International Journal of Quantum Information
Vol. 10, No. 1 (2012) 1250012 (13 pages)
© World Scientific Publishing Company
DOI: 10.1142/S0219749912500128

UNBIASED QUANTUM RANDOM NUMBER GENERATION BASED ON SQUEEZED VACUUM STATE

YANYANG ZHU*, GUANGQIANG HE† and GUIHUA ZENG‡

State Key Laboratory of Advanced Optical Communication
System and Networks, Department of Electronic Engineering,
Shanghai Jiaotong University, Shanghai 200240, China
**zhuyanyang@sjtu.edu.cn*
†gqhe@sjtu.edu.cn
‡ghzeng@sjtu.edu.cn

Received 2 July 2011

In this paper, a new quantum random number generation scheme which is implemented by measuring quantum noise of the squeezed vacuum state is proposed. In the proposed scheme, the Shannon entropy is employed to measure randomness of the generated random numbers. In addition, some characteristics of the generated random numbers are investigated. To reach the pure quantum randomness, an extraction approach based on universal hash functions for the generated quantum random numbers is presented. Results show that the proposed scheme based on squeezed vacuum state has remarkable advantages over the one associated with the vacuum state.

Keywords: QRNG; squeezed vacuum state; noise entropy.

1. Introduction

Random numbers are important in many science and technology fields, such as secure communications,[1] Monte Carlo simulations,[2] cryptography[3] and authentication.[4] One recent example is the well-known quantum key distribution (QKD),[5] in which random numbers are essential for both quantum state preparation and eavesdropping detection. Unfortunately, the widely used random numbers generated by computational algorithms or arithmetical methods are totally pseudorandom. Although these pseudorandom numbers are widely used and play important roles in practices, their intrinsic demerits, i.e. the pseudo randomness, has catastrophic impacts on some applications which require true randomness. More importantly, truly random numbers are also essential in verifying some fundamental principles of physics.[6,7] Recent years, the quest for true randomness in all these applications has motivated much attentions on physical principles and technique implementations of the quantum random number generation (QRNG) based on the Heisenberg Uncertainty Principle of quantum mechanics.

An original way to realize quantum random numbers generator is associated with single photons passing through a beam splitter.[4,8–11] Some of these generators have been developed into plug and play devices that are available for commercial uses. Another promising way to obtain quantum random numbers is to measure photon numbers in weak laser pulses.[12,13] Generally, the photon-number distribution of weak laser pulses is Poissonian,[14–17] thus the parity of the observed photon numbers can be employed to generate random bits.[12] Besides, the characteristic of random appearance of photons in a pulse has also be used to generate random bits.[13] Another method to generate random numbers is to measure the quantum phase noise of a single mode semiconductor laser.[18,19] A significant advantage of this scheme is the potential high random number generation rate. In Ref. 19, a 500 Mbit/s quantum random number generator can be achieved with commercial off-the-shelf components. Apart from its high random number generation rate, the quantum randomness is also guaranteed: a photon generated by spontaneous emission has a random phase, which contributes a small random phase fluctuation to the total electric field.[20] Especially, QRNG employing the shot noise of vacuum state[21,22] has been presented. The shot noise of vacuum state is a kind of quantum noise and is thus totally random. The verifiably unique randomness, combined with its simplicity of the setup, are important attributes for obtaining high-reliability, high-speed and low cost quantum random number generators.

In this paper, a new QRNG scheme which produces quantum random numbers by excavating the quantum uncertainty of quadrature amplitudes of the squeezed vacuum state is presented. By measuring one quadrature, the quantum noise in the squeezed vacuum state is exploited to produce higher speed random number generator. Technically, two homodyne detectors are employed to measure the quantum noise of the squeezed vacuum state. The measuring results from the homodyne detectors are processed by an optimized bit conversion method to produce unbiased random numbers.

The remainder of this article is arranged as follows. A physical model for the proposed scheme is described in Sec. 2. Then, characteristics of the generated random numbers are investigated in Sec. 3. After that we present an extraction approach for quantum randomness in Sec. 4. Finally, conclusions are drawn in Sec. 5.

