International Conference on Space Optics—ICSO 2020

Virtual Conference

30 March–2 April 2021

Edited by Bruno Cugny, Zoran Sodnik, and Nikos Karafolas

Study on application of polar codes to information reconciliation in free-space quantum key distribution

International Conference on Space Optics — ICSO 2020, edited by Bruno Cugny, Zoran Sodnik,
Nikos Karafolas, Proc. of SPIE Vol. 11852, 118525L · © 2021 ESA and CNES
CCC code: 0277-786X/21/$21 · doi: 10.1117/12.2599964

Study on application of polar codes to information reconciliation in free-space quantum key distribution

Yuma Yamashita*[a], Hiroyuki Endo[b], Shingo Fujita[a], Eiji Okamoto[a], Hideki Takenaka[b], Morio Toyoshima[b]

[a]Department of Electrical and Mechanical Engineering, Graduate School of Engineering, Nagoya Institute of Technology, Gokiso-cho, Showa-ku, Nagoya, Aichi, Japan 466-8555;
[b]National Institute of Information and Communications Technology, 4-2-1 Nukui-Kitamachi, Koganei, Tokyo, Japan 184-8795

ABSTRACT

Quantum key distribution (QKD) is a technology to securely share keys against any attack physically permitted, with the principle of quantum mechanics. In recent years, the satellite QKD, which employs artificial satellites as trusted mobile nodes, has been attracting attention in order to overcome the bottleneck of transmission distance. However, in the satellite QKD, quality degradation due to atmospheric effects is expected, as in ordinary satellite laser communications. Therefore, it is desirable to apply an error-correcting code (ECC) that has high error-correcting performance even under the atmospheric-induced effects to the error-correcting process of the satellite QKD. Therefore, in this paper, we examined the application of polar codes, which is known as an ECC with high error correction capability. First, in order to optimize the error correction efficiency, we propose a method to adaptively obtain an appropriate code rate for the received signal strength that changes momentarily due to atmospheric effects. Then, we compare the throughput performances with polar codes to it with low-density parity-check (LDPC) codes, with the numerical simulation assuming Bennett-Brassard 1984 protocol (BB84).

Keywords: Free space optics, satellite laser communications, quantum key distribution, information reconciliation, polar codes, low-density parity-check codes

1. INTRODUCTION

Various encryption technologies have been developed to meet the fundamental needs to transmit information to a specific person at a distance without being known by a third party. Nowadays, various information is encrypted, from credit card-based personal identification numbers (PINs) to social networking service (SNS) conversations. However, the security of current encryption technologies is based on the assumption of computational resources available to eavesdroppers, and it is concerned that the decryption will be available by the progress of computer technology. Quantum key distribution (QKD) [1, 2], on the other hand, is a key establishment method that does not require any assumptions on the eavesdropper's computational resources. In QKD, a key is generated from a random number shared between the sender and the receiver via photon transmission. Because an eavesdropper cannot attack without destroying the photon's quantum state, the trace of attack is left in the quantum bit error rate (QBER). This makes key establishment secure against all physically allowable attacks. Although QKD has already been studied for practical use [3, 4], fiber-based terrestrial QKD systems suffer from photon absorption in the fiber, limiting the key generation rate and the transmission distance. Recently, satellite-based QKD systems [5] are attracting much attention to overcome the bottleneck., continental-scale QKD can be realized by employing a satellite as a trusted node. However, there is a concern that the atmospheric effects, which affect the performance of satellite laser communications, such as fading-induced burst errors, may also have some impact on satellite-based QKD. Therefore, error-correction schemes exploited in satellite-based QKD are required for robust transmission against such atmospheric-induced effects.

As such an error-correction scheme appropriate for free-space optical (FSO) links, we have studied polar codes [6] because of their capacity-achieving performance and low computational complexity in encoding and decoding. Our past transmission experiment over the 7.8-km terrestrial FSO link between the University of Electro-Communications in Chofu, Tokyo, and the National Institute of Information and Communications Technology (NICT) in Koganei, Tokyo revealed that polar codes have high performance in real FSO channels [7].

Motivated by our previous experiments, we propose a new high-efficiency error correction method based on polar codes for free-space QKD systems. Unlike the uni-directional message transmission, QKD aims to share random numbers, and error correction is performed in the post-processing manner. This means that the code rate of polar codes can be finely configurated by adding or deleting parity bits. Although the application of polar codes to QKD has been studied in [8], a rate-variable error correction based on polar codes is firstly proposed in this paper. In this paper, as a basic study for applying polar codes to QKD, we derive a relation between code rate and QBER by numerical simulation to optimize the error correction efficiency. We then numerically compare the performance of our proposed scheme to that of LDPC codes. As a result, we reveal that polar codes have an advantage over LDPC codes in the short-code-length regime, in information reconciliation for free-space QKD.

