Towards Self-testing Quantum Random Number Generators in Integrated Design

P S Chernov, V S Volkov, D A Surovtsev
Penza State University, Krasnaya 40, Penza, Russian Federation
E-mail: pvllvp@yandex.ru

Abstract. Truly random numbers are in great demand in various applications. Self-testing quantum random number generators provide a way to verify that random numbers indeed come from quantum effects. Optical quantum random number generators of this type are the most promising but due to their relative complexity have been realized only as a macroscopic prototype. Miniaturization of such devices opens the way to commercial use. Quantum photonics provides the means to achieve this goal. We discuss general design of self-testing optical quantum random number generator and the ways to implement it as a compact integrated photonic circuit within current technological reach.

1. Introduction
The generation of truly random numbers plays a crucial role in a number of important applications. High-quality random numbers are very essential in the field of cryptography, numerical simulations, in the gaming industry and some other areas. Software pseudo-random generators are of deterministic nature, even though they can have a very long period (e.g. $2^{19937}-1$ for Mersenne Twister algorithm). Popular hardware random number generators (RNG) make use of a Zener diode operated in the reverse breakdown region. In this scheme, voltage fluctuations are amplified and compared to a threshold to generate random bits. There are two sources of noise in such a system: shot noise coming from quantum effects and classical thermal noise. In practice, both noises tend to appear side by side and are difficult to isolate. Some critical applications, such as secret key generation in cryptography, require truly random bits that can be obtained only from a quantum source.

Many physical processes can serve as a source of quantum randomness: radioactive decay [1], quantum tunnelling, orientation of spin in the magnetic field [2], etc. The block diagram for a hardware RNG can be represented as independent blocks performing certain tasks (Fig. 1).

![Figure 1. Block diagram for a hardware random number generator.](image)

The entropy source consists of a physical system and a measuring equipment. Analog signals are further digitized. In practice, due to the imperfection of the physical devices, the resulting set of bits may contain some degree of autocorrelation. For this reason the initial sequence is usually subjected to additional post-processing and randomness extraction. The output of a perfect RNG is a random sequence of shorter length but with delta-correlation and uniform distribution.
Optical quantum RNGs are very attractive due to their relative simplicity and a rich choice of implementations. Light from lasers, light emitting diodes or single photon sources is a convenient and affordable source of truly random numbers. Optical methods for quantum random number generation are varying from simple statistics of arrival time [3] or photon number counting [4] to advanced types based on spontaneous parametric down-conversion [5], Raman scattering [6], amplified spontaneous emission [7], laser phase noise [8] and others.

2. Classical randomness testing
The generated random numbers need to be checked to ensure the device is functioning correctly. However, it is impossible in principle to guarantee that a finite sequence is truly random. Uncomputability of Kolmogorov complexity ensures that there is no way to deduce the true randomness of a finite string [9]. The verification methods usually aim at detecting suspicious sequences, such as the bit strings like 1111111111 and 0000000000. If the generator constantly outputs the same sequence or the occurrence of ones and zeroes are not statistically equal, it is suspected not acting randomly. Statistical tests offer a common approach to randomness testing. They are covered in various sources starting from the classical book by Knuth [10]. The widely used sets of statistical tests are the NIST suite [11] and the DieHard suite. There are also other randomness testing utilities with different tests. Some of the most relevant ones include:

- The frequency test, which calculates the misbalance between zeroes and ones. The frequency test may be performed within blocks of different sizes to check some correlations.
- The runs test, which checks if the sequence of identical bits in a bit string corresponds to that in a random sequence.
- The spectral test, which detects periodic structure in the bit sequence.
- Autocorrelation test, which checks the correlation of a sequence with a delayed copy of itself as a function of delay.
- Universal Statistical Test, which detects any significant deviation of the output statistics from the statistics of a perfect RNG [12].

The result of any statistical test is the probability of a true random number generator to produce the given sequence. The threshold is different for each test type. While useful, these tests cannot with 100%-certainty guarantee that a given RNG produces truly random bits. Pseudorandom deterministic RNG like the Mersenne Twister algorithm can easily pass all the tests but nevertheless known to be predictable. Likewise, false positives results may be seen especially with relatively small sequences. In fact, even true RNGs occasionally produce long strings of zeroes or ones or any repeated substring. Statistically, any RNG would fail tests from time to time. To minimize this probability the tests run multiple times.