2. Model for QRNG Using Squeezed Vacuum State

The squeezed vacuum state can be described using the following Wigner function[23]

$$W_{sq}(x,p) = \frac{1}{\pi}\exp(-sx^2 - s^{-1}p^2), \tag{1}$$

where s is the squeezing parameter, x and p are observers of the X and P quadratures, respectively. In the squeezed vacuum state, when the vacuum noise for one quadrature is squeezed, it is anti-squeezed, i.e. amplified, for another quadrature. For example, when X quadrature is amplified then the P quadrature is squeezed, and vice versa. This property has also been demonstrated in Eq. (1). The proposed scheme assumes that the P quadrature is squeezed while the X quadrature is amplified. The amplified quantum noise for the X quadrature is used to generate random numbers. Since the Wigner function is a quasi-probability distribution,[23] the Gaussian probability function for x is given by

$$|\psi_{sq}(x)|^2 = \int_{-\infty}^{+\infty} W_{sq}(x,p)dp = \frac{\sqrt{s}}{\sqrt{\pi}}\exp(-sx^2), \tag{2}$$

where $\psi_{sq}(x)$ is the wave function of squeezed vacuum state in the X representation. Obviously, when one uses homodyne detection to measure the X quadrature of squeezed vacuum state, the measurement results forms a random variable χ which satisfies a Gaussian distribution. Making use of the obtained random variable χ one may generate a random numbers string. The approaches for generating random numbers χ will be described in the next section.

It is known that the Shannon entropy can be viewed as a measurement of randomness or unpredictability of a random variable χ.[24] In addition, a larger entropy implies a more optimal randomness for the random variable χ. In the squeezing vacuum state, the entropy of x is

$$H_{sq}(X) = -\int_{-\infty}^{+\infty} |\psi_{sq}(x)|^2 \log|\psi_{sq}(x)|^2 dx = \frac{1}{2}\log\frac{\pi}{s} + \frac{1}{2\ln 2}. \tag{3}$$

Consider that the P quadrature is squeezed and the X quadrature is amplified, the squeezing parameter s should meet the following condition, i.e.

$$0 < s < 1. \tag{4}$$

Clearly, entropy of the squeezed vacuum state is larger than that of the vacuum state in which $s = 1$. This means that the squeezed vacuum state has greater randomness than the schemes presented in Refs. 21 and 22 where vacuum state is employed. In addition, Eq. (3) demonstrates that a smaller squeezing factor will give a better quantum random numbers string. This characteristic will be described in detail in the next section.

According to the QRNG scheme proposed above, a schematic setup of the proposed scheme is shown in Fig. 1. A local oscillator (LO) is generated by a continuous-wave fiber laser source. The squeezed vacuum state can be generated by applying the unitary squeeze operator on vacuum state,[25,26] the unitary squeeze operator can be described by Eq. (5)

$$S(s) = \exp\left(\frac{1}{2}s\hat{a}^2 - \frac{1}{2}s\hat{a}^{+2}\right), \tag{5}$$

where s is the squeezing factor, which depends on nonlinear susceptibility of nonlinear optical crystal such as KTP, and amplitude of pump beam. A diagram of the

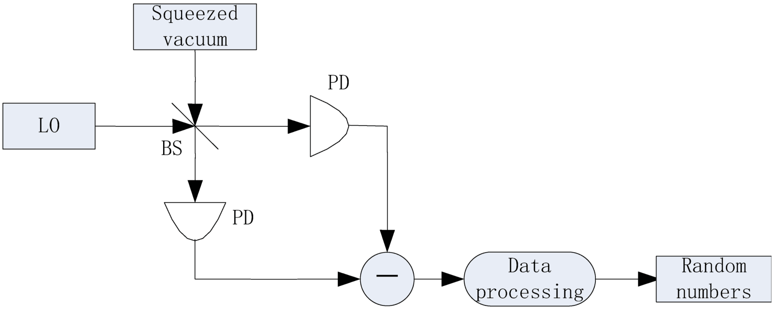


Fig. 1. Schematic setup for QRNG based on squeezed vacuum state by using the homodyne detection. The setup consists of a laser source generating a local oscillator (LO), a beamsplitter (BS) and two balanced detectors. After the subtracting operation the data is processed using encoding and unbiasing algorithms to generate unbiased random numbers.