The rest of this paper is organized as follows; Sections II and III review the encoding and decoding methods in polar codes and QKD basics, respectively. Section IV shows the description of the proposed method and the experimental results by numerical simulation. Finally, Section V gives the conclusions.

2. POLAR CODES

2.1 Encoding

Polar code is an error-correcting code (ECC) introduced by E. Arikan in 2009 [6]. It is shown that polar code achieves encoding and decoding with low complexity of $O(N\log N)$ for a code length of $N = 2^n$, where n is a natural number. The encoding exploits a property called channel polarization, which is outlined below.

We consider that we input a sequence with a length of $N = 2^n$ bits into a stationary memoryless binary symmetric channel (BSC) W. Let $I(W)$ denote the mutual information of the BSC. The input sequence is subject to the following matrix operations:

$$\begin{cases} \mathbf{G}_N = \mathbf{R}_N(\mathbf{F}\otimes\mathbf{I}_{N/2})(\mathbf{I}_2\otimes\mathbf{G}_{N/2}) \\ \mathbf{G}_1 = \mathbf{I}_1 \end{cases}. \tag{1}$$

where $\mathbf{I}_N$ is the identity matrix of order N, $\otimes$ denotes the Kronecker product, and $\mathbf{R}_N$ is a reverse shuffle matrix that rearranges the input bit sequence with even numbers in the first half and odd numbers in the second half. The matrix $\mathbf{F}$ is defined by

$$\mathbf{F} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}. \tag{2}$$

By applying the inverse operation of $\mathbf{G}_N$ onto the output sequence results, a $I(W)$ fraction of the sequence is retrieved correctly, whereas a $1 - I(W)$ fraction will results in an error with a probability 1/2 in the limit of $N \to \infty$. This phenomenon, known as channel polarization, allows polar codes to achieve error correction performance close to the Shannon limit.

A sender allocates the transmission data into the $I(W)$ fraction of the sequence (message bits). She fills the $1 - I(W)$ fraction of the sequence (frozen bits) with random bits, and announces their values and locations to the receiver in advance.

The code rate, the ratio of the message bits to the total bits, becomes $I(W)$, which is the channel capacity of BSC.

2.2 Decoding

The decoding method for polar codes is called successive cancellation decoding (SCD). In SCD, recursive estimation of codewords based on the log-likelihood ratio (LLR) is performed in the ascending order of every bit. When the vertical index is φ, and the horizontal index is Λ, the LLR at each point is L_Λ^φ and the estimated bit is $\hat{c}_\Lambda^\varphi$. Here, φ and Λ satisfy the following conditions:

$$0 \leq \Lambda \leq n, \tag{3}$$

$$0 \leq \varphi \leq N - 1. \tag{4}$$

The first step of decoding is to convert the received value of each bit r_φ into the LLR λ_φ. For a BSC with crossover probability P_e, λ_φ is given as

$$\lambda_\varphi = \begin{cases} \ln \dfrac{1-P_\mathrm{e}}{P_\mathrm{e}} \left(r_\varphi = 0\right) \\ \ln \dfrac{P_\mathrm{e}}{1-P_\mathrm{e}} \left(r_\varphi = 1\right) \end{cases}. \tag{5}$$

Then, the LLR L_Λ^φ at each point can be computed as follows

$$L_\Lambda^\varphi = \begin{cases} 2\tanh^{-1}\left(\tanh\left(\dfrac{\alpha}{2}\right)\cdot\tanh\left(\dfrac{\beta}{2}\right)\right)\begin{pmatrix} 1 \le \Lambda \le n \\ \varphi = 2\phi \end{pmatrix} \\ (-1)^u \alpha + \beta \begin{pmatrix} 1 \le \Lambda \le n \\ \varphi = 2\phi + 1 \end{pmatrix} \\ \lambda_\varphi (\Lambda = 0) \end{cases}, \tag{6}$$

where α, β, and u are defined by

$$\begin{cases} \alpha = L_{\Lambda-1}^{\{2\phi-(\phi \bmod 2^{\Lambda-1})\}} \\ \beta = L_{\Lambda-1}^{\{2^{\Lambda-1}+2\phi-(\phi \bmod 2^{\Lambda-1})\}} \\ u = \hat{c}_\Lambda^{2\phi} \end{cases}. \tag{7}$$

