The 25th Iranian Conference on
Optics and Photonics (ICOP 2019),
and the 11th Iranian Conference on
Photonics Engineering and
Technology (ICPET 2019).
University of Shiraz,
Shiraz, Iran,
Jan. 29-31, 2019

مولد اعداد تصادفی کوانتومی نوری مبتنی بر اندازه حرکت زاویه‌ای نور

سارا توفیقی و لیلا چهره‌قانی انزابی

پژوهشکده فناوری ارتباطات، مرکز تحقیقات مخابرات ایران
s.tofighi@itrc.ac.ir و leilachan@itrc.ac.ir

چکیده- اعداد تصادفی برای رمزنگاری کلاسیک و کوانتومی ضروری هستند. یک ویژگی ضروری برای مولد اعداد تصادفی این است که خروجی‌های آنها باید غیرقابل‌پیش‌بینی باشد. اعداد تصادفی ایجاد شده توسط کامپیوترها، شبه تصادفی هستند و استفاده از آنها در رمزنگاری باعث ایجاد حفره‌های امنیتی ناخواسته می‌شود. از بین انواع مختلف اعداد تصادفی کوانتومی، آنهایی که بر پایه اپتیک کوانتومی هستند به دلیل مزایایی هم‌چون پیاده‌سازی راحت‌تر، نرخ تولید اعداد تصادفی بالاتر و ابعاد کوچک‌تر، توجه بیشتری را به خود جلب کرده‌اند. مولد اعداد تصادفی کوانتومی نوری را می‌توان بر حسب نوع چشمه تصادفی و اندازه‌گیری کوانتومی به سه دسته اصلی طبقه‌بندی کرد. در این مقاله ایده جدیدی برای تولید اعداد کاملاً تصادفی بر اساس برهم‌نهی درجه آزادی اندازه حرکت زاویه‌ای فوتون‌ها پیشنهاد شده است. تکنیک پیشنهادی ما که متعلق به اولین کلاس از مولد اعداد تصادفی کوانتومی نوری است، می‌تواند هم نرخ تولید و هم غیرقابل‌پیش‌بینی بودن رشته بیت تصادفی را افزایش دهد.

کلید واژه- اپتیک کوانتومی، اندازه حرکت زاویه ای نور، تک فوتون، مولد اعداد تصادفی کوانتومی.

Optical quantum random number generator based on orbital angular momentum of light

Sara Tofighi and Leila Chehreghani Anzabi

Department of Communication Technology, Iran Telecommuniation Research Center
s.tofighi@itrc.ac.ir & leilachan@itrc.ac.ir

Abstract- Random numbers are critical to both classical and quantum cryptography. A key necessity for random-number generators is that their outputs must be unpredictable. The computer generated random numbers are pseudo-random and using them in cryptography causes unexpected security-holes. True randomness can only be extracted from the inherently random process such as quantum phenomena. Among different types of quantum random number generator, those are based on quantum optics attract more attention because of their advantages such as easier implementation, higher random number generation rate, and compact size. The quantum optical random number generators can be classified into three main classes according to the type of randomness sources and quantum measurement. In this paper, a new idea to generate truly random numbers based on the superposition of photon's orbital angular momentum (OAM) degrees of freedom is proposed. Our proposed technique which belongs to the first class of optical QRNGs can enhance both the generation rate and unpredictability of random bit string.

Keywords: Quantum optics, Orbital angular momentum of light, Single photon, Quantum random number generator.

1. Introduction

Truly random numbers play a vital role in both classical and quantum cryptography. Any lack of randomness may lead to security loopholes. Beside cryptography, random numbers are an essential resource in science and technology such as simulation, and coordination in computer networks or lotteries [1]. The output sequence of a truly random numbers generator at-least must have three important properties: unpredictable, uncorrelated and unbiased [2]. High generation rate is another aspect of a random number generator which is important in some applications such as cryptography. Obviously, the appropriate cost, compact size and lower power requirement are other determinants for choosing a suitable random number generator. There are two main methods to generate random numbers: pseudorandom number generators (PRNGs) and physical truly random number generators (TRNGs) [3]. PRNGs produce random numbers using a computational deterministic algorithm. However, the sequences generated from these algorithmic-based approaches suffer from determinism, periodicity, correlation and lack of uniformity, but for several applications which need high generation rate and less randomness are sufficient [4]. Physical (or hardware) truly random number generators are based on non-deterministic physical phenomena, such as classically chaotic systems or quantum systems. The problem of chaotic sources of entropy (such as those based on thermal and electric noises, free running oscillator and biometric methods) is that they are too sensitive to external influences and lack robustness. Nevertheless, the Chaos-based random number generators have an advantage that they are fast [5].

On the other hand, quantum random number generators (QRNG) are more robust against environmental disturbances, but they suffer from relatively low rates of random number generation. A QRNG typically consists of two main modules: quantum entropy source and a randomness extractor. The quantum entropy source exploits the randomness in quantum mechanics to generate a sequence of true random numbers. Since the quantum effects are mixed with classical noise, a module of randomness extractor is necessary to subtract the classical effect from the quantum randomness. Both of these modules are effective on the rate of random number generator [6].

