scientific reports

OPEN

Improved polar-code-based efficient post-processing algorithm for quantum key distribution

Junbin Fang[1,3,5], Zhengzhong Yi[2,5], Jin Li[1], Zhipeng Liang[2], Yulin Wu[2], Wen Lei[1], Zoe Lin Jiang[2]✉ & Xuan Wang[2,4]✉

Combined with one-time pad encryption scheme, quantum key distribution guarantees the unconditional security of communication in theory. However, error correction and privacy amplification in the post-processing phase of quantum key distribution result in high time delay, which limits the final secret key generation rate and the practicability of quantum key distribution systems. To alleviate this limitation, this paper proposes an efficient post-processing algorithm based on polar codes for quantum key distribution. In this algorithm, by analyzing the channel capacity of the main channel and the wiretap channel respectively under the Wyner's wiretap channel model, we design a codeword structure of polar codes, so that the error correction and privacy amplification could be completed synchronously in a single step. Through combining error correction and privacy amplification into one single step, this efficient post-processing algorithm reduces complexity of the system and lower the post-processing delay. Besides, the reliable and secure communicaiton conditions for this algorithm has been given in this paper. Simulation results show that this post-processing algorithm satisfies the reliable and secure communication conditions well.

Combined with one-time pad encryption scheme, quantum key distribution (QKD) can guarantee the unconditional security of communication system in theory[1–9]. Unlike the traditional encryption schemes such as RSA and Elliptical Curves whose security is based on the complexity of certain mathematical problems and hence will be influenced by the computing power of computing devices, QKD's security is based on physics law and the degree of the perfection of practical devices, which will not be influenced by computing power. Hence, in the post-quantum era during which most of the traditional encryption schemes are challenged with the formidable computing power of quantum computation, researchers have attached great attention to QKD. However, most practical QKD systems take photons as secret key carriers[10–13], which makes these systems susceptible to device defect and results in bit error and information leakage[14,15]. Therefore, it's necessary to perform error correction (also known as secret-key reconciliation) and privacy amplification in the post-processing phase to correct the error bit and eliminate the information leakage. Unfortunately, these two steps increase system overhead and introduce high time delay, which has become a bottleneck of realizing high-speed QKD and limits the further practicability of QKD systems[16,17]. The earliest error correction algorithm for QKD post-processing is BBBSS algorithm[18] which iteratively applies dichotomic parity check. Based on BBBSS algorithm, Brassard and Salvail proposed the Cascade algorithm[19] which improves the error correction efficiency of BBBSS. However, both of these two algorithms need repetitive exchange of the checking information between Alice (information sender) and Bob (information receiver) in the public channel, which leads to low error correction efficiency and high time delay in the post-processing phase. To reduce this repetitive information exchange in the public channel, Winnow algorithm[20], in which the checking information only needs transmitting for once, was proposed in 2003. However, within the security threshold of qubit error rate (QBER), Winnow still has low error correction efficiency. In 2004, Pearson proposed to apply LDPC codes in QKD post processing[21]. This idea has been followed by researchers for many years[22–26]. Though LDPC codes do improve the efficiency of error correction, its parity-check matrix relies on QBER and hence the error correction performance is quite sensitive to QBER. To overcome this shortcoming, Elkouss, Martinez-Mateo and Martin[23] proposed auto-adaptive LDPC for QKD system, but the iterative decoding of LDPC still results in high decoding overhead. In 2014, Joduget and Kunz-Jacques[27] first

[1]Department of Optoelectronic Engineering, Jinan University, Guangzhou 510632, China. [2]School of Computer Science and Technology, Harbin Institute of Technology, Shenzhen, Shenzhen 518055, China. [3]Cyberspace Security Research Center, Peng Cheng Laboratory, Shenzhen 518055, China. [4]Pengcheng Laboratory, Shenzhen 518055, Guangdong, China. [5]These authors contributed equally: Junbin Fang and Zhengzhong Yi. ✉email: zoeljiang@hit.edu.cn; wangxuan@cs.hitsz.edu.cn

| https://doi.org/10.1038/s41598-022-14145-6

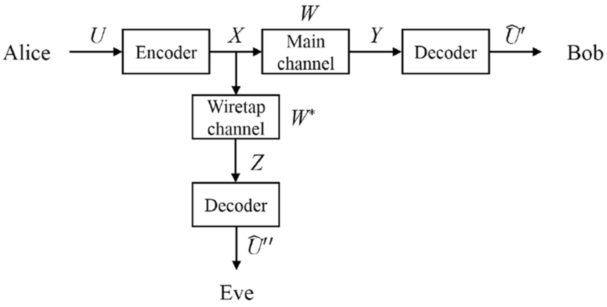

Figure 1. Wiretap channel model.

applied polar codes, whose code rate has been proved to achieve Shannon limit, to QKD, and discussed the feasibility. Later research[28] shows under short code length, the efficiency of polar codes is higher than LDPC codes. In the past several years, the application of polar codes in QKD system has drawn the attention of researchers[29–36].

In the aspect of privacy amplification, at present, a universal class of hash functions[37] was widely used in information compression to guarantee the security of secret key. However, due to its high computation complexity, this scheme has high time delay. To lower the time delay, researchers applies Toeplitz hashing, which becomes the most widely used privacy amplification method in recent years[25,38–40]. By combining Toeplitz hashing with fast Fourier transform, researchers has reduced the computation complexity of Toeplitz hashing to $O(n\log n)$.

To provide a new idea to reduce the complexity and lower the time delay of the post-processing phase in QKD systems, a polar-code-based efficient QKD post-processing algorithm is proposed in this paper. Using Wyner's wiretap channel model, we design a codeword structure of polar codes which satisfies the reliability and security for QKD post-processing. This idea has been applied to different communication systems in recent years[41,42]. By doing this, the error correction and privacy amplification which are the most time-consuming steps in the QKD post-processing could be completed synchronously in a single encoding and decoding process. Therefore, the complexity and time delay of post-processing can be reduced, and the final key generation rate can be improved. This will help with breaking through the bottleneck of realizing high-speed QKD system and promote practicability of QKD.

