Yang *et al. Cybersecurity* (2019) 2:16
https://doi.org/10.1186/s42400-019-0033-z

Cybersecurity

RESEARCH Open Access

One-way information reconciliation schemes of quantum key distribution

Li Yang[1,2,3*], Hua Dong[1,3] and Zhao Li[1,3]

Abstract

With the rapid improvement of quantum computing technology, quantum key distribution(QKD) is a hot technology. Information reconciliation is a key step of QKD which is useful for correcting key error. Classical message interaction is necessary in a practical information reconciliation scheme, which makes the efficiency of these protocols decreased. Therefore, some one-way information reconciliation schemes based on low-density parity-check(LDPC) codes and polar codes are proposed. Here we propose a concatenated method of IR schemes which can achieve any given error rate level without the need of interactions. Compared with the one-way IR schems based on LDPC codes and polar codes, the IR schemes based on the proposed concatenated method can get lower bit error rates after error correction, which can also reduce the communication delay and system complexity of QKD, improve the final key generation rate and enhance the practicability of QKD system.

Keywords: Quantum key distribution, Information reconciliation, Concatenated scheme, One-way communication

Introduction

Key distribution protocols are used to enable both communication parties to share a secure key. Generally speaking, the unconditionally secure key distribution protocols (Maurer 1991; Blundo et al. 1992) can be divided into three phases: advantage distillation (Maurer 1993), information reconciliation (IR) (Cachin and Maurer 1997) and privacy amplification (Bennett et al. 1988; Maurer and Wolf 1997; Liu and van Tilborg 2002). In 1984, Bennett and Brassard proposed the first quantum key distribution (QKD) protocol BB84 (Bennett and Brassard 1984), which is an unconditionally secure key distribution protocols. The QKD has three phases: quantum signal transmission, raw key distillation(or advantage distillation), and classical data post-processing. Data post-processing technology is one of the core technologies of QKD, which mainly includes information reconciliation, privacy amplification and other steps. In QKD protocol, the raw key distributed through the quantum physical channel needs "data post-processing" to finally become the unconditionally secure key. Among them, information reconciliation is used to correct key error caused by system noise or eavesdropper, and is one of the key technologies in QKD.

Bennett and Brassard proposed the first information coordination protocol BBBSS in 1992 (Bennett et al. 1992). In this protocol, Alice and Bob divide their key strings into several sub-strings, and exchange parity information of sub-strings. The binary search method is used to find and correct the error bits, which is simple and easy to operate, but needs frequent interactive communication. In 1993, Brassard and Salvail (1993) proposed an IR protocol called Cascade, which can correct two errors in a block. Though its error correction ability is stronger than BBBSS, its computation and communication complexity are bigger. In 1999, Biham et al. (2006) proposed an IR scheme based on syndrome error correction. After that, Mayers (2001) proposed an IR scheme based on error correcting code(ECC). Yang et al. (2002) suggested a key redistribution scheme for IR. These three IR protocols are non-interactive ones. In 2003, Buttler et al. (2003) proposed a IR scheme called Winnow. The number of the error correction rounds of Winnow is fewer than Binary and Cascade, but the error correction ability is limited. Several modifications and optimizations to the above protocol had been proposed (Gong et al. 2009a; 2009b; Yan et al. 2008; Zhao et al. 2007; Cui et al. 2013; Tomamichel et al.

*Correspondence: yangli@iie.ac.cn
A preliminary version of this paper appeared in arXiv:1201.1196, 2012.
[1]State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[2]State Key Laboratory of Cryptology, P.O.Box 5159, Beijing 100878, China
[3]School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China

2017). In the process of implementation, Cascade-based protocol requires multiple interactions between the two sides of communication, and the communication overheads will limit the key rate. Winnow-based (Yamamura and Ishizuka 2001) protocol corrects errors by exchanging syndrome information, but it still needs a certain number of interactions.

