

PAPER • OPEN ACCESS

Implementation of continuous-variable quantum key distribution with discrete modulation

To cite this article: Takuya Hirano *et al* 2017 *Quantum Sci. Technol.* **2** 024010

View the [article online](#) for updates and enhancements.

You may also like

- [Squeezing-enhanced quantum key distribution over atmospheric channels](#)
Ivan Derkach, Vladyslav C Usenko and Radim Filip
- [Improving the discretely modulated underwater continuous-variable quantum key distribution with heralded hybrid linear amplifier](#)
Yong Xiang, Yijun Wang, Xinchao Ruan *et al.*
- [Coexistence of continuous variable QKD with intense DWDM classical channels](#)
Rupesh Kumar, Hao Qin and Romain Alléaume

 **kiutra**

Easy-to-use and Helium-3 free
cryogenics solutions

LEARN MORE

Quantum Science and Technology



PAPER

Implementation of continuous-variable quantum key distribution with discrete modulation

OPEN ACCESS

RECEIVED

15 December 2016

REVISED

2 May 2017

ACCEPTED FOR PUBLICATION

10 May 2017

PUBLISHED

9 June 2017

Original content from this work may be used under the terms of the [Creative Commons Attribution 3.0 licence](#).

Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.



Takuya Hirano¹, Tsubasa Ichikawa¹, Takuto Matsubara¹, Motoharu Ono¹, Yusuke Oguri¹, Ryo Namiki¹, Kenta Kasai², Ryutaroh Matsumoto³ and Toyohiro Tsurumaru⁴

¹ Dept. of Physics, Gakushuin University, 1-5-1 Mejiro, Toshima-ku, Tokyo, 171-8588 Japan

² Dept. of Information and Communications Engineering, Tokyo Institute of Technology, 2-12-1 Ookayama, Meguro-ku, Tokyo, 152-8550 Japan

³ Dept. of Information and Communication Engineering, Nagoya University, 464-8603 Japan

⁴ Mitsubishi Electric Corporation, Information Technology R&D Center, 5-1-1 Ofuna, Kamakura-shi, Kanagawa, 247-8501 Japan

E-mail: takuya.hirano@gakushuin.ac.jp

Keywords: continuous-variable quantum key distribution, quadrature amplitude modulation, pulsed homodyne detection

Abstract

We have developed a continuous-variable quantum key distribution (CV-QKD) system that employs discrete quadrature-amplitude modulation and homodyne detection of coherent states of light. We experimentally demonstrated automated secure key generation with a rate of 50 kbps when a quantum channel is a 10 km optical fibre. The CV-QKD system utilises a four-state and post-selection protocol and generates a secure key against the entangling cloner attack. We used a pulsed light source of 1550 nm wavelength with a repetition rate of 10 MHz. A commercially available balanced receiver is used to realise shot-noise-limited pulsed homodyne detection. We used a non-binary LDPC code for error correction (reverse reconciliation) and the Toeplitz matrix multiplication for privacy amplification. A graphical processing unit card is used to accelerate the software-based post-processing.

1. Introduction

Quantum key distribution (QKD) offers secure communication based on the fundamental laws of quantum physics [1]. In contrast to public key cryptography that is currently in wide-spread use and whose security relies on the computational difficulty of solving a mathematical problem [2], the security of QKD can be guaranteed even if an eavesdropper has an infinite computational power [3]. QKD enables two parties, usually called Alice and Bob, to share a secret key that is unknown to third parties by sending quantum states from Alice to Bob [4].

Continuous-variable (CV) QKD is different from the standard QKD system in the method for detecting weak optical signals [5–11]. This feature gives an advantage to CV-QKD in terms of practical implementation. In the standard QKD system, weak light is detected by a single photon detector that measures the particle nature of light: the measured observable has a discrete spectrum [4]. The detector is usually custom built for QKD, requires cooling, and expensive, and it is sensitive to stray light. On the other hand, in the CV-QKD weak light is detected by a homodyne detector that measures wave nature of light: the measured observable has continuous spectrum. A homodyne receiver is commercially available, works 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. Since both CV-QKD and coherent optical communication exploit devices which operate on the same principle, we may be able to realise a secure and safe communication infrastructure that can offer diverse functions ranging from unconditionally secure communications to high-speed and high-security data transmission in a unified way, and seamlessly integrate them into coherent optical communication systems [12].

However, in terms of security analysis, the security proof of CV-QKD is relatively difficult compared with the discrete variable (DV) QKD that uses a single photon detector. In the case of DV-QKD, one can intuitively understand its safety as follows: if Alice sends only a single photon and Bob detects the photon, an eavesdropper

cannot read the information encoded on the photon because a single photon cannot be divided. Even when Alice may send multiple photons, using the so-called tagging idea which was proposed by Gottesman, Lo, Lütkenhaus and Preskill [13], it is possible to use the idea of single photon case to the practical case using weak coherent pulses. On the other hand, in the case of CV-QKD, Bob measures the amplitude of the electromagnetic field, and the amplitude might be divided by an eavesdropper. Indeed, it was pointed out that CV-QKD protocols require that the transmission of the optical line between Alice and Bob is larger than 50% [14], because if the transmission is less than 50%, Eve can obtain higher signal-to-noise ratio than Bob by replacing the lossy channel with her lossless channel and splitting a fraction of the signal with a ratio of larger than 50%. Fortunately, it is known that this apparent 3 dB loss limit can be beaten by using appropriate recipes [15]. One recipe is the post-selection [15, 16]. Post-selection is an intrinsic procedure in DV-QKD: if no photon is detected, the corresponding time slot is discarded. In CV-QKD, Bob can postselect a subset of data by selecting only time slots for which his homodyne detector outputs a high absolute value and the mutual information between Alice and Bob is high. Another recipe is the reverse reconciliation (RR) [6], in which the reconciliation procedure is reversed: Alice's data is corrected to match Bob's data rather than Bob's data being corrected to match Alice's. In this case, Eve has to guess what was received by Bob rather than what was sent by Alice, and Alice is advantageous than Eve in guessing Bob's measurement results. Some other recipes such as multidimensional reconciliation [17] and repetition code [18] were proposed to improve the performance of CV-QKD. As the bit error rate is crucial when evaluating the security of DV-QKD, an excess noise is crucial in CV-QKD. It is known that if the excess noise of a quantum channel is Gaussian and two times larger than the transmission of the channel, no form of optical communication that uses coherent states and homodyne detection can be secured quantum mechanically since there is a realistic intercept-resend attack [19].

CV-QKD protocols can be classified into two types by the modulation method of coherent states sent by Alice. One is Gaussian-modulation protocol [6, 14] and the other is discrete-modulation protocol [16, 20]. In the former protocol, Alice's state preparation can be formally described in an entanglement based scheme where Alice has CV entanglement [21]. Heid *et al* pointed out that all collective attacks are unitarily equivalent if the quantum channel can be verified as being symmetric and Gaussian, then secure key rate in the collective attack scenario can be calculated by choosing the entangling cloner attack (see section 3) as an optimal attack including post-selection [22]. Security analysis for the former is more advanced than for the latter, and recently a composable security proof including finite-size setting was reported [23]. Various reconciliation methods for the former protocol have been studied [17, 18, 24, 25]. As for the latter discrete-modulation protocol, it was reported that secure long-distance QKD is possible if the quantum channel can be verified as being linear [20, 26]. The former protocol is more advanced than the latter also in experimental implementation. In 2009, a field test of the former CV-QKD protocol was demonstrated over 9 km fibre with 8 kbit s⁻¹ key generation rate in the SECOQC project [27]. Recently, a long-distance experiment over 100 km was reported by controlling excess noise [9]. In a field implementation of CV-QKD network, computed key rates of 0.25, 2, 6, 10 kbps for 17.52, 15.34, 19.92, 2.08 km link, respectively, were reported using a 500 KHz pulse train [28].

In this paper, we experimentally demonstrate the discrete-modulation (four states) CV-QKD protocol proposed in [5] over a 10 km single mode fibre (SMF) and theoretically evaluate the secure key rate on the assumption that the eavesdropper performs the entangling cloner attack [21, 22]. To our knowledge, this is the first practical implementation of the four-state CV-QKD in which secure keys can be continuously generated by programmed operation. The system is simple, can be built at low cost and operate robustly, thus addresses some of the important challenges toward practical popularisation of QKD [29]. On the theoretical side, we give an algebraic formula for the key rate by using Gramian matrices and show that reverse reconciliation (RR) gives better key rate than direct reconciliation (DR), as shown for CV-QKD protocols with Gaussian modulations [6]. An average photon number of the weak coherent pulse is selected to maximise the secure key rate. On the experimental side, we developed a CV-QKD system that can continuously generate secret key. Key generation rate is 50 kbps when the quantum channel is a 10 km optical fibre. We use a pulsed light source whose wavelength is 1550 nm and repetition rate is 10 MHz. A commercially available balanced receiver is used to realise shot-noise-limited pulsed homodyne detection. We use a non-binary low-density parity check (LDPC) code for error correction [34] and a fast privacy amplification algorithm using the Toeplitz matrix multiplication [35]. A graphical processing unit (GPU) card is used to accelerate the software-based post-processing.

This paper is organised as follows. In section 2, we introduce our CV-QKD protocol and present a set of basic formulas to describe the performance of our protocol under a noisy channel. In section 3, we introduce the entangling cloner attack and calculate the Holevo quantity for DR and RR. Key rates and optimised average photon number are given in section 4. In section 5, we show our experimental implementation and in section 6 we report automated QKD demonstration over 10 km. Section 7 concludes this paper.

