IEICE Communications Express, Vol.13, No.7, 268–271

ComEX

LETTER

Error-control information reconciliation scheme for continuous-variable quantum key distribution using fixed-bit polar codes

Kensuke Yamaura[1, a)], **Hiroyuki Endo**[2], **Eiji Okamoto**[1], **Masahide Sasaki**[2], **Mikio Fujiwara**[2], **and Morio Toyoshima**[2]

Abstract A challenging issue in continuous-variable quantum key distribution (CV–QKD) is the improvement in error correction efficiency because random number bits are encoded in a quadrature of faint optical pulses. Herein, we propose an error-control information reconciliation method for CV-QKD based on our recently proposed fixed-bit polar code. In the present scheme, unreliable bits are embedded in the prepared "fixed bits," enabling the detection and reproduction of errors in these bits without error correction, effectively improving the error-correction efficiency. Numerical simulations demonstrate that the efficiency of the proposed scheme is 10% higher than that of polar code-based reconciliation without fixed bits.

Keywords: continuous-variable quantum key distribution, information reconciliation, polar codes, fixed bit polar codes

Classification: Fiber-optic transmission for communications

1. Introduction

Quantum key distribution (QKD) [1, 2] can establish a key that is secure against plausible physical attacks and unlimited computational resources. QKD protocols can be classified into two branches, based on whether the discrete or continuous nature of the quantum is exploited. In the latter scheme, continuous-variable QKD (CV-QKD) [3, 4], a sender (Alice) encodes a random bit into a quadrature of faint coherent-state pulses, and a receiver (Bob) utilizes a homodyne (or heterodyne) detector. CV-QKD protocols have the advantage of lower implementation costs because their components are compatible with those used in conventional optical communication. Furthermore, they are insensitive to stray light owing to a local oscillator.

Because random bits are encoded in faint optical pulses in CV-QKD, the homodyne detector outputs highly erroneous outcomes. The discrepancies in the shared bit sequences between Alice and Bob should be corrected in classical post-processing after quantum signal transmission. Error correction in QKD, or information reconciliation, accompanies information exchange over an authenticated public channel. The exposed information is regarded as leaked and deleted in the subsequent privacy amplification step, which decreases the total length of the generated secure key. Therefore, a highly efficient error correction scheme is crucial for the development of long-distance and high-speed CV-QKD systems.

One method to realize a highly efficient information-reconciliation scheme involves utilizing highly efficient error-correction codes. Among these, polar codes [5] are gaining considerable attention because they support a higher error-correction performance approaching the Shannon limit at lower computational costs for encoding and decoding. Polar codes have been applied to reconciliation schemes for CV-QKD [6] and other QKD protocols [7, 8].

Recently, inspired by punctuation schemes in polar codes [9], we proposed "fixed-bit polar codes" [10]. In fixed-bit polar codes, the sender and receiver can agree on the values of some code word bits before transmission. Therefore, errors in these bits can be detected and reproduced without error correction at the receiver side [10]. We refer to these bits as "fixed bits," from which the name of the scheme is derived. Although fixed bits degrade the error-correction performance of polar codes, they can be employed for additional functions. We proposed the application of fixed-bit polar codes for channel estimation in free-space optical communications [10] and decoding complexity reduction in chaos modulation [11].

Herein, we propose the application of fixed-bit polar codes for the reverse information reconciliation of an easily implementable four-state CV-QKD protocol [4]. In the four-state CV-QKD, Bob obtains a bit value by distinguishing the measurement outcome output from the homodyne detector. These outcomes work as a measure of the unreliability of the received bits. Bob can reassign unreliable received bits as fixed bits to negate the contribution of these bits in the error correction process. The process can be regarded as the control of the quantum bit error rate (QBER), and the proposed scheme is termed "error-control information reconciliation" based on fixed-bit polar codes, to stress the difference between other schemes without fixed bits [7]. Numerical results show that the proposed method achieves approximately 10% higher efficiency than existing polar code-based information reconciliation.

2. Four-state CV-QKD protocol

We summarize the procedure in a four-state CV-QKD protocol [4]:

Step 1. Alice randomly sends one of four coherent states $\{|\pm\alpha\rangle, |\pm i\alpha\rangle\}$ to Bob over a quantum channel.