In 2019, we proposed polar codes-based one-step post-processing for quantum key distribution in our previous work[43]. However, there are three main drawbacks in our previous work. First, the security condition (see Eq. (5) in[43]) is inaccurate and ambiguous. Thus we modify the security condition in this paper (see Eq. (5) in this paper). Second, the protocol in[43] is incomplete which may result in decoding failure and insecurity (see the steps 1 to 10 and Fig. 3 in[43]). In this paper, we modify the protocol (see the steps 1 to 10 and Fig. 4 in this paper), which makes it more reliable and secure. The last but the most important point is that our previous work lacks experimental verification, since we only calculated the coding rate, and analyzed the reliability and security in theory. In this paper, we verify the reliability and security of the protocol through a large number of simulation experiments (see the whole section—"Simulation results").

The rest of this paper is organized as follows. In second section, we introduce the basic theory about Wyner's wiretap channel model, the secrecy capacity of discrete variable QKD (DVQKD) systems and polar codes. Then in third section, polar-code-based efficient QKD post-processing algorithm is introduced, after which we illustrate the reliability and security for the polar-code-based efficient QKD post-processing algorithm. The fourth section gives the simulation experiment result on code rate, decoding reliability and com1munication security. In last section, we summarize our work.

Basic theory

Wyner's wiretap channel model.

The goal of secret communication is to realize reliable and secure information transmission between two authentic communication sides even under eavesdropping. The channel under eavesdropping can be depicted by Wyner's wiretap channel model[44] which is shown in Fig. 1. Authentic information sender Alice encodes the original information U of length k to code X of length n and sends code X to authentic information receiver Bob through the main channel W, after which Bob gets information Y. In the meantime, eavesdropper Eve eavesdrops through the wiretap channel W^* and gets information Z. After decoding, Bob gets the estimation $\widehat{U}'$ of original information U and Eve gets the estimation $\widehat{U}''$.

In the Wyner's wiretap channel model, when the wiretap channel W^* is degenerative with respect to the main channel W (that is to say, the channel capacity of the wiretap channel $C(W^*)$ is smaller than the channel capacity of the main channel $C(W)$), with the code length tending to infinite, one can design a secure coding scheme which satisfies the communication reliability and security. Furthermore, the largest code rate is equal to the secrecy capacity C_{sec} which is defined by $C_{\text{sec}} \equiv C(W) - C(W^*)$. In other words, for all $\epsilon > 0$, there exist coding schemes of rate $R \geq C_{\text{sec}} - \epsilon$ that asymptotically achieve both the reliability and the security objectives[45]. Here, the reliability is measured by the decoding bit error rate (BER) of Bob, and the security is measured by the mutual information of $\widehat{U}''$ and U. Reliable communication means that

$$\lim_{n\to\infty} Pr(\widehat{U}'_i \neq U_i) = 0, \tag{1}$$

where the subscript i means the ith bit in $\widehat{U}'$ and U. Secure communication means that

$$\lim_{n\to\infty} I(\widehat{U}_i''; U_i) = 0, \tag{2}$$

where $I(\widehat{U}_i''; U_i)$ is the mutual information between Alice and Eve, $\widehat{U}_i''$ is the ith bit in $\widehat{U}''$. Combining Eq. (2) with the relation between mutual information $I(\widehat{U}_i''; U_i)$ and conditional entropy $H(U_i|\widehat{U}_i'')$ depicted by Eq. (3), and the definition of conditional entropy depicted by Eq. (4),

$$I(\widehat{U}_i''; U_i) \equiv H(U_i) - H(U_i|\widehat{U}_i'') = 1 - H(U_i|\widehat{U}_i''), \tag{3}$$

$$H(U_i|\widehat{U}_i'') \equiv -\sum_{a\in U_i}\sum_{b\in\widehat{U}_i''} p(a,b)\log p(a|b), \tag{4}$$

we can rewrite eqaution (2) to

$$\lim_{n\to\infty} Pr(\widehat{U}_i'' \neq U_i) = \lim_{n\to\infty} Pr(\widehat{U}_i'' = U_i) = 0.5. \tag{5}$$

Equation (1) is the *reliable communication condition* and Eq. (5) is the *secure communication condition*. They imply that a reliable and secure coding scheme demands that, with code length tending to infinite, Bob asymptotically achieves 0 and the decoding BER of Eve asymptotically achieves 0.5.

Channel capacity of DVQKD post-processing systems under Wyner's wiretap channel model.

In QKD systems, after qubit transmission and sifting, Alice obtains sifted key KA_{sifted} and Bob obtains sifted key KB_{sifted}. Due to the defect of devices, channel noise and possible eavesdropping in the practical QKD system, in general, $KA_{\text{sifted}} \neq KB_{\text{sifted}}$. Namely, there are error bits. Denote the bit error rate in practical QKD system by p.

DVQKD is the maturest and the most widely used QKD system. For those DVQKD systems which apply BB84 protocol, their qubit transmission channel can be regarded as binary symmetric channel (BSC). Under this assumption, the mutual information between Alice and Bob is

$$I_{\text{AB}} = 1 - h_2(p), \tag{6}$$

where $h_2(\cdot)$ is binary entropy function[22]. Considering the maximum safety of communication, we can regard all the noise in practical systems results from eavesdropping. Hence, all information Eve can obtain is at most

$$I_{\text{AE}} = h_2(p). \tag{7}$$

If we adopt Wyner's wiretap channel model to depict QKD system, the channel capacity of main channel W is

$$C(W) = I_{AB} = 1 - h_2(p), \tag{8}$$

the channel capacity of the wiretap channel is

$$C(W^*) = I_{\text{AE}} = h_2(p), \tag{9}$$

and the secrecy capacity is

$$C_{\text{sec}} = C(W) - C(W^*) = 1 - 2h_2(p). \tag{10}$$

The secrecy capacity is equal to the secure final key generation rate k_{th}[2].

Practical DVQKD systems require that $k_{\text{th}} = 1 - 2h_2(p) \geq 0$. This means that the value range of QBER p is [0, 0.11] and $C(W) \geq C(W^*)$. Hence, according to the Wyner's wiretap channel model theory, within this range of p, channel W^* between Alice and Eve is degenerative to channel W between Alice and Bob, and we can design a coding scheme which achieves the secrecy capacity. The rest of this paper is based on this prerequisite.

Polar codes.

