High Spectral Efficiency Digital Coherent Continuous Variable Quantum Key Distribution System Using Polarization-Multiplexed QPSK Reference Signal

Tetsuo Kawakami[(1)], Ken-ichiro Yoshino[(1)], Wakako Maeda[(1)], Takuya Hirano[(2)]

[(1)] Advanced Network Research Laboratories, NEC Corporation, Kawasaki, Kanagawa, Japan, tetsuo-kawakami@nec.com
[(2)] Department of Physics, Gakushuin University

Abstract *We designed a digital coherent continuous variable quantum key distribution system achieving higher spectral efficiency by extracting timing information from a polarization-multiplexed QPSK reference signal and demonstrated the feasibility of distributing a secret key over a 100 km SMF link.*

Introduction

Quantum key distribution (QKD) ensures unconditional security in combination with one-time pad encryption [1]. QKD is classified into two types: Discrete Variable (DV) and Continuous Variable (CV) QKD. Whereas DV-QKD requires dedicated hardware like a single photon detector, CV-QKD is potentially implementable with hardware used in a common optical communication system; therefore, CV-QKD attracts attention [2-6]. A widespread CV-QKD network can be achieved by realizing long-distance key distribution, which has the potential for compatibility with optical WDM networks [3].

However, two issues exist in conventional CV-QKD systems for practical implementation. (1)Short QKD distance: The amplitude of the quantum signal is so weak that carrier recovery of the quantum signal alone is impossible. To solve this problem, the conventional CV-QKD detects the quantum signal by a self-homodyne detection. In such detection, the LO light is polarization-multiplexed to the quantum signal and experiences the same phase fluctuation as the quantum signal, so carrier recovery is unnecessary [2]. A self-homodyne detection limits the QKD distance short because the LO power is attenuated over the transmission path. (2)Low spectral efficiency (SE): The amplitude of the quantum signal is so weak that it is impossible to extract timing information from the quantum signal itself. Therefore, a timing information signal is wavelength-multiplexed to the quantum signal, but it reduces the SE [3].

Recently the combination of CV-QKD with digital signal processing has attracted much attention [4-6]. Digital coherent CV-QKD is expected to extend the QKD distance because it has the LO at the receiver side. This scheme realizes its carrier recovery of the quantum signal by carrier recovery of a reference signal, polarization-multiplexed to the quantum signal. Digital coherent CV-QKD can become a long-distance and high-SE CV-QKD system by modulating the reference signal by the same clock as the quantum signal and extracting timing information.

In this paper, we designed a Digital coherent CV-QKD system achieving higher SE by extracting timing information from a QPSK reference signal. For accomplishing long-distance QKD, we set the reference signal power high. Using the CMA algorithm [8], we successfully demultiplexed the quantum signal and the strong reference signal. We demonstrated the feasibility of distributing a secret key over a 100 km SMF link.

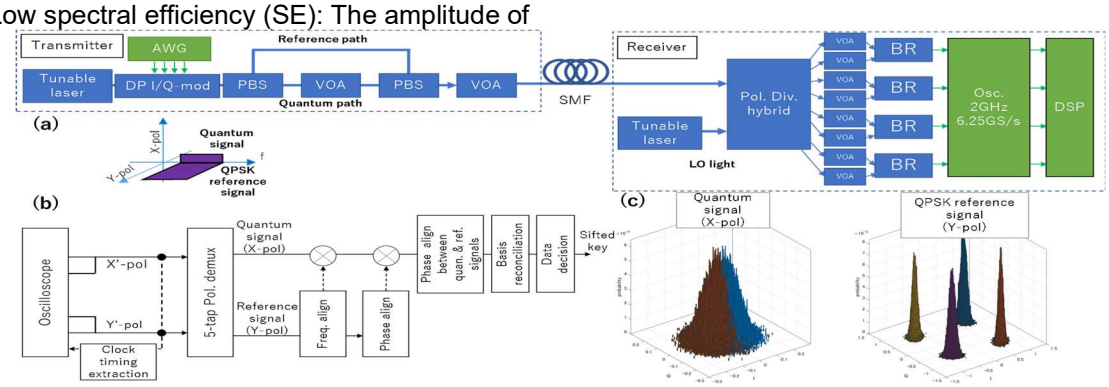

Fig. 1(a)Experimental setup for the proposed CV-QKD system. (b) Flow of digital signal processing. (c) Histogram of the demodulated quantum signal (left) and reference signal (right).