Step 2. Bob performs homodyne measurement on the re-

[1] Graduate School of Engineering, Nagoya Institute of Technology, Gokiso-cho, Showa-ku, Nagoya, Aichi 466-8555, Japan
[2] National Institute of Information and Communications Technology, Nukui-Kitamachi, Koganei, Tokyo 184-8795, Japan
[a)] k.yamaura.186@nitech.jp

DOI: 10.23919/comex.2024XBL0050
Received March 13, 2024
Accepted April 19, 2024
Publicized May 9, 2024
Copyedited July 1, 2024

ceived coherent state by randomly setting the phase of the local oscillator to 0 ($\hat{x}$-measurement) or $\pi/2$ ($\hat{p}$-measurement.) The measurement outcome $m \in \mathbb{R}$ follows a Gaussian distribution owing to the quantum noises, the electrical noises in receiving apparatus, and the excess noises caused by malicious attacks by Eve.

Step 3. Upon repeating Steps 1 and 2 several times, Alice and Bob expose the bases they used over the public channel. The bases are correct when Alice sends $|\pm\alpha\rangle$ ($|\pm i\alpha\rangle$) and Bob performs $\hat{x}$-measurement ($\hat{p}$-measurement.) Otherwise, bases are considered incorrect.

Step 4. Bob distinguishes the measurement outcome m measured in correct basis into a bit value based on a certain threshold $T > 0$. He assigns bit 1 for $m > T$ and bit 0 for $m < -T$. If m falls into $[-T, T]$, he discards it because the bit would be erroneous. Bob then discloses the locations of the discarded outcomes.

Step 5. Alice assigns a bit value to the coherent states to which Bob assigns a bit value. Bits 1 and 0 are assigned to $\{|+\alpha\rangle, |+i\alpha\rangle\}$ and $\{|-\alpha\rangle, |-i\alpha\rangle\}$, respectively.

Step 6. Alice and Bob estimate the QBER by exchanging randomly extracted test bits from the common locations of their bit sequences. The test bits are discarded. The remaining bit sequences are called "sifted keys."

Step 7. (Reverse information reconciliation) Bob calculates the information required for error correction (correction information) and discloses it to Alice. Alice performs an error correction and obtains an estimation of Bob's sifted key. We call the resulting bit sequences "reconciled keys."

Step 8. (Privacy amplification) Alice and Bob compress their reconciled keys to delete leaked information, which includes the contribution of Eve's attack and the correction information disclosed in Step 7. We call the resulting keys "final keys."

3. Proposed error-control information reconciliation based on fixed-bit polar codes

First, the basics of polar codes are described. Polar codes are characterized by a linear transformation represented by an N-order square matrix

$$\begin{cases} \mathbf{G}_N = \begin{bmatrix} \mathbf{G}_{N/2} & \mathbf{0} \\ \mathbf{G}_{N/2} & \mathbf{G}_{N/2} \end{bmatrix} \\ \mathbf{G}_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \end{cases}. \tag{1}$$

Figure 1 illustrates the butterfly-like transformation for $N = 8$. This transformation divides an N-bit input sequence $\mathbf{u} := [u_1, \ldots u_N]$ into reliable bits (with higher channel capacity) or unreliable bits (with lower channel capacity). To encode K-bit message $\mathbf{m} := [m_1, \ldots m_K]$ using polar codes, the sender assigns $\mathbf{m}$ onto the reliable bits. The values of remaining $(N-K)$-bits $\mathbf{f} := [f_1, \ldots, f_{N-K}]$ can be set arbitrary and should be shared between the sender and receiver in advance. We call the bits $\mathbf{f}$ frozen bits. The codeword $\mathbf{c} := [c_1, \ldots, c_N]$ of polar codes is then obtained as

$$\mathbf{c} = \mathbf{u}\mathbf{G}_N. \tag{2}$$

The coding rate of the polar codes is defined as $R = K/N$. The decoding of polar codes proceeds in the reverse direction