2. Four-state CV-QKD protocol

The protocol we are going to analyse consists of the following eight steps: (i) Alice sends Bob a quantum state $|S\rangle$, which is randomly chosen out of four coherent states $|\pm\alpha\rangle$, $|\pm i\alpha\rangle$ of a given mode. Here, $\alpha > 0$. (ii) Bob performs a measurement on the received state with x -basis or p -basis randomly chosen. Here, we defined the quadratures

$$x = \frac{a + a^\dagger}{2}, \quad p = \frac{a - a^\dagger}{2i}, \quad (1)$$

through the annihilation operator a of the mode A . (iii) Alice and Bob repeat processes (i) and (ii) sufficiently many times. (iv) Alice reveals which basis she used in each process through a classical channel. She also randomly chooses a part of the processes and reveals the state she sent. (v) Bob estimates the parameters of the quantum channel using the data of the processes that Alice revealed her states. Then he selects the data to be used for key generation in accordance with his measurement and the estimated channel parameters. He uses only the processes for which he made a correct choice of the measurement basis. Here, the correct basis refers to the x -basis for $|\pm\alpha\rangle$, whereas the p -basis for $|\pm i\alpha\rangle$. Bob informs Alice which process was selected. In the theoretical analysis, we assume that Bob reveals also the absolute value $|m|$ of his outcome m . (vi) Bob makes a bit string by assigning 0 for the negative m , while 1 for the positive m of selected measurement, respectively. (vii) Alice makes a bit string by assigning 0 for $|\pm\alpha\rangle$, $|\pm i\alpha\rangle$, whereas 1 for $|\pm\alpha\rangle$, $|\pm i\alpha\rangle$. (viii) Alice and Bob share a secure key by applying error correction and privacy amplification to the bit strings obtained. The efficiency of the post-processing could be substantially different whether one chooses DR or RR.

The role of the quadrature x, p is clearly symmetric in this protocol. Without loss of generality, therefore, we may restrict ourselves only to the case of the correct measurements that Alice sends the coherent states $S = \pm\alpha$ and Bob performs the x -basis measurements. Note that the probabilities that $S = \pm\alpha$ is given by $P(\alpha) = P(-\alpha) = 1/2$, respectively.

Let us assume that quantum channel is not ideal, but characterised by excess noise ξ and transmission η . The probability density to obtain m conditioned by S is given by [30]

$$P(m|S) = \sqrt{\frac{2}{\pi(1+\xi)}} e^{-2\frac{(m-\sqrt{\eta}S)^2}{1+\xi}}, \quad (2)$$

when the vacuum noise variance is $1/4$. Note that

$$P(m|S) = P(-m| -S). \quad (3)$$

It immediately follows from equation (3) that given the absolute value $|m|$, the protocol can be seen as a binary symmetric channel [31]. To show this, let us define the probability ϵ that Alice's 0 goes to Bob's 1. We then find

$$\epsilon := \frac{P(-|m||\alpha)}{P(m|\alpha) + P(-m|\alpha)} = \frac{P(|m||-\alpha)}{P(m|-\alpha) + P(-m|-\alpha)} = \left[1 + e^{8\frac{\sqrt{\eta}}{1+\xi}|m|\alpha} \right]^{-1}, \quad (4)$$

which proves the claim, since from the second equality ϵ now reads the probability that Alice's 1 goes to Bob's 0. Thus, we may use the Shannon formula and find the mutual information I_{AB} between Alice and Bob as

$$I_{AB} = 1 - h(\epsilon), \quad (5)$$

where $h(\epsilon) = -\epsilon \log_2 \epsilon - (1 - \epsilon) \log_2 (1 - \epsilon)$ is the binary entropy.

An advantage of this four-state CV-QKD protocol is its implementation simplicity. In step (i), Alice performs one of four kinds of phase modulations and in step (ii), Bob performs one of two kinds of phase modulations. Therefore, only a phase modulator for each station is necessary as an experimental device for modulation, and the required random number is 2 bits for Alice and 1 bit for Bob. In the Gaussian-modulated coherent states CV-QKD protocol [6–9], Alice needs also an amplitude modulator and two random real numbers, which are not computable in principle and experimentally she needs random bit strings longer than at least the resolution of the digital-to-analogue converters.

3. Entangling cloner attack

We shall consider the key rate of our protocol against collective attacks assuming that the quantum channel is Gaussian. When the quantum channel is symmetric and Gaussian, all collective attacks are unitarily equivalent [22]. Therefore, in the following we calculate the secret fraction against the entangling cloner attack [21]. Prior to this, we present the details of the entangling cloner attack and evaluate the information accessible by an eavesdropper, say Eve, in this section.

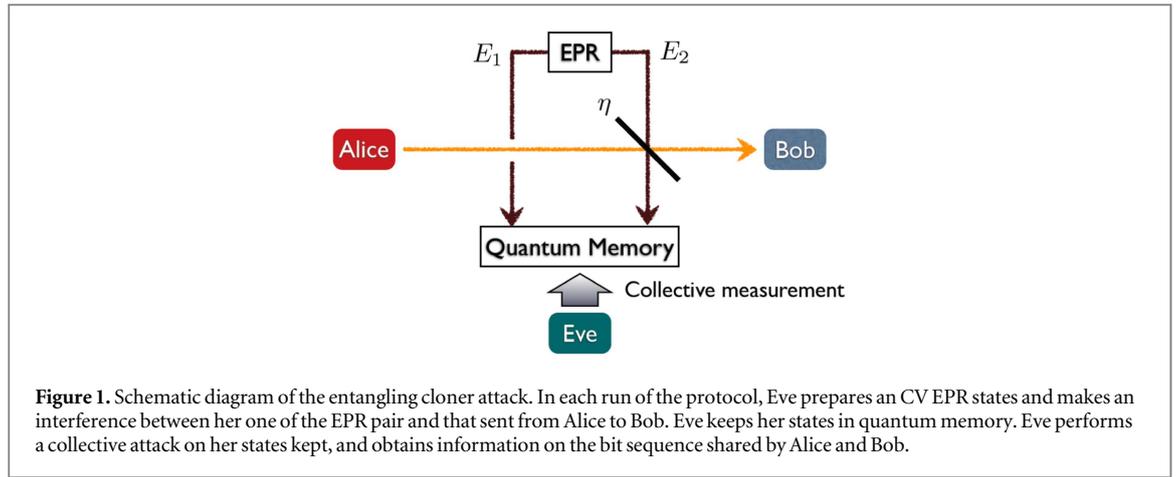


Figure 1. Schematic diagram of the entangling cloner attack. In each run of the protocol, Eve prepares an CV EPR states and makes an interference between her one of the EPR pair and that sent from Alice to Bob. Eve keeps her states in quantum memory. Eve performs a collective attack on her states kept, and obtains information on the bit sequence shared by Alice and Bob.

For the entangling cloner attack, Eve prepares an Einstein-Podolsky-Rosen (EPR) state

$$|EPR\rangle = \sqrt{\frac{2}{\pi}} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} dx_1 dx_2 e^{-Vx_1^2 - x_2^2/V} \left| \frac{x_1 + x_2}{\sqrt{2}} \right\rangle_{E_1} \left| \frac{x_1 - x_2}{\sqrt{2}} \right\rangle_{E_2} \quad (6)$$

of modes E_1 and E_2 . Here $|x\rangle_{E_i}$ represents the eigenstate of a quadrature operator x of the mode E_i with eigenvalue x . The parameter $V \geq 1$ is chosen in such a way that

$$\frac{1}{2} \left(V + \frac{1}{V} \right) = \frac{1 - \eta + \xi}{1 - \eta} \quad (7)$$

so as to emulate the noisy quantum channel introduced in the previous section. Eve next replaces the noisy quantum channel with a lossless and noiseless quantum channel followed by a beam splitter of transmission η (see figure 1). She then makes interference between the mode A and E_2 by using the beam splitter. After Alice and Bob make a sufficiently long bit sequence, Eve obtains the information of the sequence by performing a collective measurement on the states coming from E_1 and E_2 modes kept in her quantum memory.

Let us describe the attack in detail. Since the coherent state $|S\rangle$ can be written as

$$|S\rangle = \left(\frac{2}{\pi} \right)^{\frac{1}{4}} \int_{-\infty}^{\infty} dx e^{-(x-S)^2} |x\rangle \quad (8)$$

and the beam splitter of transmission η leads to a transformation

$$|x\rangle_A |x_2\rangle_{E_2} \rightarrow |\sqrt{\eta}x - \sqrt{1-\eta}x_2\rangle_A |\sqrt{1-\eta}x + \sqrt{\eta}x_2\rangle_{E_2}, \quad (9)$$

the state after the interference takes the form of

$$|S\rangle_A |EPR\rangle \rightarrow \int_{-\infty}^{\infty} dm |m\rangle_A |\psi(S, m)\rangle, \quad (10)$$

where

$$|\psi(S, m)\rangle = \left(\frac{8}{\pi^3 \eta^2} \right)^{\frac{1}{4}} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} dx_1 dx_2 \psi(S, m) \left| \frac{x_1 + x_2}{\sqrt{2}} \right\rangle_{E_1} \left| \sqrt{\frac{1-\eta}{\eta}} m + \frac{x_1 - x_2}{\sqrt{2\eta}} \right\rangle_{E_2} \quad (11)$$

with

$$\psi(S, m) = e^{-\left[\sqrt{\frac{1-\eta}{2\eta}} (x_1 - x_2) + \frac{m}{\sqrt{\eta}} - S \right]^2 - Vx_1^2 - x_2^2/V}. \quad (12)$$

To obtain this, we have changed the variable x in equation (8) to $m = \sqrt{\eta}x - \sqrt{1-\eta}(x_1 - x_2)/\sqrt{2}$. Note that $|\psi(S, m)\rangle$ has the following normalisation:

$$\langle \psi(S, m) | \psi(S, m) \rangle = P(m|S). \quad (13)$$

For later convenience, we introduce

$$|e_{ij}\rangle = \mathcal{N} |\psi((-1)^i |S\rangle, (-1)^j |m\rangle)\rangle, \quad (14)$$

where $i, j = 0, 1$ and \mathcal{N} is a normalisation factor which implicitly depends on i, j .