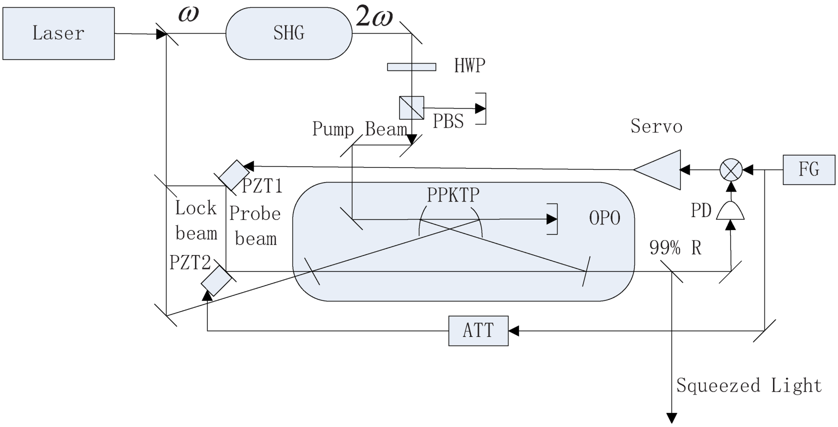


Fig. 2. Schematic setup of squeezed vacuum state. SHG: second harmonic generator, OPO: optical parametric oscillator, PPKTP: pericdically poled KTiOPO4 crystal, PD: photo detector, ATT: electrical attenuator, Servo: servo amplifier circuit for feed-back system, PZTs: piezoelectric transducers, ⊗: mixing circuit (multiplier).

squeezed vacuum state is shown in Fig. 2. The LO interferes with the signal from the squeezed vacuum state in the BS and then two outputs are measured with two intensity detectors with carefully balanced amplifications, and the resulting electrical currents are digitized, subtracted and stored. After the subtracting operation, the LO's impacts on the electrical currents are removed, so the difference current is proportional to the quadrature amplitudes of the squeezed vacuum state. Consequently, measurement outputs are obtained from the system. To improve the random number generation rate remarkably, the obtained measurement outputs are divided into many bins. Each bin is encoded into n bits with $n > 1$ by making use of an encoding algorithm. There are probably some unavoidable bias in the raw bits. In order to remove these biases, a simple unbiasing method is employed. The encoding for n and unbiasing approaches will be described in detail in the next section. After these operations, unbiased random numbers can be obtained from the stored results processed by the encoding and unbiasing algorithms in the data processing stage.

A remarkable feature of the proposed QRNG scheme should be noted, that the generated random-number string is independent of the LO signal source since this signal will be removed in the balanced homodyne measurement. Therefore, noise carried by the LO signal may be ignored in principle.

3. Characteristics of Generated Random Numbers

The randomness and the generation rate of the random-number string are very important characteristics for an obtained random-number string in practice. In this section we investigate the unbiasing property and influences of the parameters n and the squeezing factor s on the generated quantum random-number string.

Clearly, measurement outcomes are associated with the quantum noise and classic noise. Let $|\psi(x)|^2$ be the probability distribution of the measurement outcomes, then one obtains

$$|\psi(x)|^2 = |\psi_{sq}(x)|^2 + |\psi_c(x)|^2, \tag{6}$$

where $|\psi_{sq}(x)|^2$ and $|\psi_c(x)|^2$ are the probability distributions of the amplitudes originated from quantum noise and classic noise, respectively. Without loss of generality, we assume that both quantum noise and classic noise follows the Gaussian distributions in the proposed scheme. This way has also been adopted in Refs. 21 and 22.

3.1. *Bias removal*[22]

Unbiasedness is an important characteristic of the generated random numbers. This characteristic will influence the randomness of the random numbers. Generally, an arbitrated bit in a true random numbers string must be unbiased.

To obtain unbiased random numbers from measuring outputs of homodyne detectors, we divide the measurement outcomes into bins so that the integrated probabilities of the measurement outcomes to be found in each bin are equal, i.e.

$$p_1 = \cdots = p_i = \cdots = p_{l+1}, \quad i = 2, 3, \ldots, l \tag{7}$$

where

$$\begin{cases} p_1 = \displaystyle\int_{-\infty}^{x_1} |\psi(x)|^2 dx, \\ p_i = \displaystyle\int_{x_{i-1}}^{x_i} |\psi(x)|^2 dx, \qquad i = 2, 3, \ldots, l, \\ p_{l+1} = \displaystyle\int_{x_l}^{+\infty} |\psi(x)|^2 dx, \end{cases} \tag{8}$$

$l+1$ is the number of bins, and p_i is the probability of finding a measurement outcome in ith bin of the probability distribution of the measurement outcomes. Each bin is assigned a bit sequence with fixed length n to represent the measurement outputs from the homodyne detectors. Since the probability of each bin is equal, the probability of each fixed bit sequence assigned to each bin is also equal as a result. Consequently, the probability of bit "1" and bit "0" is equal. Accordingly, the generated random numbers is unbiased.