Polar codes are the only coding scheme which has been proved in theory that their code rate can achieve Shannon limit[46]. Besides, the encoding and decoding complexity of polar codes is relatively small compared with LDPC codes[46]. Through recursively polarizing N independent identically distributed (i.i.d.) channels whose capacity are all C, one can get N coordinate subchannels whose capacity polarizes - with the growth of code length N, the capacity of $N \cdot C$ coordinate subchannels asymptotically tends to 1, while the capacity of the other $N \cdot (1 - C)$ coordinate subchannels asymptotically tends to 0. That is to say, the former $N \cdot C$ coordinate subchannels are optimized and the latter $N \cdot (1 - C)$ coordinate subchannels are degraded. The optimized channels will be used to transmit information bits and the degraded ones will be used to transmit frozen bits. Hence, the code rate asymptotically achieves the channel capacity which equals to $N \cdot C$.

Denote the original N i.i.d. channels by W. As shown in Fig. 2, through channel combining in a recursive way, we get the combining channel W_N of all N i.i.d. channels. Then through channel splitting, we can obtain N coordinate subchannels $W_N^{(i)}$[46]. The superscript (i) means the ith subchannel. In the rest of this paper, $1 \leq i \leq N$.

Under finite code length N, we need to evaluate the channel quality of each coordinate subchannel. According to the channel quality, we rank all coordinate subchannels in descending order. Then, the first K of them are chosen to transmit information bits according to concrete error correction requirement. In this way, the construction of polar codes is fulfilled. It's noticeable that the determination of K will impact the reliability and

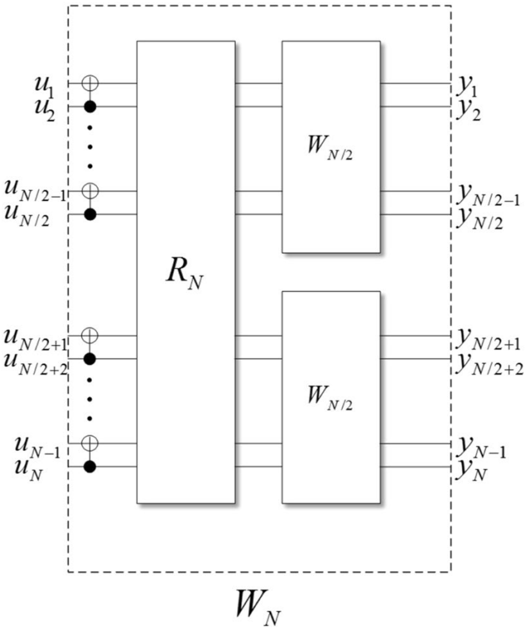

Figure 2. Channel polarization. R_N is the bit-reversal operation. When $N = 1$, W_1 is the original channel W.

the code rate of the code structure we design - if K is too high, the decoding reliability will be unacceptable; if it is too low, the channel-capacity-reachable characteristic of polar code cannot be fully used and hence the code rate will be unsatisfactory. K can be determined by setting target frame error rate (TFER, it is a predefined value which Alice and Bob try to make the practical frame error rate of their communication lower than through error correction), which is used in our algorithm in "Simulation results".

At present, there are several ways to realize the construction of polar codes[46–49]. In this paper, we adopt Tal's method[47] to construct polar codes, in which the probability of error $P_e(W_N^{(i)})$ under maximum-likelihood decision is used to measure the quality of each coordinate subchannel $W_N^{(i)}$. Through a asymptotic method called channel degradation[47], we calculate the upper bound of each $P_e(W_N^{(i)})$ which will be used to construct polar codes.

Polar-code-based efficient post-processing algorithm

Error correction and privacy amplification are two crucial steps in QKD post-processing. The goal of error correction is to eliminate the difference between Alice's sifted key KA_{sifted} and Bob's sifted key KB_{sifted} through information exchange between Alice and Bob, so that they can obtain the information which is equal to the capacity $C(W^*)$ of the main channel. The goal of privacy amplification is to compress the exchanged information between Alice and Bob to remove the information Eve can obtain, which is equal to the capacity $C(W^*)$ of wiretap channel.

Aiming at these two functions of the two crucial steps, we propose an efficient post-processing algorithm which can fulfill error correction and privacy amplification at the same time. This algorithm is called polar-code-based efficient post-processing (PCEP) algorithm. The concrete steps of PCEP are as follows. Denote the TFER by FER_{target}, the target privacy amplification index (TPAI, it is a predefined value which Alice and Bob try to make the practical privacy amplification index lower than. Privacy amplification index is the leaked information rate, which is equal to the amount of leaked information leaked in a single code block divided by the code block length) by PAI_{target}.

Steps of PCEP algorithm.

Step 1: Parameter estimation

Alice and Bob compare the bases they use in the qubit transmission phase and get their own sifted key KA_{sifted} and KB_{sifted}. Then they choose some bits from their own sifted key to estimate the bit error rate p_{m} (to distinguish the indexes of main channel and wiretap channel, we write an "m" in the subscript to represent that this index belongs to "main channel" or a "w" to represent that this index belongs to "wiretap channel") in the main channel as in other common post-processing algorithm . If p_{m} exceeds the security threshold, they abort this key distribution, or else they enter into next step.

Step 2: Polarization of the main channel

Alice and Bob polarize the main channel W by Arikan's method[46] and obtain N coordinate subchannels $W_N^{(i)}$.

Step 3: Channel quality evaluation in the main channel

Denote the code length that Alice and Bob use by N, Alice and Bob take p_{m} as the channel quality index of the main channel, according to which they adopt Tal's polar code construction algorithm[47] to calculate the upper bound $UP_{\text{e,m}}(W_N^{(i)})$ (not necessarily the supremum) of the decoding error rate $P_{\text{e,m}}(W_N^{(i)})$ under maximum-likelihood decision of each coordinate subchannel $W_N^{(i)}$. $UP_{\text{e,m}}(W_N^{(i)})$ are used to evaluate the channel quality of each coordinate subchannel, the lower the better.

