A continuous variable quantum key distribution protocol based on
multi-dimension data reconciliation with Polar code

Bao Feng*, Chao Lv, Jinsuo Liu, Tianbing Zhang
NARI information communication technology Co., Ltd, Nanjing 211000, China;

*nrgd_lw@163.com

Abstract. The continuous variable quantum key distribution protocol (CV-QKD) has the advantages of easy generation of quantum signals, convenient measurement and high communication capacity. However, the multi-dimensional data reconciliation is mainly implemented by binary LDPC code as quantum error correction code, which is greatly affected by complex environments and the bit error rate is high. In order to solve this problem, a continuous variable quantum key distribution protocol based on multi-dimension data reconciliation with Polar code, that can be applied to long-distance transmission in power systems, is proposed. First, we prepare an EPR quantum state, and perform heterodyne detection on one of the quantum states, and obtain the values of two orthogonal components at the same time which is the coherent state of the information carrier. Then the continuous variable quantum key distribution is realized by six steps (i.e., quantum state preparation, gaussian random detection, data filtering, calculation of bit error rate, data reconciliation, privacy amplification). In data reconciliation, we use Polar code as the error correction code and use reverse coding technology to achieve key error correction, which can effectively improve the negotiation efficiency. Numerical simulation verifies the feasibility of the protocol, and the protocol is more efficient than the multi-dimension data reconciliation protocol based on LDPC code under the same conditions.

Keywords: Continuous variable quantum key distribution, Multi-dimension data reconciliation protocol; Polar code; Gaussian random;

1. Introduction
Quantum key distribution (QKD)[1] technology is a quantum secret communication method that has been proven to have unconditional security. It combines the functions of key generation and key transmission in the original secret system. In combination with the safety requirements of power communication systems, QKD has great application value and application prospects in power production scheduling, power marketing and integrated management. According to the different carriers of information transmission, it can be divided into discrete variable QKD (DV-QKD)[2] protocol and continuous variable QKD (CV-QKD)[3] protocol. In the DV-QKD protocol, information is encoded in a single quantum state, and the information is carried by discrete physical quantities represented by a single photon. CV-QKD usually uses continuous variable EPR entangled state[4] as the information carrier, such as position and momentum[5-8]. Compared with the DV-QKD protocol, the light source in the CV-QKD system, such as squeezed state[9-10], Gaussian modulated coherent state[11-13] and other light sources, is greatly reduced in difficulty and cost, and the required physical equipment for detection is simple, and the system has many advantages such as high communication capacity.

In the CV-QKD technology, the Gaussian Modulated Coherent State (GMCS) protocol is the most eye-catching[14]. In 2011, Dai et al. built an integrated quantum secure communication system based on the GMCS protocol[15], which can obtain a secure key rate of 3.9 kb/s in a 27.2 km fiber channel. In 2013, CV-QKD made major breakthroughs in theoretical research and experimental progress. Leverrier A. et al. used the rotation invariance in the phase space to strictly prove the security of the finite-length key CV-QKD under coherent attacks[16]. However, the actual coherent state CV-QKD system will be affected by actual non-ideal factors such as non-ideal Gaussian modulation, laser phase noise, and detector calibration error, causing a variety of potential security vulnerabilities[17-20]. Therefore, the actual security of the coherent state CV-QKD system has gradually become a research focus.

Polar code is a forward error correction coding method, that is proposed by Arikan in 2007, and it is widely used in source and channel coding in data reconciliation protocols. For binary symmetrical channels, Polar codes can theoretically reach the channel capacity[21-22]. Taking advantage of these advantages of Polar codes, Jouguet et al. applied Polar codes to the quantum key distribution protocol[23], and the simulation results show that the QKD negotiation protocol based on Polar codes has a certain improvement in performance such as decoding speed.

Numerous theories and experimental results show that, among all current quantum information technologies, quantum key distribution is the closest to practical technology. Continuous variable quantum key distribution technology is rapidly entering the practical process after the key theoretical problems have been solved. The specific work of this paper is to design an efficient quantum key distribution multi-dimension negotiation protocol based on the multi-dimension negotiation algorithm using Polar inverse coding technology to ensure the consistency of the encryption key and reduce the leakage of key information during the negotiation.
The outline of this paper is as follows: The preliminary knowledge (i.e., polar code and quantum key distribution protocol) is briefly reviewed in Section 2, and the proposed continuous variable quantum key distribution protocol based on multi-dimension data reconciliation with Polar code is described in detail in Sect. 3. Then, we simply analyze the complexity and perform the simulation experiment in Sect. 4. Subsequently, the brief conclusion and discussion are summarized in the last section.