Finally, the estimated bit $\hat{c}_\Lambda^\varphi$ at each point is calculated by

$$\hat{c}_\Lambda^\varphi = \begin{cases} \hat{c}_{\Lambda+1}^{\varphi+\Phi} \oplus \hat{c}_{\Lambda+1}^{\varphi+\Phi+1} \left(0 \le \Lambda \le n-1, \Phi > 2^\Lambda\right) \\ \hat{c}_{\Lambda+1}^{\varphi-\Phi+\left(2\Phi \bmod 2^{\Lambda+1}\right)} \left(0 \le \Lambda \le n-1, \Phi \le 2^\Lambda\right) \\ 0\left(\Lambda = n, \mathcal{F}_\varphi = 0, L_n^\varphi > 0\right) \\ 1\left(\Lambda = n, \mathcal{F}_\varphi = 0, L_n^\varphi \le 0\right) \\ c_\varphi\left(\Lambda = n, \mathcal{F}_\varphi = 1\right) \end{cases}, \tag{8}$$

where Φ denotes (φ mod $2^{\Lambda+1}$) and $\mathcal{F}_\varphi$ returns 1 if the index φ is a frozen bit, and 0 otherwise. After LLR calculations, the estimated codeword $\hat{c}_n^\varphi$ is outputted.

For the decoding of polar codes, SCD was first proposed, and its improved version, successive cancellation list decoding (SCLD) [9], was also proposed. In addition, CRC-aided SCLD (CA-SCLD) [10], which is concatenated with cyclic redundancy check (CRC) codes, has been proposed as an improved version of SCLD, and it can outperform low-density parity-check (LDPC) codes.

3. QUANTUM KEY DISTRIBUTION

3.1 The flow of the QKD protocol

We briefly review the flow of QKD based on the Bennett-Brassard 1984 protocol (BB84) [1], which was the first proposed QKD protocol. In BB84, random numbers are encoded into a single photon's polarization state. A sender (Alice) generates a random bit sequence, selects one of two pairs of polarization directions, $(0,\ \pi/2)$ or $(\pi/4,\ 3\pi/4)$, and rotates the photon polarization to the corresponding direction. For example, to transmit bit 0, the photon polarization is rotated to 0 or $\pi/4$. Bob also randomly selects the basis from $(0,\ \pi/2)$ or $(\pi/4,\ 3\pi/4)$ when he receives a photon from Alice. If the Alice's and Bob's basis match, the bit is retrieved correctly, but if a different basis is selected, an error occurs with a probability of 50%. Such random selection of basis is necessary to ensure security against Eve. For example, Eve would tap a photon sent by Alice, obtain the random bit from it, and retransmit a copy of the photon to Bob. However, Eve needs to select Alice's basis randomly, just as Bob does. Therefore, even if Alice and Bob's bases are identical, this operation will induce errors in the bit values. After completing random number transmission, the sifted-keys are created by notifying the receiving time and matching Alice's and Bob's bases via an authenticated public channel. When this operation is performed, the bit positions that were in different bases between the sender and receiver are notified, and the bits are eliminated. If the protocol is implemented under ideal conditions, the sifted-keys are identical, but errors are caused by imperfections in the optical system, bit errors due to dark counting in photon detectors, and Eve's attack. Therefore, by exchanging information over the authenticated public channel, the error is corrected and the leakage information is removed. This sequence of operations is called the key-distillation processing.

The key-distillation processing roughly consists of (A) QBER estimation, (B) information reconciliation, and (C) privacy amplification. First, in (A), the QBER is estimated using a test bit sequences composed by random sampling from the sifted-keys. If the error rate exceeds the specified value, the session is discarded because the information leakage to Eve is too large to be removed by this key-distillation process. Then, in (B), the sifted-keys of Alice and Bob are error-corrected. Alice and Bob calculate the parity bits for error correction from their sifted-keys and exchange them on the public channel. Finally, in (C), privacy amplification, the final key is obtained by compressing the sifted-key after information reconciliation by the amount of leakage information estimated from the QBER.