Step 4: Optimized coordinate subchannels selection in the main channel

Alice and Bob sort all coordinate subchannels $W_N^{(i)}$ according to $UP_{\mathrm{e,m}}(W_N^{(i)})$ *in ascending order*, and chooses the first K_{m} coordinate subchannels which satisfy Eq. (11) to compose the optimized channel set $G_N(W, FER_{\mathrm{target}})$. The rest of coordinate subchannels compose the degraded channel set $B_N(W, FER_{\mathrm{target}})$.

$$\sum_i UP_{\mathrm{e,m}}(W_N^{(i)}) \le FER_{\mathrm{target}}. \tag{11}$$

That is to say, Alice and Bob divide all coordinate subchannels in the main channel to two sets:

$$G_N(W, FER_{\mathrm{target}}) \equiv \{i|1 \le i \le N\} \cap \{i| \sum_i UP_{\mathrm{e,m}}(W_N^{(i)}) \le FER_{\mathrm{target}}\}, \tag{12}$$

$$B_N(W, FER_{\mathrm{target}}) \equiv \{i|1 \le i \le N\} \setminus G_N(W, FER_{\mathrm{target}}). \tag{13}$$

From Eqs. (12) and (13), we can see that G_N and B_N are functions of W and FER_{target}. This is why we write G_N as $G_N(W, FER_{\mathrm{target}})$ and B_N as $B_N(W, FER_{\mathrm{target}})$. For convenience, G_N and B_N will be used in the rest of this paper.

Step 5: Polarization of the wiretap channel

Alice and Bob polarize the wiretap channel W^* by Arikan's method[46] and obtain N coordinate subchannels $W_N^{(i)}$.

Step 6: Channel quality evaluation in the wiretap channel

Alice and Bob calculate the bit error rate p_{w} of wiretap channel according to $I_{\mathrm{AE}} = 1 - h_2(p_{\mathrm{w}}) = h_2(p_{\mathrm{m}})$ as mentioned in "Polar-code-based efficient post-processing algorithm". Then they take p_{w} as the channel quality index of the wiretap channel, according to which they adopt Tal's polar codes construction algorithm[47] to calculate the upper bound $UP_{\mathrm{e,w}}(W_N^{*(i)})$ (not necessarily the supremum) of the probability of error $P_{\mathrm{e,w}}(W_N^{*(i)})$ under maximum-likelihood decision of each coordinate subchannel $W_N^{*(i)}$ in wiretap channel. Using Eq. (14), Alice and Bob calculate the channel capacity of $C_{\mathrm{w}}(W_N^{*(i)})$ each coordinate subchannel.

$$C_{\mathrm{w}}(W_N^{*(i)}) = 1 - h_2(P_{\mathrm{e,w}}(W_N^{*(i)})). \tag{14}$$

The channel capacity $C_{\mathrm{w}}(W_N^{*(i)})$ is used to evaluate the channel quality of each coordinate subchannel, the higher the better.

Step 7: Optimized coordinate subchannels selection in the wiretap channel

Alice and Bob sort all coordinate subchannels $W_N^{*(i)}$ according to $C_{\mathrm{w}}(W_N^{*(i)})$ *in ascending order* and chooses the first K_{w} ones which satisfy Eq. (15) to compose degraded channel set $B_N^*(W^*, PAI_{\mathrm{target}})$ with respect to Eve. The rest of coordinate subchannels compose optimized channel set $G_N^*(W^*, PAI_{\mathrm{target}})$ with respect to Eve.

$$\sum_i C_{\mathrm{w}}(W_N^{*(i)}) \le PAI_{\mathrm{target}}. \tag{15}$$

That is to say, Alice and Bob divide all coordinate subchannels in the wiretap channel to two sets:

$$B_N^*(W^*, PAI_{\mathrm{target}}) \equiv \left\{ i|1 \le i \le N\} \cap \{i| \sum_i C_{\mathrm{w}}(W_N^{*(i)}) \le PAI_{\mathrm{target}} \right\}, \tag{16}$$

$$G_N^*(W^*, PAI_{\mathrm{target}}) \equiv \{i|1 \le i \le N\} \setminus B_N^*(W^*, PAI_{\mathrm{target}}). \tag{17}$$

From Eqs. (16) and (17), we can see that B_N^* and G_N^* are functions of W^* and PAI_{target}. This is why we write G_N^* as $G_N^*(W^*, PAI_{\mathrm{target}})$ and B_N^* as $B_N^*(W^*, PAI_{\mathrm{target}})$. For convenience, G_N^* and B_N^* will be used in the rest of this paper.

Step 8: Determination of code structure

After the above steps, Alice and Bob obtain four sets of coordinate subchannels. The first set G_N is the optimized coordinate subchannels to Bob, the second set B_N is the degraded ones to Bob, the third set G_N^* is the optimized ones to Eve, and the last set B_N^* is the degraded ones to Eve. As shown in Fig. 3, the subchannels which belong to B_N must belong to B_N^*, and the ones which belong to G_N^* must belong to G_N. This is because that the wiretap channel is degenerative with respect to the main channel. Therefore, those subchannels which are degraded to Bob must be degraded to Eve, and those which are optimized to Eve must be optimized to Bob. Hence, G_N and B_N^* have intersection.

Based on the above analysis of the four sets G_N, B_N, G_N^*, and B_N^*, Alice and Bob can redivide all subchannels into three sets without intersection as follows.

$$R \equiv G_N^*, \tag{18}$$

$$A \equiv B_N^* \cap G_N, \tag{19}$$

$$B \equiv B_N. \tag{20}$$

Alice and Bob choose the subchannels in A to transmit the information bits (in this situation, they are the bits of secret key), the subchannels in R to transmit random bits, and the subchannels in B to transmit frozen bits. By this redivision, the code structure is determined. Notice that, actually, all the code construction work, including

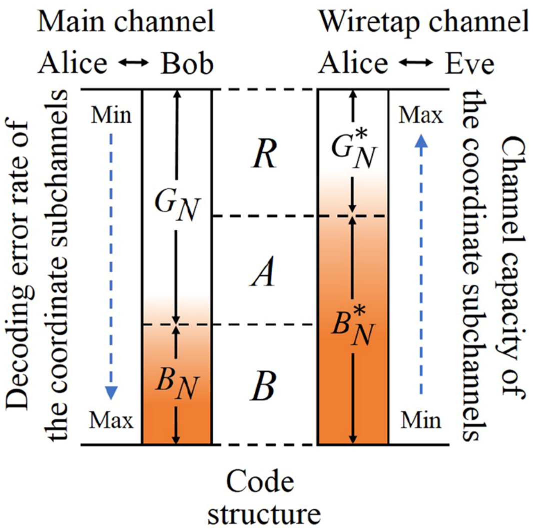

Figure 3. Code construction. The two columns which are colored by gradient represent the coordinate subchannels of the main channel and the wiretap channel. The deeper the color is, the worse the channel quality is.

