Photonics* **2** (12), 728–732.
- Um, M., X. Zhang, J. Zhang, Y. Wang, S. Yangchao, D.-L. Deng, L.-M. Duan, and K. Kim (2013), “Experimental certification of random numbers via quantum contextuality,” *Scientific reports* **3**, 1627.
- University of Geneva, (2004), <http://www.randomnumbers.info/> “Online randomness source”.
- Vadhan, S. (2007), “The unified theory of pseudorandomness: Guest column,” *SIGACT News* **38** (3), 39–54.
- Vallone, G., D.G. Marangon, M. Tomasin, and P. Villoresi (2014), “Quantum randomness certified by the uncertainty principle,” *Physical Review A* **90** (5), 052327.
- Vartsky, D., D. Bar, P. Gilad, and A. Schon (inventors), and Soreq Nuclear Research Center, El-Mul Technologies Ltd. (assignees) (2011), “High-speed, true random-number generator,” Patent US 7930333 B2.
- Vaskova, A., C. López-Ongil, A. Jiménez-Horas, E. San Millán, and L. Entrena (2010), “Robust cryptographic ciphers with on-line statistical properties validation,” in *Proceedings of the 2010 IEEE 16th International On-Line Testing Symposium, IOLTS 2010*, pp.208–210.
- Vaskova, A., C. López-Ongil, E. San Millán, A. Jiménez-Horas, and L. Entrena (2011), “Accelerating secure circuit design with hardware implementation of diehard battery of tests of randomness,” in *Proceedings of the 2011 IEEE 17th*

- International On-Line Testing Symposium, IOLTS 2011*, pp. 179–181.
- Vattulainen, I., T. Ala-Nissila, and K. Kankaala (1994), “Physical tests for random numbers in simulations,” *Physical Review Letters* **73** (19), 2513–2516.
- Vattulainen, I., T. Ala-Nissila, and K. Kankaala (1995), “Physical models as tests of randomness,” *Physical Review E* **52** (3), 3205–3214.
- Vazirani, U. V. (1987a), “Strong communication complexity or generating quasi-random sequences from two communicating semi-random sources,” *Combinatorica* **7** (4), 375–392.
- Vazirani, U. (1987b), “Efficiency considerations in using semi-random sources,” in *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing*, STOC ’87 (ACM, New York, NY, USA) pp. 160–168.
- Vazirani, U.V., and V.V. Vazirani (1985a), “Efficient and Secure Pseudo-Random Number Generation (Extended Abstract),” in *Advances in Cryptology -CRYPTO’84, Lecture Notes in Computer Science Vol. 196* (Springer, Berlin, Heidelberg) pp. 193–202.
- Vazirani, U. V., and V. V. Vazirani (1985b), “Random polynomial time is equal to slightly-random polynomial time,” in *Foundations of Computer Science, 1985., 26th Annual Symposium on*, pp. 417–428.
- Vazirani, U., and T. Vidick (2011), “Certifiable Quantum Dice - Or, testable exponential randomness expansion,” *Philosophical Transactions of the Royal Society A* **370** (1971), 21.
- Vazirani, U., and T. Vidick (2014), “Fully device-independent quantum key distribution,” *Physical Review Letters* **113**, 140501.
- Vincent, C.H. (1970), “The generation of truly random binary numbers,” *Journal of Physics E: Scientific Instruments* **3** (8), 594.
- Vincent, C.H. (1971), “Precautions for accuracy in the generation of truly random binary numbers,” *Journal of Physics E* **4**, 825–828.
- Vivoli, V.C., P. Sekatski, J.-D. Bancal, C.C.W. Lim, A. Martin, R.T. Thew, H. Zbinden, N. Gisin, and N. Sangouard (2015), “Comparing different approaches for generating random numbers device-independently using a photon pair source,” *New Journal of Physics* **17** (2), 023023.
- Wahl, M., M. Leifgen, M. Berlin, and O. Benson (2014), “Addendum: An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements,” *Applied Physics Letters* **101** (15), 159901.
- Wahl, M., M. Leifgen, M. Berlin, T. Röhlicke, H.-J. Rahn, and O. Benson (2011), “An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements,” *Applied Physics Letters* **98** (17), 7–10.
