Chinese Journal of Electronics
Vol.27, No.2, Mar. 2018

An Improved Polar Codes-Based Key Reconciliation for Practical Quantum Key Distribution*

YAN Shiling[1], WANG Jindong[1], FANG Junbin[2,3], JIANG Lin[4] and WANG Xuan[4]

(1. *Laboratory of Quantum Engineering and Quantum Materials, South China Normal University, Guangzhou 510006, China*)

(2. *Department of Optoelectronic Engineering, Jinan University, Guangzhou 510632, China*)

(3. *The Edward S. Rogers Sr. Department of Electrical & Computer Engineering, University of Toronto, Canada*)

(4. *Harbin Institute of Technology Shenzhen Graduate School, Shenzhen 518055, China*)

Abstract — Key reconciliation is important for practical Quantum key distribution (QKD) systems since it corrects the error bits in a key string by sacrificing some key bits. Therefore, its performance directly affects the secret key rate of a practical QKD system. Although key reconciliation scheme based on polar codes can achieve a high coding efficiency, the high frame error rate causes discarding key strings and decreases the secret key rate. In this paper, we fist analyze the limitation of successive cancellation decoding of polar codes, and then we propose an improved key reconciliation scheme using polar codes with successive cancellation list decoding and optimized coding structures, which can decrease the frame error probability, resulting in a higher secret key rate. Numerical results show that the proposed scheme can achieve a 12.8% higher secret key rate than the previous polar codes-based scheme with a code length of 2^{16} bits and a quantum bit error rate of 2%. Besides, the proposed scheme is robust and it can extract secret key bits even when the quantum bit error rate reaches 10.2% with a code length of 2^{20} bits and a coding efficiency of 90.6%.

Key words — Quantum key distribution, Polar codes, Successive cancellation list decoding, Secret key rate.

I. Introduction

Quantum key distribution (QKD)[1] is theoretically proven to be one key distribution method which can provide secret keys for remote communication parties with unconditional security, and many QKD schemes have been proposed to operate by a variety of protocols over optical fibers or free space[2−6]. However, in practical systems, quantum states during the process of preparation, transmission and detection may be affected by physical noises, eavesdroppers' attacks[7] and other factors resulting in error bits[8−10]. In order to obtain a consistent secret key string for both parties, says Alice and Bob, QKD requires them to interact with each other via a classical channel to perform a series of post-processing operations on the original key bits which have been transmitted through the quantum channel. Post-processing procedures mainly include sifting, error estimation, key reconciliation, verification and privacy amplification. And all the information disclosed over the classical channel should be deducted from the final secret key to reduce the amount of eavesdropper's information to zero.

Compared with classical communication, QKD usually has a relatively high Quantum bit error rate (QBER) and the key reconciliation schemes dedicated to QKD tend to be complicated with a low coding efficiency. Since key reconciliation may consume a significant proportion of key bits and introduce a high decoding latency, it may become a "bottleneck" in a practical high-speed QKD system[11]. Key reconciliation algorithms used for QKD mainly include BBBSS[12], Cascade[13−16], Winnow[17,18], Low density parity check (LDPC)[19−22] and so on. Existing QKD systems mainly adopt Cascade and LDPC for key recon-

*Manuscript Received Mar. 1, 2017; Accepted May 26, 2017. This work is supported by the National Natural Science Foundation of China (No.61401176, No.61401262, No.U1636106, No.61472048, No.61771205, No.61771222), the Natural Science Foundation of Guangdong Province, China (No.2014A030310205, No.2015A030313388), the Special Science and Technology Foundation of Guangdong Province, China (No.2016A010101017), the Project of Guangdong High Education (No.YQ2015018), the Application-oriented Special Scientific Research Foundation of Application Type of Guangdong Province, China (No.2015B010128012), the Key Technology Program of Shenzhen, China (No.JSGG20160427185010977), and Science and Technology Project of Guangzhou (No.201707010253).