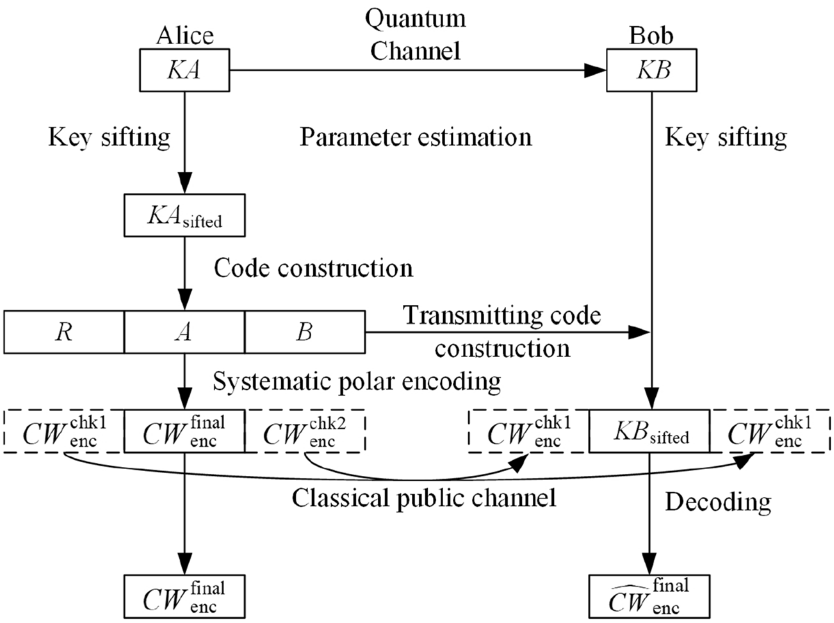
Alice
KA
Quantum Channel
Bob
KB
Key sifting
Parameter estimation
Key sifting
KA_{sifted}
Code construction
R
A
B
Transmitting code construction
Systematic polar encoding
$CW_{\text{enc}}^{\text{chk1}}$
$CW_{\text{enc}}^{\text{final}}$
$CW_{\text{enc}}^{\text{chk2}}$
$CW_{\text{enc}}^{\text{chk1}}$
KB_{sifted}
$CW_{\text{enc}}^{\text{chk1}}$
Classical public channel
Decoding
$CW_{\text{enc}}^{\text{final}}$
$\widehat{CW}_{\text{enc}}^{\text{final}}$

Figure 4. Polar-code-based efficient post-processing algorithm.

steps 4 to steps 8, can be done by Alice alone. Once Alice finish this work, she will transmit the code structure to Bob. Hence, Fig. 4 has not shown that Bob joins in the code construction work.

Step 9: Code transmission

Alice randomly generates the bits which belong to R, sets all bits which belong to B to zero, and puts KA_{sifted} into the bits which belong to A. Then she connects them according to the order of corresponding coordinate subchannels to form the original code. After encoding the original code by systematic polar coding algorithm[50], Alice gets code CW_{enc}. As shown in Fig. 4, CW_{enc} is composed of $CW_{\text{enc}}^{\text{chk1}}$, $CW_{\text{enc}}^{\text{final}}$(under systematic polar coding, $CW_{\text{enc}}^{\text{final}} = KA_{\text{sifted}}$) and $CW_{\text{enc}}^{\text{chk2}}$, which are the systematic polar encoding results of the bits belong to R, A, and B, respectively. Alice only sends the check bits $CW_{\text{enc}}^{\text{chk1}}$ and $CW_{\text{enc}}^{\text{chk2}}$ to Bob through classical public channel.

Step 10: Error correction

Bob puts his sifted key KB_{sifted} into the bits which belong to A, puts $CW_{\text{enc}}^{\text{chk1}}$ into the bits which belong to R, and puts $CW_{\text{enc}}^{\text{chk2}}$ into the bits which belong to B. Then he decodes this bit string to get $\widehat{CW}_{\text{enc}}^{\text{final}}$. At last, Alice and Bob take $CW_{\text{enc}}^{\text{final}}$ and $\widehat{CW}_{\text{enc}}^{\text{final}}$ as their final key respectively. The reliable communication condition Eq. (21) asks that

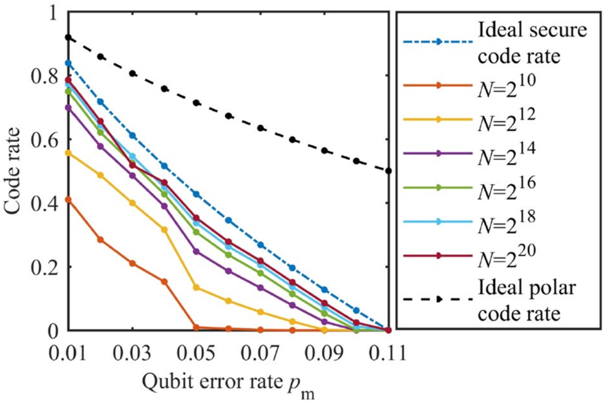

Figure 5. Code rate. The ideal polar code rate is the ideal code rate of polar code itself without considering wiretap channel. The ideal secure code rate is the ideal code rate of PCEP algorithm under wiretap channel model.

$$\lim_{n\to\infty} Pr(\widehat{CW}_{\text{enc}}^{\text{final}} \neq CW_{\text{enc}}^{\text{final}}) = 0. \tag{21}$$