3.2 Information Reconciliation

In this paper, we apply polar codes to (B) information reconciliation step in the above key-distillation processing. Although there are several methods for calculating the parity bits disclosed in this step, we adopt Dodis's method [11]. In this method, a codeword $\boldsymbol{c}_{\mathrm{EC}}$ is randomly generated by an ECC encoder of C_{EC}, and the exclusive-OR (XOR) of the codeword and the sifted-key is transmitted to the other party via the public channel. This method has been implemented in various systems [12, 13] because of its simplicity. Also, the cost of authentication is low because the authenticated public channel is used only once. Figure 1 shows the flowchart of Dodis's method. First, Bob determines an appropriate code rate R' based on the QBER P_{e}' and transmits R' value to Alice. Next, Bob generates a random bit sequence of $K(=\lceil NR' \rceil)$ bits, where $\lceil\cdot\rceil$ is the ceiling function and N is the length of the sifted-key. Then, these K bits are encoded into N bits codeword $\boldsymbol{c}_{\mathrm{EC}}$ by an ECC with the code rate of R', and XORed into Bob's sifted-key $\boldsymbol{\kappa}_{\mathrm{B}}$ as $\boldsymbol{\kappa}_{\mathrm{B}} \oplus \boldsymbol{c}_{\mathrm{EC}}$. Alice obtains the bit sequence $(\boldsymbol{\kappa}_{\mathrm{B}} \oplus \boldsymbol{c}_{\mathrm{EC}}) \oplus \boldsymbol{\kappa}_{\mathrm{A}}$ by XORing her sifted-key $\boldsymbol{\kappa}_{\mathrm{A}}$ with the received codeword, resulting in the error pattern $\boldsymbol{\kappa}_{\mathrm{A}} \oplus \boldsymbol{\kappa}_{\mathrm{B}}$ onto $\boldsymbol{c}_{\mathrm{EC}}$. This error can be removed by decoding the received sequence $(\boldsymbol{\kappa}_{\mathrm{A}} \oplus \boldsymbol{\kappa}_{\mathrm{B}}) \oplus \boldsymbol{c}_{\mathrm{EC}}$ because of R' encoding, and the random number generated at Bob can be correctly transmitted to Alice. This $\lceil NR' \rceil$ bits are the reconciled key. Note that we consider the case where Bob transmits the parity bits, and this method is generally called reverse reconciliation. It can generate keys more efficiently than the case of direct reconciliation in which Alice transmits keys. Therefore, it is widely used in continuous-variable QKD [14, 15] and other similar protocols [12, 16] as well as BB84.

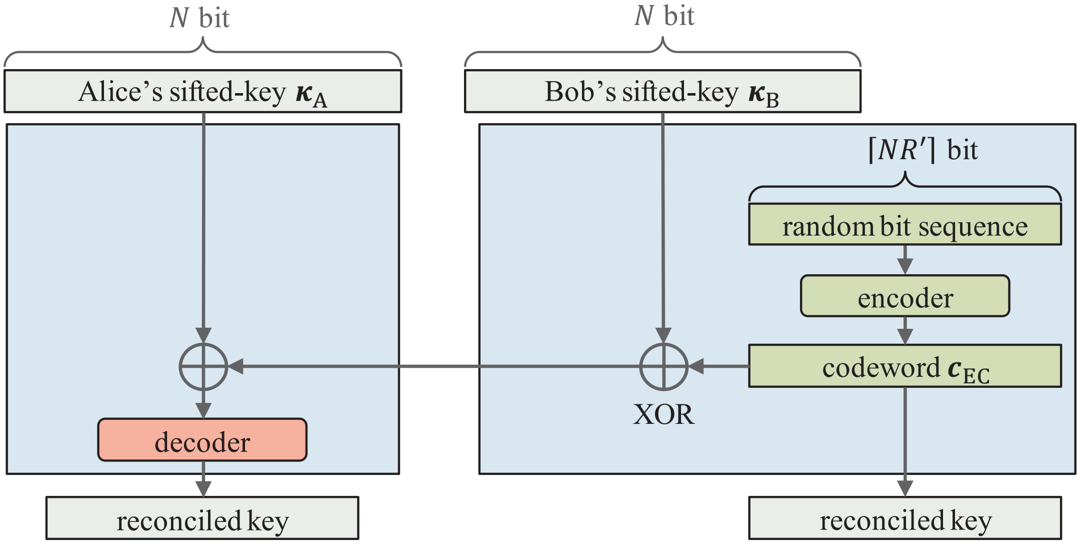
N bit
N bit
Alice's sifted-key $\boldsymbol{\kappa}_{\mathrm{A}}$
Bob's sifted-key $\boldsymbol{\kappa}_{\mathrm{B}}$
$\lceil NR' \rceil$ bit
random bit sequence
encoder
codeword $\boldsymbol{c}_{\mathrm{EC}}$
XOR
decoder
reconciled key
reconciled key

Figure 1. Flow chart for information reconciliation.