 DOI:10.1049/cje.2017.07.006

ciliation. Cascade is an improved parity dichotomy key reconciliation protocol originated from BBBSS, using recursive backtracking method to identify the location of the error bits and to reduce the number of searching required by BBBSS. It takes benefit from the high interaction between Alice and Bob over an authenticated public channel to simplify the problem of reconciliation. Therefore, its error correction efficiency is relatively high and the implementation is simple without error estimation before error correction. However, many exchanges between Alice and Bob are required to reconcile a sifting string even when carefully implemented, which may lead to a high latency sensitive to network communication quality and severely limit the achievable key generation rate in long-distance QKD. LDPC is a kind of Forward error correction (FEC) codes, whose parity check matrices are sparse. It only needs to send checking information one-time and one-way. Besides, the coding efficiency of LDPC codes can approach Shannon limit. It is shown in Ref.[23] that LDPC can achieve a similar efficiency as Cascade when the QBER is less than 2%. However, its error correction matrix is sensitive to QBER, and it is necessary to construct different matrices to adapt to different QBERs. Furthermore, LDPC adopts iterative decoding algorithm, and the decoding complexity is relatively high.

Polar codes is an error correction coding method proposed by Arikan in 2009 based on channel polarization theory[24]. It has been proved that the Shannon limit can be achieved on Binary-input Discrete memoryless channel (B-DMC) with codec complexity of $O(N\log N)$ (N is the code length). Jouguet[25] first used polar codes for post-processing of QKD, and the experiments show that the polar codes-based post-processing scheme for QKD can achieve a high coding efficiency and a high processing speed. However, it has a higher Frame error rate (FER) and results in more key frames discarded[26]. Consequently, the final secret key generation rate is also limited.

Although the well-known Cascade protocol is usually used as representative of the traditional reconciliation methods, it achieves high efficiency by exchanging information frequently. In terms of interactivity, both LDPC and Polar Codes need a single information exchange to reconcile the two variables while Cascade is very greedy in communication resources. Therefore, we conduct numerical experiments to show the performance of the proposed scheme compared with LDPC, as well as the previous scheme based Polar Codes.

In this paper, we fist analyze the limitation of Successive cancellation (SC) decoding algorithm of polar codes used for key reconciliation, and then we propose an improved key reconciliation scheme using polar codes with a successive cancellation list decoding algorithm and optimized coding structures, which can decrease the frame error probability resulting in a higher final secret key generation rate. Numerical results show that the secret key rate of the proposed scheme reaches 0.68 with a code length of $N = 2^{16}$, which is 12.8% higher than that in Ref.[25] and 6.25% higher than that in Ref.[26]. Besides, the proposed scheme is robust and it can extract secret key bits even when the quantum bit error rate reaches 10.2% with a code length of 2^{20} bits and a coding efficiency of 90.6%. Therefore, it is able to support practical QKD systems with a longer distance transmission.

The rest of this paper is organized as follows. Section II introduces the theoretical calculation model of the key generation rate of post-processing. Section III analyzes the limitation of SC decoding and proposes the improved post-processing method based on polar codes. Numerical simulations and results are explained and discussed in Section IV. Section V concludes this paper.

II. Secret Key Rate of Practical QKD

For Discrete-variable QKD (DV-QKD) systems, the quantum channel can be viewed as a Binary systematic channel (BSC) whose error probability is QBER. During the phase of transmitting quantum bits, Alice first chooses a random key bit string and a random sequence of bases, and then she sends Bob a train of photons, each of which represents one bit of the string in the basis chosen for that bit position. Bob detects the photons using randomly basis. Alice and Bob exchange information about bases through classical channel and discard the bits measured by inconsistent bases and share two strings called sifted key: X and Y. Eve, the possible eavesdropper, gets a bit string E which is partially correlated to X and Y. Due to the physical imperfection of practical QKD systems and possible eavesdropping, the sifted key Y may contain some inconsistent bits with X. Therefore, key reconciliation is essential for Alice and Bob to obtain the mutual information ($I(X:Y)$) which is the largest information Alice and Bob can extract. The theoretical secret key rate of a DV-QKD system can be calculated as follows:

$$r_{th} = I(X:Y) - S(X:E) \tag{1}$$

where $-S(X:E)$ is the entropy between Eve and Alice, and it also includes the amount of information disclosed during the procedures of post-processing.