The principal concept

Fig. 1 shows the principal concept of the proposed long-distance and higher-SE CV-QKD. The quantum and the strong QPSK reference signals were polarization-multiplexed.

The timing information of the quantum signal was obtained using the Gardner method [7] based on the knowledge that one polarization should contain the strong reference signal modulated by the same clock as the quantum signal. The frequency and phase alignment of the weak quantum signal was performed by applying the phase tracking value of the strong reference signal. We set the reference power so high that the phase tracking of the reference signal works correctly even over long-distance. By investigating the nonlinearity of the radius of the I/Q envelop of the quantum signal and optimizing the CMA algorithm's target radius, we brought off polarization-demultiplexing the mixed polarization signal to the quantum signal and the strong reference signal.

Experimental setup

Fig. 1 (a) shows the experimental setup. The transmitter had a light source tuned to 1550.12 nm. CV-QKD modulation using four phase states was implemented using a DP-I/Q-modulator, in which each polarization was driven by an arbitrary waveform generator (AWG) generating 1.25-GBaud RZ signals. The modulator output polarization-multiplexed signals. The first (X-pol) and second polarization (Y-pol) were used for the quantum and the QPSK reference signal, respectively. The quantum signal was attenuated using a polarization beam splitter (PBS) and a variable optical attenuator (VOA) so that its power was lower than that of the reference signal. The second PBS multiplexed the quantum and reference signals. They were attenuated by the VOA so that the quantum signal power was equal to the power of 1 photon / 1 symbol.

The quantum and reference signals were transmitted over a 100-km SMF. A second tunable laser was used as the LO, operating at +15.5 dBm output power. An optical DP-90-degree hybrid was used followed by four sets of balanced receivers (BRs) with a bandwidth of 1.6-GHz. The quantum and reference signals were digitized using a 2-GHz-bandwidth real-time oscilloscope with a 6.25-GS/s sampling rate.

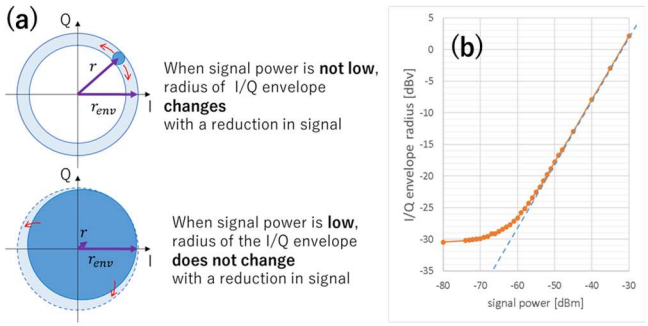

Fig. 2(a) Relationship between signal power of coherent detection and radius of I/Q envelope. (b) The result of the measurement of radius of I/Q envelope vs. signal power.

Digital signal processing

Fig. 1 (b) shows the digital signal processing procedure. After extracting timing information from the reference signal, polarization demultiplexing was done by the CMA algorithm with 5-tap butterfly-structured FIR filters. We set the Nth filter's X- and Y-pol error signals $\varepsilon_X(n)$ and $\varepsilon_Y(n)$ as

$$\varepsilon_X(\mathrm{n}) = \left({R_{envQ}}/{R_{envR}}\right)^2 - |I_X(n) + jQ_X(n)|^2$$
$$\varepsilon_Y(\mathrm{n}) = \left({R_{envR}}/{R_{en\ R}}\right)^2 - |I_Y(n) + jQ_Y(n)|^2, \qquad (1)$$

where R_{envQ} (R_{envR}) is the quantum signal's (the reference signal's) target I/Q envelope, I_X (I_Y) is the X-pol's (Y-pol's) measured in-phase, and Q_X (Q_Y) is that of quadrature-phase. Note that the quantum signal power and the radius of the I/Q envelope are not proportional when the quantum signal power on the receiver side is extremely low. Therefore, for precise polarization demultiplexing, the target ratio of the quantum signal to the reference signal must be less than the optical power ratio of the quantum signal to the reference signal. We confirmed this nonlinearity of the radius of the I/Q envelope by the measurement in Fig. 2 setup. In Fig. 2 (b), when the signal power is extremely low (<<-60 dBm), the signal power and the radius of the I/Q envelope are not proportional.