4. NUMERICAL RESULTS OF PROPOSED METHOD

4.1 Performance indicator

In this paper, we construct an efficient transmission scheme that makes the ratio of the length of the successfully information-reconciled bit sequence N_{corr} to the length of the sifted-key N_{sift}, $N_{\text{corr}}/N_{\text{sift}}$, as large as possible. At first, instead of encoding a random bit sequence of length N_{sift} with a single codeword, we consider dividing it into B blocks of length N_{B} and encoding them. The following equation holds:

$$N_{\text{sift}} = N_{\text{B}}B. \tag{9}$$

Then, we define block error rate (BLER) as the ratio of unsuccessful decoding to B expressed by

$$BLER = \frac{B_{\text{fail}}}{B}, \tag{10}$$

where B_{fail} is the number of unsuccessfully decoded blocks. Because N_{corr} is the product of the information length K_{B} and the number of successfully transmitted blocks, it can be denoted by

$$N_{\text{corr}} = K_{\text{B}}(B - B_{\text{fail}}). \tag{11}$$

Then, $N_{\text{corr}}/N_{\text{sift}}$ can be transformed as follows.

$$\begin{aligned}\frac{N_{\text{corr}}}{N_{\text{sift}}} &= \frac{K_{\text{B}}(B - B_{\text{fail}})}{N_{\text{B}}B}\\ &= R(1 - BLER),\end{aligned} \tag{12}$$

where R is the code rate defined by $K_{\text{B}}/N_{\text{B}}$. In this paper, we specify $R(1 - BLER)$ as the evaluation function called throughput. In numerical simulations, we assumed that the errors in the sifted-key are symmetric for the bit 0 or 1, that is, BSC. Furthermore, the QBER estimation is assumed to be perfect.

4.2 Performance of polar codes

We simulated the polar code transmission in information reconciliation described in Section 3, in which the simulation conditions are shown in Table 1. Figure 2 shows the results of the throughput performances when the code rate R_{polar}(= R in (12)) and the crossover probability P_{e} are changed. It can be seen that the throughput performances of high-rate polar codes are superior when P_{e} is small, and those of low-rate polar codes are superior in high P_{e} region. As shown in the figure, the crossover probability region with superior throughput differs depending on the code rate, and it is necessary to change the code rate according to P_{e} for more efficient transmission.

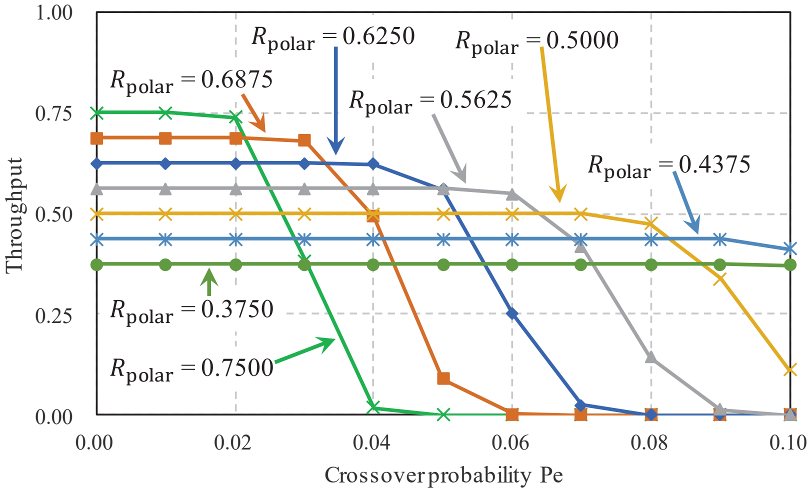

Figure 2. Throughput performances of polar codes.

Table 1. Simulation conditions of polar codes.

