# Demonstration of quantum cipher communication using quadrature amplitude modulation technologies over 100 km optical fiber

Takuya Hirano[1], Ryo Namiki[1], Motoharu Ono[1], Tsubasa Ichikawa[1],
Masato Yoshida[2], Toshihiko Hirooka[2], Keisuke Kasai[2], and Masataka Nakazawa[2]

[1] Department of Physics, Gakushuin University
[2] Research Institute of Electrical Communication, Tohoku University

We report a hybrid secure communication of continuous-variable quantum key distribution (CV-QKD) and quadrature amplitude modulation/quantum noise stream cipher (QAM/QNSC). In QAM/QNSC a coherent multi-level optical signal is hidden in quantum noise. We demonstrated 70 Gbit/s on-line QAM/QNSC transmission over 100 km using an FPGA-based transmission and receiver, where secure keys are delivered by a CV-QKD system. In the security analysis, we adopt a realistic assumption that an eavesdropper does not have a lossless fiber. This hybrid system is highly compatible with commercial optical communication system, will contribute to realize high capacity and secure communication.

Coherent optical communication systems are based on the QAM technology and homodyne detection of coherent light, and is now becoming widely spread in commercial use, as it provides major advantages over communication systems based on direct detection of light intensities. It is an important challenge to develop a secure optical network system based on the same technologies, since such system may enable secure and safe communication infrastructure that can offer diverse functions ranging from unconditionally secure communications to high-speed and high-secure data transmission in a unified way.

In this paper, we report an integration of CV-QKD and QAM/QNSC, where both are based on the same operating principle as the coherent optical communication. In CV-QKD, weak optical signal is measured by homodyne detection. A homodyne receiver is commercially available, operates at room temperature, is low cost and small, and insensitive to stray light because the local oscillator (LO) itself works as a spectral, temporal and spatial mode filter. This insensitiveness to stray light is very important when multiplexing CV-QKD with coherent optical communications. We show that the effect of stray light on the excess noise of our CV-QKD system is negligible even when the intensity of the stray light is higher than the signal light provided that the stray light is weaker than the LO light.

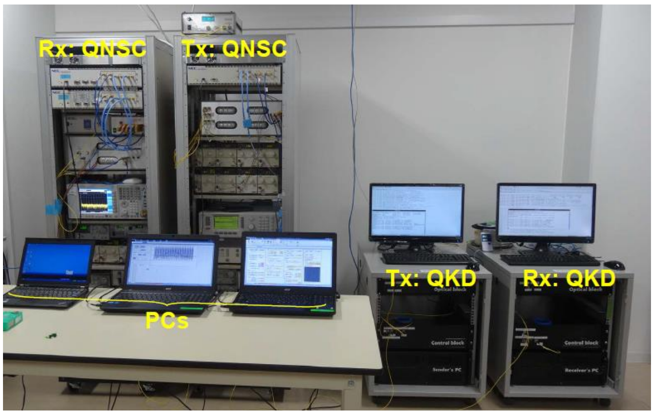

Fig.1 Photograph of CV-QKD-QAM/QNSC system.

Figure 1 shows a photograph of CV-QKD-QAM/QNSC system. Both systems are packaged in 19 inch racks. The QKD and QNSC signals, respectively, are delivered through two different 100 km standard single-mode fibers. In our CV-QKD system, self-homodyne detection with a commercially available balanced photodiode (BPD) is used. The light source is a pulsed InGaAsP 1.55 μm DFB laser diode with a pulse duration of 5 ns and a repetition rate of 10 MHz. The signal pulse is QPSK-modulated by a phase modulator and then attenuated to a single photon level [1]. A 1.3 μm LD is used to send a 100 MHz clock to realize synchronous operation between the QKD transmitter and the receiver. We use non-binary LDPC code developed by Kasai *et al.* for error correction [2], and Toeplitz matrix multiplication for privacy amplification [3].

QNSC scheme using QAM was proposed in 2014 [4, 5], in which the encrypted data consist of a multi-bit data signal and a multi-bit pseudo-random binary sequence (PRBS) for encryption that are modulated in a QAM format. The PRBS is generated from a common key supplied from the CV-QKD. An increase in the number of bits in the PRBS greatly increases the multiplicity in amplitude and phase, namely the multiplicities in the I and Q levels. Hence, the distance between two adjacent symbols becomes so small that the system becomes weak against noise. When such an encrypted multi-level data signal is intentionally embedded in quantum noise, an eavesdropper without the shared key has no way of receiving data correctly, whereas a legitimate receiver can receive the data without error after a mathematical process thanks to the shared key. We use an FPGA-based on-line transmitter consisted of four FPGAs and two digital-to-analog converters (DACs) operated at 10 GS/s with a 10-bit resolution. They were mutually synchronized with a 10 GHz clock. In the FPGA, $n_I$-bit I and $n_Q$-bit Q data were generated by using binary data streams from a PRBS generator, and they were encoded using Reed-Solomon FEC codes of RS (255, 239). The bandwidth of the encrypted QAM signal was 6 GHz by adopting a root raised cosine Nyquist filter. Sine and cosine wave signals with a sampling rate of 3 samples per period were added to the QAM/QNSC signal to generate a 3.33 GHz-shifted single sideband from the carrier frequency. This signal was used as a tone signal for tracking the optical phase of a local oscillator (LO) under optical phase-locked loop (OPLL) operation at the receiver. The receiver consisted of four FPGAs and two analog-to-digital converters (ADCs) operated at 10 GS/s with an 8-bit resolution.

We demonstrated on-line 70 Gbits/s, 128 QAM/QNSC transmission over 100 km with secret keys delivered by a CV-QKD with QPSK. The spectral efficiency reached as high as 10.3 bits/s/Hz, and the capacity-distance product reached 7 Tbits/s km. In the present system, the seed keys for encryption and decryption in the QNSC system can be renewed every 0.5~1 second by using the secret key obtained by the CV-QKD.

Acknowledgements
This work was partially supported by the National Institute of Information and Communications Technology (NICT), Japan, and by ImPACT Program of Council for Science, Technology and Innovation (Cabinet Office, Government of Japan).

References

[1] T. Hirano, H. Yamanaka, M. Ashikaga, T. Konishi, and R. Namiki, Phys. Rev. A 68, 042331 (2003).
[2] K. Kasai, Y. Fujisaka and M. Onsjö, http://www.comm.ce.titech.ac.jp/~kenta/index-e.html.
[3] T. Tsurumaru and M. Hayashi, IEEE Trans. Inf. Theory 59(7), 4700 (2013).
[4] M. Nakazawa et al., Opt. Express, Vol. 22, p. 4098 (2014).
[5] M. Yoshida, T. Hirooka, K. Kasai, and M. Nakazawa, Opt. Express 24(1), 652-661 (2016).