Reliability and security for PCEP algorithm. In PCEP algorithm, Bob gets $CW_{\text{enc}}^{\text{chk1}}$, $CW_{\text{enc}}^{\text{chk2}}$ and KB_{sifted} which is obtained through the quantum channel with bit error rate p_{m}. Assume Eve has full access to the classical channel, and all that she can get is $CW_{\text{enc}}^{\text{chk1}}$, $CW_{\text{enc}}^{\text{chk2}}$ and KB_{sifted} which is obtained by eavesdropping the quantum channel with bit error rate p_{w}. According to Eq. (7), we obtain

$$1 - h_2(p_{\text{w}}) = h_2(p_m). \tag{22}$$

When wiretap channel W^* is degenerative to main channel W, $p_{\text{m}} < p_{\text{w}}$. The key KA_{sifted} has been encoded into $CW_{\text{enc}}^{\text{final}}$, and under systematic polar coding, $CW_{\text{enc}}^{\text{final}} = KA_{\text{sifted}}$. To obtain the key, Bob decodes $CW_{\text{enc}}^{\text{chk1}}$, $CW_{\text{enc}}^{\text{chk2}}$ and KB_{sifted} to get $\widehat{CW}_{\text{enc}}^{\text{final}}$, Eve decodes $CW_{\text{enc}}^{\text{chk1}}$, $CW_{\text{enc}}^{\text{chk2}}$ and KE_{sifted} to get $\widehat{CW}_{\text{enc}}^{\prime final}$. Because the coordinate subchannels in set A is optimized to Bob but degraded to Eve, the code structure which is determined in step 8 is optimized to Bob but degraded to Eve. Hence, with the growth of code length N, the decoding error rate of Bob tends to 0 while the decoding error rate of Eve tends to 0.5 (namely, the information in the wiretap channel has been compressed to zero). That is to say, $\lim_{n\to\infty} Pr(\widehat{CW}_{\text{enc}}^{\text{final}} \neq CW_{\text{enc}}^{\text{final}}) = 0$ and $\lim_{n\to\infty} Pr(\widehat{CW}_{\text{enc}}^{\text{final}} = CW_{\text{enc}}^{\prime final}) = 0$, which satisfies the reliable communication condition (Eq. 1) and secure communication condition (Eq. 5).

Simulation results

To prove the feasibility of PCEP algorithm, we conduct a series of simulation experiment on code rate, reliability and security. It should be noticed that the range of p_{m} has been limited to [0, 0.11] because as mentioned in "Polar-code-based efficient post-processing algorithm", only in this range is W^* degenerative to W. In all simulation experiment, we set FER_{target} to 0.1 and PAI_{target} to 10^{-7}.

Code rate. As shown in Fig. 5, under different code length N, we calculate the code rate. It is observed that with the increase of QBER p_{m} of the main channel, the code rate tends to zero. Moreover, except a single point (where $N = 2^{20}$, $p_{\text{m}} = 0.03$), under the same QBER p_{m}, the longer the code length is, the higher the code rate is. This is in accord with the asymptotic property of polar codes.

Figure 6 shows the ratio of the practical code rate and the theoretical secure code rate. It can be observed that with the increase of QBER p_{m}, the ratio decreases to zero. The theoretical secure code rate can be regarded as a measurement of the error correcting capability of polar codes, while the practical code rate can be regarded as a measurement of the specific requirement for error correcting capability in certain setting. Therefore, the ratio can be used to measure the extent to which the requirement can be met - the lower the ratio is, the higher the extent is, and hence the better the error correcting performance is. Hence, the lower the ratio is, the higher the decoding reliability should be, which is consistent with the simulation result in "Reliability".

Security: the decoding FER and BER of Eve. According to Eq. (5), the security of PCEP algorithm can be measured by the decoding FER and BER of Eve, which is shown in Figs. 7 and 8. It can be observed that when QBER p_{m} is small, the decoding FER and BER of Eve well satisfies the security condition Eq. (5) ($FER = 1$, $BER \sim 0.5$), while there is a threshold of QBER beyond which the decoding FER and BER of Eve dramatically decrease to zero. Moreover, the longer the code length, the higher the threshold, which coheres with the asymptotic property of polar codes.

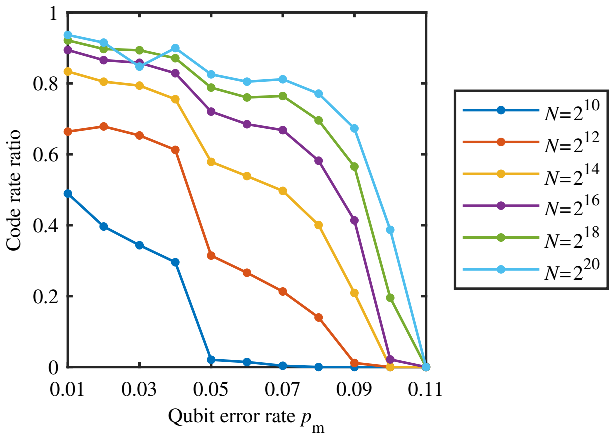

Figure 6. The ratio of the practical code rate and the theoretical secure code rate.

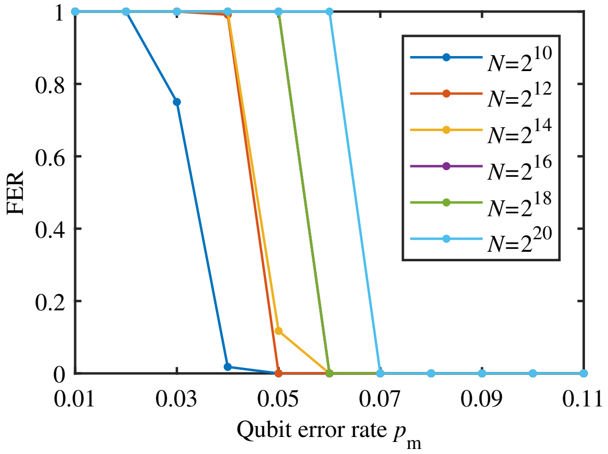

Figure 7. The decoding FER of Eve. The number of simulation tests is 1×10^5.

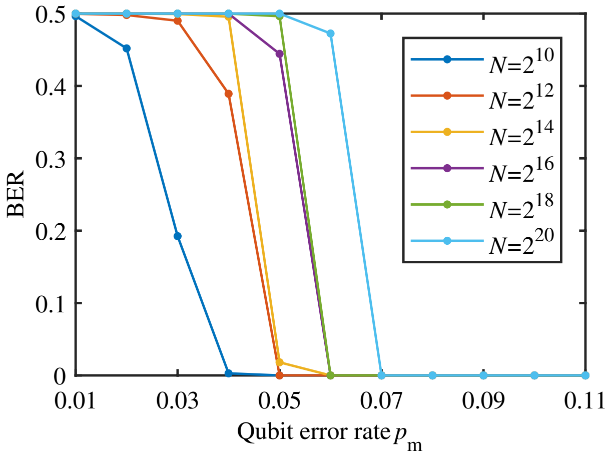

Figure 8. The decoding BER of Eve. The number of simulation tests is 1×10^5.