Now, suppose that Bob performs the x -basis measurement to the mode A and find an outcome m . On this situation, Eve has the following two strategies to attack, depending on the reconciliation Alice and Bob adopted: (a) For DR, Eve attacks Alice to estimate her bit. This estimation results in distinguishing

$$\begin{aligned}\rho_A^0 &= (1 - \epsilon)|e_{00}\rangle\langle e_{00}| + \epsilon|e_{01}\rangle\langle e_{01}|, \\ \rho_A^1 &= (1 - \epsilon)|e_{11}\rangle\langle e_{11}| + \epsilon|e_{10}\rangle\langle e_{10}|.\end{aligned}\quad (15)$$

(b) For RR, Eve attacks Bob, aiming at estimate of his bit. By the similar way to DR, this results in distinguishing two density matrices

$$\begin{aligned}\rho_B^0 &= (1 - \epsilon)|e_{00}\rangle\langle e_{00}| + \epsilon|e_{10}\rangle\langle e_{10}|, \\ \rho_B^1 &= (1 - \epsilon)|e_{11}\rangle\langle e_{11}| + \epsilon|e_{01}\rangle\langle e_{01}|.\end{aligned}\quad (16)$$

In both cases, it is known that the information accessible to Eve is bounded from above by the Holevo quantity χ , which is given by

$$\chi = \begin{cases} S(\rho) - S(\rho_A^0)/2 - S(\rho_A^1)/2 & \text{for DR,} \\ S(\rho) - S(\rho_B^0)/2 - S(\rho_B^1)/2 & \text{for RR,} \end{cases}\quad (17)$$

where $\rho := (\rho_A^0 + \rho_A^1)/2 = (\rho_B^0 + \rho_B^1)/2$ and $S(\rho) = -\text{Tr}(\rho \log_2 \rho)$ denotes the von Neumann entropy.

To compute the Holevo quantity χ , we will determine the eigenvalues of all the density matrices appearing in equation (17). Despite all these are infinite dimensional Hermite operators written as a convex combination of projectors not necessarily orthogonal to one another, it is straightforward to find their non-zero eigenvalues by using scaled Gramian matrices, which is defined below.

Given a density matrix $\sigma = \sum_i p_i |\varphi_i\rangle\langle\varphi_i|$, where $\{p_i\}$ is a probability distribution, the rescaled Gramian matrix $G = (G_{ij})$ associated with σ is defined by

$$G_{ij} = \sqrt{p_i p_j} \langle\varphi_i|\varphi_j\rangle.\quad (18)$$

We then find the following proposition.

Proposition 1. *All the non-zero eigenvalues of σ are identical to all those of the associated Gramian matrix G .*

Proof. See [32]. ■

This proposition reduces the calculation of the Holevo quantity to much milder problems: the eigenvalue problems of the Gramian matrices associated with ρ_A^i , ρ_B^i , and ρ . In what follows, we list the Gramian matrices and their eigenvalues. (1) For ρ_A^i , G is independent of i and given by

$$G = \begin{pmatrix} 1 - \epsilon & \delta s \\ \delta s & \epsilon \end{pmatrix}\quad (19)$$

whose eigenvalues are readily found to be

$$\frac{1}{2}[1 \pm \sqrt{1 - 4\delta^2(1 - s^2)}],\quad (20)$$

where we introduced

$$\begin{aligned}s &= \langle e_{00}|e_{01}\rangle = \langle e_{11}|e_{10}\rangle = e^{-2\frac{\xi(\xi+\eta)}{1+\xi}m^2}, \\ \delta &= \sqrt{\epsilon(1 - \epsilon)}.\end{aligned}\quad (21)$$

Note that, independent of α and η , it holds

$$S(\rho_A^0) = S(\rho_A^1).\quad (22)$$

(2) For ρ_B^i , the Gramian matrix is also independent of i and takes the form of

$$G = \begin{pmatrix} 1 - \epsilon & \delta t \\ \delta t & \epsilon \end{pmatrix},\quad (23)$$

whose eigenvalues are

$$\frac{1}{2}[1 \pm \sqrt{1 - 4\delta^2(1 - t^2)}],\quad (24)$$

where

$$t = \langle e_{00}|e_{10}\rangle = \langle e_{11}|e_{01}\rangle = e^{-2\frac{1+\xi-\eta}{1+\xi}\alpha^2}.\quad (25)$$

Note also that, independent of m , it holds

$$S(\rho_B^0) = S(\rho_B^1).\quad (26)$$

(3) For ρ , we obtain

$$G = \frac{1}{2} \begin{pmatrix} 1 - \epsilon & \delta s & \delta t & (1 - \epsilon)stu \\ \delta s & \epsilon & est/u & \delta t \\ \delta t & est/u & \epsilon & \delta s \\ (1 - \epsilon)stu & \delta t & \delta s & 1 - \epsilon \end{pmatrix} \quad (27)$$

with

$$u = e^{4\frac{\xi\sqrt{\eta}}{1+\xi}\alpha|m|}. \quad (28)$$

The eigenvalues of G in equation (27) can be written as

$$\frac{1}{4u}(v_+ \pm \sqrt{v_+^2 - w_+}), \quad \frac{1}{4u}(v_- \pm \sqrt{v_-^2 + w_-}), \quad (29)$$

where we defined

$$\begin{aligned} v_{\pm} &= u \pm st[\epsilon + (1 - \epsilon)u^2], \\ w_{\pm} &= 4\delta^2u[st(1 - u)^2 \pm (1 - s^2)(1 - t^2)u]. \end{aligned} \quad (30)$$

Plugging equations (22) and (26) into equation (17), we clearly observe that $S(\rho_A^i)$ is responsible for the behaviour of χ_E in case of the DR, whereas $S(\rho_B^i)$ is responsible for the behaviour of χ_E in case of the RR: the difference between the behaviour of the Holevo quantities for the DR and RR comes from the difference between $S(\rho_A^i)$ and $S(\rho_B^i)$.

4. Secret fractions

Now we come to the point to evaluate the secret fraction r of the protocol under the entangling cloner attack. Here, the secret fraction r is given by the average of the information difference:

$$r = \sum_{S=\pm\alpha} \int dm P(m, S) \Delta I, \quad (31)$$

where

$$\Delta I = I_{AB} - \chi. \quad (32)$$

Here, the integral is taken over the region where $\Delta I \geq 0$. This means that we perform a post-selection to the parameter region where the accessible information of Alice and Bob exceeds that of Eve. This corresponds to the selection in step (v). Note that the joint probability density $P(m, S)$ satisfies $P(m, S) = P(m|S)P(S) = P(m|S)/2$, since $P(\pm\alpha) = 1/2$. We also note that