2. Preliminaries

2.1. Polar Code

Polar code is a linear block code based on the theory of channel polarization, which has the advantages of low complexity of encoding and decoding and can theoretically achieve channel capacity. The key of constructing Polar code is to make each sub-channel present different reliability on the coding side by channel polarization processing. Channel polarization process can be divided into two parts: channel combining and channel splitting.

(1) Channel combination is to copy the binary discrete memory-free channel \( W \) for \( N \) times and then obtain the combined channel \( W_N \) through linear transformation. For the combined channel \( W_N: X^N \rightarrow Y^N \), here \( N = 2^n, n \geq 0 \). Fig. 1 shows the general form of the recursive structure. The input vector \( u_i^N \) enters the channel \( W_N \) and is first converted to \( s_i^N \):

\[
s_{2i-1} = u_{2i-1} \oplus u_{2i}, \quad s_{2i} = u_{2i}, \quad 1 \leq i \leq N / 2.
\]

\( R_N \) stands for bit-reversal sorting operation. The input is \( s_i^N \) and the output is \( v_i^N = (s_1, s_3, \ldots, s_{N-1}, s_2, s_4, \ldots, s_N) \). \( v_i^N \) becomes the input of two independent copies of \( W_{N/2} \).
Fig. 1 Combination of channel $W_N$.

(2) Channel splitting is to split the synthesized channel $W_N$ into $N$ independent Coordinate Channels $W_N^{(i)} : X \rightarrow Y^N \times X^{i-1}, 1 \leq i \leq N$. The transition probability is defined as

$$W_N^{(i)}(y_1^N, u_1^{i-1} | u_i) \equiv \sum_{u_1^N, X^{i-1}} W_N(y_i^N | u_i),$$

where $(y_i^N, u_1^{i-1})$ represents the output of $W_N^{(i)}$ and $u_i$ represents the input of $W_N^{(i)}$. The transition probability of an odd-order splitter channel and an even-order splitter channel is obtained by two recursions.

2.2. Quantum key distribution protocol

Quantum key distribution (QKD), which makes use of quantum mechanical properties to ensure communication security, enables the two parties of communication to generate and share a random secure key to encrypt and decrypt messages. Continuous variable quantum key distribution (CV-QKD) is a quantum key distribution protocol that uses entangled light, squeezed light or coherent state as the light source. The specific process of CV-QKD protocol is described as follows (as shown in Fig. 2):
Fig. 2 CV-QKD protocol

1. **Preparation**: Alice randomly selects two strings of data from a Gaussian distribution probability function with a mean value of 0 and a variance of $V_A N_0$, as the values of $x_A$ and $p_A$ respectively. And then Alice sends the coherent state $|x_A + ip_A\rangle$ to Bob.

2. **Random measurement**: After Bob receives the signal light sent by Alice, he uses the balanced homodyne detection technology to randomly select and measures $x_A$ or $p_A$.

3. **Data filtering**: Bob tells Alice through the classic public channel whether it is detecting the amplitude component or the phase component.

4. **Calculation of bit error rate**: Alice and Bob exchange part of the measured data for comparison, and the bit error rate is measured.

5. **Data reconciliation**: Alice and Bob first exchange part of the measurement data for comparison, and use the bit error rate to determine that there is no eavesdropping. The obtained filtered data (sifted key) also needs to use a certain algorithm to use the open channel Perform error correction to remove key errors caused by channel noise or third-party eavesdropping to ensure the security of the negotiated keys $A_{rec}$ and $B_{rec}$. This process is called data reconciliation which is shown in Fig. 3.
(6) Privacy amplification: It is a method to reduce or remove part of the key information that Eve has eavesdropped on.

3. A continuous variable quantum key distribution protocol based on multi-dimension data reconciliation with Polar code

The continuous variable quantum key distribution uses the standard components of the light field state to encode information. However, the continuous variable quantum key distribution protocol does not meet the actual requirements in the secure transmission distance and secure code rate of the system. In order to solve this problem, a continuous variable quantum key distribution protocol based on multi-dimension data reconciliation with Polar code, that can meet the requirements of ultra high voltage (UHV) and long distance application in power system, is proposed.