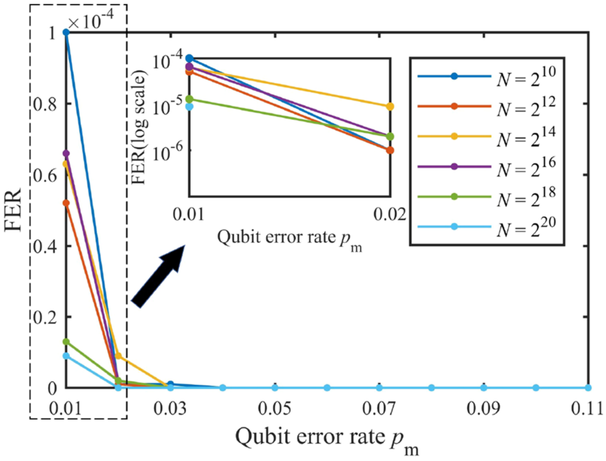

Figure 9. The decoding FER of Bob.

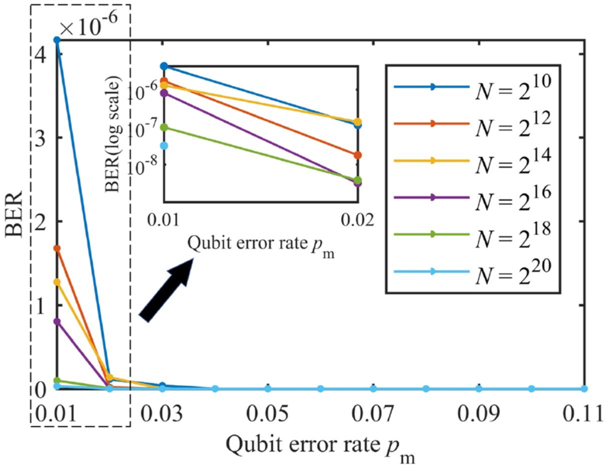

Figure 10. The decoding BER of Bob.

Reliability. According to Eq. (1), the reliability of PCEP algorithm can be measured by the decoding FER and BER of Bob, which is shown in Figs. 9 and 10. It is observed that the practical decoding FER and BER are satisfying under all code lengths shown in Figs. 9 and 10. Besides, as shown in Fig. 9, the maximum FER in the simulation is around 1^{-4} when $N = 2^{10}$ and $p = 0.01$. Notice that the TFER has been set to 0.1, hence this target is well achieved.

Moreover, under different code lengths, the decoding FER and BER of Bob decrease to zero rapidly with the increase of QBER p_{m}. The reason for this counterintuitive phenomenon has been explained in the last paragraph in "Code rate".

Conclusion

In this paper, an efficient QKD post-processing algorithm PCEP which is based on polar codes is proposed. In PCEP algorithm, by analyzing the channel capacity of the main channel and the wiretap channel respectively under the Wyner's wiretap channel model, we design a codeword structure of polar codes, so that the error correction and privacy amplification could be completed synchronously in a single encoding and decoding process. That is to say, PCEP algorithm realizes combining these two post-processing steps into one step. Through this, PCEP algorithm can reduce the complexity and lower the post-processing delay of QKD systems. This provides a new way to develop high-speed QKD systems. To clarify the reliability and security of PCEP algorithm, the reliability and security conditions have deen deduced from the perspective of information theory. Simulation results show that PCEP algorithm well satisfies the reliable and secure communication conditions.

