# A Quantum random number generator integrated into a transmitter of BB84 QKD system

Weiyang Zhang[1]* Akihisa Tomita[1] Kuzuhisa Ogawa[1] and Atsushi Okamoto[1]

1.Graduate School of Information Science and Technology, Hokkaido University, Japan

*Email: zhangweiyangjida@yahoo.co.jp

**Abstract** We propose a simple construction of a quantum random number generator (QRNG) by adding only a few devices to a time-bin BB84 QKD transmitter. This QRNG can be integrated into QKD system and supply random numbers with high generation rate. We implemented experimental set up of QRNG and use randomness extraction and post-processing analysis to generate the random number bits which passed random number test successfully. This integrated QRNG also provides a method of on-line investigation on the interpulse phase randomness for implementation security certification by testing the quality of generated random numbers.

**Keywords** QRNG, BB84 QKD, randomness extraction, phase randomness

## 1. Introduction

As the new generation cryptography, quantum key distribution (QKD) requires reliable random number generation. Unlike pseudo-RNG based on computational algorithms, QRNG has true randomness obtained via quantum process. For example, phase randomized optical pulses from a gain-switch DFB laser diode have been utilized to provide high speed random number generation [1][2], where the randomness originated from the spontaneous emission. However, production cost and equipment size are increased, because an extra light source and interferometer are required in these proposals. Here, we propose a QRNG sharing a light source and interferometer with a transmitter of a time-bin BB84 QKD system.

## 2. System configuration

As shown in Fig.1, our QRNG shares the LD and Asymmetrical Mach-Zehnder interferometer (AMZI) with the QKD system. We connect a Faraday mirror (FM) to an idle output port and a high-speed photodetector (PD) to an idle input port. Since the time difference generated in the AMZI is set to the half of pulse interval from the LD, the reflected pulse can interfere with the adjacent pulse at the input beam splitter of the AMZI and generate random interference signal

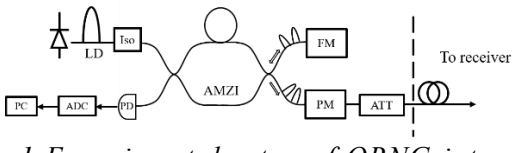


*Fig. 1 Experimental setup of QRNG integrated into transmitter in BB84 QKD system.*

intensities. To avoid the back reflection into the laser cavity, an isolator (Iso) is placed. An analog to digital converter (ADC) with 12 bits resolution and 5.4 GS/s sampling rate were used to extract random bits from random interference intensities.

Since the phase randomness from LD depends on operating condition [3]. We optimized laser operating condition to maximize the randomness of raw data. The optimal Min-entropy of 7.9bits per pulse was obtained with 625MHz clock frequency, which is smaller than the ADC resolution, because signal pulse does not obey the ideal arcsine distribution under the influence of an electrical noise and the limited dynamic range of PD and ADC. Nevertheless, the theoretical generation rate is exceeded the required rate, 5 bits per pulse for a two-decoy BB84 transmitter. We implemented the extraction method (Toeplitz-hashing matrix) in PC and generated random numbers passing random number test successfully. This construction of the QRNG will reduce the production cost and footprint of equipment, pave the way to the social deployment of QKD.

**Acknowledgement**

This work is partly supported by SIP “Photonics and Quantum Technology for Society 5.0”, GSB Hokkaido Univ, and JSPS KAKENHI18H05237.

**References**

[1] F. Xu, *et al.*, Opt. Express **20**(11), 12366-12377, 2012.

[2] C. Abellán, *et al.*, Opt. Express **22**(2), 1645-1654, 2014.

[3] T. Kobayashi, *et al.*, Phys. Rev. A. **90**, 03232, 2014.