3.1. A continuous variable quantum key distribution protocol

In 2002, the Philipe Granier group of the French Institute of Optics proposed the GG02 protocol, a continuous variable quantum key distribution protocol based on coherent states. Due to the ease of preparation of coherent states and high detection efficiency, the GG02 protocol quickly received widespread attention and became the mainstream of the industry. Based on the GG02 protocol, this paper proposes a continuous variable quantum key distribution protocol for power system uHV long-distance application scenarios. The specific steps are as follows:

(1) Quantum state preparation: Alice prepares an EPR state, performs heterodyne detection on one of the quantum states, and obtains the values of two orthogonal components \( \left( a_x, a_\rho \right) \) at the same time.

(2) Gaussian random detection: Alice randomly generates two mutually independent random
numbers \( (a_s, a_p) \) with Gaussian distribution with mean 0 and variance \( V_A \), and prepares a coherent state with the center at \( (a_s, a_p) \). By repeating the above process for \( N \) times, Alice prepares \( N \) coherent states and sends them to Bob through the quantum channel;

(3) **Data filtering:** Bob randomly selects a quadrature component for each coherent state received to perform homodyne balance detection, obtains \( N \) measurement results, and the quantum communication phase ends. Bob announces the measurement base selection to Alice through the classic channel. Alice retains the random variables that correspond to Bob's measurement results, and discards those that do not correspond. So far, Alice and Bob have shared \( N \) sets of relevant data;

(4) **Calculation of bit error rate:** Alice and Bob randomly select group \( m \) from the \( N \) groups of data and publish their values. Using these public data, Alice and Bob can estimate the transmission rate and excess noise of the quantum channel, and then determine the upper limit of information obtained by Eve;

(5) **Data reconciliation:** For the remaining \((N-m)\) group of data, Alice and Bob use the mature error correction code technology developed in classic communication to coordinate data, and the \((N-m)\) group of continuous data with correlation into two identical binary bit strings;

(6) **Privacy amplification:** With the help of a hash function, Alice and Bob compress the shared binary bit string to eliminate the amount of information in Eve and generate the final key.

For each state transmission in the quantum communication phase, Alice prepares two EPR states, performs heterodyne detection on one of the modes, and obtains the values of two orthogonal components at the same time \( (a_s, a_p) \). The initial EPR state of Alice includes two modes, \( A \) and \( B_0 \), with a mean value of 0, and the covariance matrix can be expressed as

\[
\gamma_{AB_0} = \begin{pmatrix}
V1 & \sqrt{V^2 - 1}\sigma_z \\
\sqrt{V^2 - 1}\sigma_z & V1
\end{pmatrix}
\]  

Because Alice needs to perform heterodyne detection on mode \( A \), a 3dB beam splitter is needed to divide mode \( A \) into two. The other input of the beam splitter is the vacuum state defined as mode \( C \), then the covariance matrix of the entire system before the beam splitting operation can be written as
After beam splitting operation, the covariance matrix becomes

$$
\gamma_{ACB_0} = \begin{pmatrix}
V1 & 0 & \sqrt{V^2 - 1}\sigma_z \\
0 & 1 & 0 \\
\sqrt{V^2 - 1}\sigma_z & 0 & V1
\end{pmatrix}
$$

(2)

After beam splitting operation, the covariance matrix becomes

$$
\gamma'_{AC'C'B_0} = \left[ S_{AC}^{BS} \otimes I_{B_0} \right]^{T} \gamma_{ACB_0} \left[ S_{AC}^{BS} \otimes I_{B_0} \right], \text{here, } S_{AC}^{BS} = \begin{pmatrix}
\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\
\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}
\end{pmatrix}
$$

(3)

Using the heterodyne operation to transform the first-order statistic and the second-order statistic of the Gaussian state, the heterodyne measurement by Alice can be calculated and the result \( \left( a_x, a_p \right) \) is obtained, and the mode \( B_0 \) is projected onto such a Gaussian state, The displacement vector and covariance matrix are respectively:

$$
d_{B_0} = \sqrt{\frac{V-1}{V+1}} \begin{pmatrix} a_x, a_p \end{pmatrix}, \gamma_{B_0} = \begin{pmatrix} 1 & 0 \\
0 & 1 \end{pmatrix}
$$

(4)

Then, we can calculate that \( \left\langle \Delta^2 d_{B_0} \right\rangle = V - 1 = V_A \) by \( \left\langle a_x^2 \right\rangle = (V + 1) / 2 \), and perform a classic multiplication operation on the measurement results of Alice, and finally we can perform a quantitative analysis of von Neumann entropy on this protocol.