This nonlinearity is because, when the signal power is not very low, the lower the signal power, the smaller the radius of the I/Q envelope circle, and when the signal power is so low that the I/Q symbols of the signal are all contained within the I/Q outer envelope shell, the radius of the I/Q envelope circle does not change with a reduction in signal power (see Fig. 2 (a)). Given this finding, we carefully optimized the target radius of the I/Q envelope circle ratio and achieved demultiplexing of the mixed polarization signal into the quantum signal and the strong reference signal. After polarization demultiplexing, the power difference between the X-pol and the Y-pol corresponded to the optical power difference of 30 dB between the quantum and the reference signals, meaning that polarization demultiplexing was correctly done. (See the grey dotted line in Fig3 (a)).

After polarization demultiplexing, frequency and phase alignment were done. Because the signal-to-noise ratio of the quantum signal is very low, the phase alignment of the quantum signal is

performed by applying the phase tracking value of the strong reference signal. The phase tracking of the QPSK reference signal was done by the Mth-power method and the decision-directed phase-locked loop (DDPLL) method. For these methods to work correctly, the reference power must be sufficiently high. Therefore, we set the high-power ratio of the reference signal to +30dB from that of the quantum signal. The phase difference alignment between the quantum and reference signals was then done by publishing some quantum signal data and rotating the phase of the quantum signal.

Finally, basis reconciliation was done by rotating the phase of the quantum signal by the basis information published from the transmitter via a classical communication channel, and the sifted key was shared between the transmitter and receiver.

Secret key rate calculating method

After error correction and privacy amplification, a secret key is obtained from a sifted key. The estimated secret key rates (SKRs) are given as

$$SKR = \int dmP(m|\alpha)\Delta I\,, \tag{2}$$

where

$$P(m|\alpha) = \sqrt{\frac{2}{\pi(1+\xi)}}\, e^{-2\frac{(m-\sqrt{\eta}\alpha)^2}{1+\xi}}, \Delta I = I_{AB} - \chi, \tag{3}$$

and the integral is taken over the region where $\Delta I > 0$, P is the probability density to obtain m the total transmission, I_{AB} is the mutual information between transmitter (Alice) and receiver (Bob), and χ is the information accessible to the eavesdropper. η and ξ can be written as

$$\eta = \eta_1\eta_2, \qquad \xi = \xi_1\eta_2 + \xi_2, \tag{4}$$

where, η_1 and ξ_1 are the quantum channel's transmission and excess noise, and η_2 and ξ_2 are the receiver's transmission and excess noise. We measured η and ξ before the experiment.

Depending on the method of assumption of the eavesdropper's ability, there are several methods of estimating χ. We estimated SKRs in two assumptions: the eavesdropper can perform collective attacks [9] and the eavesdropper can perform individual attacks [10].

Results

Fig. 3 (a) shows the bit error rate (BER) for transmission distances up to 100 km. The orange solid line shows the BER after basis reconciliation, and the blue dotted line shows it before basis reconciliation. The BER of the quantum signal was better after basis reconciliation, meaning that the quantum signal was correctly demodulated.

Fig. 3 (b) shows the SKRs estimated using measured transmission and excess noise. The solid line shows the ideal SKRs ($\xi_1 = \xi_2 = 0$) when the eavesdropper can perform individual attacks, and the dotted line shows the ideal SKRs ($\xi_1 = \xi_2 = 0$) when the eavesdropper can perform collective attacks. The SKR for collective attacks decreased more rapidly because its security proof is stricter. At 100 km, the quantum channel's transmission η_1 = 0.010 (−19.9 dB) and excess noise ξ_1 =0.01, the receiver's transmission η_2 = 0.264 (including the optical polarization diversity 90-degree hybrid's natural loss) and excess noise ξ_2 =1.06, and the SKRs were subjected to individual attacks at 6.17 bps. These results demonstrated the feasibility of distributing a secret key over a 100-km SMF link.