Since the Wigner function is given in Eq. (2), to ensure Eq. (7) be satisfied, two parameters, i.e. the bin positions x_i with $i = 1, 2, \ldots, l$ and the bin number $l+1$, should be obtained. Firstly, we consider how to calculate the appropriate bin positions x_i. The number of bins depends on length of the bit sequence n,

$$l + 1 = 2^n, \tag{9}$$

where n is the length of the bit sequence for each sample output. Making use of Eqs. (7) and (9) yields,

$$p_i = \frac{1}{2^n}, \quad i = 1, 2, \ldots, l, \tag{10}$$

since

$$\begin{aligned} \int_{-\infty}^{x_i} |\psi(x)|^2 dx &= \int_{x_{i-1}}^{x_i} |\psi(x)|^2 dx + \int_{x_{i-2}}^{x_{i-1}} |\psi(x)|^2 dx \\ &\quad + \cdots + \int_{-\infty}^{x_1} |\psi(x)|^2 dx \\ &= p_i + p_{i-1} + \cdots + p_1 = \frac{i}{2^n}, \end{aligned} \tag{11}$$

with $i = 1, 2, \ldots, l$, Eq. (8) can be written in a uniform way as following,

$$\frac{i}{2^n} = \int_{-\infty}^{x_i} |\psi(x)|^2 dx. \tag{12}$$

Thus, the positions x_i can be calculated out using Eq. (12) for a fixed n.

Figure 2 is a binning example for $n = 3$ and $l + 1 = 2^n = 8$. Since n is associated with the Shannon entropy, a detail description on this parameter will be presented in next section.

3.2. *Optimal bit sequence length n*

As described above, proper bin number $l+1$ and l bin positions x_i may lead an unbiased random numbers string. In applications, the generation rate of random numbers string is also an important parameter. In the proposed scheme, the generation rate is associated with length of the bit sequence n for each sample output. Consequently, the bit sequence n is very important in the proposed QRNG scheme. In the following the influence of n on the generation rate and the data processing is discussed in detail, and a method for choosing an appropriate n is proposed.

Let $H_t(X)$ be the total Shannon entropy of the bit sequences. Generally, the total entropy $H_t(X)$ contains both the entropy $H_q(X)$ originated from the quantum noise and the entropy $H_c(X)$ from the classical noises, such as the electronic noise and LO noise due to imperfect balancing. Then the entropy of the quantum noise can be calculated by

$$H_q(X) = H_t(X) - H_c(X), \tag{13}$$

with

$$H_t(X) = -\sum_{i=1}^{l+1} p_i \log_2 p_i, \tag{14}$$

where p_i is defined in Eq. (10). For convenience, $H_q(X)$ is called as quantum noise entropy in the follows. One may easily obtain $H_t(X) = n$. While the entropy of the classic noise can be obtained in a similar way. Let p_i' be the probability for each measurement outputs of the classic noise in each bin. Then, the entropy of the classic noise can be easily calculated out using the following way,

$$H_c(X) = -\sum_{i=1}^{l+1} p_i' \log_2 p_i', \tag{15}$$

where

$$p_i' = \int_{-\infty}^{x_i} |\psi_c(x)|^2 dx - \int_{-\infty}^{x_{i-1}} |\psi_c(x)|^2 dx, \tag{16}$$

with $i = 1, 2, \ldots, l$ and x_i given by Eq. (12). Combining Eqs. (13), (14) and (15) gives

$$H_q(X) = n + \sum_{i=1}^{2^n} p_i' \log_2 p_i'. \tag{17}$$

Clearly, $H_q(X)$ is a function of n. Accordingly, we have a formal expression as following,

$$H_q(X) = f(n). \tag{18}$$

Generally, one may get the relationship between the quantum noise entropy and the bit sequence length n. However, the theoretically expression is difficult to obtain from the above equation for the reason that the x_i cannot be theoretically calculated out from Eq. (12) since $\int_{-\infty}^{x_i} |\psi(x)|^2 dx$ is a complementary error function. Therefore a numerical simulation way is presented in the following. The aim is to propose an available encoding algorithm for how to choose an optimal bit sequence length n.