3.2. Multi-dimension data reconciliation with Polar code

The legitimate users (the sender Alice and the receiver Bob) respectively perform channel estimation to generate their own original keys. Alice and Bob directly group their continuous variable keys in the order of key generation, and each \( d \) continuous variable keys are combined into a \( d \)-dimension vector as shown in Fig. 4. In this way, for a key of length \( L \), both parties can get a total of \( L/d \) groups after grouping, and each grouping is a set of \( d \)-dimension continuous vectors.
Next, we take one set of data as an example to describe the protocol. Suppose the \( d \)-dimension vector at Alice's end is denoted as \( X \), and the \( d \)-dimension vector at Bob’s end is denoted as \( Y \), then \( Y = X + Z \), where \( Z \) is the noise with channel variance \( \sigma^2 \).

Define a set of \( d \)-dimension vectors of Alice and Bob as \( X \) and \( Y \), \( X \sim N\left(0, \Sigma^2\right)^d \), \( \Sigma^2 \) is the modulation variance of the signal at the Alice end; according to the introduction of the CVQKD protocol above, \( Y = X + Z \), where \( Z \) is the noise of the channel, and \( Z \sim N\left(0, \sigma^2\right)^d \), \( \sigma^2 \) is the variance of the channel noise. From the knowledge of information theory, we know that \( Y \) also obeys the Gaussian distribution \( Z \sim N\left(0, \Sigma^2 + \sigma^2\right)^d \), where \( \Sigma^2 + \sigma^2 \) is the variance of \( Y \). Next, the \( d \)-dimension keys \( X \) and \( Y \) of Alice and Bob are input into the multi-dimension negotiation module. After normalization, spherification and rotation, they are converted into a set of input \( Y \) and output \( X \) similar to the BIAWGN channel.
In order to correct the error caused by noise in quantum communication to the key, the Polar code inverse encoding technique was used to correct the continuous variable key, and finally the completely consistent security key was obtained. This process is shown in the following figure. Bob performs Polar code inverse encoding on his original keys. And the frozen bit information is transmitted to Alice as negotiation information. After receiving the negotiation information, Alice uses the channel coding model with its position information to decode the Polar code, corrects the error of the original key, and finally obtains the key sequence consistent with Bob through the Polar encoding.

Fig. 6 Error correction procedure with Polar code.
The Polar code encoding process can be obtained by multiplying the information sequence and its generating matrix. For a Polar code of a given length $N$, the generator matrix $G_N$ of the Polar code is an invertible matrix, and $G_N^{-1} = G_N$, then the inverse coding formula can be expressed as $u_i^N = y_i^N G_N$.

If set $A$ is used to represent any subset of set $\{1, ..., N\}$, then the inverse coding formula can be expressed as $y_i^N = u_A G_N(A) \oplus u_{A'} G_N(A')$, here $G_N(A)$ is a subset of $G_N$ composed of the row vector corresponding to the index in the information bit set $A$. $A'$ is a collection of other rows. $u_A$ is the bit value of the corresponding position, called frozen bit or frozen vector. In Polar code, $A'$ and $u_A$ are usually fixed, and $u_A$ is fixed to 0, and only $u_{A'}$ is used as a variable to transmit information. Finally, the final consistent key is obtained through the secret amplification operation.