Code length N_B	2048
Information length K_B	768 to 1536
Code rate R_{polar}	0.375 to 0.75
Decoding	Successive cancellation list decoding[9, 10]
Parity length of cyclic redundancy check	24

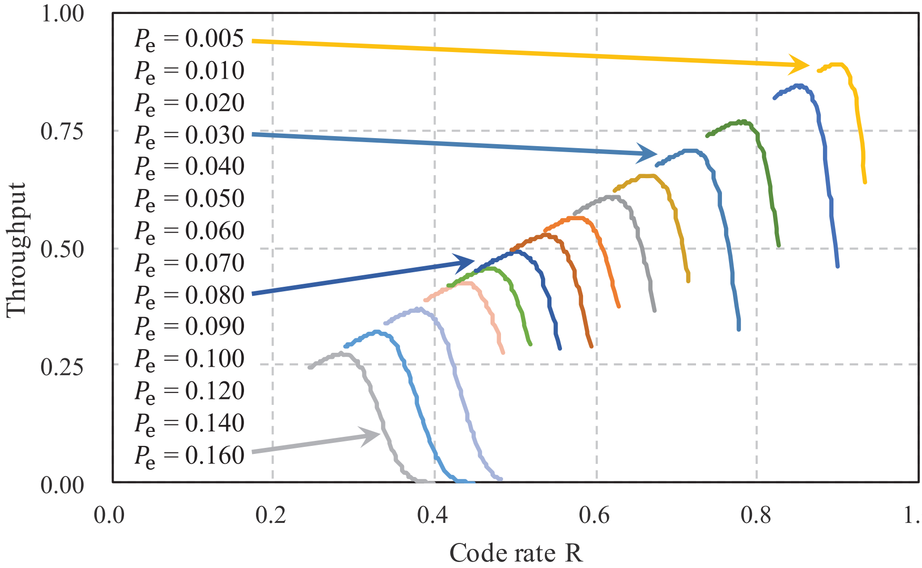

Figure 3. Throughput performances versus code rate R_{polar}.

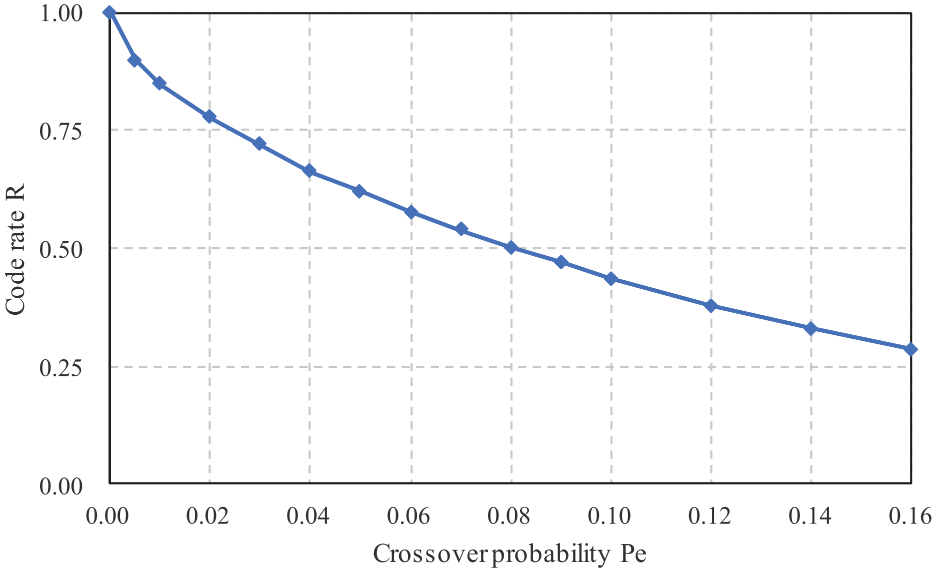

Figure 4. Proposing rule to select the optimal code rate of polar codes.

4.3 Optimization of information reconciliation applied polar codes

Based on the discussion in the previous section, we derive an equation relating the code rate R_{polar} and the crossover probability P_{e} to obtain the best throughput for polar codes. First, Figure 3 shows the throughput performances when R_{polar} is changed by gradually increasing the number of frozen bits with a fixed crossover probability. This figure shows that for each crossover probability, there is an optimal code rate that maximizes throughput. Figure 4 shows a graph rearranging these points, with the crossover probability on the horizontal axis and the code rate on the vertical axis. We derived the following approximation equation as the selection rule for the code rate R_{polar} from the curve in Figure 4.

$$R_{\mathrm{polar}} = -16507P_{\mathrm{e}}^5 + 7883.2P_{\mathrm{e}}^4 - 1450P_{\mathrm{e}}^3 + 139.25P_{\mathrm{e}}^2 - 10.77P_{\mathrm{e}} + 0.947. \tag{13}$$