Since the quantum channel in DV-QKD systems can be viewed as a BSC, the information eavesdropped by Eve can be further simplified as[23]: $S(X:E) = h(p)$, where p stands for the QBER of quantum channel and $h(p)$ is the binary Shannon entropy with $h(p) = -p\log_2(p) - (1-p)\log_2(1-p)$. Besides, the mutual information of both parties can be estimated as: $I(X:Y) = 1 - h(p)$.

However, practical key reconciliation schemes may not be able to achieve the capacity of a quantum channel, i.e. the maximum of $I(X:Y)$, due to the error correction capability of coding designs and the finite-size effect. Therefore, a coding efficiency β is introduced to evaluate the real secret key rate:

$$r_{real} = \beta \cdot I(X:Y) - S(X:E) \tag{2}$$

Denote R as the code rate of realistic error correction codes, β can be calculated as the ratio of the realistic code rate over the mutual information of Alice and Bob: $\beta = R/I(X:Y)$.

In QKD systems, sifted key blocks decoded incorrectly will be discarded by Alice and Bob. Therefore, FER is also an important factor affecting the real secret key rate. Taking FER into account, the formula of real secret key rate is rewritten as follows:

$$r_{real} = (1 - FER) \cdot [\beta \cdot I(X:Y) - S(X:E)] \tag{3}$$

Using the real QBER as the parameter in this formula, we can obtain the simplified equation of secrete key rate related to realistic system metrics:

$$r_{real} = (1 - FER) \cdot [\beta \cdot (1 - h(p)) - h(p)] \tag{4}$$

III. The Proposed Key Reconciliation Method Based on Polar Codes

1. Polar coding

Polar codes is based on a phenomenon called "channel polarization": channel combining and channel splitting. Using channel polarization, N individual copies of symmetric B-DMCs can be converted into a new set of bit-channels composed of more and more differentiated channels, such that in the asymptotic limit bit-channels are either error-free ("good") or completely noisy ("bad"), with a proportion of error-free bit-channels equal to the channel capacity. While a detailed description and proof of polar codes is available in Ref.[24], we present here how to apply polar coding to QKD key reconciliation.

According to the construction method of polar codes, Alice chooses K "good" bit-channels to place her sifted key bits (denoted as X) and $(N-K)$ "bad" bit-channels are set to be frozen bits "0", so sifted key bits and frozen bits form a new sequence of N bits (denoted as X'). Then Alice encodes the sequence into a codeword of N bits (denoted as C) by systematic encoding of polar codes[27] and only sends $(N-K)$ checking bits on "bad" bit-channels to Bob through a classical channel. Then, Bob combines the $(N-K)$ checking bits with his K sifted key bits (Y) together like Alice does to form a new sequence Y' of N bits, then he performs the decoding operation on Y' to correct the error bits among Y. Note that the coding efficiency of this scheme is: $\beta = (K/N)/h(p)$

2. Limitation of SC decoding

The SC decoding algorithm of polar codes[24] was first proposed by Arikan. The algorithm is recursively calculated according to the theory of channel splitting. Compute the likelihood probability of the bit channel recursively and make hard decision to get the decoded output. We assume Bob's string $Z = \{z_0, z_1, \cdots, z_{N-1}\}$ and SC decoding algorithm is described as follows:

Step 1: Initialize the received sequence $Z = \{z_0, z_1, \cdots, z_{N-1}\}$,

$$L_0^{(i)}(z_i) = \frac{W(z_i|0)}{W(z_i|1)}, \quad i = 0, 1, \cdots, N-1 \tag{5}$$

Step 2: Calculate the likelihood probability of bit i ,

$$L_N^{(i)}(z_0^{N-1}, \hat{u}_0^{i-1}) = \frac{W_N^{(i)}(z_0^{N-1}, \hat{u}_0^{i-1}|0)}{W_N^{(i)}(z_0^{N-1}, \hat{u}_0^{i-1}|1)} \tag{6}$$

where $\hat{u}_0^{i-1} = \{\hat{u}_0, \hat{u}_1, \cdots, \hat{u}_{i-1}\}$ are the bits that have been decoded out.