There are multiple quantum entropy sources such as radioactive decay, electrical noises and quantum optical processes. Among them quantum optical entropy sources reach higher generation rates on the order of megabits to gigabits per second and new generations of these systems are still being proposed [7].

While there is a race to utilize ultra-fast quantum optical phenomena and declare the highest possible generation rate of random numbers, the realistic implementations are limited by speed of the electronic systems and the post-processing methods. So, selecting a fast post-processing technique that is resistant against quantum attacks is also crucial for random number generator[7,8].
Optical QRNGs are developed very well in recent years and commercial products of optical QRNGs are available in the market. Generally, and as shown if Fig. 1, the quantum optical QRNGs can be classified in three groups according to the type of devices used in the entropy source module. Optical QRNGs of first group which utilize quantum devices such as single photon sources and detectors, as well as photon number resolving detectors take profit of the intrinsic randomness present in the quantum state of photon. The second group of optical QRNG does not require quantum devices which are technically challenging and extracts quantum origin entropy from optical sources using standard classical detectors such as homodyne detection system or standard photo-detectors. Finally, the third class considers experimental imperfect devices which are not fully trusted or characterized inaccurately. Using the

nonlocal property of entanglement, the methods of this class can certify the randomness of generated bits. In this paper, a novel idea for quantum random number generation using orbital angular momentum of light is proposed which belongs to the first class of QRNGs.

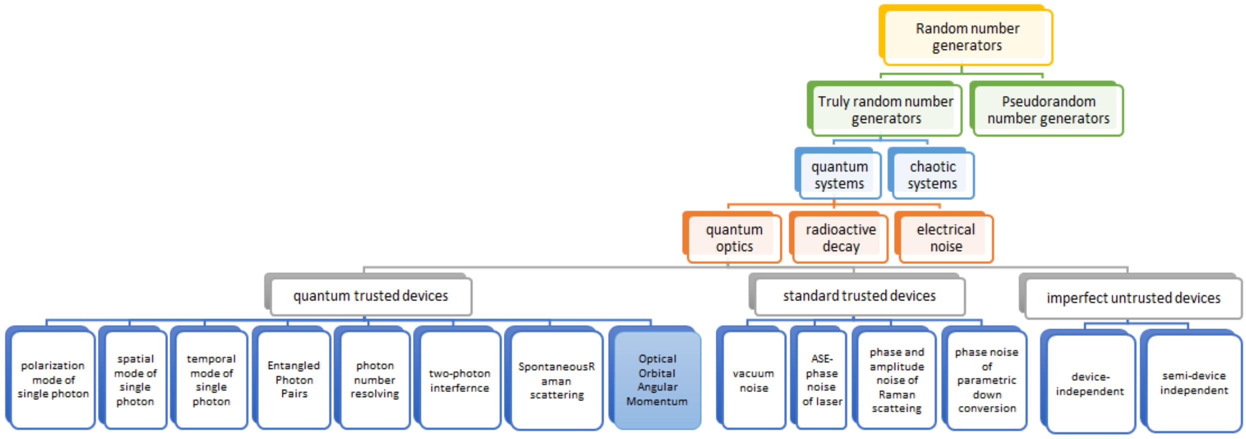

Fig.1 Classification of random number generators

2. QRNG based on orbital angular momentum of light

Recently, orbital angular momentum (OAM) of light attracts considerable attention for achieving higher data transmission capacity in both classical and quantum communication [9,10]. Moreover, in quantum communication protocols based on OAM of light the security is also enhanced [11].

OAM is a degree of freedom of light which is related to the spatial distribution of field. The OAM-carrying beams (such as Laguerre-Gaussian modes) are characterized with azimuthal phase dependence of $e^{il\varphi}$, where 'l' can be any integer number. The positive (negative) values correspond to clockwise (counter-clockwise) helical phase front, while a zero value corresponds to Gaussian beam. Therefore, despite polarization which can takes only two orthogonal states, the OAM-carrying beam have infinite number of orthogonal states for encoding both classical and quantum information [12]. In this paper we use the high dimensional quantum space of photon's OAM to enhance the generation rate of optical QRNG. A schematic diagram illustrating the working principles of QRNG based on OAM is depicted in Fig. 2. The entropy source of our proposed method belongs to the first category of optical QRNGs and extract randomness by measuring the superposition of orbital angular momentum states.

Mutually unbiased bases (MUBs) are specific linear combination of OAM states. These modes which are generally called ANG modes are appropriate superposition states for our purpose. Because according to equation (1) the measurement of a photon in the ANG mode provides no information about its OAM state: $\left|{}_{ANG}\langle n|l\rangle_{OAM}\right|^2 = \frac{1}{d}$.

$$|n\rangle_{ANG} = \frac{1}{\sqrt{d}} \sum_{l=-L}^{L} e^{i\frac{2\pi n l}{d}} |l\rangle_{OAM}, \qquad (1)$$

where $d = 2L + 1$. Generally, for preparing superposition of OAM modes with arbitrary amplitude and phase ratios different methods have been proposed such as interferometric method and computer-generated holograms. However, due to the complex implementation and difficult control of interferometer setup, a computer generated hologram is more convenient for preparation of ANG modes [13]. A variable attenuator is placed after the hologram to achieve single photon ANG mode.