The tests usually do not include physical models of RNG into account and designed with orientation on a pseudorandom number generators. Some device-specific correlations linked to implementation of physical realizations are not specifically addressed. The tests however are useful when applied to detection of sudden hardware failures. Testing is also vulnerable to an active attacker that feeds the device with pregenerated random sequences that pass all the tests. In the next section we will address quantum mechanics approach to solve this issue.

3. Self-testing optical quantum random number generators
All random number generators face a problem of trust. An attacker having an access to the device can influence the produced numbers by inserting hardware Trojans. There are also some problems for physical RNGs such as imperfection of components, degradation of physical properties and the possibility of spontaneous failure which can be hard to detect.

It is hard for majority of the quantum RNGs to estimate the proportion of quantum noise in the output signal. Consider for an example a simple quantum RNG consisting of a single-photon laser, a beam splitter (half-silvered mirror) and two photon detectors. Theoretically the detectors should produce perfectly random bits since a photon has 50% probability to pass the beam splitter and 50% to reflect. In practice there always exist problems with imperfection of detectors, laser, beam splitter.
and functional dependences of their characteristics on external conditions and time. There are devicespecific approaches to check to some extent the quantum nature of the signal but usually software randomness extractors and post-processing are used to correct the probability distribution.

Quantum mechanics provides a new way to deal with untrusted devices [13]. It is possible to check the quantum nature of the source based only on the output binary sequences ignoring the implementation details of the quantum RNG. The Kochen-Specker theorem guarantees that no classical system can simulate certain quantum properties [14]. The entanglement of spacelike separated subsystems and the use of Bell-like inequalities can serve as a device independent test for randomness.

Optics is the optimal choice for constructing this new generation quantum RNGs. Figure 2 shows the simplified block diagram for a self-testing optical quantum random number generator.

\[ |\psi^+ \rangle = \frac{1}{\sqrt{2}} (|x\rangle|y\rangle + |y\rangle|x\rangle) \]  

where \(|x\rangle\) and \(|y\rangle\) denote the state of a single vertically or horizontally polarized photon. Absorptive polarizers let photon pass through with 50% probability. If polarizing axes are at the same angle, photon detectors give the opposite outcomes. In theory, coincidence counter in this case registers perfect anti-correlation. Perpendicular orientation of polarizing axes gives 100% correlated photon detections. Quantum correlations disappear if relative angle has been chosen to be 45 degrees.

Entanglement allows one to perform effective tests on the noise quality, that is to ensure its true quantum nature. The angles of the polarizers are set at random in accordance with the variables \(x\) and \(y\) from classical (pseudo)random number generators RNG 1 and RNG 2. Verification that a random sequence \((a, b)\) is obtained from quantum processes boils down to the calculation of the conditional probabilities \(p(a, b | x, y)\). Statistical tests based on Bell-like inequalities are independent of physical realization and include only classical stochastic variables \(a, b, x, y\).

4. Quantum photonic designs

Classical realizations of the described scheme are usually obtained in the laboratory setup and have considerable weight and size. Recent progress in integrated quantum photonics promise that very compact designs are nearly within technological reach.

It is known that polarization-entangled photon pair states are difficult to prepare in an integrated photonic circuit [15]. Despite that fact, spontaneous parametric down-conversion (SPDC) is typically exploited in III-V materials, such as AlGaAs [16], and can be made integrated on a silicon chip. Alternative designs are also demonstrated [17].
Early arrangements used optical lens or glass-based waveguides. Semiconductor waveguides are very promising as they offer the prospect of integrating several components onto the same chip [18]. Silicon waveguides are usually formed by etching the device layer of a silicon-on-insulator (SOI) wafer. They are already used as an optical interconnect between several processor cores or between cores and memory [19].

In any quantum circuit at the end we must always extract some classical information. This is done by using detectors sensitive to single photons. Silicon avalanche photodiode (APD) detectors are widely used for this purpose. Other types of single-photon detectors are now developing such as superconducting nanowire single-photon detectors [20]. Unfortunately no waveguide-coupled single-photon detector of this type has been demonstrated operational at room temperature yet.