Step 3: Determine the bit value of $\hat{u}_i$ using hard decision,

$$\hat{u}_i = \begin{cases} 0, & \text{if } L_N^{(i)}(z_0^{N-1}, \hat{u}_0^{i-1}) \geq 1 \\ 1, & \text{if } L_N^{(i)}(z_0^{N-1}, \hat{u}_0^{i-1}) < 1 \end{cases} \tag{7}$$

After the ith bit is obtained by step 3, the process returns to step 2 to calculate the $(i+1)$th bit. Using SC decoding algorithm, the likelihood probability of each bit is dependent on the previous bits, and decided to be "0" or "1" directly. Since decoding a latter bit depends on the values of preceding ones, bits must be decoded one by one in sequence. Therefore, SC decoding can be viewed as a greedy tree search algorithm which can only achieve a local optimum instead of a global optimum. The local optimum decisions are easy to make wrong judgments when bits are set on good channels but not completely reliable, especially for short polar codes whose polarization effect is not perfect. In short polar codes, there are more channels between completely error-free channel and completely noisy channel, and the SC decoding algorithm is more likely to make error decisions. Furthermore, once an error decision is made, it will be propagated through the rest of the decoding process and will affect the subsequent decoding results.

3. Successive cancellation list decoding

In order to improve the performance of SC decoding algorithm, Tal proposed a Successive cancellation list (SCL)[28] decoding. When L (the size of list or the number of decoding paths) is large enough, the decoding performance can be close to an optimal Maximum-likelihood (ML) decoder.

Polar codes, with code length of N and key length of K, corresponds to a binary tree with a depth of N and a breadth of 2^N. Any path from the root node to any one

of the leaves is regarded as a possible decoding result and there are 2^K possible paths in total since the frozen bits are fixed. SC decoding makes hard decisions by searching the "local best" value and choses one path as decoding result from 2 local possible paths at each stage. It means that SC decoding only maintains one path during the decoding process.

In contrast, SCL decoding algorithm holds L possible paths parallelly. The decoding path in SCL is split into two sub-paths corresponding to $\hat{u_i} = 0$ and $\hat{u_i} = 1$ and SCL decoding does not immediately prune the decoding paths until the maximum number of paths L is reached. When the number of possible parallel paths exceeds L, SCL will evaluate the path metrics of the paths and prune the paths having lower likelihood. Because SCL retains L paths with the greatest probability instead of making hard decisions like SC does, it reduces the possibility of losing the correct result. Finally, when all the likelihood probabilities of N bits are calculated, there are L possible decoding results in the candidate list and only the path with the maximum path metric will be selected as the decoded output.

It can be seen that SCL decoding preserves L paths with the greatest probability using the "global optimal" approach, which overcomes the limitations of "local optimum" of SC decoding. Therefore, the proposed scheme can reduce the high FER caused by SC decoding and improve the yield of secret key generation.

IV. Numerical Results and Discussions

A series of numerical simulations were conducted to evaluate the efficiency and the robustness of the proposed scheme in terms of secret key rate and the maximum reconcilable QBER, respectively.

1. Secret key rate

As shown in Eq.(4), given a specific QBER, the secret key rate of key reconciliation mainly depends on coding efficiency β and FER. Therefore, the secret key rate can be improved by optimizing the coding structure: selecting the appropriate number of paths to improve error correction performance while maintaining the coding efficiency. Besides, Tal's coding construction of polar codes was also adopted in following numerical experiments to further improve coding efficiency[29]. The realistic secret key rates of the proposed scheme were evaluated at two code lengths of 2^{16} and 2^{20} and a QBER of 2%, compared with the performances of the previous polar codes-based scheme in Ref.[25] and the LDPC-based scheme with IEEE/ETSI DVB matrices in Ref.[26]. The numerical results are shown in Table 1 with different coding efficiencies β and different number of decoding paths L. Note that the FERs were statistically analyzed from 1000 tests with independent key strings.