Received: 23 December 2021; Accepted: 6 May 2022
Published online: 16 June 2022

References

1. Lo, H.-K. A simple proof of the unconditional security of quantum key distribution. *J. Phys. A: Math. Gen.* **34**, 6957 (2001).
2. Gottesman, D., Lo, H.-K., Lutkenhaus, N. & Preskill, J. Security of quantum key distribution with imperfect devices. In *International Symposium on Information Theory, 2004. ISIT 2004. Proceedings*, 136 (IEEE, 2004).
3. Koashi, M. Simple security proof of quantum key distribution based on complementarity. *New J. Phys.* **11**, 045018 (2009).
4. Molotkov, S. N. & Nazin, S. S. A simple proof of unconditional security of relativistic quantum cryptography. *J. Exp. Theor. Phys.* **92**, 871–878 (2001).
5. Leverrier, A. & Grangier, P. Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. *Phys. Rev. Lett.* **102**, 180504 (2009).
6. Lo, H.-K. Proof of unconditional security of six-state quantum key distribution scheme. arXiv:quant-ph/0102138 (2001).
7. Gottesman, D. & Lo, H.-K. Proof of security of quantum key distribution with two-way classical communications. *IEEE Trans. Inf. Theory* **49**, 457–475 (2003).
8. Lo, H.-K. & Chau, H. F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **283**, 2050–2056 (1999).
9. Shor, P. W. & Preskill, J. Simple proof of security of the bb84 quantum key distribution protocol. *Phys. Rev. Lett.* **85**, 441 (2000).
10. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145 (2002).
11. Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theoret. Comput. Sci.* **560**, 7–11 (2014).
12. Chen, Y.-A. *et al.* An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature* **589**, 214–219 (2021).
13. Sibson, P. *et al.* Chip-based quantum key distribution. *Nat. Commun.* **8**, 13984 (2017).
14. Xu, F., Ma, X., Zhang, Q., Lo, H.-K. & Pan, J.-W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **92**, 025002 (2020).
15. Cui, Z.-X., Zhong, W., Zhou, L. & Sheng, Y.-B. Measurement-device-independent quantum key distribution with hyper-encoding. *Sci. China Phys. Mech. Astron.* **62**, 110311 (2019).
16. Diamanti, E., Lo, H.-K., Qi, B. & Yuan, Z. Practical challenges in quantum key distribution. *NPJ Quant. Inf.* **2**, 16025 (2016).
17. Fung, C.-H.F., Ma, X. & Chau, H. Practical issues in quantum-key-distribution postprocessing. *Phys. Rev. A* **81**, 012318 (2010).
18. Bennett, C. H., Bessette, F., Brassard, G., Salvail, L. & Smolin, J. Experimental quantum cryptography. *J. Cryptol.* **5**, 3–28 (1992).
19. Brassard, G. & Salvail, L. Secret-key reconciliation by public discussion. In *Workshop on the Theory and Application of of Cryptographic Techniques*, 410–423 (Springer, 1993).
20. Buttler, W. T. *et al.* Fast, efficient error reconciliation for quantum cryptography. *Phys. Rev. A* **67**, 052303 (2003).
21. Pearson, D. High-speed qkd reconciliation using forward error correction. In *AIP Conference Proceedings*, vol. 734, 299–302 (American Institute of Physics, 2004).
22. Elkouss, D., Leverrier, A., Alléaume, R. & Boutros, J. J. Efficient reconciliation protocol for discrete-variable quantum key distribution. In *2009 IEEE International Symposium on Information Theory*, 1879–1883 (IEEE, 2009).
23. Elkouss, D., Martinez-Mateo, J. & Martin, V. Information reconciliation for quantum key distribution. arXiv:1007.1616 (2010).
24. Walenta, N. *et al.* A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing. *New J. Phys.* **16**, 013047 (2014).
25. Yuan, Z. *et al.* 10-mb/s quantum key distribution. *J. Lightwave Technol.* **36**, 3427–3433 (2018).
26. Mao, H., Li, Q., Han, Q. & Guo, H. High-throughput and low-cost ldpc reconciliation for quantum key distribution. *Quantum Inf. Process.* **18**, 232 (2019).
27. Jouguet, P. & Kunz-Jacques, S. High performance error correction for quantum key distribution using polar codes. arXiv:1204.5882 (2012).
28. Lee, S., Park, J. & Heo, J. Improved reconciliation with polar codes in quantum key distribution. *arXiv preprint* arXiv:1805.05046 *(2018).*
29. Renes, J. M., Renner, R. & Sutter, D. Efficient one-way secret-key agreement and private channel coding via polarization. In *International Conference on the Theory and Application of Cryptology and Information Security*, 194–213 (Springer, 2013).
30. Yan, S., Wang, J., Fang, J., Jiang, L. & Wang, X. An improved polar codes-based key reconciliation for practical quantum key distribution. *Chin. J. Electron.* **27**, 250–255 (2018).
31. Yi, Z. *et al.* Efficient quantum key distribution protocol based on classical-quantum polarized channels. *Quantum Inf. Process.* **18**, 356 (2019).
32. Nakassis, A. Polar codes for quantum key distribution. *J. Res. Nat. Inst. Stand. Technol.* **122**, 1–10 (2017).
33. Kim, Y., Suh, C. & Rhee, J.-K. K. Reconciliation with polar codes constructed using gaussian approximation for long-distance continuous-variable quantum key distribution. In *2017 International Conference on Information and Communication Technology Convergence (ICTC)*, 301–306 (IEEE, 2017).
34. Lee, S. & Heo, J. Efficient reconciliation protocol with polar codes for quantum key distribution. In *2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN)*, 40–43 (IEEE, 2018).
35. Zhao, S., Shen, Z., Xiao, H. & Wang, L. Multidimensional reconciliation protocol for continuous-variable quantum key agreement with polar coding. *Sci. China Phys. Mech. Astron.* **61**, 090323 (2018).
36. Zhang, M., Hai, H., Feng, Y. & Jiang, X.-Q. Rate-adaptive reconciliation with polar coding for continuous-variable quantum key distribution. *Quant. Inf. Process.* **20**, 318 (2021).
37. Bennett, C. H., Brassard, G., Crépeau, C. & Maurer, U. M. Generalized privacy amplification. *IEEE Trans. Inf. Theory* **41**, 1915–1923 (1995).
38. Hayashi, M. Exponential decreasing rate of leaked information in universal random privacy amplification. *IEEE Trans. Inf. Theory* **57**, 3989–4001 (2011).
39. Zhang, H.-F. *et al.* A real-time qkd system based on fpga. *J. Lightwave Technol.* **30**, 3226–3234 (2012).
40. Li, Q. et al. High-speed and adaptive fpga-based privacy amplification in quantum key distribution. *IEEE Access* **7**, 21482–21490.
41. Che, Z. et al. A physical-layer secure coding schcme for visible light communication based on polar codes. In *2017 Conference on Lasers and Electro-Optics Pacific Rim*, s1810 (Optica Publishing Group, 2017).
42. Chen, B. & Willems, F. M. Secret key generation over biased physical unclonable functions with polar codes. *IEEE Internet Things J.* **6**, 435–445 (2018).
43. Li, J., Jiang, L., Lin, X. & Fang, J. Polar codes-based one-step post-processing for quantum key distribution. *J. South China Normal Univ. Nat. Sci. Edition* **51**, 1–6 (2019).
44. Wyner, A. D. The wire-tap channel. *Bell Syst. Tech. J.* **54**, 1355–1387 (1975).
45. Mahdavifar, H. & Vardy, A. Achieving the secrecy capacity of wiretap channels using polar codes. *IEEE Trans. Inf. Theory* **57**, 6428–6443 (2011).
46. Arikan, E. Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels. *IEEE Trans. Inf. Theory* **55**, 3051–3073 (2009).
47. Tal, I. & Vardy, A. How to construct polar codes. *IEEE Trans. Inf. Theory* **59**, 6562–6582 (2013).
48. Mori, R. Properties and construction of polar codes. arXiv:1002.3521 (2010).

49. Mori, R. & Tanaka, T. Performance and construction of polar codes on symmetric binary-input memoryless channels. In *2009 IEEE International Symposium on Information Theory*, 1496–1500 (IEEE, 2009).
50. Arikan, E. Systematic polar coding. *IEEE Commun. Lett.* **15**, 860–862 (2011).

Acknowledgements

This work was supported in part by the National Key Research and Development Program of China (2018YFB1801900), in part by the National Natural Science Foundation of China (61771222, 61872109), in part by the Science and Technology Project of Guangzhou (201803020023), in part by the Project of Guangzhou Industry Leading Talents (CXLJTD-201607), in part by the Science and Technology Project of Shenzhen (JCYJ20170815145900474, JSGG20170824163239586), in part by the Peng Cheng Laboratory Project of Guangdong Province (PCL2018KP004), and in part by the Fundamental Research Funds for the Central Universities (21620439).

Author contributions

J.F., Z.Y., J.L., Z.L., Y.W., W.L., Z.L.J and X.W. conceived the work, carried out experiments, analysed the results and wrote the manuscript.

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to Z.L.J. or X.W.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.