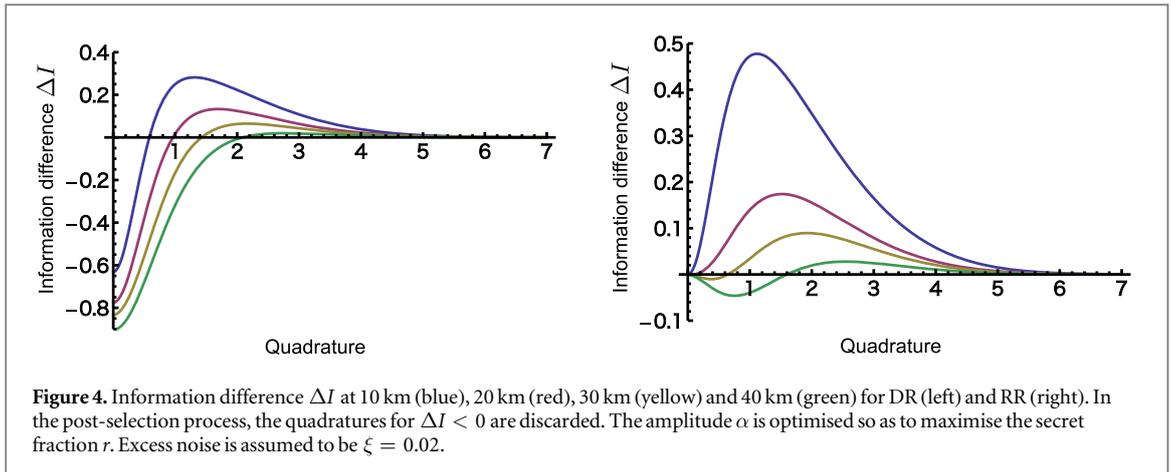
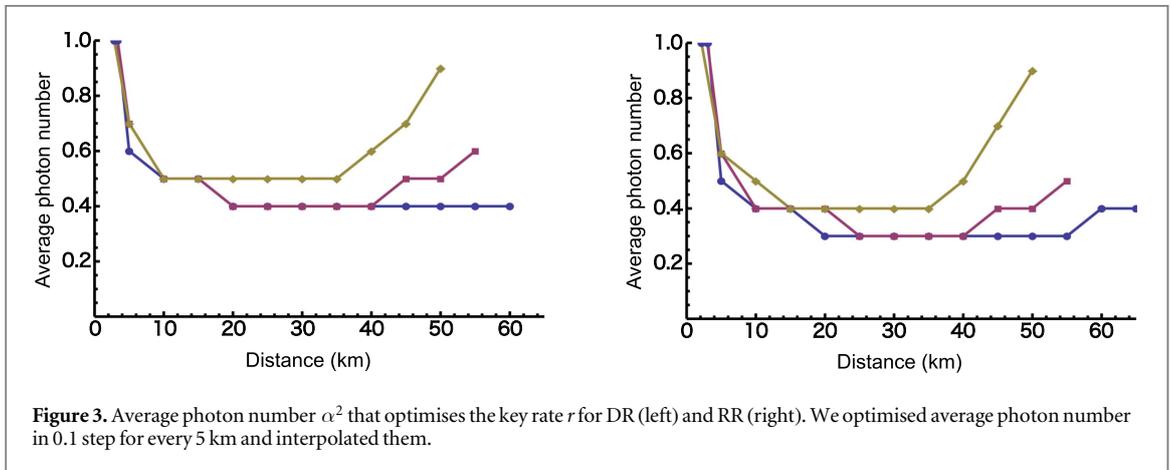
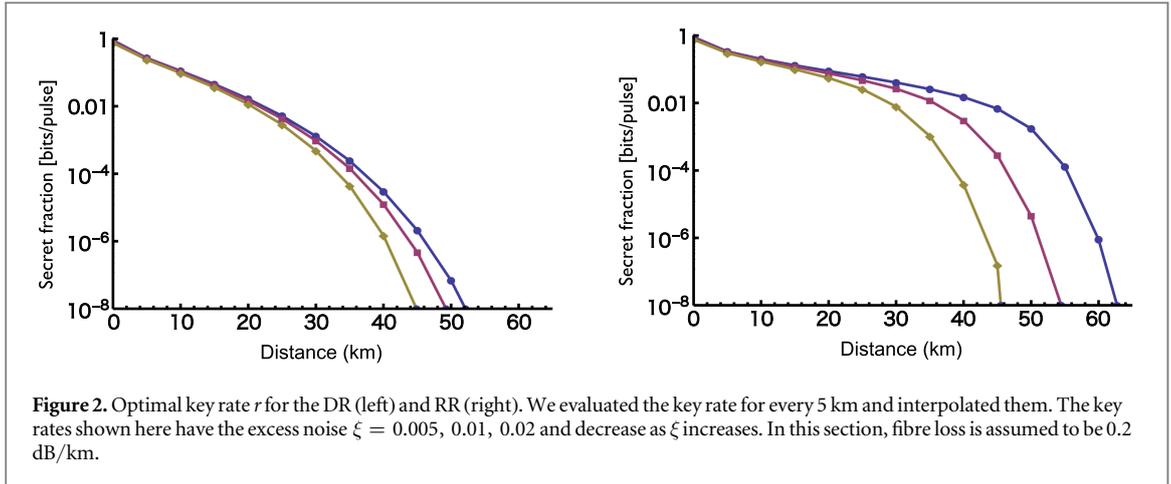
$$\Delta I_{m,S} = \Delta I_{-m,-S}, \quad (33)$$

since ϵ, s, t, u are symmetric with respect to the conversions $S \rightarrow -S$ and $m \rightarrow -m$, respectively. By using equations (3) and (33), we can rewrite the secret fraction r as the following simpler form

$$r = \int dm P(m|\alpha) \Delta I. \quad (34)$$

Figure 2 shows the optimised secret fractions in the cases of DR and RR, respectively. In the short distance less than 10 km, these two schemes make not so much difference in the secret fraction. In contrast to this, in a longer-distance, RR clearly yields the better secret fraction than DR, as shown in a CV-QKD with Gaussian modulations [22]. Unlike the secret fraction, however, the associated average photon number in DR shows the similar behaviour to that in RR (see figure 3).

The information difference ΔI at the optimal case is of interest, since it determines how many measurement outcomes should be chosen by the post-selections. From figure 4, we observe the followings. First, there is at most one non-zero zero point such that $\Delta I = 0$ in both the schemes. Thus, it turns out that the post-selection should be performed over the outcomes whose absolute values are larger than this zero point. Note that this post-selection scheme is exactly the same as that in [5] introduced so as to reduce the bit error rate of sifted keys. Second, RR requires almost no post-selection in the short distance less than about 20 km for the excess noise $\xi = 0.02$ when the error correction is ideal, whereas DR requires post-selection for the several distances we examined. Third, the zero point for DR is in general larger than that for RR. This implies that the former yields the smaller secret fraction, consistent with the direct evaluation of r .



Let us define the post-selection rate p as

$$p = \sum_{S=\pm\alpha} \int dm P(m, S). \quad (35)$$

Figure 5 shows p at the parameters that optimise the key rate of figure 2. RR almost attains $p = 1$ in the short-distance region, in parallel to the observation drawn from figure 4. The behaviours of p in the both reconciliations are basically same to those of the optimal r , respectively.

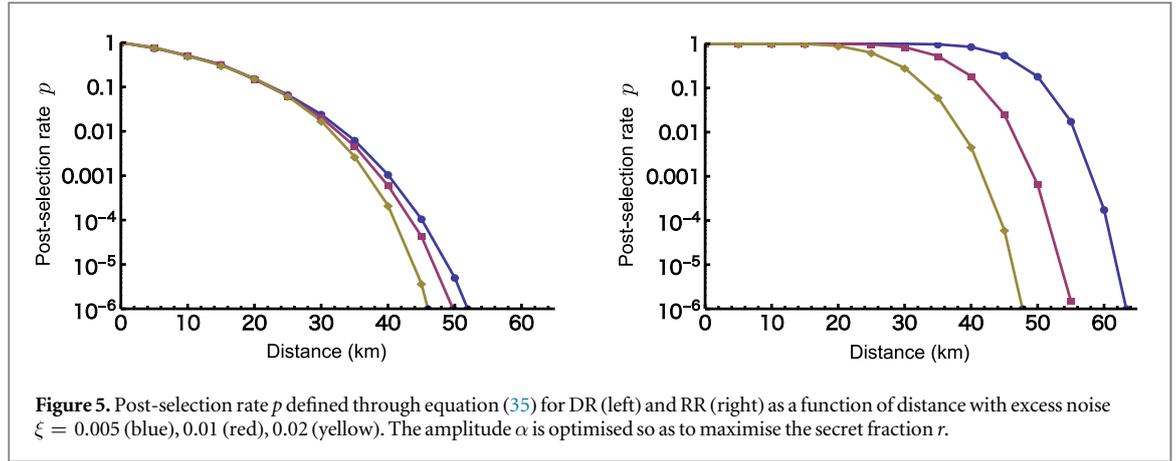


Figure 5. Post-selection rate p defined through equation (35) for DR (left) and RR (right) as a function of distance with excess noise $\xi = 0.005$ (blue), 0.01 (red), 0.02 (yellow). The amplitude α is optimised so as to maximise the secret fraction r .

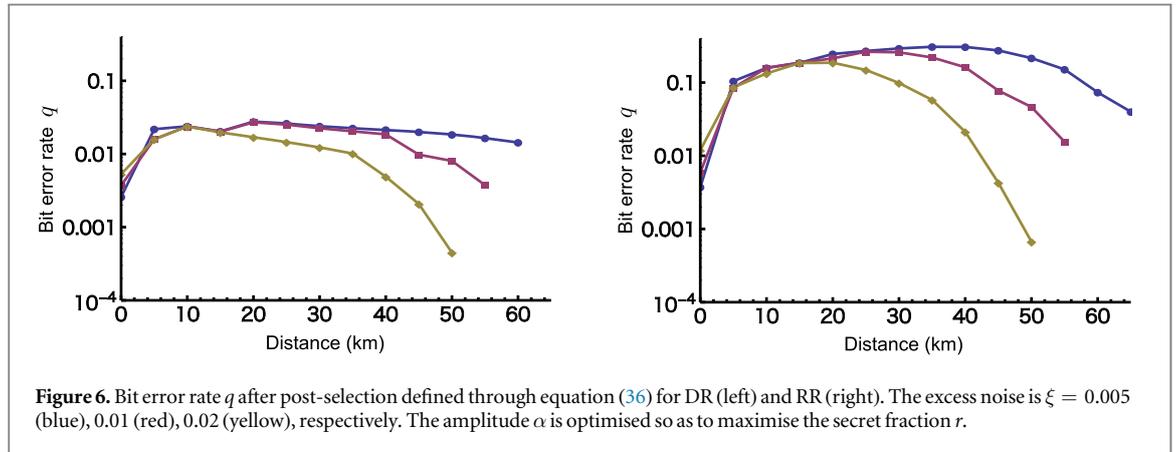


Figure 6. Bit error rate q after post-selection defined through equation (36) for DR (left) and RR (right). The excess noise is $\xi = 0.005$ (blue), 0.01 (red), 0.02 (yellow), respectively. The amplitude α is optimised so as to maximise the secret fraction r .

After the post-selection, average bit error rate reads

$$q = \frac{1}{p} \left[\int_{R_-} dm P(m, \alpha) + \int_{R_+} dm P(m, -\alpha) \right], \quad (36)$$

where R_- , (R_+) is the region of the negative (positive) m with $\Delta I \geq 0$ when $S = \alpha$, ($-\alpha$). Figure 6 shows clear contrast of the behaviour of q depending on the reconciliation scheme: DR has $q = \mathcal{O}(10^{-2})$ at most, whereas RR has $q = \mathcal{O}(10^{-1})$. Thus, we find that to attain the optimal key rate in RR, it is essential to employ an error correction code which works under considerably high bit error rate.