- Walenta, N., M. Soucarros, D. Stucki, D. Caselungha, M. Domergue, M. Hagerman, R. Hart, D. Hayford, R. Houlmann, M. Legré, T. McCandlish, J.-B. Page, M. Tourville, and R. Wolterman (2015), “Practical aspects of security certification for commercial quantum technologies,” in *Proc. SPIE 9648, Electro-Optical and Infrared Systems: Technology and Applications XII; and Quantum Information Science and Technology*, 96480U.
- Walker, J. (1996), <http://www.fourmilab.ch/hotbits/> “HotBits: Genuine random numbers, generated by radioactive decay”.
- Walmsley, I.A., and M.G. Raymer (1983), “Observation of Macroscopic Quantum Fluctuations in Stimulated Raman Scattering,” *Physical Review Letters* **50** (13), 962–965.
- Wang, F.-X., C. Wang, W. Chen, S. Wang, F.-S. Lv, D.-Y. He, Z.-Q. Yin, H.-W. Li, G.-C. Guo, and Z.-F. Han (2015a), “Robust quantum random number generator based on avalanche photodiodes,” *Journal of Lightwave Technology* **33** (15), 3319–3326.
- Wang, J.-M., T.-Y. Xie, H.-F. Zhang, D.-X. Yang, C. Xie, and J. Wang (2015b), “A Bias-Free Quantum Random Number Generation Using Photon Arrival Time Selectively,” *IEEE Photonics Journal* **7** (2), 1–8.
- Wang, P.X., G. Longo, and Y.S. Li (2006), “Scheme for a quantum random number generator,” *Journal Of Applied Physics* **100** (5), 56107.
- Watson, T. (2016), “The complexity of estimating min-entropy,” *computational complexity* **25** (1), 153–175.
- Wayne, M.A., E.R. Jeffrey, G.M. Akselrod, and P.G. Kwiat (2009), “Photon arrival time quantum random number generation,” *Journal of Modern Optics* **56** (4), 516–522.
- Wayne, M.A., and P.G. Kwiat (2010), “Low-bias high-speed quantum random number generator via shaped optical pulses,” *Optics Express* **18**(9), 9351–9357.
- Wegman, M.N., and J.L. Carter (1981), “New hash functions and their use in authentication and set equality,” *Journal of Computer and System Sciences* **22** (3), 265 – 279.
- Wei, W., and H. Guo (2009a), “Bias-free true random-number generator,” *Optics Letters* **34** (12), 1876.
- Wei, W., and H. Guo (2009b), “Quantum random number generator based on the photon number decision of weak laser pulses,” in *2009 Conference on Lasers & Electro Optics & The Pacific Rim Conference on Lasers and Electro-Optics* (IEEE) pp. 1–2.
- Wei, W., W. Tang, and H. Guo (2010), “High speed true random number generation using chaotic light,” *Lasers and Electro-Optics (CLEO) and Quantum Electronics and Laser Science Conference (QELS)*, 2010 Conference on , 1–2.
- Weih, G., T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger (1998), “Violation of Bell’s Inequality under Strict Einstein Locality Conditions,” *Physical Review Letters* **81** (23), 5039.
- Wheeler, J.A. (1978), “The “Delayed-Choice” Double-Slit Experiment,” in *Mathematical Foundations of Quantum Theory* (Academic Press).
- Williams, C.R.S., J.C. Salevan, X. Li, R. Roy, and T.E. Murphy (2010), “Fast physical random number generator using amplified spontaneous emission,” *Optics Express* **18** (23), 23584–23597.
- Wong, W.S., H.A. Haus, L.A. Jiang, P.B. Hansen, and M. Margalit (1998), “Photon statistics of amplified spontaneous emission noise in a 10-Gbit/s optically preamplified direct-detection receiver,” *Optics Letters* **23** (23), 1832.
- Wu, L.-A., H.J. Kimble, J.L. Hall, and H. Wu (1986), “Generation of Squeezed States by Parametric Down Conversion,” *Physical Review Letters* **57** (20), 2520–2523.