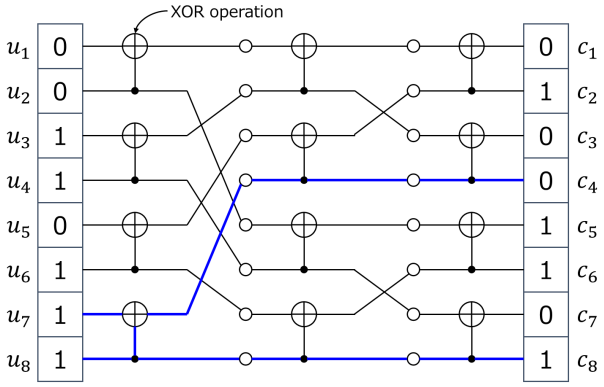

Fig. 1 Illustration of transformation in Eq. (1) for $N = 8$. A symbol $\oplus$ denotes the XOR operation of two inputs.

of encoding.

Subsequently, we introduce the fixed-bit polar codes. As shown in Fig. 1, the number of input bits $u \in \mathbf{u}$ that contributes to a codeword bit $c \in \mathbf{c}$ is different for each c. For example, all input bits contribute to c_1. In contrast, c_8 equals to u_8, and c_4 is an XOR of u_7 and u_8 (see blue lines). Therefore, if the sender and receiver share the values of u_7 and u_8, the receiver can detect the errors in c_4 and c_8 and reproduce them without error correction. We call these bits in the codeword "fixed bits." Generally, provided by the number $N_\mathrm{f} = 2^n$ (n is an integer) of fixed bits, they appear at every N_f bit in the codeword $\mathbf{c}$ and are calculated from some of the tail N_f bits of the input sequence $\mathbf{u}$. We present a formal description of the encoding process for fixed-bit polar codes as follows:

(1) The tail N_f bits in input sequence $\mathbf{u}$ are set as frozen bits to induce fixed bits.
(2) Assign the $N - K - N_f$ bits with the lowest channel capacity out of the remaining bits in $\mathbf{u}$ as frozen bits.
(3) As in normal polar codes, assign message bits $\mathbf{m}$ to the remaining bits in $\mathbf{u}$, and encode $\mathbf{u}$ into codeword $\mathbf{c}$.

The concept of fixed bits differs from that of frozen bits. The frozen bits belonging to the input sequence $\mathbf{u}$ are selected before encoding based on the channel capacity of each input bit. However, the fixed bits belong to codeword $\mathbf{c}$. In fixed-bit polar codes, the input bits that induce fixed bits are selected from frozen bits for efficient sharing. However, these bits are located at the tail of the input bits, regardless of the channel capacity, which degrades the error-correction performance of polar codes in exchange for the useful properties provided by the fixed bits [10, 11].

Finally, we describe the proposed fixed-bit polar code-based error-control information reconciliation scheme in a four-state CV-QKD. A flowchart of the scheme is illustrated in Fig. 2, and the detailed procedure is provided below.

(1) Alice and Bob share a coding rate R determined based on the estimated QBER, a fixed bit length N_f, a frozen bit table with which they determine the locations of the frozen bits and their values.
(2) Bob inputs his sifted key $\mathbf{b}$ into the swap operation to swap an unreliable bit in $\mathbf{b}$ with a bit at the fixed-bit location that appears in every N_f bit. This step is illustrated in Fig. 3. Although we simply set $T = 0$ in this example, this scheme can be applied for any

values of T. The fixed-bit locations are at b_4 and b_8, for $N_f = 2$. The most unreliable bit is b_3 as its measurement outcome is the closest to $\alpha = 0$. Bob then swaps b_3 and b_4. In addition, he swaps b_6 and b_8. He repeats the operation until the unreliable bits are located at the fixed-bit locations, and obtains a swapped key $\mathbf{b}'$.

(3) Bob transmits the location of the swapped bits to Alice. She applies a swap operation similar to Bob on her sifted key $\mathbf{a}$ and obtains a swapped key $\mathbf{a}'$.

(4) Bob generates a K-bit random sequence from his random bit generator (RBG) as information bits $\mathbf{m}$.

(5) Alice and Bob agree on the frozen bits $\mathbf{f}$ including fixed bits, by referring to the preshared information listed in Step (1).