Now we move to design an encoding algorithm for choosing an optimal bit sequence n. Equation (17) suggests that the quantum noise entropy $H_q(X)$ is associated with the bit sequence length n. Suppose that the optimal bit sequence is

n_o, then Eq. (18) gives $\hat{H}_q(X) = f(n_o)$, where $\hat{H}_q(X)$ is the quantum noise entropy which corresponds to the optimal bit sequence length n. Consider that the bit sequence length n is determined by the encoding algorithm, to obtain finally a high speed random-number string an optimal encoding algorithm which gives appropriate bit sequence length, i.e. the optimal n_o should be employed in the data processing phase. Clearly, if the chosen n is too small, i.e. $n < n_o$, the used quantum noise entropy $H_q(X)$ is smaller than the actually quantum noise entropy $\hat{H}_q(X)$ provided by the system. Consequently, the quantum noise is not employed completely and some of are wasted. However, if n is too big, i.e. $n > n_o$, the complexity of the encoding algorithm will immensely increase since a larger n can only generate an entropy $\hat{H}_q(X)$ while the generated bits string in the data processing phase will become much larger. While the additional bits $\Delta n = n - n_o$ are not useful. Therefore, a proper n is very important in the proposed system.

For clarity, an example is presented using numerical simulation. In the simulation the mean of the signal (i.e. quantum noise) and classic noise are both 0 and the SNR is 25dB,[22] and a squeezing vacuum state with the squeezing parameter $s = 1/10$ is adopted. According to Eq. (17), the simulation results are depicted in Fig. 3. Dependencies of the total entropy and the classic noise entropy on the bit sequence n are plotted in Fig. 4(a) and the entropy of the signal, i.e. the quantum noise, is demonstrated in Fig. 4(b). Figure 4 shows that there is a knee point in the quantum noise entropy. After the knee point, the quantum noise entropy becomes almost a constant, and the total increased entropy almost comes from the contribution of classic noise. This means that a larger n is not useful to employ the quantum noise entropy $H_q(X)$ after the knee point. Thus, we only need to choose the smallest n after the knee point as the length of the bit sequence for each measurement outcome bin. In this situation, almost all the entropy originated from quantum noise has been exploited to generate the true random numbers, while the complexity of the data processing is minimized. From Fig. 4, one may easy obtain the most proper value of n is $n = 6$, the corresponding quantum noise entropy obtained from the system is

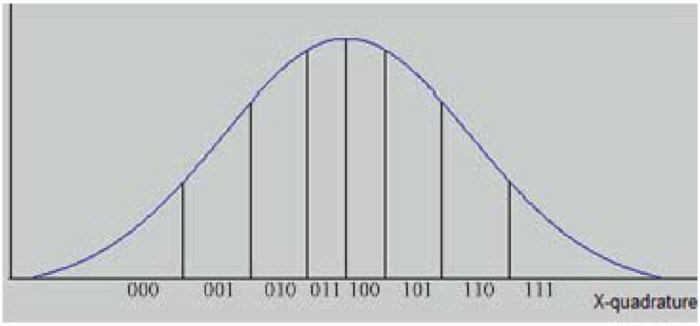


Fig. 3. The binning of the probability distribution of the sample measurement outcomes for $n = 3$. The random numbers are then produced by assigning a fixed bit sequence of length n to each sample output in a certain bin.

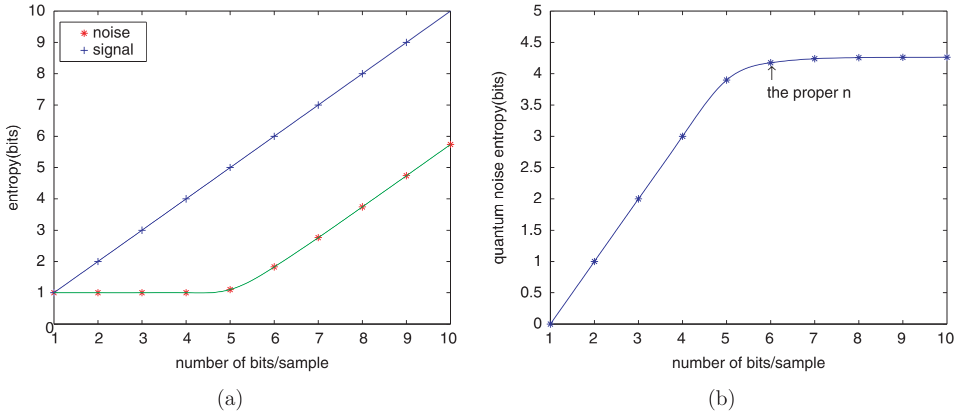


Fig. 4. Total entropy, classic noise entropy and quantum entropy for different binnings when $s = 1/10$. (a) The total entropy and the entropy of the classic noise for different binnings (different number of bits n per sample). (b) Quantum noise entropy achieved for different binnings (different number of bits n per sample).