Secure key generation rate N_{secure} is expressed using the secret fraction r by the following equation:

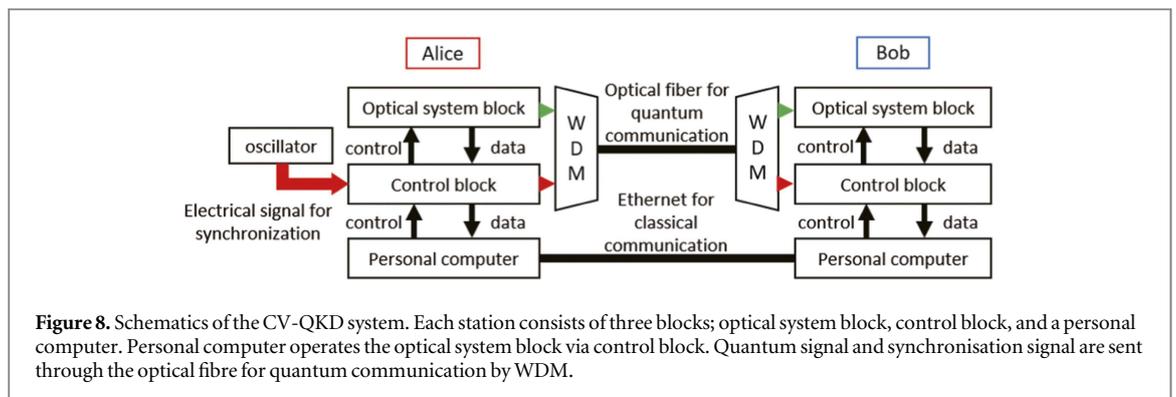
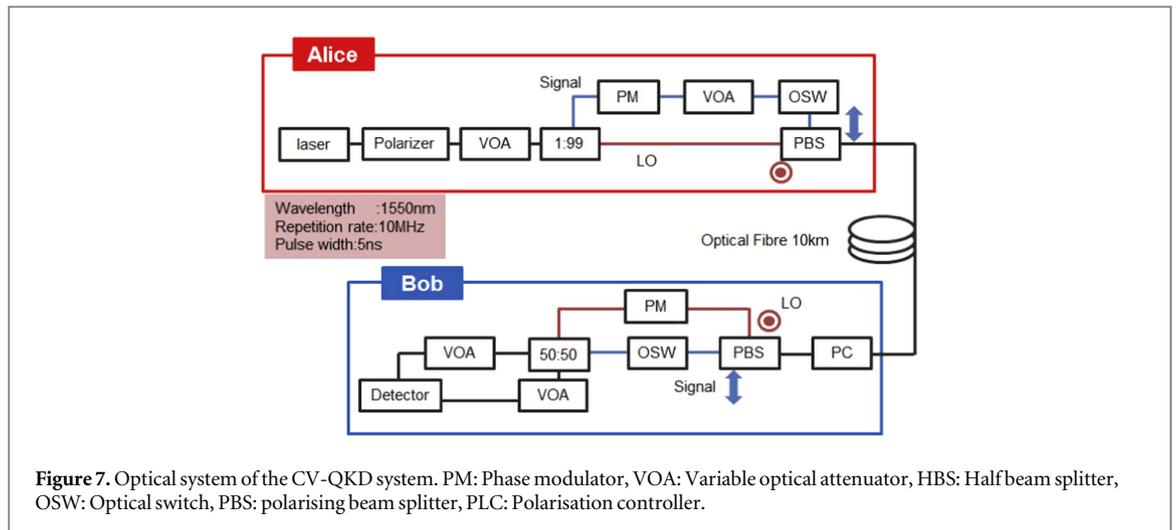
$$N_{\text{secure}} = f_{\text{pulse}} \eta_{\text{sys}} \eta_{\text{est}} \eta_{\text{pr}} r, \quad (37)$$

where f_{pulse} is a repetition rate of the light pulse, η_{sys} is the operating efficiency of the QKD machine, $1 - \eta_{\text{est}}$ is the fraction used for parameter estimation, η_{pr} is the efficiency of the QKD protocol. In the present implementation, $f_{\text{pulse}} = 10$ MHz, $\eta_{\text{sys}} \sim 0.3$ due to the slow data transfer rate explained below, $\eta_{\text{est}} = 0.5$. And η_{pr} is the probability of correct basis measurement and it is set to 0.5.

5. Experimental implementation

In figure 2, we observe that even though RR offers higher secret fraction, when the distance is longer than 30 km, the secret fraction is sensitive to the value of excess noise. However when the distance of a quantum channel is shorter than 20 km, the secret fraction is insensitive to excess noise. This insensitivity relaxes the requirements for the experimental system and makes stable key generation easier. The target of the present implementation is this relatively short-distance operation [33].

Figure 7 shows the schematic of our optical setup. The optical system includes Alice's and Bob's apparatus, and quantum channel. All of components in the optical system including a homodyne receiver are off-the-shelf fibre components and commercially available. We use a DFB laser of 1550 nm wavelength as a light source. Repetition frequency of the light pulse is 10 MHz and the pulse duration is 5 nsec. The optical configuration is a



polarisation and time division multiplexed interferometer. In order to stabilise the relative phase between the signal and LO pulse, we packaged the interferometer part of Alice's and Bob's components with thermal insulation materials. Light pulse from the laser is split by a beam splitter of 1:99 ratio. Weaker light is used as the signal light and stronger light is as the LO. The signal light is randomly phase modulated into one of four states by a phase modulator (PM), then attenuated to an appropriate intensity by a variable optical attenuator (VOA). The signal and LO light enter an optical fibre with orthogonal linear polarisations and also with a time delay of about 50 nsec with each other. Since the polarisation is not maintained in the quantum channel, a polarisation controller (PL) is placed at the entrance of Bob's apparatus. Then, the LO and the signal are split by a polarising beam splitter (PBS). The LO light is randomly phase modulated by a PM: Bob randomly selects x - or p - measurement. Finally, the signal and LO are combined at a half beam splitter, and two outputs incident to two optical paths and reach balanced photo detectors and the quadrature amplitude of the signal light is measured by homodyne detection. Two VOAs in front of photo detectors are used to balance the light intensity of two outputs.

Figure 8 shows the schematics of our CV-QKD system. Each station consists of three blocks; the optical system block, a control block, and a personal computer. From the optical block of Alice, quantum signals are sent to Bob, and they are received by the optical block of Bob. The components such as VOAs in optical blocks can be controlled by applying voltages from control blocks. The control blocks contain commercially available FPGA boards with daughter boards that perform Analogue-to-Digital conversion (ADC) and Digital-to-Analogue conversion (DAC) and are used to control the optical components in optical blocks. The FPGA boards operate with a master clock of 100 MHz which is generated by an oscillator. This clock is sent from Alice's block to Bob's block by 1310 nm light using Small Form-factor Pluggable (SFP) modules. The quantum signal and the clock light are transmitted over the same path by wavelength-division multiplexing (WDM). The control blocks are also equipped with ICs for generating random numbers. The random number generator ICs can generate physical random numbers at 1 Mbps. Pseudo-random numbers can be generated by FPGAs for 10 MHz operation. Personal computers (PC) and the FPGA boards are connected by USB cables. The output of the homodyne receiver is recorded by an ADC board connected to a PCI-express bus of the PC. PCs are also equipped with GPU cards to accelerate the software-based post-processing. We use non-binary LDPC code [34]

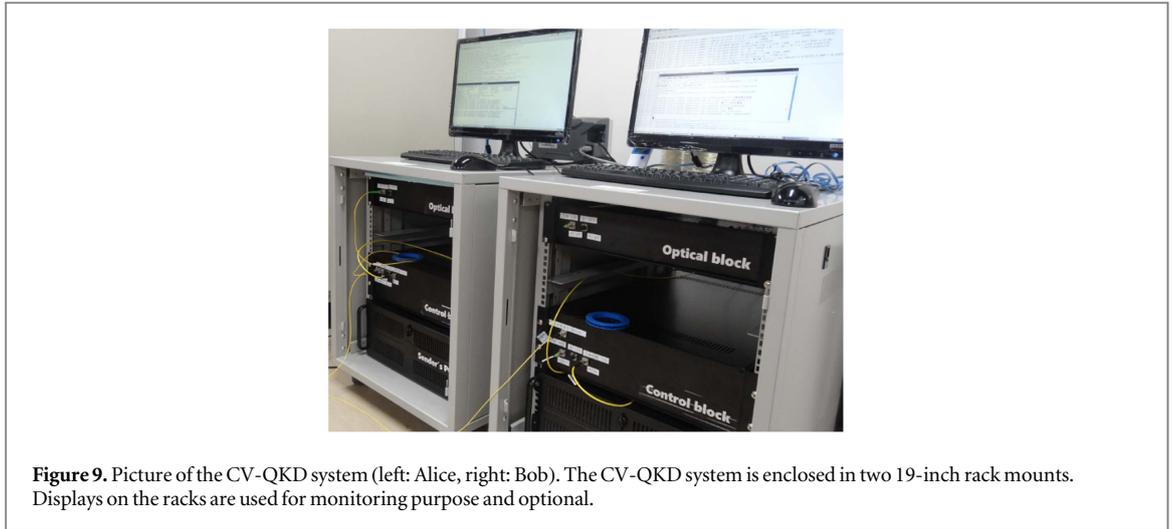


Figure 9. Picture of the CV-QKD system (left: Alice, right: Bob). The CV-QKD system is enclosed in two 19-inch rack mounts. Displays on the racks are used for monitoring purpose and optional.