(6) Bob constructs an input sequence $\mathbf{u}$ from information bits $\mathbf{m}$ and frozen bits $\mathbf{f}$. He inputs $\mathbf{u}$ into a polar encoder and obtains a codeword $\mathbf{c}$ with fixed bits.

(7) Bob calculates a bitwise XOR between polar codeword $\mathbf{c}$ and swapped key $\mathbf{b}'$. He transmits the resultant sequence $\mathbf{c} \oplus \mathbf{b}'$ to Alice.

(8) Alice calculates bitwise XOR between her swapped key $\mathbf{a}'$ and the sequence transmitted from Bob. She obtains the resultant sequence $(\mathbf{c} \oplus \mathbf{b}') \oplus \mathbf{a}'$.

(9) Alice reproduces the fixed bits in $(\mathbf{c} \oplus \mathbf{b}') \oplus \mathbf{a}'$ and then inputs it into a polar decoder to obtain an estimation $\mathbf{m}'$ of message sequence.

(10) Bob and Alice adopt message bit $\mathbf{m}$ and its estimation $\mathbf{m}'$ as their reconciled keys.

The swap operation in Step (2) is the core of the proposed scheme. The sequence $(\mathbf{c} \oplus \mathbf{b}') \oplus \mathbf{a}'$ generated in Step (8) can be regarded as the erroneous version of $\mathbf{c}$, on which the discrepancies between $\mathbf{b}'$ and $\mathbf{a}'$ are transferred. The swap operation ensures that the error bits in $(\mathbf{c} \oplus \mathbf{b}') \oplus \mathbf{a}'$ caused by the unreliable bits in $\mathbf{b}'$ are at the fixed bits and hence reproduced before error correction. Thus, the QBER is suppressed, and the error-correction efficiency is effectively enhanced. We should investigate the leaked information during the swap operation. In the process, Bob only discloses the locations of the swapped bits. This information did not include the values of the sifted keys. Therefore, the swap operation prevents the leakage of information from the sifted key.

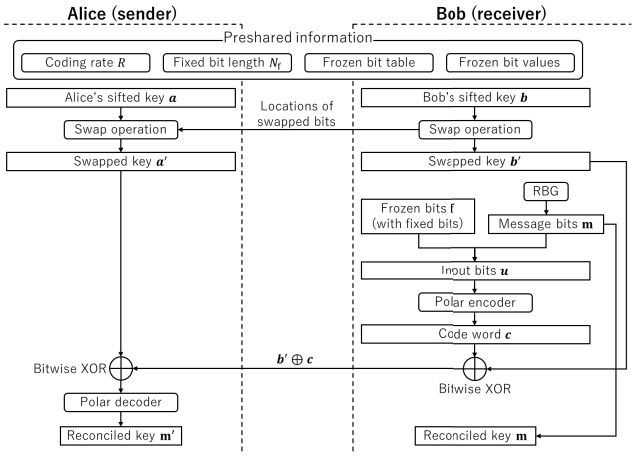

Fig. 2 Flowchart of proposed error-control reconciliation method based on fixed-bit polar codes.

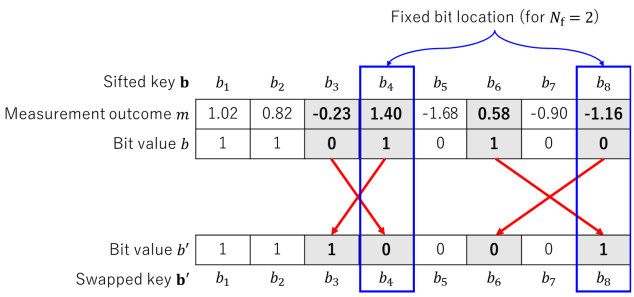

Fig. 3 Example of swap operation with $N_f = 2$ and $T = 0$.