4.26 bits. While the number of binnings is $l + 1 = 2^n = 64$ as a result. In addition, the classic noise entropy is 1.74 bits which should be removed. Clearly, not only most of the entropy originated from quantum noise has been exploited to generate random numbers, but also the increasing complexity of the data processing for an unnecessary larger n is avoided.

3.3. *Influences of squeezing parameter s*

Equations (2) and (3) show that both the probability distribution function $|\psi_{sq}(x)|^2$ and the quantum noise entropy $H_q(X)$ depend on the squeezing parameter s. Thus, the encoding algorithm is associated with this parameter. Consequently, the generation rate of the final random-number string depends on the squeezing parameter s of the squeezing vacuum state. In this subsection we investigate the influence of the squeezing parameter s on the generated random-number string.

In the proposed QRNG scheme, the squeezing parameter s should satisfy Eq. (4). In this scenario, the quantum noise in the P quadrature is transferred to be the quantum noise in the X quadrature, which is the measuring object of our system. So the quantum noise can be fully used to generate true random numbers. Consequently, when the quantum noise of the system is measured, the quantum noise entropy that one may obtain in squeezed vacuum state is more than that in common vacuum state. This is just a comparison between QRNG based on squeezed vacuum state in which s satisfies Eq. (4) and QRNG based on vacuum state in which $s = 1$. To clearly show the influence of the squeezing parameter s on the proposed system, the relationship between the quantum noise entropy and the squeezing parameter s is depicted in Fig. 5. It demonstrates that the quantum noise entropy decreases with increasing of the squeezing parameter s. Consequently, the random number generation rate decreases with the increasing of squeezing parameter s.

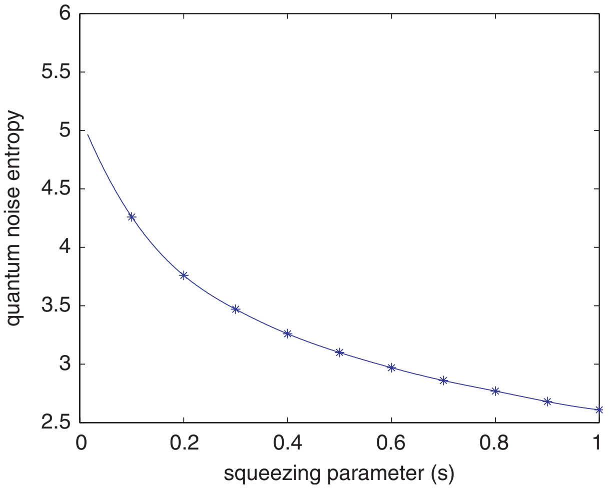
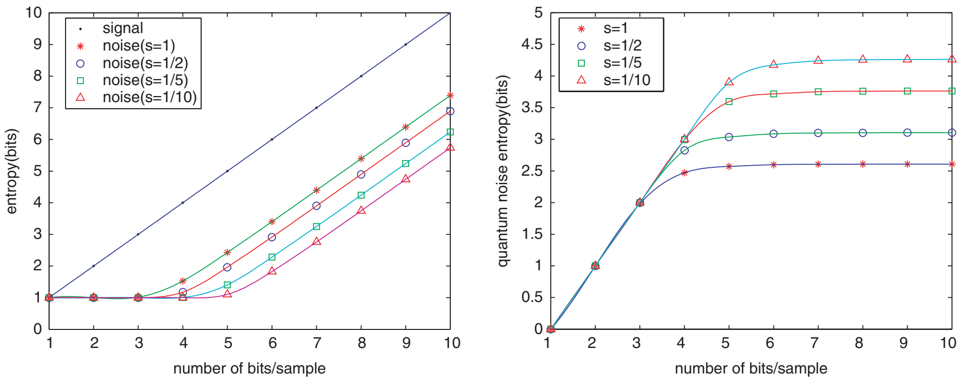


Fig. 5. Quantum noise entropy obtained for different squeezing parameter s.