4. Complexity analysis and simulation experiment

In terms of computational complexity, the complexity of a modulo two addition in the negotiation error correction process is 1, and the complexity of a sequence with a length of $N$ flipped once is $N$, then the computational complexity of Polar code encoding and decoding can be obtained as:

$$\chi_e(N) \leq \frac{3}{2} N \log N, \chi_d(N) = N \log N,$$

here, $\chi_e(N)$ and $\chi_d(N)$ represents coding complexity and SC decoding complexity respectively. The proposed multi-dimension data reconciliation protocol of continuous quantum key distribution protocol, based on Polar inverse encoding, includes two encoding processes (Alice's reverse encoding process and Bob obtaining the final key encoding process) and one SC decoding process, so the complexity of the Polar code negotiation scheme $\chi(N)$ is:

$$\chi(N) = 2\chi_e(N) + \chi_d(N) \leq 4N \log N = O(N \log N).$$

The following is a numerical simulation to analyze the impact of the negotiation protocol on key consistency. The basic parameter settings in the numerical simulation are as follows: The maximum number of frames is set to 2000, and the error correction codes use Polar codes with a code length of 2048 and code rates of 0.75 and 0.5, and a code length of 4096 Polar codes and LDPC codes with a code rate of 0.5, and the maximum number of BP decoding frames for LDPC codes is set to 100 times.

Figure 3.4 shows the relationship between the decoding success rate and the signal-to-noise ratio obtained by comparing the error correction of Polar codes with different parameters. It can be seen from Figure 3.4 that when the code rate is the same, as the signal-to-noise ratio increases, the decoding success rate becomes higher, that is, the probability of successfully completing the error correction
becomes higher and higher, and under the same signal-to-noise ratio conditions, the decoding success rate of the Polar code with a code length of 4096 is always higher than that of the Polar code with a code length of 2048; on the other hand, when the code length is the same, the decoding of the Polar code with a code rate of 0.5 under the same SNR conditions, the code success rate has always been higher than the Polar code with a code rate of 0.75.

![Graph](image)

**Fig. 7** Relationship between Polar decoding success rate and signal to noise ratio.

Figure 3.5 is based on the initial inconsistency rate of the original keys of the two communicating parties, comparing the decoding success rate of Polar codes with a code rate of 0.5 and a code length of 2048 and LDPC codes, and the obtained decoding success rate and the initial inconsistency rate. When the initial error rate is in an interval greater than 0.2, Polar codes can still achieve better decoding and error correction effects, while LDPC codes are basically difficult to achieve successful decoding.
Fig. 8 The relationship between the initial error rate and the success rate of decoding of LDPC codes and Polar codes.

5. Conclusion

In actual power systems, quantum key distribution protocols can effectively improve the secure transmission performance of dispatching data networks. However, these protocols are limited by the key distribution distance, and their performance is greatly affected by complex environments. There are hidden safety hazards in the actual application environment, and the system's safe transmission distance and safe bit rate are also far from actual requirements. So in this paper, a continuous variable quantum key distribution protocol based on multi-dimension data reconciliation with Polar code, that can be applied to long-distance transmission in power systems, is proposed. Then the continuous variable quantum key distribution is realized by six steps (i.e., quantum state preparation, Gaussian random detection, data filtering, calculation of bit error rate, data reconciliation, privacy amplification). In data reconciliation process, we use Polar code as the error correction code and use reverse coding technology to achieve key error correction, which can effectively improve the negotiation efficiency. Numerical simulation verifies the feasibility of the protocol. The experiment result shows that when the code rate is the same, as the signal-to-noise ratio increases, the decoding success rate becomes higher and higher, that is, the probability of successfully completing error correction becomes higher. And the protocol is more efficient than the multi-dimension negotiation protocol based on LDPC codes under the same conditions.

Acknowledgments

The authors would like to thank the anonymous reviewers and editor for their comments that improved the quality of this paper. This work is support by National key R & D project under Grant No. 2018YFE0200603.
Reference

[1] Bennett C H and Brassard G 1984 Quantum cryptography: Public key distribution and coin tossing *IEEE ICC* vol 560 pp 175-179

[2] Bennett C H and Brassard G 2014 Quantum Cryptography: Public Key Distribution and Coin Tossing [J]. Theoretical Computer Science vol 560 pp 7-11

[3] Grosshans F and Grangier P 2002 Continuous variable quantum cryptography using coherent states *Phys. Rev. Letters* vol 88 p 057902

[4] Ekert A K 1991 Quantum cryptography based on bell’s theorem *Phys. Rev. Letters* vol 67 no 6 pp 661-663