4. Numerical evaluation of the proposed scheme

We present the results of a numerical simulation to verify the error-correction performance of the proposed scheme. As a figure of merit, we utilized the error-correction efficiency, defined as

$$\eta = N_{\mathrm{rec}}/N_{\mathrm{sift}}, \tag{3}$$

where N_{sift} denotes sifted key length and N_{rec} denotes reconciled key length. The larger the η, the more efficient the information reconciliation becomes. The code length N was set to 2048, frozen bit table was determined using Monte Carlo method, and a successive cancellation list decoder with a list number of eight was used as the decoding algorithm.

Figure 4 shows an average value of η as a function of QBER for different coding rates R and fixed bit lengths N_f. Each curve has two regions: the plateau where the QBER is smaller, and the decreasing region where the QBER is larger; hence, the block error rate (BLER) increases. When $R = 0.75$ (solid lines), the curves for $N_f = 128$ (red line with circular markers) and 256 (blue line with triangular markers) almost overlap and outperform those for $N_f = 512$ (green line with square markers). However, when $R = 0.5$ (dashed lines), the curve for $N_f = 512$ surpasses the others. This suggests increase in optimal N_f value with increase in coding rate R.

We also show the results for the polar code-based rec-

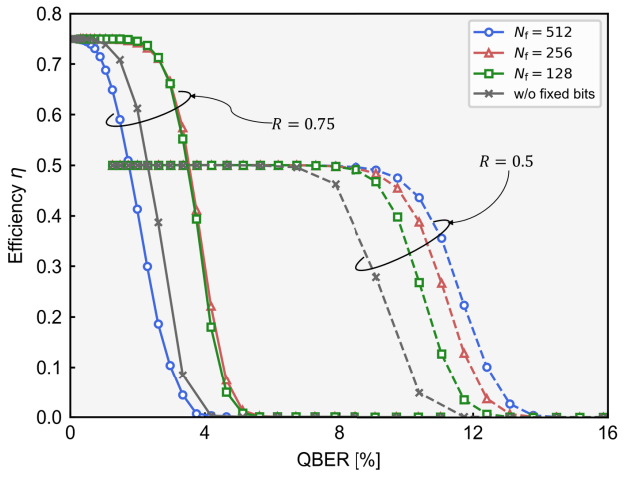

Fig. 4 Error correction efficiency.

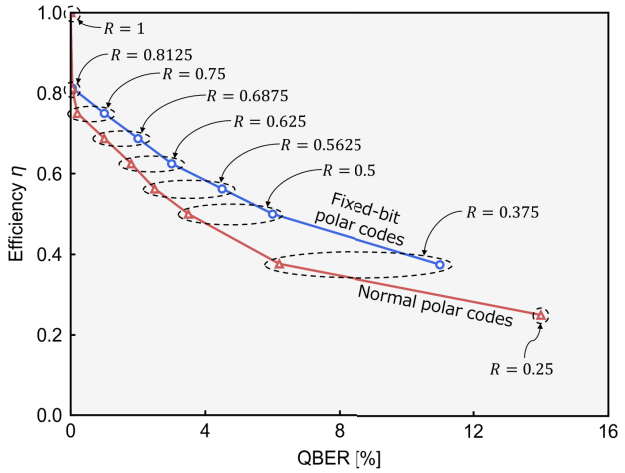

Fig. 5 Performance comparison with or without using fixed bits.

onciliation method without fixed bits (gray lines with cross markers), which are essentially the same as the protocol proposed in [7]. The comparison illustrates that the curve of the method without fixed bits is lower than that of the fixed-bit polar code-based method; specifically, the fixed bits improve the error-correction performance. However, when $R = 0.75$, the curve with $N_\mathrm{f} = 512$ is lower than that without fixed bits. In this case, all frozen bits (512 bits) are used to generate fixed bits. Except for such extreme cases, the improvement in error-correction performance induced by the fixed bits outweighs the reduction in error-correction performance.

In practical situations, Alice and Bob must select a coding rate such that the code corrects more errors with a lower BLER. Such a coding rate is located at the right-end of the plateau region of QBER-η curves. In Fig. 5, such points attaining a BLER of 10^{-5} are arranged for various coding rates. We simultaneously show the results of our proposed scheme based on a fixed-bit polar code (blue line with circular markers) and the scheme without fixed bits (red line with triangular markers) [7]. The fixed bit length N_f used for each coding rate R is set as follows:

$$N_\mathrm{f} = \begin{cases} 128\,(R > 0.75) \\ 256\,(0.75 \geq R > 0.5) \\ 512\,(R \leq 0.5) \end{cases} \tag{4}$$

The results show that the proposed method is more efficient in all QBER regions, with a maximum efficiency increase of approximately 10%, indicating the effectiveness of the proposed method.