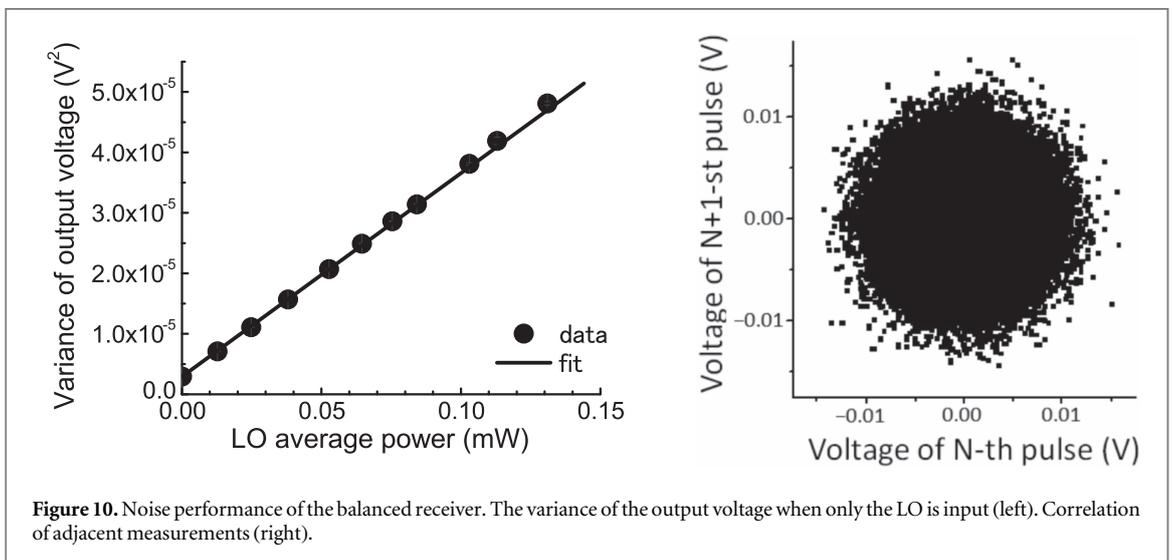


Figure 10. Noise performance of the balanced receiver. The variance of the output voltage when only the LO is input (left). Correlation of adjacent measurements (right).

for error correction (RR) and a fast privacy amplification algorithm using the Toeplitz matrix multiplication [35] (see [appendix](#)). Alice's station and Bob's station are enclosed in two 19-inch rack mounts as shown in figure 9.

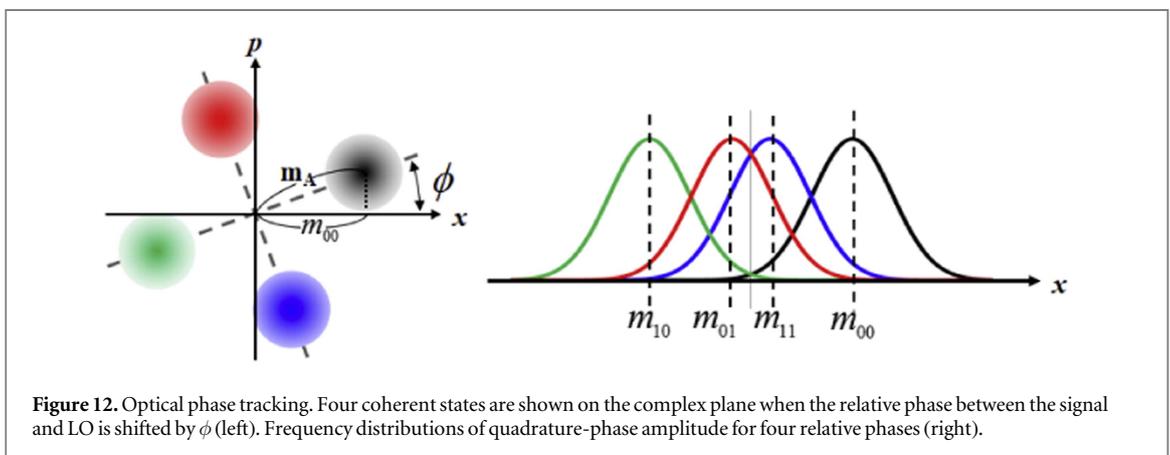
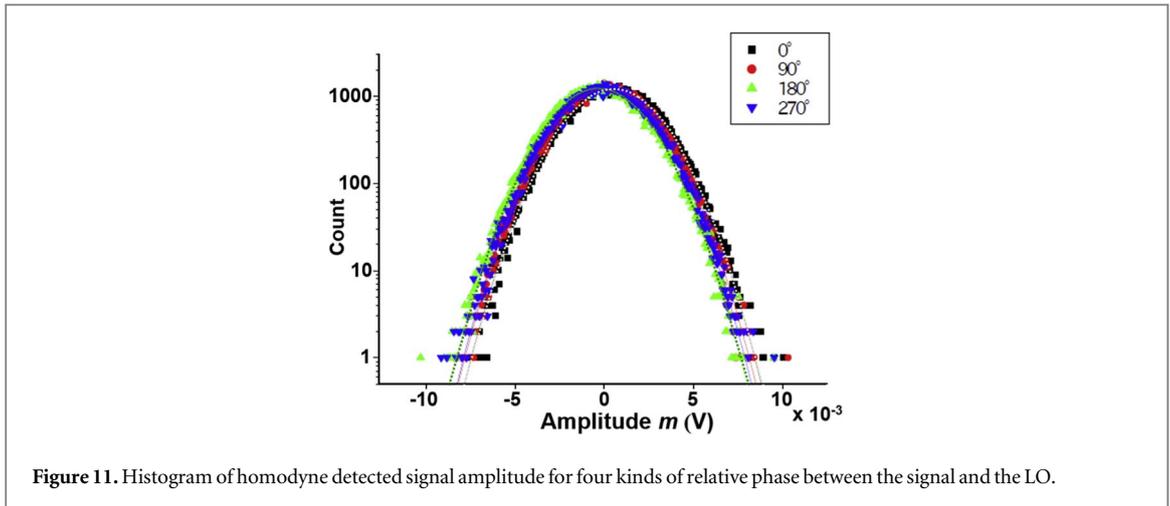
Figure 10 shows the noise characteristics of the commercially available balanced receiver (General photonics, BPD-001-50) used for homodyne detection. In the figure on the left, the variance of the output voltage when the photo detectors are irradiated only by the LO is shown as a function of the average power of the LO light. As the average power of the LO increases, the variance of output voltage increases linearly. This linear dependence indicates that shot-noise-limited homodyne detection is possible using the commercial receiver. When the average power of the LO is 0.1 mW, the shot noise level is about 10 times larger than the dark noise of the receiver.

In the time domain, correlation between measured values of the N -th pulse and the $(N + 1)$ -st pulse was investigated in order to know whether adjacent pulses could be measured independently. In the right of figure 10 we observe an isotropic distribution and the correlation coefficient of the data is less than 0.01, indicating that each pulse light can be independently measured.

In figure 11, typical distributions of the voltage output of the homodyne receiver for four kinds of relative phase between the signal and LO are shown in a semi-log scale. We can see that these distributions are well represented by Gaussian distribution. The average values of the amplitude m for 90 and 270 degrees data are almost zero, and those for 0 and 180 degrees data are plus and minus values, respectively.

6. Automated operation of CV-QKD system

In the key generation operation, Alice sends 10^6 pulses at a time and a half of them is used for the parameter estimation: In the parameter estimation, the mean values and variances of the measurement results for four



kinds of relative phases are calculated. From these values, excess noise and transmissivity of the quantum channel can be evaluated. In addition, the relative phase offset between the signal and the LO is obtained and this offset value is used to stabilise the phase offset. At present, this procedure can be repeated every 0.3 seconds; the repetition time is limited by the transfer time of random numbers from Alice's FPGA board to Alice's PC through a USB cable. By improving the transfer rate, three times faster operation will be possible.

6.1. Optical phase tracking

The optical system shown in figure 7 is basically a Mach-Zehnder interferometer. The relative phase between the signal and LO should be kept stable with higher accuracy than the wavelength of the light. Especially in the case of CV-QKD, the relative phase variation must be made very small in order to keep excess noise small.

The relative phase offset between the signal and LO can be estimated relatively easily in four-state CV-QKD. In figure 12, the effect of phase offset is schematically shown. Let be the average value of the measured voltage for the relative phase $\theta_{ij} = i \times \pi + j \times \pi/2$ ($i, j = 0$ or 1) $m_{ij} = m_A \cos(\theta_{ij} + \phi)$, here m_A is the amplitude of the signal and ϕ is the phase offset. Then, from the measured average values m_{ij} , the amplitude m_A is calculated as $m_A = \sqrt{\sum m_{ij}^2}/2$ and the phase offset ϕ is calculated as the average of $\arccos(m_{ij}/m_A) - \theta_{ij}$. This phase offset value is fed to the voltage of the phase modulator in Bob's optical box. Typical phase fluctuation after stabilisation is 0.05 radian. Excess noise can be kept less than 0.02 for most of the time. When the phase offset is suddenly increased, such data are discarded.