Conclusions

We designed a Digital coherent CV-QKD system achieving higher SE by extracting timing information from a polarization-multiplexed QPSK reference signal and demonstrated the feasibility of distributing a secret key over a 100 km SMF link.

Acknowledgments

The estimated SKRs were calculated by the program supported by ImPACT (Impulsing Paradigm Change through Disruptive Technologies) Program of Council for Science.

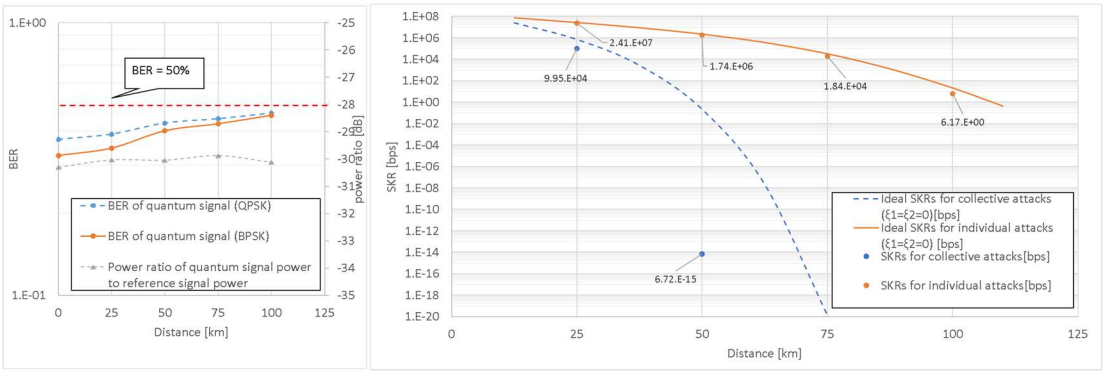

Fig. 3(a) The measurement result of BER and the power ratio of the quantum signal power to the reference signal power. (b) The estimated SKRs from the measurement results.

References

[1] C. H. Bennett, G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, 10-12 dEcember, 175-179. (1984)

[2] T. Hirano, et al., “Implementation of continuous-variable quantum key distribution with discrete modulation,” Quantum Science and Technology, Volume 2, Number 2 (2017), DOI:10.1088/2058-9565/aa7230

[3] T. A. Eriksson, et al., “Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 Tbit/s data channels,” Communications Physics volume 2, Article number: 9 (2019), DOI:10.1038/s42005-018-0105-5

[4] T. A. Eriksson, et al., “Digital Self-Coherent Continuous Variable Quantum Key Distribution System,” in Optical Fiber Communication Conference (OFC) 2021, paper T3D.5(2020)

[5] H. Wang, et al., “Sub-Gbps key rate four-state continuous-variable quantum key distribution within metropolitan area,” Commun Phys 5, 162 (2022), DOI:10.1038/s42005-022-00941-z

[6] B. Schrenk, et al., “High-rate continuous variable QKD with optically carrier-suppressed pilot,” ECOC 2019 22-26 September (2019), DOI:10.1049/cp.2019.1090

[7] F. Gardner, “A BPSK QPSK Timing-Error Detector for Sampled Receivers,” IEEE Transactions on Communications Volume: 34, Issue: 5, May (1986) DOI:10.1109/TCOM.1986.1096561

[8] K. Kikuchi, “Fundamentals of Coherent Optical Fiber Communications,” Journal of Lightwave Technology Volume: 34, Issue: 1, 01 January (2016), DOI:10.1109/JLT.2015.2463719

[9] R. Namiki, et al., "Secret key rate of a continuous-variable quantum-key-distribution scheme when the detection process is inaccessible to eavesdroppers," Phys. Rev. A 98(4), 042319 (2018), DOI: 10.1103/PhysRevA.98.042319

[10] T. Ichikawa, et al., " Notes on a Continuous-Variable Quantum Key Distribution Scheme," J. Phys. Soc. Jpn. 86, 094001 (2017), DOI: 10.7566/JPSJ.86.094001