[5] Zhiyue Zuo, Yijun Wang, Yun Mao, Wei Ye, Liyun Hu, Duan Huang and Ying Guo 2020 Quantum catalysis-assisted attenuation for improving free-space continuous-variable quantum key distribution *Journal of physics b-atomic molecular and optical physics* vol 53 no 18 pp 125-138

[6] Wu, XD, Wang, YJ, Zhong, H, Ye, W, Huang, D and Guo, Y 2020 Performance improvement of plug-and-play dual-phase-modulated continuous-variable quantum key distribution with quantum catalysis *Quantum Information Processing* vol 19 no 8

[7] Samsonov, E, Goncharov, R, Gaidash, A, Kozubov, A, Egorov, V and Gleim, A 2020 Subcarrier wave continuous variable quantum key distribution with discrete modulation: mathematical model and finite-key analysis *Scientific Reports* vol 10 no 1

[8] Erementchouk, M and Mazumder, P 2020 Continuous-variable quantum key distribution with discretized modulations in the strong noise regime *Phys. Rev. A* vol 101 no 6

[9] Cerf N J, Levy M and Van Assche G 2001 Quantum distribution of Gaussian keys using squeezed states *Phys. Rev. A* vol 63 p 052311

[10] LY Hu, S Wang and ZM Zhang 2012 Photon-number distribution of two-mode squeezed thermal states by entangled state representation *Chinese Physics B* vol 21 no 6

[11] TY Wang, S Yu, YC Zhang and WY Gu 2015 A generalized entanglement-based scheme for Gaussian-modulated coherent state continuous-variable quantum key distribution. *Journal of physics b-atomic molecular and optical physics* vol 48 no 13

[12] BQi,P G and WP Grice 2018 Passive state preparation in the Gaussian-modulated coherent-states quantum key distribution *Phys. Rev. A* vol 97 no 1

[13] Pan K C, Jin X J and Sun X L 2011 Optical manipulations of quantum states with continuous variables Acta Optica Sinica vol 31 no 9 p 0300107.
[14] Grosshans F and Grangier P 2002 Continuous Variable Quantum Cryptography Using Coherent States[J]. Phys. Rev. Letters vol 88 no 05 p057902

[15] Dai W C, Lu Y and Zhu J 2011 An Integrated Quantum Secure Communication System Science China vol 54 no 12 pp 2578-2591

[16] Leverrier A, Garcia-Patron R and Renner R 2013 Security of Continuous Variable Quantum Key Distribution against general attacks Phys. Rev. A Letter vol 110 no 3 p 030502

[17] Jouguet P 2013 Experimental Demonstration of Long-Distance Continuous-Variable Quantum Key Distribution Nature Photonics vol 7 no 05 pp 378-381

[18] Shen Y 2014 A Fiber-based Quasi-Continuous-Wave Quantum Key Distribution System Science Reports vol 4 no 02 p 4563

[19] Y Zheng, P Huang and A Huang 2019 Practical security of continuous-variable quantum key distribution with reduced optical attenuation arXiv

[20] Jouguet P 2012 Analysis of Imperfections in Practical Continuous-Variable Quantum Key Distribution Phys. Rev. A vol 86 no 03 p 032309

[21] Y Huang, Y C Zhang and L Huang 2020 A modified practical homodyne detector model for continuous-variable quantum key distribution: detailed security analysis and improvement by the phase-sensitive amplifier arXiv

[22] C Li, L Qian and H K Lo 2019 Simple security proofs for continuous-variable quantum key distribution with intensity fluctuating sources arXiv

[23] Arikan, E 2009 Channel Polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels IEEE Transactions on Information Theory vol 55 no 7 pp 3051-3073

[24] K. Liang, B. Feng, J. Jiao, S. Wu and Q. Zhang 2018 An Efficient Channel Estimation Scheme based on Frozen Bits of Polar Codes over Fading Channel. 2018 10th International Conference on Wireless Communications and Signal Processing (WCSP), Hangzhou pp 1-6

[25] Korada S B, Sasoglu E and Urbanke R 2010 Polar codes: characterization of exponent, bounds, and constructions IEEE Transactions on Information Theory vol 56 no 12 pp 6253-6264

[26] Jouguet P, Kunz-Jacques S 2012 High performance error correction for quantum key distribution using polar codes Quantum Information and Computation vol 14 no 3 pp 5882-5893