6.2. Real-time key generation

In a real operation, it is necessary to take account the efficiency of the error correction in the secret fraction. When the error correction efficiency f is not unity, the mutual information between Alice and Bob is given as

$$I'_{AB} = 1 - fh(\epsilon). \quad (5')$$

Then the secret fraction is modified to $r' = \int dm P(m|\alpha) \Delta I'$, where $\Delta I' = I'_{AB} - \chi$ and the integral is taken over the region where $\Delta I' \geq 0$. The compression factor of the classical post-processing, r_{comp} , is defined as the

Table 1. Post-selection rate and compression factor. Error correction efficiency f is set to be 1.3.

Excess noise	Distance (km)	Photon number	p	r_{comp}
0.5%	1	4.3	0.960208	0.648948
	5	2.7	0.820866	0.349567
	10	2.2	0.64053	0.214132
1%	1	4.2	0.956934	0.624086
	5	2.7	0.817244	0.336959
	10	2.2	0.631302	0.203932
2%	1	4.1	0.952484	0.578773
	5	2.8	0.818266	0.310443
	10	2.3	0.624872	0.182115

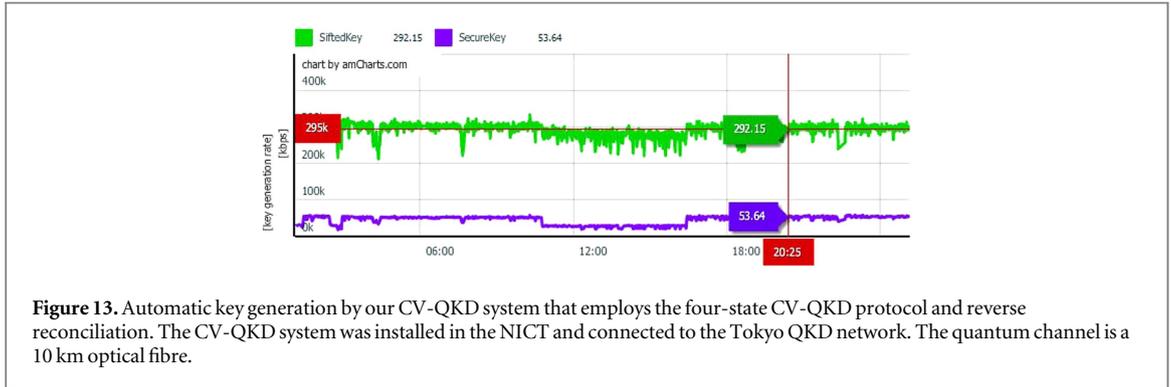


Figure 13. Automatic key generation by our CV-QKD system that employs the four-state CV-QKD protocol and reverse reconciliation. The CV-QKD system was installed in the NICT and connected to the Tokyo QKD network. The quantum channel is a 10 km optical fibre.

ratio of the secret fraction to the post-selection rate p :

$$r_{\text{comp}} = r'/p. \quad (38)$$

Table 1 shows numerical examples of the post-selection rate and the compression factor. In this numerical calculation, the channel loss is 0.2 dB/km, the error correction efficiency is $f = 1.3$, and the signal photon number $|\alpha|^2$ is optimised.

Figure 13 shows an example of key generation results. This is the data when the CV-QKD system was installed in the NICT facility and connected to the Tokyo QKD network [36, 37]. The quantum channel is a 10 km optical fibre. Sift key rate is about 300 kbps and secure key rate is about 50 kbps.

We performed RR using non-binary LDPC code [34]. The error correction efficiency parameter was set to be 1.3 although the code can operate stably even when the f parameter is 1.08 and error rate is 0.15. The speed of error correction is about 300 kbps per thread using a GPU (GTX 680). Privacy amplification was performed by Toeplitz matrix multiplication [35]. Its calculation complexity can be reduced to $O(n \log n)$ for an input length n by exploiting the FFT algorithm.

In an automated operation, the compression factor is calculated by using a linear approximation function for numerical calculation shown in table 1, that gives the compression factor as functions of transmissivity and excess noise. Here we assume that Eve cannot control Bob's receiver which has optical loss and excess noise. We also assume that Eve's knowledge about the sift key when Bob has an ideal receiver is smaller than her knowledge about the sift key when Bob uses a lossy and noisy receiver because in the RR Eve has to infer lossy and noisy signal in the latter situation. Under these assumptions, the Holevo quantity in the former situation, χ , should be larger than that in the latter situation, χ' :

$$\chi \geq \chi'. \quad (39)$$

In addition, we assume that the mutual information between Alice and Bob in the latter situation, H'_{AB} , is larger than that in the former situation, H_{AB} :

$$H'_{AB} \geq H_{AB}. \quad (40)$$

This assumption on mutual information can be satisfied when the error rate in the latter case (actual experiment) is set be smaller than that in the former case (ideal calculation) by increasing the threshold of post-selection. When equations (39) and (40) are satisfied, the following equation holds;

$$\Delta I' = H'_{AB} - \chi' \geq H_{AB} - \chi = \Delta I. \quad (41)$$

That means the compression factor shown in table 1 can be safely used for the actual experiment where Bob uses a lossy and noisy receiver. In the experiment, the post-selection rate was kept about 0.4 which is smaller than the numerical calculation shown in table 1.

7. Summary

We described the security and experimental implementation of the four-state CV-QKD protocol using post-selection. We evaluated the secret fraction of the protocol against a collective attack both for DR and RR. As the quantum channel becomes longer, RR yields better secret fraction than DR. When the distance is shorter than 30 km, the secret fraction is insensitive to the value of the excess noise and this makes experimental implementation easier.

We experimentally demonstrated automated secure key generation with a rate of 50 kbps when a quantum channel is a 10 km optical fibre. A commercially available balanced receiver is used to realise shot-noise-limited pulsed homodyne detection. We use a non-binary LDPC code for error correction and the Toeplitz matrix multiplication for privacy amplification. A GPU card is used to accelerate the software-based post-processing. Real-time stabilisation of relative phase between the signal and LO has been demonstrated. The present CV-QKD system is simple and can be built at low cost, and it is possible to achieve better performance in the future. We believe the present implementation will make a significant contribution toward practical popularisation of QKD.

Acknowledgements

This work was partially supported by the Commissioned Research of 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). TI is grateful to Hosho Katsura, Toshihiko Sasaki and Shu Tanaka for valuable discussions.

Appendix

In this appendix, we explain details of software-based post-processing used in our system.

Error correction by a non-binary LDPC code

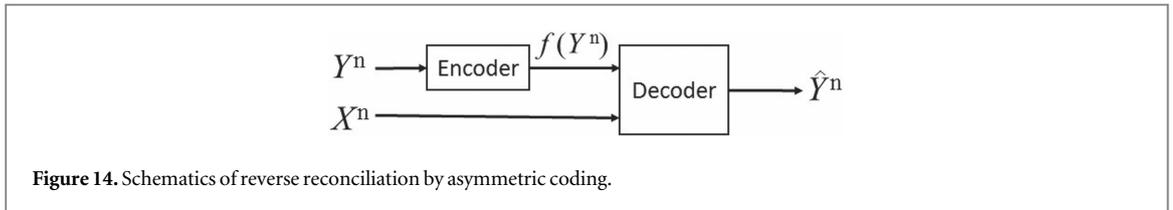
Non-binary LDPC codes were invented by Gallager [38] and it was found by Davey and MacKay that it can show better performance than binary LDPC codes [39]. In the case of the LDPC codes, it is necessary to choose properly from a collection of codes that are optimised for multiple error rates. By utilising a rate-compatible non-binary LDPC code which supports a wide-range of rates, it is possible to simplify the error-correction system while achieving efficient information reconciliation [40].

Details of the error correction procedure used in the present CV-QKD system is as follows. After Bob and Alice obtained their sifted keys, i.e. after step (vi) explained in section 2, Bob has an n -bit binary string $Y^n = (Y_1, Y_2, \dots, Y_n)^T$ and Alice has $X^n = (X_1, X_2, \dots, X_n)^T$. They know an estimate of bit error rate of their sift keys. In the reverse reconciliation scenario, the goal of the error correction is for Alice to reproduce a string \hat{Y}^n by conversation with Bob over a public channel. The content of the conversation depends on Y^n , and $c(Y^n)$ denotes the content of the conversation. The error correction should have the following properties:

- the probability of $Y^n \neq \hat{Y}^n$ is sufficiently close to zero; and
- the mutual information $I(Y^n; c(Y^n))$ is as small as possible.

The second property is important because Alice and Bob must subtract $I(Y^n; c(Y^n))$ bits from the corrected key during the privacy amplification procedure as $I(Y^n; c(Y^n))$ is the amount of information leaked to Eve during the conversation over the public channel. We can use a good error correction method by saving the number of bits in $c(Y^n)$ while enabling Alice to decode Y^n from X^n and $c(Y^n)$.

Schematics of the reverse reconciliation by an asymmetric coding is shown in figure 14 [40]. The encoder only uses Y^n for generating the codeword $f(Y^n)$. The decoder uses both $f(Y^n)$ and X^n . In the reverse reconciliation, Bob has Y^n and Alice has X^n . Therefore, Bob generates the codewords $f(Y^n)$ from Y^n and sends $f(Y^n)$ to Alice. Then Alice uses the decoder for recovering Y^n . The amount of information leaked to Eve is estimated as $I(Y^n; f(Y^n)) \leq H(f(Y^n)) \leq$ the number of bits in $f(Y^n)$. If the length of $f(Y^n)$ is shorter, upper



bound on the leaked information is smaller. LDPC codes can be used for the asymmetric coding [41]. At some fixed rate, the information bits are encoded as a syndrome of an irregular LDPC code. The information can be estimated by an efficient algorithm, belief propagation decoding, with a help from the syndrome and the correlated information. However, in an actual QKD system, the bit error rate of the sift keys may fluctuate with time. In this case, the encoder and decoder must be equipped with multiple LDPC codes: each irregular LDPC code of channel coding rate R_c is designed to have lower decoding error probability over channel with $H(Y|X)$ which is as close to the bound $1 - R_c$ as possible. A rate-adaptive error correction scheme with a set of optimised irregular LDPC codes for multiple channel coding rates were proposed by Elkouss *et al* [42]. However, since the number of LDPC codes equipped is limited in an actual QKD system, Alice and Bob have to use one of the LDPC codes equipped that may have degraded performance for the actual sift-key data. This degradation leads to the so-called saw effect [42].

