Classical-Noise-Suppressed Quantum Random Number Generator Based On Phase Noise

Ziyang Chen, Zhengyu Li, Yulong Feng, Gan Wang, Hong Guo[*]

State Key Laboratory of Advanced Optical Communication System and Network, School of Electronics Engineering and Computer Science, and Center for Quantum Information Technology, Peking University, Beijing 100871, China.

[*] *Corresponding author: hongguo@pku.edu.cn*

Abstract: We present a random number generation scheme based on measuring the phase noise of two laser beams. Without using optical delay line, we only use electrical heterodyning system and mixer to measure the random phase fluctuation, realizing quantum random number generation with a rate of 600Mbps. The final random bit streams have passed all the DIEHARD tests. The classical noise induced by fiber jitter can be removed with the help of this 'delay-line-free' scheme. Furthermore, this scheme is comparatively suitable for on-chip integration because of its simplified optical structure.

1. Introduction

Random number generator (RNG) has wide applications in variety of fields, such as numerical simulations [1] and cryptography [2]. One recent example is quantum key distribution (QKD), in which the unconditional security of QKD is guaranteed only when a true random number generator is available, and quantum-mechanical process is used to achieve this. Over past few years, various quantum random number generator (QRNG) schemes have been proposed and demonstrated. Among them, schemes based on quantum phase fluctuation of laser, or spontaneous emission inherently, are widely adopted, and Mach-Zehnder interferometer (MZI) is used to help extract the randomness of phase fluctuation [3]. Based on this method, QRNGs with a generation rate of 5.4 Gbps [4], 68 Gbps [5] have been proposed respectively.

However, it is inevitably using optical delay line for time delay between the two arms in the MZI to ensure the time interval is longer than the coherence time of the laser. The delay line in this method may easily induce classical noise caused by fiber jitter and others. what's more, the optical delay line is difficult to integrate on-chip especially for large time delay scenario.

2. Phase Noise Based Quantum Random Number Generator scheme

To overcome the drawback above, we propose a QRNG scheme based on phase fluctuation of laser with heterodyne detection and mixer, which employs only electrical devices as the randomness readout and has the potential for com-

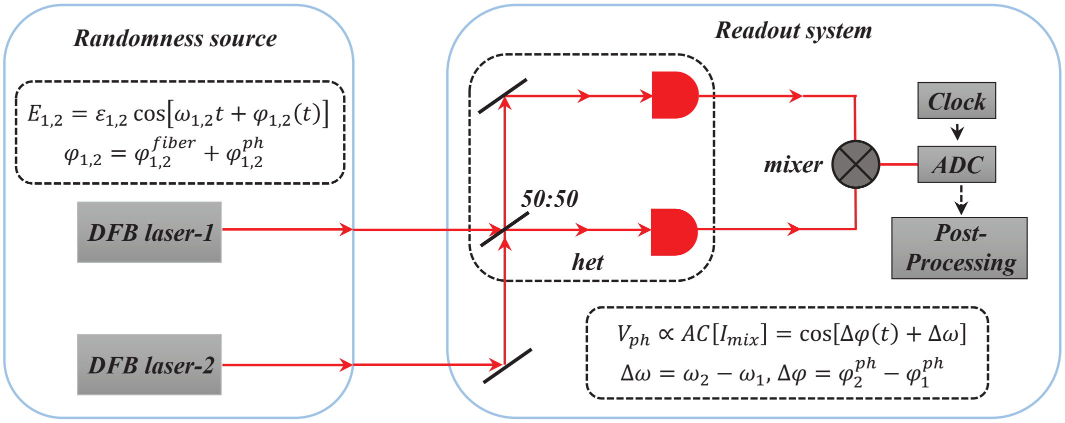
Randomness source
$E_{1,2} = \varepsilon_{1,2}\cos[\omega_{1,2}t + \varphi_{1,2}(t)]$
$\varphi_{1,2} = \varphi_{1,2}^{fiber} + \varphi_{1,2}^{ph}$
DFB laser-1
DFB laser-2
Readout system
50:50
het
mixer
Clock
ADC
Post-Processing
$V_{ph} \propto AC[I_{mix}] = \cos[\Delta\varphi(t) + \Delta\omega]$
$\Delta\omega = \omega_2 - \omega_1, \Delta\varphi = \varphi_2^{ph} - \varphi_1^{ph}$

Fig. 1. The experimental setup of phase noise based QRNG without delay line, where the mixer is used to generate the final random voltage. The 12-bit analog-to-digital conventer (ADC) is also used with the sampling rate of 100MHz

pact designs and practical applications. The experimental setup is shown in Fig. 1. Two DFB laser diodes, with the difference of center wavelength between 600-800MHz, is utilized to emit continuous-wave (CW) beams. We treat the fields of two laser beams as $E_{1(2)} = \varepsilon_{1(2)} \cos\left[\omega_{1(2)} t + \varphi_{1(2)}(t)\right]$ contain two parts, the fiber jitter part $\varphi_{1(2)}^{fiber}(t)$ and the phase noise part $\varphi_{1(2)}^{ph}(t)$. The bandwidths of two photodetectors are 1.9GHz, slightly larger than the difference of center wavelength between two laser beams. Also, the output of the two photodetectors are combined with a mixer to generate random voltage caused by the difference of two phase noise of lased beams. The function of mixer with filter is to distill the term of frequency difference that we needed, and suppress other noises. These sampled voltages are digitized by an 12-bit ADC with the sampling rate of 100MHz, and we take the least-significant bit (LSB) by post-processing to obtain the final random bit with 6-bit in each sample. The generation rate can reach 600Mbps in total and the final random bit streams have passed all the DIEHARD tests.

Acknowledgement

This work is supported by the National Science Fund for Distinguished Young Scholars of China (Grant No. 61225003), the State Key Project of National Natural Science Foundation of China (Grant No. 61531003).

References

[1] N. Metropolis and S. Ulam, “The Monte Carlo method,” J. Am. Stat. Assoc. 44(247), 335C341 (1949).

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” Rev. Mod. Phys. 74(1), 145C195 (2002).

[3] H. Zhou, X. Yuan, and X. Ma, “Randomness generation based on spontaneous emissions of lasers,” Phy. Rev. A. **91**, 062316 (2015).

[4] J. Yang, J. Liu, Q. Su, Z. Li, F. Fan, B. Xu, and H. Guo, “5.4 Gbps real time quantum random number generator with simple implementation,” Opt. Express. 24(24), 27475C27481 (2016).

[5] X. G. Zhang, Y. Q. Nie, H. Zhou, H. Liang, X. Ma, J. Zhang, and J. W. Pan, “68 Gbps quantum random number generation by measuring laser phase fluctuations,” Rev. Sci. Instrum. 86(6), 063105 (2015).