5. Conclusion

We proposed an error-control information reconciliation scheme for four-state CV-QKD based on fixed-bit polar codes. Numerical calculations show that the proposed method can achieve an error-correction performance that is 10% higher than that of the polar code-based information reconciliation method without fixed bits [7]. This efficiency can be improved further by employing a more sophisticated decoding scheme aided by cyclic redundancy codes [8, 12]. The proposed scheme can contribute to the development of long-distance and high-speed CV-QKD systems. However, we only showed the efficacy of our method for a limited number of coding rates and fixed bit lengths, and clarified their behaviors. To implement our method in practical systems, intensive studies are required to determine the optimum length of the fixed bits.

References

[1] C.H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, vol. 560, pp. 7–11, Dec. 1984. DOI: 10.1016/j.tcs.2014.05.025

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum Cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, Jan. 2002. DOI: 10.1103/RevModPhys.74.145

[3] N.J. Cerf and P. Grangier, "From quantum cloning to quantum key distribution with continuous variables: a review (Invited)," *JOSA B*, vol. 24, no. 2, pp. 324–334, Feb. 2007. DOI: 10.1364/JOSAB.24.000324

[4] T. Hirano, H. Yamanaka, M. Ashikaga, T. Konishi, and R. Namiki, "Quantum cryptography using pulsed homodyne detection," *Phys. Rev. A*, vol. 68, no. 4, 042331, Oct. 2003. DOI: 10.1103/PhysRevA.68.042331

[5] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Tran. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, July 2009. DOI: 10.1109/TIT.2009.2021379

[6] M. Zhang, H. Hai, Y. Feng, and X.-Q. Jiang, "Rate-adaptive reconciliation with polar coding for continuous-variable quantum key distribution," *Quantum Inf. Process*, vol. 20, no. 10, p. 318, 2021. DOI: 10.1007/s11128-021-03248-0

[7] S. Yan, J. Wang, J. Fang, L. Jiang, and X. Wang, "An improved polar codes-based key reconciliation for practical quantum key distribution," *Chin. JElectron.*, vol. 27, no. 2, pp. 250–255, 2018. DOI: 10.1049/cje.2017.07.006

[8] B.-Y. Tang, C.-Q. Wu, W. Peng, B. Liu, and W.-R. Yu, "Polar-code-based information reconciliation scheme with the frozen-bit erasure strategy for quantum key distribution," *Phys. Rev. A*, vol. 107, no. 1, 012612, 2023. DOI: 10.1103/PhysRevA.107.012612

[9] R. Wang and R. Liu, "A novel puncturing scheme for polar codes," *IEEE Commun. Lett*, vol. 18, no. 12, pp. 2081–2084, Dec. 2014. DOI: 10.1109/LCOMM.2014.2364845

[10] K. Yamaura, H. Ito, E. Okamoto, H. Endo, M. Sasaki, M. Fujiwara, and M. Toyoshima, "Adaptive polar coding scheme using hybrid pilot and frozen bits for satellite laser communications," *IEICE Commun. Express*, vol. 12, no. 9, pp. 480–485, Sept. 2023. DOI: 10.1587/comex.2023XBL0085

[11] K. Asano, T. Abe, K. Kato, E. Okamoto, and T. Yamamoto, "High-quality and low-complexity polar-coded radio-wave encrypted modulation utilizing multipurpose frozen bits," *IEICE Trans. Commun.*, vol. E106-B, no. 10, pp. 987–996, Oct. 2023. DOI: 10.1587/transcom.2022EBT0007

[12] K. Niu and K. Chen, "CRC-aided decoding of polar codes," *IEEE Commun. Lett.*, vol. 16, no. 10, pp. 1668–1671, Oct. 2012. DOI: 10.1109/LCOMM.2012.090312.121501