A 5.4 Gbps real time quantum random number generator with simple implementation

JIE YANG,[1] FAN FAN,[1] QI SU,[2] JINLU LIU,[1] BINGJIE XU[1,*]

[1]*Science and Technology on Security Communication Laboratory, Institute of Southwestern Communication,*
Chengdu 610041, China
[2]*State Key Laboratory of Cryptology, Beijing 100878, China*
*e-mail: *xbjpku@pku.edu.cn*

***Abstract*—A new QRNG scheme based on measuring the quantum phase noise with a simple and cost effective implementation is proposed. A simple theoretical model is established to analyze the randomness and the simulation result based on this model fits well with the experiment data. After real time postprocessing, the final random bit sequences with a generation rate of 5.4 Gbps are achieved and have passed all the NIST and DIEHARD tests.**

I. INTRODUCTION

Random numbers play a key role in many fields of science and technology, such as numerical simulations, lottery games and cryptography. Classical pseudo random number generators (PRNGs) based on computational algorithms have been widely studied and used, but are not suitable for certain applications where true randomness is required due to the deterministic features of the algorithms. Distinct from the PRNGs, the true random number generators (TRNGs) rely on the randomness of physical processes. An important type of the TRNGs is the quantum random number generator (QRNG), which is based on the intrinsic randomness of fundamental quantum processes to guarantee the true randomness. Over the past two decades, various QRNG schemes have been proposed and demonstrated [1].

In this paper, based on the scheme of quantum phase fluctuations, a 5.4 Gbps real time QRNG with a simple and cost effective implementation is demonstrated, which employs only one beam splitter (BS) and has the potential for compact designs for practical applications.

II. EXPERIMENTAL SETUP AND SYSTEM MODEL

Experimental setup of the proposed QRNG is shown in Fig. 1(a). A DFB laser diode with a center wavelength of 1550.12nm is driven to emit continuous-wave (CW) beams. The laser diode is operated around the threshold to maximize the quantum phase noise due to spontaneous emission. The CW beams are split into two paths by a 2×2 50/50 polarization-maintaining beam splitter (BS). One of the output ports is directly coupled into a 1.8 GHz photo-detector (PD). The other is coupled into the delay loop, which consists of the BS and a 4m delay line (DL). The output from the PD can be either acquired by a DSO to analyze the distribution and the optimal performance of the raw data or be processed by an ADC and a randomness-extractor to distill the final random bits in real time.

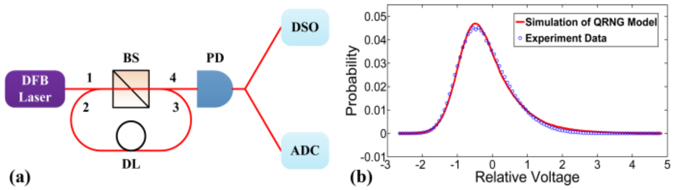

Fig.1. (a) The Experimental setup of the proposed QRNG. (b) The normalized distribution of the simulation result of the theoretical model for the proposed QRNG and the experimental measured interference intensity.

We derive the analytical expressions of the detected signals, which is given by

$$I=\frac{1}{2}A^2\sum_{k=0}^{N}\left(\frac{\beta}{2}\right)^k+A^2\sum_{k=1}^{N}\left(\frac{\beta}{2}\right)^{\frac{k}{2}}\left(-\cos\left(k\omega\Delta t+\Delta\varphi_N^k\right)\right)+ \\ A^2\sum_{k=1}^{N}\left(\frac{\beta}{2}\right)^{\frac{k}{2}}\left(\sum_{j=1}^{k-1}\left(\frac{\beta}{2}\right)^{\frac{j}{2}}\cos\left[(k-j)\omega\Delta t+\Delta\varphi_{N-j}^{k-j}\right]\right) \tag{1}$$

where A is the amplitude of electric field, ω is the optical center angular frequency, and $\varphi(t)$ is the phase of the laser, β is the overall effective gain of the components in the fiber loop, Δt is the time delay induced by DL, j and k are integers, $k\in[1,N]$, $j\in[1,k)$ and $\Delta\varphi_N^k=\varphi(N\Delta t)-\varphi((N-k)\Delta t)$ is the phase fluctuation between *N*-th order circulation and *N*-*k*-th circulation laser beam. $\Delta\varphi_N^k$ is a Gaussian random variable due to spontaneous emission [2], and therefore *I*, which is a superposition of $\Delta\varphi_N^k$, can be quantified to random bits. The simulation result is shown in Fig. 1(b), which fits well with the experimental measured data acquired by the DSO.

III. MEASUREMENT RESULTS

The measurement in the frequency domain is performed by using an RF spectrum analyzer. Fig. 2(a) shows that the phase fluctuations dominate the output of the PD in terms of the power and hence the randomness is guaranteed.

To analyze the optimal performance of the scheme, the raw data acquired by a high speed DSO is post processed with the Toeplitz-matrix hash function, achieving final random bit sequences with an offline generation rate of 117 Gbps [3]. To acquire the random bit sequences in real time, we employ a 12bit-ADC with a sampling rate of 1.8 GSps to sample the raw output. The bitwise XOR operation and 6-least-significant-bit

(6-LSB) procedure are employed for randomness extraction, which is integrated in a field programmable gate array (FPGA) for real time processing, yielding a 5.4 Gbps quantum random bit generation rate in real time [4].

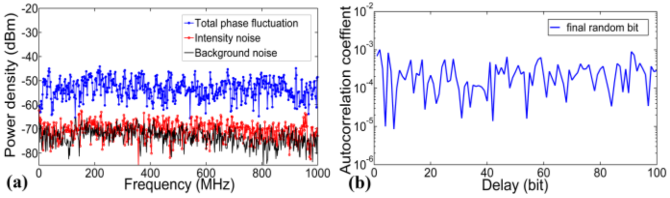

Fig.2 (a) Noise spectra. The spectral density of total phase fluctuation (blue), intensity noise (red), and background noise (black).. (b) Autocorrelation analysis of 10^7 extracted random bits after XOR operation and 6-LSB procedure within 100 bit delay. The average value is 1.68×10^{-5} .

In order to verify the randomness of the final sequences extracted in real time, firstly the autocorrelations within 100 bit-delay are calculated, shown in Fig 2(b), indicating good randomness. Then we applied two test batteries, the NIST-STS and Diehard, the final random bit sequences have passed both tests.

REFERENCES

[1] M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," arXiv:1604.03304v1, 2016.

[2] K. Vahala, and A. Yariv, "Occupation fluctuation noise: A fundamental source of linewidth broadening in semiconductor lasers," Appl. Phys. Lett. 43, 140 (1983).

[3] L. J. Lu, J. Yang, Z. Y. Li, Q. Su, W. Huang, B. J. Xu and H. Guo, "117 Gbits/s quantum random number generation with simple structure", Photonics Technol. Lett. 29(3), 283–286 (2017).

[4] J. Yang, L. J. Lu, Q. Su, Z. Y. Li, F. Fan, B. J. Xu and H. Guo, "5.4 Gbps real time quantum random number generator with simple implementation", Opt. Express 24(26), 27475-27481 (2016).