4.4 Application of LDPC codes in the conventional method

As a benchmark against polar codes, we calculated LDPC codes' performance under the conditions shown in Table 2. Figure 5 shows the throughput performances of the LDPC codes versus P_{e} with the parameter of code rate $R_{\mathrm{LDPC}}(= R$ in (12)). Using the five LDPC codes shown in the figure, the selection rule for the code rate R_{LDPC} optimizing the throughput performances can be derived as

$$R_{\mathrm{LDPC}} = \begin{cases} 0.750\ (0 \le P_{\mathrm{e}} < 0.015) \\ 0.625\ (0.015 \le P_{\mathrm{e}} < 0.044) \\ 0.500\ (0.044 \le P_{\mathrm{e}} < 0.071) \\ 0.375\ (0.071 \le P_{\mathrm{e}} < 0.0856) \\ 0.250\ (0.0856 \le P_{\mathrm{e}} < 0.1) \end{cases}. \tag{14}$$

It can be seen that the throughput performances are superior for high-rates in the small crossover probability region and low-rates in the large crossover probability region, as well as in Figure 2.

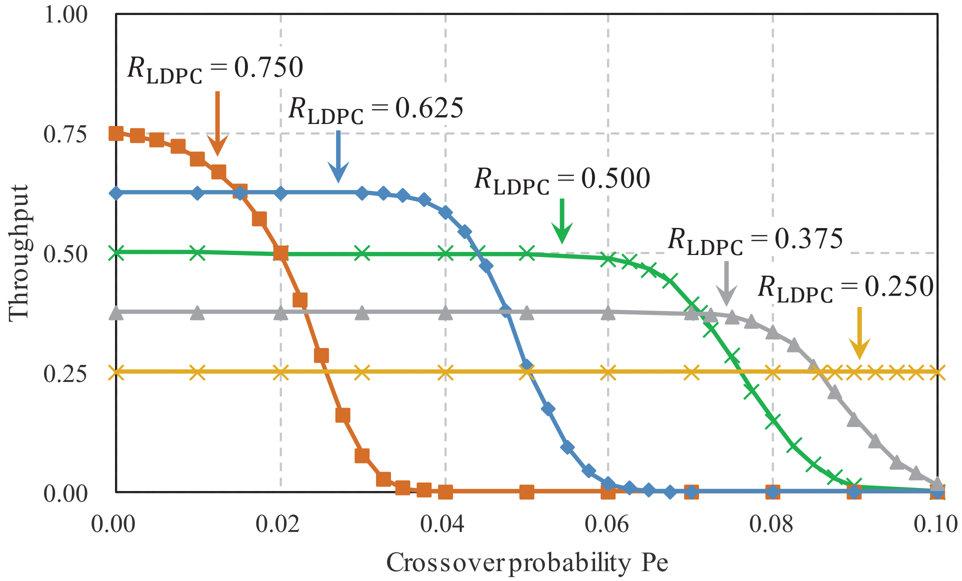

Figure 5. Throughput performances of LDPC codes.

Table 2. Simulation conditions of LDPC codes.

Code length N_B	2048				
Information length K_B	512	768	1024	768	1536
Code rate R_{LDPC}	0.25	0.375	0.5	0.625	0.75
Decoding	Sum-product decoding				
Weighting of parity-check matrices	(3,4)	(5,8)	(3,6)	(3,8)	(3,12)
The maximum number of reprising decoding	20				

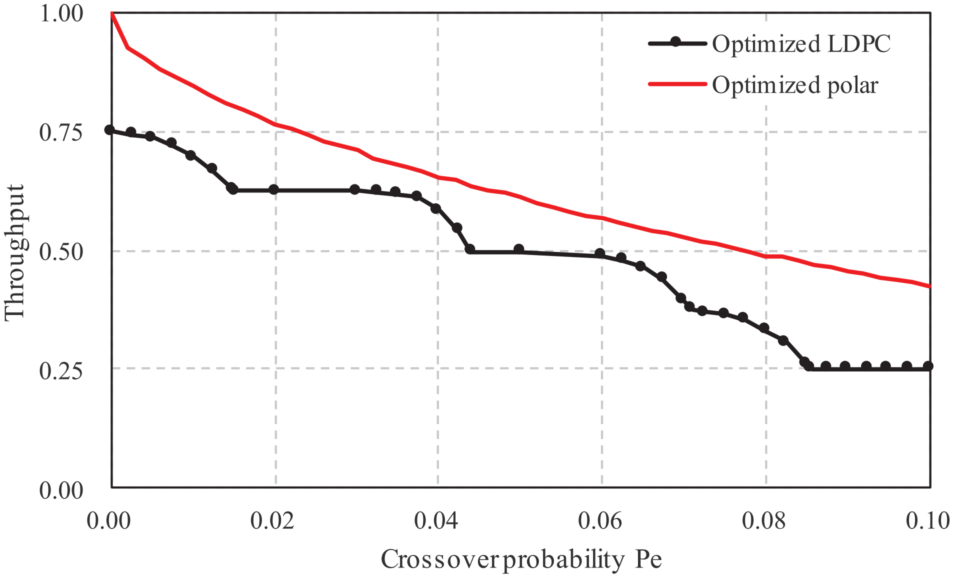

Figure 6. The comparison of optimized throughput performances.