A rate-compatible coding uses only a single mother LDPC code and can solve the issue of the saw effect. Two of the authors of this paper (KK and RM) and Sakaniwa proposed an error correction scheme in conjunction with rate-compatible non-binary LDPC codes [40]. The $(2, d_c)$ -regular non-binary LDPC code on the Galois field $GF(2^p)$ with $2^p \geq 64$ are empirically known as the best performing error-correction codes. In the present CV-QKD implementation, we use a $(2, 3)$ -regular non-binary LDPC code on $GF(256)$. The main shortcoming of non-binary LDPC codes is decoding complexity. We use a programme that uses GPUs for faster processing. The programme can be downloaded from one of the authors (KK) web site [34].

Privacy amplification using Toeplitz matrix multiplication

Privacy amplification is a procedure to extract random numbers unknown to third parties by applying a random hash function to a random source which may be partially leaked to third parties. This procedure is realised with a help of another auxiliary random source which is public and called a random seed. The most typical random hash function for this purpose is the universal₂ hash function, and the most widely used of it is the one using the (modified) Toeplitz matrix [35]. The hash function using the Toeplitz matrix allows an efficient implementation with complexity of $O(n \log n)$ for input length n and with a short seed length.

The Toeplitz matrix is a matrix whose diagonal elements are all same. It is parametrised by $r = (r_1, r_2, \dots, r_{n-1}) \in \{0, 1\}^{n-1}$ as

$$T(r) = \begin{pmatrix} r_m & r_{m+1} & \cdots & r_{n-1} \\ r_{m-1} & r_m & \cdots & r_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ r_1 & r_2 & \cdots & r_{n-m-1} \end{pmatrix}. \quad (42)$$

For example, a multiplication of a 3×4 Toeplitz matrix and a four-element vector $z = (z_1, z_2, z_3, z_4)^T$ outputting a three-element vector $y = (y_1, y_2, y_3)^T$ is written as

$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} r_3 & r_4 & r_5 & r_6 \\ r_2 & r_3 & r_4 & r_5 \\ r_1 & r_2 & r_3 & r_4 \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \end{pmatrix}. \quad (43)$$

This can be embedded in a multiplication of a square matrix and a vector by concatenating extra elements to vectors y, z as

$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ * \\ * \\ * \end{pmatrix} = \begin{pmatrix} r_3 & r_4 & r_5 & r_6 & r_1 & r_2 \\ r_2 & r_3 & r_4 & r_5 & r_6 & r_1 \\ r_1 & r_2 & r_3 & r_4 & r_5 & r_6 \\ r_6 & r_1 & r_2 & r_3 & r_4 & r_5 \\ r_5 & r_6 & r_1 & r_2 & r_3 & r_4 \\ r_4 & r_5 & r_6 & r_1 & r_2 & r_3 \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \\ 0 \\ 0 \end{pmatrix}. \quad (44)$$

As explained in appendix C of [35], a multiplication of a square Toeplitz matrix and a vector can be performed by three calculations, i. e., two discrete Fourier transforms (DFT), a convolution and an inverse Fourier transform. Since the complexity of a DFT is $O(n \log n)$ using the FFT algorithm and the complexity of convolution is $O(n)$, the total complexity of the multiplication is $O(n \log n)$.

References

- [1] Bennett C H and Brassard G 1984 *Proceeding of the IEEE International Conference on Computers Systems, and Signal Processing, Bangalore, India* (New York: IEEE) 175–9
- [2] Rivest R L, Shamir A and Adleman L M 1978 *Commun. ACM* **21** 120
- [3] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301
- [4] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
- [5] Hirano T, Yamanaka H, Ashikaga M, Konishi T and Namiki R 2003 *Phys. Rev. A* **68** 042331
- [6] Grosshans F, Van Assche G, Wenger J, Brouri R, Cerf N J and Grangier P 2003 *Nature* **421** 238
- [7] Jouguet P et al 2013 *Nat. Photon.* **7** 378
- [8] Wang Chao, Huang Duan, Huang Peng, Lin Dakai, Peng Jinye and Zeng Guihua 2015 *Sci. Rep.* **5** 14607
- [9] Huang Duan, Huang Peng, Lin Dakai and Zeng Guihua 2016 *Sci. Rep.* **6** 19201
- [10] Imre S and Gyongyosi L 2012 *Advanced Quantum Communications—An Engineering Approach* (Hoboken, New Jersey: Wiley-IEEE Press)
- [11] Hanzo L, Haas H, Imre S, O'Brien D, Rupp M and L Gyongyosi 2012 Wireless myths, realities, and futures: from 3G/4G to optical and quantum wireless *Proc. IEEE* **100** 1853–88 Issue: Special Centennial Issue
- [12] Nakazawa M et al ECOC2016, paper W.4.P1.SC5.59. <http://ieeexplore.ieee.org/document/7767755/>
- [13] Gottesman D, Lo H-K, Lütkenhaus N and Preskill J 2004 *Quant. Info. Compu.* **4** 325–60 <http://rintonpress.com/journals/qicabstracts/qicabstracts4-5.html>
- [14] Grosshans F and Grangier P 2002 *Phys. Rev. Lett.* **88** 057902
- [15] Silberhorn C, Ralph T C, Lütkenhaus N and Leuchs G 2002 *Phys. Rev. Lett.* **89** 167901
- [16] Hirano T, Konishi T and Namiki R [quant-ph/0008037](http://arxiv.org/abs/quant-ph/0008037)
- [17] Leverrier A, Alléaume R, Boutros J, Zémor G and Grangier P 2008 *Phys. Rev. A* **77** 042325
- [18] Leverrier A and Grangier P [quant-ph/1002.4083](http://arxiv.org/abs/quant-ph/1002.4083)
- [19] Namiki R and Hirano T 2004 *Phys. Rev. Lett.* **92** 117901
- [20] Leverrier A and Grangier P 2009 *Phys. Rev. Lett.* **102** 180504
- [21] Grosshans F and Grangier P 2003 *Quant. Info. Compu.* **3** 535
- [22] Heid M and Lütkenhaus N 2007 *Phys. Rev. A* **76** 022313
- [23] Leverrier A 2015 *Phys. Rev. Lett.* **114** 070501
- [24] Gyongyosi L and Imre S 2014 *SPIE Photonics West OPTO 2014, Advances in Photonics of Quantum Computing, Memory, and Communication VII* **8997** 89970C
- [25] Mraz A, Imre S and Gyongyosi L 2016 *IEEE Signal Processing Conference Proceedings, 2016 24th European Signal Processing Conference (EUSIPCO 2016), section on Quantum Communications Budapest, 29 Aug–2 Sept* (<https://doi.org/10.1109/EUSIPCO.2016.7760298>)
- [26] Leverrier A and Grangier P 2011 *Phys. Rev. Lett.* **106** 259902
- [27] Fossier S, Diamanti E, Debuisschert T, Villing A, Tualle-Brouri R and Grangier P 2009 *New J. Phys.* **11** 045023
- [28] Huang D, Huang P, Li H, Wang T, Zhou Y and Zeng G 2016 *Opt. Lett.* **41** 3511
- [29] Diamanti E, Lo H-K, Qi B and Yuan Z 2016 *npj Quantum Information* **2** 16025
- [30] Symul T, Alto D J, Assad S M, Lance A M, Weedbrook C, Ralph T C and Lam P K 2007 *Phys. Rev. A* **76** 030303(R)
- [31] Nielsen M A and Chuang I C 2000 *Quantum Information and Quantum Computation* (Cambridge: Cambridge University Press)
- [32] Jozsa R and Schlienz J 2000 *Phys. Rev. A* **62** 012301
- [33] Matsuura T et al 2016 *Proc. SPIE 9996, Quantum Information Science and Technology II* October 24 **9996** 99960S
- [34] Kasai K, Fujisaka Y and Onsjö M 2009 <http://comm.ce.titech.ac.jp/~kenta/index-e.html>
- [35] Hayashi M and Tsurumaru T 2016 *IEEE Trans. Inf. Theory* **62** 2213
- [36] Sasaki M et al 2011 *Optics Express* **19** 10387–409
- [37] <http://tokyoqkd.jp/>
- [38] Gallager R G 1963 *Low Density Parity Check Codes, in Research Monograph Series* (Cambridge: MIT Press)
- [39] Davey M and MacKay D 1998 *IEEE Commun. Lett.* **2** 165–7
- [40] Kasai K, Matsumoto R and Sakaniwa K 2010 *Proc. of International Symposium on Information Theory and its Applications (ISITA 2010) 922–7 Taichung, Taiwan* <https://doi.org/10.1109/ISITA.2010.5649550>
- [41] Liveris A, Xiong Z and Georgiades C 2002 *IEEE Commun. Lett.* **6** 440–2
- [42] Elkouss D, Leverrier A, Alleaume R and Boutros J J 2009 *Proc. 2009 IEEE International Symposium on Information Theory* pp 1879–83