In order to clearly show the influence of s on the random-number string, especially the generation rate, the total entropy, classic noise entropy and the quantum noise entropy obtained from the system with different squeezing parameter s are depicted in Fig. 6. From Fig. 6, we also find that the quantum noise entropy is closely related to the squeezing parameter s. That is, more quantum noise entropy can be obtained from the system with a smaller s. For example, when $s = 1$, $1/2, 1/5, 1/10$, the obtained quantum noise entropies are 2.61 bits, 3.10 bits, 3.76 bits, 4.26 bits, respectively, and the corresponding optimal bit sequence lengths n are 4, 5, 6 and 6, respectively. We note in Fig. 6 that a smaller squeezing



(a) (b)

Fig. 6. Influence of squeezing parameter s on the entropy of the system for different binnings. (a) The total entropy and the entropy of the classic noise for different squeezing parameter s and different binnings (different number of bits n per sample). (b) Quantum noise entropy achieved for different binnings (different number of bits n per sample).

parameter s will benefit the generated quantum random number string, e.g. the generation rate. Of course, when s becomes smaller the experimental implementation becomes more difficult. In addition, Fig. 6 demonstrates that a very small s can only play a slight role on the bit sequence lengths n. For example, above calculations have shown that the optimal bit sequence lengths n are 6 and about 6 when $s = 1/5$ and $1/10$, respectively. Thus we suggest to choose a proper squeezing parameter s in the experiment. From the numerical simulation, we note that 2.61 bits quantum noise entropy can be obtained from the system with parameter $s = 1$ (this is the vacuum state), while from the system with squeezing parameter $s = 1/10$, 4.26 bits quantum noise entropy can be obtained. In Ref. 22, the random number generation rate is 6.5 Mbps using vacuum state, hence, a random number generation rate of $\frac{4.26}{2.61} \times 6.5 = 10.6$ Mbps is achievable from the proposed system with squeezing parameter $s = 1/10$.

4. Quantum Randomness Extraction

As mentioned in the introduction, the generated true random number can be applied in many fields. In this paper, our main aim is in the well-known quantum key distribution. In this case, the security of the generated random is an important issue. Surely, if all bits in the generated string come from pure quantum effects, i.e. the squeezing vacuum state, the attacker cannot obtain any useful information. However, classic noises such as the electric noises are inevitable in the proposed system. Since all classical noise could in principle be known by an adversary or an adversary may be able to control at least some of these sources of classic noise, the contribution from the classic noise should be removed. Otherwise, the generated quantum random-number string might be insecure.

Actually, the classic noise entropy $H_c(X)$ has been removed, in principle, in the encoding algorithm for bit sequence n. This has been described in detail in Sec. 3.2. To further remove the classic correlation which may be revealed slight partial information to the adversary, one may employ the quantum randomness extraction techniques. The quantum randomness extraction may be implemented using a quantum randomness extractor. Assume that a bit sequence $X_1, \ldots, X_n$ is the input of the extractor, the extractor considers successive pairs X_{2i},X_{2i+1}. For each pair, if $X_{2i} \neq X_{2i+1}$ then X_{2i} is sent to the output, otherwise nothing is sent. Another mostly used method is the hashing function, which is called the entropy smoothing[22] by hashing. Because the amount of quantum-mechanical entropy contained in the raw data is known, a suitably chosen one-way function can be applied to project these data onto a shorter set for which the length is determined by this amount of entropy. A simple and efficient randomness extractor based on complexity theory[27] is proved that it works for all sources of sufficiently high-entropy, even if individual bits in the source are correlated. The following is the model of such a random extractor. Firstly, choose a string $s \in \{0,1\}^{\ell+m-1}$ at random, and then calculate out the m bits, with the ith bit decided by $\oplus_{j=0}^{\ell}(x_i \oplus s_{i+j})$, where ℓ is the length (in bits) of each sample from the high-entropy source, m is the length (in bits) of the output of the randomness extractor, and x is the raw random bits generated from the high-entropy source.

All these approaches may be applied in the proposed scheme. But here we would like to employ the privacy amplification technique to distill a private random-number string. The privacy amplification is an important ingredient in the quantum key distribution procedures. Then, the security analysis of the generated random numbers can be processed in a unified way with the involved quantum key distribution system. In this situation, the key technique relies on choice of universal hash function. An intuitive way is to use the XOR operation as the randomness extractor which has been applied in the one-time pad, quantum key distribution, and the other random-number generation approaches. Here would like to adopt the following way. Let $\mathscr{A} = GF(2^l)$ and $\mathscr{B} = \{0,1\}^k$. Define $h_c(x)$ as the first k bits of the product cx in a polynomial representation of $GF(2^l)$. It has been proven that the set $\mathscr{H}_{\mathscr{A}\to\mathscr{B}} = \{h_c : c \in GF(2^l)\}$ is a universal class of hash functions. Therefore we may use this universal class of hash functions to remove the slight partial information obtained by the attacker. Let x be the input bits which has been obtained in the data processing procedure in the proposed system, then the output $h_c(x)$ is the final bit string.