4.5 Performance comparison of the proposed method to LDPC codes

Figure 6 compares the throughput performances of LDPC codes and polar codes based on the selection rules obtained above. It is shown that the throughput performances of polar codes are higher than those of LDPC codes in all areas. Therefore, the application of polar codes to satellite QKD is expected to improve information reconciliation efficiency. LDPC codes can also have finer coding ratios, but it is necessary to share the parity-check matrices for all code rates in advance. However, polar codes have the advantage that no matrix share is needed.

5. CONCLUSION

In this paper, we proposed applying polar codes to the information reconciliation step to increase the efficiency of key distribution in QKD and evaluated its performances. First, we chose the throughput as the measure of the efficiency of information reconciliation. Then, we derived the throughput performances for different code rates and crossover probabilities by numerical simulations. From these results, we derived a selecting rule of code rate that maximizes throughput for each crossover probability, constructed a polar code with the best throughput performances for information reconciliation, and confirmed the improvement of its performances. Then, We compared the polar codes with the LDPC codes in the region where the crossover probability is less than 10% and confirmed the superiority of the polar codes in all regions. In the future, we plan to study concatenating with rateless codes in order to improve the performance of the system, including (A) QBER estimation in addition to (B) information reconciliation.

REFERENCES

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public Key Distribution and Coin Tossing," Proc. IEEE Int'l Conf. on Computers, Systems and Signal Proc., Bangalore India, 175-179 (1984).

[2] A. K. Ekert, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett. 67(6), 661-663 (1991).

[3] M. Sasaki, et al., "Field test of quantum key distribution in the Tokyo QKD Network," Optics Express 19(11), 10387-10409 (2011).

[4] M. Peev, et al., "The SECOQC quantum key distribution network in Vienna," New J. Phys. 11(7), 075001 (2009).

[5] R. Bedington, J. M. Arrazola, and A. Ling, "Progress in satellite quantum key distribution," npj Quantum Information 3, (2017).

[6] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," IEEE Trans. on Information Theory 55(7), (2009).

[7] S. Fujita, K. Ito, E. Okamoto, H. Takenaka, H. Kunimori, H. Endo, M. Fujiwara, M. Kitamura, R. Shimizu, M. Sasaki, and M. Toyoshima, "Experimental evaluation of polar code transmission in terrestrial free space optics," Proc. IEEE Int'l Conf. on Commun., (2019).

[8] P. Jouguet and S. K. Jacques, "High Performance Error Correction for Quantum Key Distribution using Polar Codes," Quantum Information and Computation 14(3&4), (2013).

[9] I. Tal and A. Vardy, "List decoding of polar codes," IEEE Trans. on Information Theory 61(5), (2012).

[10] K. Niu and K. Chen, "CRC-aided decoding of polar codes," IEEE Commun. Lett. 16(10), 1668-1671 (2012).

[11] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," International Conf. on the Theory and Applications of Cryptographic Techniques, 523-540 (2004).

[12] H. Endo, M. Fujiwara, M. Kitamura, O. Tsuzuki, T. Ito, R. Shimizu, M. Takeoka, and M. Sasaki, "Free space optical secret key agreement," Optics Express 26(18), 23305-23332 (2018).

[13] A. Tanaka, et al., "High-Speed Quantum Key Distribution System for 1-Mbps Real-Time Key Generation," in IEEE J. of Quantum Electronics 48(4), 542-550 (2012).

[14] F. Grosshans, G. van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using gaussian-modulated coherent states," Nature 421(6920), 238-241 (2003).

[15] T. Hirano, et al., "Implementation of continuous-variable quantum key distribution with discrete modulation," Quantum Science and Technology 2(2), 024010 (2017).

[16] H. Endo and M. Sasaki, "Secret key agreement for satellite laser communications, " Proc. 37th Int'l Commun. Satellite Systems Conf. (ICSSC), (2019).