# Real-time 70 Gbit/s, 128 QAM quantum noise stream cipher transmission over 100 km with secret keys delivered by continuous variable quantum key distribution system

Masataka Nakazawa

Tohoku University
E-mail: nakazawa@riec.tohoku.ac.jp

## 1. Introduction

We have been intensively studying quantum noise stream cipher (QNSC) transmission technique using quadrature amplitude modulation (QAM) with a view to realizing a high-speed and long-distance secure communication system [1]. In this talk, we describe our recent demonstration of an on-line 70 Gbit/s, 128 QAM/QNSC transmission over 100 km with a continuous variable quantum key distribution (CV-QKD) system [2], in which a shared key is transmitted online via the CV-QKD so that the key is shared for a certain time period with absolutely no risk of being eavesdropped.

## 2. On-line 70 Gbit/s, 128 QAM/QNSC transmission over 100 km with CV-QKD system

Figure 1 shows our experimental set-up for an on-line QNSC transmission over 100 km with secret keys, which are stored in key control systems (KCSs) located on the transmitter and receiver sides of the CV-QKD system [2, 3]. Here, the seed keys for QNSC encryption and decryption can be changed synchronously with the secret keys supplied from the KSCs, which greatly increases the encryption security because there is no need for Alice and Bob to share the key from the beginning. In the CV-QKD system shown in the upper of Fig.1, homodyne detection with a commercial balanced photodiode (BPD) can be used for the key distribution instead of a single photon detector [3]. The generation rate of the secure keys was higher than 600 bit/s, which was sufficient to renew the seed key in the QNSC system every 0.5 s.

On the other hand, the QNSC system shown in the lower of Fig. 1 operates as follows. In a real-time transmitter based on FPGA, n bit I and Q data are encrypted by modulating their amplitude with m bit basis states, which are generated by PRBS generators driven by the secret keys from the QKD system via a PC. As a result, n+m bit encrypted I and Q data are generated. The bit numbers of n and m can be arbitrarily selected by an external control signal from a PC by keeping the relationship of n+m=10. This multiplicity change is also useful for increasing system security. In this way, 4-128 QAM data are encrypted in a $2^{10}$ x $2^{10}$ QAM pattern. By using the transmitter, we generated a polarization-multiplexed 5 Gsymbol/s, 4-128 QAM/QNSC (20-70 Gbit/s) signal, whose power $P_{out}$ was reduced with an optical attenuator to increase the level of data security against Eve. After 100 km transmission, an error free detection of 4-128 QAM data was achieved for Bob with the detection failure probability of more than 99.8 % for Eve.

## 3. Conclusions

We described our high-speed secure optical communication system with a combination of QAM/QNSC and CV-QKD techniques.

## References

[1] M. Nakazawa et al., Opt. Express 22(4), 4098-4107 (2014).
[2] M. Nakazawa et al., ECOC2016, paper W.4.P1.SC5.59.
[3] T. Hirano et al., Phys. Rev. A 68, 042331 (2003).

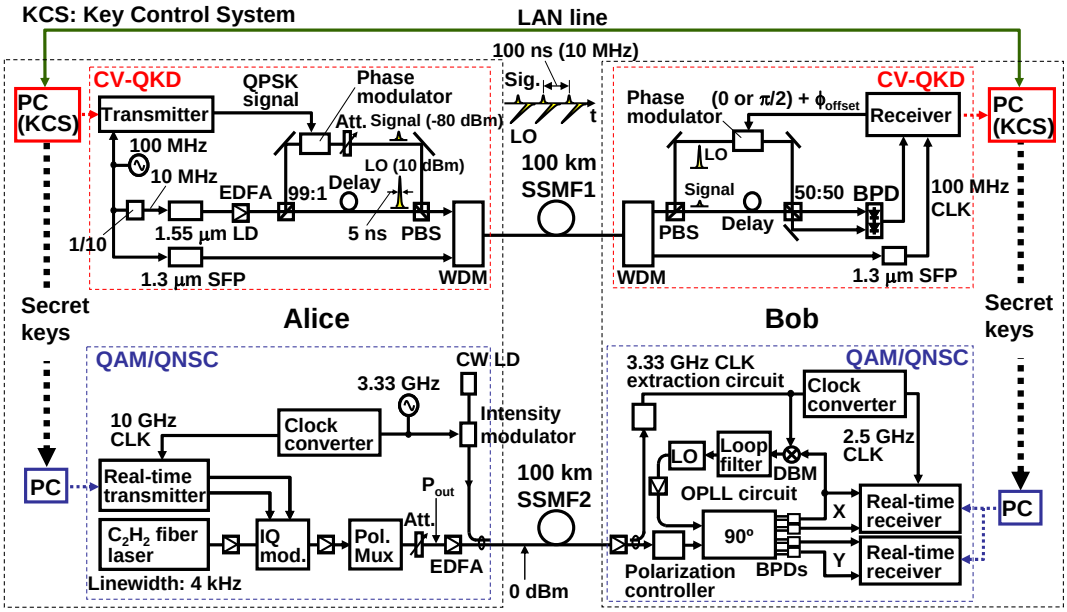


Fig. 1 Experimental set-up for on-line 70 bit/s, 128 QAM/QNSC transmission over 100 km with secret keys delivered by CV-QKD system.