Table 1. Secret key rate of the proposed scheme

N	L	$QBER$	β	FER	Secret key rate
2^{16}	2	2%	93.4%	0	0.661
	2	2%	95.3%	21.2%	0.534
	4	2%	95.3%	4.6%	0.646
	8	2%	95.3%	1.2%	0.669
	16	2%	95.3%	0.3%	0.676
	32	2%	95.7%	0.2%	0.680
2^{20}	2	2%	96.2%	0	0.685
	4	2%	96.7%	0.3%	0.688
	8	2%	96.9%	0.3%	0.689
	16	2%	97.1%	0.1%	0.692

In Table 1, for the code length of $N = 2^{16}$, given the coding efficiency of 93.4%, which are similar to the parameters in Ref.[25], the secret key rate of the proposed scheme is 0.661, higher than that in Ref.[25] (0.604) and in Ref.[26] (0.652). Given a higher coding efficiency of 95.3%, when the number of decoding paths is increased from 2 to 16, FER can be significantly reduced from 21.2% to 0.3%, resulting in a 26.6% increment of secret key rate from 0.534 to 0.676. Thus, it is possible to increase the secret key rate by increasing the number of decoding paths of the SCL algorithm. If the number of decoding paths is set to 32, the coding efficiency can be also increased to 95.7% and a secret key rate of 0.680 can be achieved. It means that the proposed scheme can improve the secret key rate 12.8% higher than that of the previous scheme in Ref.[25]. For the code length of $N = 2^{20}$, the performances of the proposed scheme are further improved due to the longer code length. When the number of decoding paths is increased from 2 to 16, the secret key rate can be increased from 0.685 to 0.692. These results show that the proposed scheme can achieve a higher secret key rate by optimizing the coding structure of choosing the appropriate encoding efficiency and the number of decoding paths.

2. The maximum reconcilable QBER

While the security threshold of QBER is 11% in theory, practical key reconciliation schemes usually cannot reach this upper bound. To evaluate the robustness of the proposed scheme, we further investigate the maximum QBER where secret key bits can still be extracted using the proposed scheme. The greater the maximum reconcilable QBER is, the more robust the proposed scheme is, and the longer transmission distance of QKD systems can be reached. Given a code length of $N = 2^{20}$, the secret key rates of the proposed scheme with different coding efficiencies and 4 decoding paths are shown in Fig.1, varying with QBERs ranging from 0 to 11%. It can be seen that the proposed scheme with different coding efficiencies can be applied to different QBER levels to achieve a trade-off between robustness and efficiency. For the curve with $\beta = 90.6\%$, when QBER reaches 10.2%, numerical results show that the proposed scheme has a FER of 0 and it can still achieve a secret key rate of $6.5 \cdot 10^{-4}$, and the secret

key rate of the proposed scheme will drop below 0 at a QBER of 10.3%. Therefore, it can be concluded that a maximum reconcilable QBER of 10.2% is reachable using the proposed scheme with a code length of $N = 2^{20}$ and a coding efficiency of $\beta = 90.6\%$.

In addition, we conduct experiments at QBERs ranging from 0 to 11% by 1% step to obtain the asymptote curve of secret key rate with code length $N = 2^{20}$ and 4 decoding paths, shown in Fig.1. The curve intersects each secret key rate line of different coding efficiencies at the inflection points, which are the upper limit of secret key rate at the corresponding QBER, and are also the balance between coding efficiency and the FER. Therefore, it is possible to find the most appropriate coding efficiency according to QBER, so that to maximize the secret key rate.