Tunable polarizers are the most undeveloped part in the setup. Classical polarizers and waveplates may be made of various nanoparticles embedded in thin plates. But to change the polarizing axis of such a plate one has to physically rotate it. Electrically controlled polarizers for integrated quantum circuits are just emerging. Promising approaches include electrically tunable polarizer based on anisotropic absorption of graphene ribbons [21], tunable wave plate based on active plasmonic metasurfaces [22] and others.

All these building blocks have now been demonstrated separately by the quantum photonics community. The challenge for future work is to improve the performance of individual blocks and to integrate these blocks on a common platform.

5. Acknowledgments
The authors thank the Ministry of Education and Science of Russian Federation for the financial support (Project Code MK-621.2017.8).

6. References
[1] Isida M, Ikeda H 1956 Random number generator Annals of the Institute of Statistical Mathematics 8 (2) pp 119–126
[2] Katsoprinakis G E , Polis M, Tavernarakis A, Dellis A T, and Kominis I K 2008 Quantum random number generator based on spin noise Physical Review A 77 (5), 054101
[3] Nie Y Q, Zhang H F, Zhang Z, Wang J, Ma X, Zhang J and Pan J W 2014 Practical and fast quantum random number generation based on photon arrival time relative to external reference Applied Physics Letters 104 (5), 051110
[4] Lopes S, Mendonça F A, Ramos R V 2014 Quantum Random Number Generator Using Only One Single-Photon Detector IEEE Photonics Technology Letters 26 (9), 851–853
[5] Marandi A, Leindecker N C, Vodopyanov K L and Byer R L 2012 All-optical quantum random bit generation from intrinsically binary phase of parametric oscillators Optics Express 20 (17), 19322–19330
[6] Argyris A, Pikasis E, Deligiannidis S, and Syvridis D 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
[8] Jofre M, Curty M, Steinlechner F, Anzolin G, Torres J P, Mitchell M W and Pruneri V 2011 True random numbers from amplified quantum vacuum Optics Express 19 (25), 25173–25180
[9] Rukhin A J, Nechvatal S J, Smid M, Barker E, Leigh S, Levenson M, Vangel M, Banks D, Heckert A, Dray J, Vo S and Bassham L E 2010 A statistical test suite for random and pseudorandom number generators for cryptographic applications NIST Special Publication 800-22, Revision 1.a
[12] Maurer U 1992 A Universal Statistical Test for Random Bit Generators Journal of Cryptology 5 (2) pp 89–105
[13] Herrero-Collantes M and Garcia-Escartin J C 2017 Quantum random number generators Rev. Mod. Phys. 89, 015004
[14] Kochen S and Specker E P 1967 The problem of hidden variables in quantum mechanics Journal of Mathematics and Mechanics 17 pp 59–87
[15] Kultavewuti P, Zhu E Y, Xing X, Qian L, Pusino V, Sorel M and Aitchison J S 2017 Sci. Rep 7 5785
[16] Horn R T et al. 2013 Inherent polarization entanglement generated from a monolithic semiconductor chip Sci. Rep 3 2314
[17] Olislager L et al. 2013 Silicon-on-insulator integrated source of polarization-entangled photons Opt. Lett. 38 1960–1962
[18] Cry J, Rarity J G, Yu S and OBrien J L 2008 Silica-on-silicon waveguide quantum circuits Science 320 646–649
[19] Sun C et al. 2015 Single-chip microprocessor that communicates directly using light Nature 528 534–538
[20] Dauler E A et al. 2014 Review of superconducting nanowire single-photon detector system design options and demonstrated performance Optical Engineering 53 081907-081907
[21] Zhu Z H, Guo C C, Liu K, Zhang J F, Ye W M, Yuan X D, Qin S Q 2014 Electrically tunable polarizer based on anisotropic absorption of graphene ribbons Applied Physics A 114 4 1017-1021
[22] Li T, Huang L, Liu J, Wang Y, Zentgraf T 2017 Tunable wave plate based on active plasmonic metasurfaces Opt Express 25(4) 4216–4226