- Wu, L.-A., M. Xiao, and H.J. Kimble (1987), “Squeezed states of light from an optical parametric oscillator,” *Journal of the Optical Society of America B* **4** (10), 1465.
- Xu, F., B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo (2012), “Ultrafast quantum random number generation based on quantum phase fluctuations,” *Optics Express* **20** (11), 12366.
- Xu, M., J. Huang, W. Liang, C. Zhang, S. Wang, Z. Yin,

- W. Chen, and Z. Han (2015), “Adjustable unbalanced quantum random-number generator,” *Chinese Optics Letters* **13** (2), 21405.
- Yamazaki, T., and A. Uchida (2013), “Performance of Random Number Generators Using Noise-Based Superluminescent Diode and Chaos-Based Semiconductor Lasers,” *IEEE Journal of Selected Topics in Quantum Electronics* **19** (4), 0600309.
- Yan, Q., B. Zhao, Z. Hua, Q. Liao, and H. Yang (2015), “High-speed quantum-random number generation by continuous measurement of arrival time of photons,” *Review of Scientific Instruments* **86** (7), 073113.
- Yang, B., V. Rozic, N. Mentens, and I. Verbauwhe (2015), “On-the-fly tests for non-ideal true random number generators,” in *Proceedings - IEEE International Symposium on Circuits and Systems 2015-July*, 2017–2020.
- Yao, A.C. (1982), “Theory and application of trapdoor functions,” in *23rd Annual Symposium on Foundations of Computer Science (SFCS 1982)* (IEEE) pp. 80–91.
- Yariv, A., and P. Yeh (2007), *Photonics: Optical Electronics in Modern Communications*, sixth ed. (Oxford University Press).
- Yu, L.M., M.J. Yang, P.X. Wang, and S. Kawata (2010), “Note: A sampling method for quantum random bit generation,” *Review of Scientific Instruments* **81** (4), 046107.
- Yuen, H.P., and V.W.S. Chan (1983), “Noise in homodyne and heterodyne detection,” *Optics Letters* **8** (3), 177–179.
- Yurke, B., and D. Stoler (1992), “Bells-inequality experiments using independent-particle sources,” *Physical Review A* **46** (5), 2229–2234.
- Zhao, Y., C.-H.F. Fung, B. Qi, C. Chen, and H.-K. Lo (2008), “Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems,” *Physical Review A* **78**, 042333.
- Zheng, Y., and T. Matsumoto (1997), “Breaking real-world implementations of cryptosystems by manipulating their random number generation,” in *Proceedings of the 1997 Symposium on Cryptography and Information Security, Fukuoka, Japan*, pp. 6B1–6.
- Zhou, H., and J. Bruck (2012), “Efficient generation of random bits from finite state Markov chains,” *IEEE Transactions on Information Theory* **58** (4), 2490–2506.
- Zhou, H., X. Yuan, and X. Ma (2015), “Randomness generation based on spontaneous emissions of lasers,” *Physical Review A* **91** (6), 062316.
- Zhu, Y., Y. Lu, J. Zhu, and G. Zeng (2011), “High speed quantum-random-number generation via measurement on phase noise of laser,” *International Journal of Quantum Information* **09** (04), 1113–1122.
- Zhu, Y., G. He, and G. Zeng (2012), “Unbiased Quantum Random Number Generation Based on Squeezed Vacuum State,” *International Journal of Quantum Information* **10** (01), 1250012.
- Ziff, R.M. (1998), “Four-tap shift-register-sequence random-number generators,” *Computers in Physics* **12** (4), 385.
- Zuckerman, D. (1990), “General weak random sources,” in *Proceedings of the 31st Annual IEEE Symposium on Foundations of Computer Science, 1990* (IEEE) Vol. 2, pp. 534–543.
- Zuckerman, D. (1996), “Simulating BPP using a general weak random source,” *Algorithmica* **16** (4), 367–391.
- Zukowski, M., A. Zeilinger, M.A Horne, and A.K. Ekert (1993), ““Event-ready-detectors” Bell experiment via entanglement swapping,” *Physical Review Letters* **71** (26), 4287–4290.