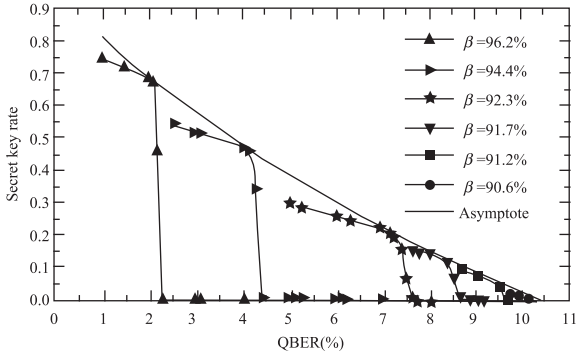


Fig. 1. Secret key rate of the proposed scheme with a code length of $N = 2^{20}$ and 4 decoding paths

V. Conclusions

In this paper, an efficient key reconciliation scheme based on polar codes is proposed for practical QKD systems. With a successive cancellation list decoding algorithm and optimized coding structures, the proposed scheme can achieve a secret key rate of 0.68, which is 12.8% higher than that of the previous polar codes-based key reconciliation scheme. Furthermore, the proposed scheme is robust with the maximum reconcilable QBER of 10.2% and it is able to support a longer transmission distance for practical QKD systems.

References

[1] N. Gisin, G. Ribordy, W. Tittel, *et al.*, "Quantum cryptography", *Physics*, Vol.74, No.1, pp.145–195, 2002.

[2] S. Wang, W. Chen, Z.Q. Yin, *et al.*, "Field and long-term demonstration of a wide area quantum key distribution network", *Optics Express*, Vol.22, No.18, pp.21739–21756, 2014.

[3] J. Li, N. Li, L.L. Li, *et al.*, "One step quantum key distribution based on EPR entanglement", *Scientific Reports*, Vol.6, No.28767, 2016.

[4] S. Wang, Z.Q. Yin, W. Chen, *et al.*, "Experimental demonstration of a quantum key distribution without signal disturbance monitoring", *Nature Photonics*, Vol.9, No.12, pp.832–836, 2015.

[5] C. Wang, X.T. Song, Z.Q. Yin, *et al.*, "Phase-reference-free experiment of measurement-device-independent quantum key distribution", *Physical Review Letters*, Vol.115, No.16, pp.160502, 2015.

[6] S. Wang, W. Chen, J.F. Guo, *et al.*, "2 GHz clock quantum key distribution over 260 km of standard telecom fiber", *Optics Letters*, Vol.37, No.6, pp.1008–1010, 2012.

[7] J. Li, Z.S. Pan, J. Zheng, *et al.*, "The security analysis of quantum "SAGR04" protocol in collective-rotation noise channel", *Chinese Journal of Electronics*, Vol.24, No.4, pp.689–693, 2015.

[8] B. Qi, C.F. Fung, H.K. Lo, *et al.*, "Time-shift attack in practical quantum cryptosystems", *Quantum Information and Computation*, Vol.7, No.1, pp.73–82, 2006.

[9] B. Kraus, N. Gisin and R. Renner, "Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication", *Physical Review Letters*, Vol.95, No.95, pp.080501, 2005.

[10] M. Williamson and V. Vedral, "Eavesdropping on practical quantum cryptography", *Journal of Modern Optics*, Vol.50, No.13, pp.1989–2011, 2003.

[11] A.R. Dixon and H. Sato, "High speed and adaptable error correction for megabit/s rate quantum key distribution", *Scientific Reports*, Vol.4, No.7275, 2013.

[12] C.H. Bennett, F. Bessette, G. Brassard, *et al.*, "Experimental quantum cryptography", *Journal of cryptology*, Vol.5, No.1, pp.3–28, 1992.

[13] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion", *Lecture Notes in Computer Science*, Vol.765, pp.410–423, 1994.

[14] C. Crepeau, "Reconciliation et distillation publiques de secret", Ecole Normale Superieure, France, 1995.

[15] T. Sugimoto and K. Yamazaki, "A study on secret key reconciliation protocol cascade", *IEICE Transactions on Fundamentals of Electronics*, Communications and Computer Sciences, Vol.E83-A, No.10, pp.1987–1991, 2000.

[16] T. Pedersen and M. Toyran, "High performance information reconciliation for QKD with CASCADE", *Quantum Information and Computation*, Vol.15, No.5, pp.419–434, 2013.

[17] S. Liu, H.C.A.V. Tilborg and M.V. Dijk, "A practical protocol for advantage distillation and information reconciliation", *Designs Codes and Cryptography*, Vol.30, No.1, pp.39–62,2003.