With the help of such a randomness extractor, the classic correlation has been removed completely so that only the quantum noise plays role for the final random-number generation. The security is guaranteed even if an adversary has some influences on the source. Actually, the final random-number string has the same security as the BB84 QKD scheme since universal class of hash functions have been employed. The analysis approach is the same as that in the privacy amplification procedures of the QKD scheme. Since the privacy amplification technique has been investigated widely, we here do not describe it again. In application, when the generated random-number string is employed to a secure communication, the attacker cannot get any available information.

5. Conclusions

A new quantum random number generation scheme which employs the quantum properties of the squeezed vacuum state is proposed in this paper. To generate unbias and high speed quantum random-number string, an unbiasing approach and an encoding algorithm for choosing the bit sequence length are presented based on the information theory. In addition, the influence of the squeezing parameter on the generated random-number string is also investigated, we find that the smaller s will benefit the proposed system. To remove the classic correlation so that the generated random-number string is secure, the randomness extractor based on universal class of hash functions is suggested for the proposed quantum random number generation scheme. Results demonstrate that the proposed scheme may obtain higher speed random-number string than the scheme based on vacuum state, and the final random-number string has the same security as the QKD scheme.

Acknowledgment

This work was supported by the National Natural Science Foundation of China (Grant Nos. 61102053, 61170228, 60970109, and 60801051).

References

1. D. R. Stinson, *Cryptography: Theory and Practice* (CRC Press, 1995).
2. N. Metropolis and S. Ulam, *J. Am. Stat. Assoc.* **44** (1949) 335.
3. A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography* (CRC, 1997).
4. id Quantique, Random Number Generation using Quantum Physics, August 2004.
5. G. Zeng, *Quantum Private Communication* (Springer-Verlag, Berlin, 2010), pp. 112−117.
6. G. Weihs, T. Jennewein, C. Simon, H. Weinfurter and A. Zeilinger, *Phys. Rev. Lett.* **81** (1998) 5039.
7. V. Jacques, E. Wu, F. Grosshans, F. Treussart, P. Grangier, A. Aspect and J.-F. Roch, *Science* **315** (2007) 966.
8. A. Stefanov, N. Gisin, L. Guinnard and H. Zbinden, *J. Mod. Opt.* **47** (2000) 595.
9. T. Jennewin, U. Achleitner, G. Weihs, H. Weinfurter and A. Zeilinger, *Rev. Sci. Instrum.* **71** (2004) 1675.
10. P. Wang, G. Long and Y. Li, *J. Appl. Phys.* **100** (2006) 056107-1.
11. T. Jennewein *et al.*, arXiv: quant-ph/9912118v1.
12. M. Furst *et al.*, *Quant. Cryptography* 270.5568 (2010).
13. W. Wei and H. Guo, Quantum random number generator based on the photon number decision of weak laser pulses, in *Conf. Lasers and Electro-Optics, PACIFIC RLM '09*, Shangai, 2009.
14. S. Nakamura *et al.*, *Jpn. J. Appl. Phys.* **34** (1995) L1332.
15. N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, *Rev. Mod. Phys.* **74** (2002) 145.
16. R. Loudon, *The Quantum Theory of Light*, 3rd edn. (Oxford University Press, 2000).
17. R. Short and L. Mandel, *Phys. Rev. Lett.* **51** (1983) 384.
18. H. Guo *et al.*, arXiv: 0908.2893v1.
19. B. Qi *et al.*, arXiv: 0908.3351v2.
20. C. H. Henry, *IEEE J. Quantum Electron.* **QE-18** (1982) 259.
21. Y. Shen, L. Tiran and H. Zou, *Phys. Rev. A* **81** (2010) 063814.
22. C. Gabriel *et al.*, *Nature Photonics* **4** (2010) 711, doi: 10.1038/NPHOTON.2010.197.
23. U. Leonhardt, *Measuring the Quantum State of Light* (Cambridge University Press, Cambridge, 1997).
24. P. L'ecuyer, A. Compagner and J. F. Cordeau, *ACM Trans. Model. Comput. Simell.* (1997).
25. C. M. Caves, *Phys. Rev. D* **23** (1981) 1693.
26. L.-A. Wu *et al.*, *Phys. Rev. Lett.* **57** (1986) 2520.
27. B. Barak, R. Shaltiel and E. Tromer, *True Random Number Generators Secure in a Changing Environment* (Springer-Verlag, Berlin, Heidelberg, 2003).