Contribution ID: **764** Type: **Oral (Student, Not in Competition) / Orale (Étudiant(e), pas dans la compétition)**

True Random Number Generation based on Interference between Two Independent Lasers

Tuesday 16 June 2015 10:00 (15 minutes)

Reliable true random number generation is essential for information theoretic security in a quantum cryptographic system based on quantum key distribution (QKD) and one-time pad encryption [1]. Various random number generation methods have already been proposed and demonstrated, such as schemes based on the detection of single photons [2], whose rate is limited by the dead time of single photon detectors. Alternative approaches are based on the chaotic light emission from a semiconductor laser [3, 4]. In this talk we propose and demonstrate a novel scheme to generate random numbers based on interference between two independent lasers, i.e. a continuous wave (CW) laser and a gain-switched pulsed laser, each emitting light at around 1550 nm wavelength. The physical basis of our random number generator is the randomness of the phase difference between light emitted from the two independent lasers. Using only off-the-shelf components, we achieve a random number generation rate of 250 MHz. The properties of the generated random numbers are tested using National Institute Standards and Technology (NIST) statistical test suite. We also discuss the extension of our methods from random bits to randomly selected symbols with more than two different values.

References

[1] N. Gisin, and R. Thew, "Quantum communication,"Nature Photon. 1, 165 (2007).

[2] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, "Optical quantum random number generator,"J. Mod. Opt. 47, 595 (2000).

[3] T. Symul, S. M. Assad, and P. K. Lam, "Real time demonstration of high bitrate quantum random number generation with coherent laser light,"Appl. Phys. Lett. 98, 231103 (2011).

[4] A. Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kuashige, M. Shiki, S. Yoshimori, K. Yoshimura, and P. Davis, "Fast physical random bit generation with chaotic semiconductor lasers,"Nature Photon. 2, 728 (2008).

Author: JOHN, Caleb (University of Calgary)

Co-authors: Dr ZHOU, Qiang (Institute for Quantum Science and Technology, University of Calgary); Mr VALIVARTHI, Raju (Institute for Quantum Science and Technology, University of Calgary); Dr TITTEL, Wolfgang (Institute for Quantum Science and Technology, University of Calgary)

Presenter: JOHN, Caleb (University of Calgary)

Session Classification: T1-10 THz science and applications (DAMOPC) / Sciences et applications des THz (DPAMPC)

Track Classification: Division of Atomic, Molecular and Optical Physics, Canada / Division de la physique atomique, moléculaire et photonique, Canada (DAMOPC-DPAMPC)