[18] S.K. Lamoreaux, J.R. Torgerson, G.H. Nickel, *et al.*, "Fast, efficient error reconciliation for quantum cryptography", *Physical Review A*, Vol.67, No.5, pp.125–128, 2003.

[19] Z.Y. HE, Q. ZHAO, H.S. XU, *et al.*, "An encoder with speed over 40Gbps for RC LDPC codes with rates up to 0.96", *Chinese Journal of Electronics*, Vol.25, No.5, pp.921–927, 2016.

[20] S. Watanabe, R. Matsumoto and T. Uyematsu, "Tomography increases key rates of quantum-key distribution protocols", *Physical Review A*, Vol.78, No.4, 2008.

[21] D. Pearson, "High-speed QKD reconciliation using forward error correction", *AIP Conference Proceedings*, Vol.734, No.1, pp.299–302, 2004.

[22] C. Elliott, A. Colvin, D. Pearson, *et al.*, "Current status of the DARPA quantum network", *Quantum Information and computation III*, Vol.5815, No.1, pp.138–149, 2005.

[23] D. Elkuss,A. Leverrier,R. Aume, *et al.*, "Efficient reconciliation protocol for discrete variable quantum key distribution", *IEEE International Symposium on Information Theory*, Vol.3, pp.1879–1883, 2009.

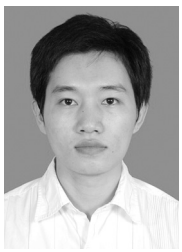
[24] E. Arikan, "Channel polarization: A method for constructing capacity achieving codes for symmetric binary-input memoryless channels", *IEEE Transactions on Information Theory*, Vol.55, No.7, pp.3051–3073, 2009.

[25] P. Jouguet and S. Kunz-Jacques. "High performance error correction for quantum key distribution using polar codes", *Quantum Information and Computation*, Vol.14, No.3, pp.329–338,

2014.
[26] A. Mink and A. Nakassis, "Practical strategies for QKD key production", *Proc. of SPIE*, Vol.8749, No.7, pp.874908, 2013.
[27] E. Arikan, "Systematic polar coding", *IEEE communications letters*, Vol.15, No.8, pp.860–862, 2011.
[28] I. Tal and A. Vardy, "List decoding of polar codes", *IEEE International Symposium on Information Theory*, Vol.19, No.5, pp.1–5, 2012.
[29] I. Tal and A. Vardy, "How to construct polar codes", *IEEE Transactions on Information Theory*, Vol.59, No.10, pp.6562–6582, 2013.

YAN Shiling received the bachelor degree in electronic and information engineering from Shandong University of Science and Technology, Qingdao, China, in 2014. Now she is pursuing the master's degree in optics at South China Normal University. Her research interest is post-processing of quantum key distribution. (Email: yanshiling40@foxmail.com)

WANG Jindong received the B.S. (1997) Degree in physics from Northwestern Polytechnical University, and received the M.S. (2005) and Ph.D. (2009) in optics from South China Normal University. Currently, he is a professor with school for information and optoelectric technology, South China Normal University. His current research interests include quantum key distribution, security of the quantum communication system, and the infrared single photon detection. He has published over 50 research papers in international journals and conferences. (Email: Wangjd@scnu.edu.cn)



FANG Junbin (corresponding author) is an associate professor with the Department of Optoelectronic Engineering, Jinan University and a visiting professor in the Edward S. Rogers Sr. Department of Electrical & Computer Engineering, University of Toronto, Canada. His research interests include quantum cryptography and visible light communication. (Email: tjunbinfang@jnu.edu.cn)

JIANG Lin is an assistant professor with School of Computer Science and Technology, Harbin Institute of Technology Shenzhen Graduate School, China. Her research interests include cryptography and digital forensics. (Email: zoeljiang@gmail.com)

WANG Xuan is a professor and Ph.D. supervisor in the Computer Application Research Center, Harbin Institute of Technology Shenzhen Graduate School. His main research interests include artificial intelligence, computer vision, computer network security and computational linguistics. (Email: wangxuan@cs.hitsz.edu.cn)