In the QRNGs based on polarization modes of single photon, the two eigenstates of polarization are sorted by a polarization beam splitter. Similarly, a method for sorting OAM eigenstates with high separation efficiency and high power transmission efficiency is required for designing a QRNG based on OAM modes of single photon. This can be done with different proposed OAM sorting methods at the single-photon level [14-18].

As shown in Fig. 2, in order to have a cost-efficient QRNG and employing only one single photon detector for measuring the OAM content of a single photon, we use an unbalanced interferometer. Each branch of interferometer has a definite delay time. By detecting the time of arrival of single photon, one can understand which path it took and consequently which OAM it carried. Finally, by attributing a sequence of bits to each OAM, one can obtain a sequence of truly random bits. Since the coding space is expanded to high dimensional OAM space, the rate of QRNG is increased considerably.

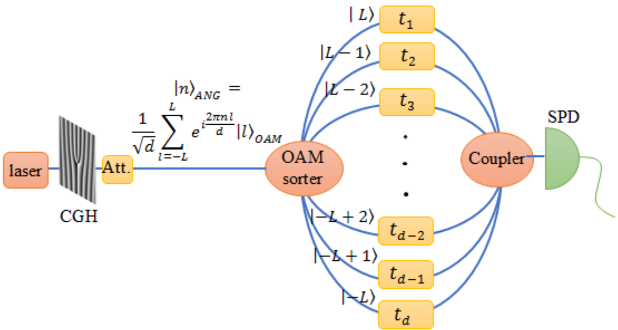

Fig. 2. A schematic configuration of QRNG based on OAM. CGH: computer generated hologram, SPD: single photon detector, Att.: attenuator.

By considering entropy $(H = -\sum p_i \log_2(p_i))$ as a measure of unpredictability, it is obvious that a random bit string generated using QRNG based on high dimensional OAM space $(d > 2)$ is more unpredictable with respect to that generated by polarization-based QRNG.

3. Conclusion

In this paper a new idea for quantum random number generation based on orbital angular momentum of light is proposed. Since the quantum superposition state of single photons are prepared in high-dimensional OAM space, our proposed method has the potential of generating more unpredictable random numbers with higher rate.

References

[1] B. Hayes, "Computing Science: Randomness as a Resource."*American Scientist* 89.4 (300-304), (2001).

[2] B. Hayes, *Foolproof, and Other Mathematical Meditations*. MIT Press, 2017.

[3] L. Kocarev, and S. Lian, eds. *Chaos-based cryptography: theory, algorithms and applications.* Vol. 354. Springer Science & Business Media, 2011.

[4] A. Roeck, *Quantifying Studies of (Pseudo) Random Number Generation for Cryptography.* **Ph.D.** dissertation, Ecole Polytechnique X, 2009.

[5] L. L. Bonilla, M. Alvaro, & M. Carretero, "Chaos-based true random number generators." *Journal of Mathematics in Industry* 7.1 (2016): 1.

[6] X. Ma, et al. "Quantum random number generation." *npj Quantum Information* 2 (2016): 16021.

[7] M. Herrero-Collantes, and J. C. Garcia-Escartin. "Quantum random number generators." *Reviews of Modern Physics* 89.1 (2017): 015004.

[8] F. Xu, et al. "Ultrafast quantum random number generation based on quantum phase fluctuations." *Optics express* 20.11 (2012): 12366-12377.

[9] J. Wang, et al. "Terabit free-space data transmission employing orbital angular momentum multiplexing." *Nature photonics* 6.7 (2012): 488.

[10] A. Sit, et al. "High-dimensional intracity quantum cryptography with structured photons." *Optica* 4.9 (2017): 1006-1010.

[11] F. Farman, et al. “Ping-Pong protocol based on orbital angular momentum of light” J. Opt. Soc. Am. B **35**(10), 2348-2355 (2018).

[12] D. L. Andrews, *Structured light and its applications: An introduction to phase-structured beams and nanoscale optical forces*. Academic press, 2011.

[13] A. Vaziri, et al. "Superpositions of the orbital angular momentum for applications in quantum experiments." *Journal of Optics B: Quantum and Semiclassical Optics* 4.2 (2002): S47.

[14] M. Mirhosseini, et al. "Efficient separation of the orbital angular momentum eigenstates of light." *Nature communications* 4 (2013): 2781.

[15] G.C.G. Berkhout, et al. "Efficient sorting of orbital angular momentum states of light." *Physical review letters* 105.15 (2010): 153601.

[16] J. Leach, et al. "Measuring the orbital angular momentum of a single photon." *Physical review letters* 88.25 (2002): 257901.

[17] B. Jassemnejad, et al. "Mode sorter and detector based on photon orbital angular momentum." *Optical Engineering* 47.5 (2008): 053001.

[18] J. Leach, et al. "Interferometric methods to measure orbital and spin, or the total angular momentum of a single photon." *Physical review letters* 92.1 (2004): 013601.