Then, coding-based IR protocols become the trend of research. Several IR protocols based on coding were proposed (Zhao et al. 2008; Martinez-Mateo et al. 2010; Kiktenko et al. 2017; Li et al. 2019), such as BCH-based protoocls, LDPC-based protocols and polar-based protocols. Traisilanun et al. applied BCH code to IR (Traisilanun et al. 2007), which further reduced the number of reconciliation interactions, but still could not achieve the same efficiency as Cascade. Afterwards, LDPC code and polar code are applied to IR with one-way communication. In 2004, Pearson first proposed the LDPC-based error reconciliation algorithm on PC (Pearson 2004). In view of the low processing rate of error code reconciliation algorithm implemented by software on PC, then IR protocols are realized by hardware based on LDPC. In 2009, Elkouss proposed one QKD post-processing scheme using LDPC codes to achieve better error correction performance (Elkouss et al. 2009). However, since LDPC code is very sensitive to bit error rate of quantum channel, it has better performance in a narrow range with a bit error rate as the center, so the bit error rate of quantum channel has a wide range in practical applications (Elkouss et al. 2011). The required checksum matrix requires high storage resources, and iterative decoding also leads to high decoding complexity (Jouguet et al. 2014). In 2012, polar codes are used to transmit quantum information and an efficient decoder is provided for QKD channels (Renes et al. 2012). In the same year, Jouguet first used polar code for error code correction in QKD post-processing (Jouguet and Kunzjacques 2014). Significant performance improvements were achieved. Both the processing rate and the reconciliation efficiency are higher than IR protocols based on LDPC. In 2014, Nakassis et al. continued to study the application of polar code in IR (Nakassis and Mink 2014). In 2015, A delayed error correction reconciliation protocol was proposed using polar codes, where the results show that the performance of the proposed protocol was better than those using LDPC. And the corrected bit error rate based on polar code is always smaller than those based on LDPC code, and the lowest error rate was about 1×10^{-6} when the initial error rate is 0.02 (Xiao et al. 2015). In 2019, (Li et al. 2019) proposes a one-step post-processing algorithm based on polar codes. When the initial error correction code is lower than 0.08, the corrected bit error rate can reach 1×10^{-7}. As the increase of bit error rate of quantum bits is greater than 0.08, it cannot meet the same reliability.

The above protocols based on the BBBSS, Cascade, and Winnow are all multi-rounds interactive protocols. They adopt interactive communication to achieve an acceptable error rate level. However, the interactive communication causes extra time consuming and the communication overhead of multiple interactions limits the key rate. On the other hand, many non-interactive IR protocols, such as those early presented in (Biham et al. 2006; Mayers 2001; Yang et al. 2002), cannot achieve the practically acceptable low error rate. Additionally, there are some limitations about LDPC-based and plar-based non-interactive IR schemes. The LDPC-based schemes need to anticipate the bit error rate and construct better coding algorithms which are not at the cost of coding delays. In addition, the corrected bit error rate of LDPC-based and polar-based schemes is around 1×10^{-7}, when the initial bit error rate is lower than 0.08. In this paper, our goal is to achieve a lower error rate after correcting erros while meet the requirement of one-way communication.

Our contributions. In order to achieve a more reliable error rate after error correction without increasing complexity caused by frequent interactions, we propose a concatenated method of IR schemes which requires only one time one-way communication to achieve any given error rate level. The details are as follows.

- We rigorously demonstrate the selection criteria of the error correcting code and error correcting rounds when executing concatenated IR schemes under the premise of the given error rate. Based on the initial channel error rate, we can choose the appropriate concatenating depth and error correction code to achieve the ultimate actual communication acceptance error rate.
- Based on the proposed concatenated method, we present the reconstruction of three QKD post-processing schemes. In particular, we improve the key redistribution scheme based on the concatenated method of IR scheme. The improved scheme can realize authentication, privacy amplification and IR simultaneously. Additionally, we also utilize the concatenated method to reconstruct and improve the other two original schemes - Biham's scheme and Mayer's scheme. According to the demonstrated criteria, we can choose the appropriate error correction code and concatenated depth of the reconstructed schemes so that they can achieve any given error rate level.

The IR schemes based on the proposed concatenated method have the following advantages:

1. Since the IR schemes designed based on this method are non-interactive and achieve the more reliable error rate level, they may reduce the post-processing

delay and system complexity of QKD, and improve the final key generation rate and enhance the practicability of QKD system.
2. The proposed concatenated method of IR schemes can achieve a more reliable error rate after error correction in practical QKD channel. Currently, the initial bit error rate of QKD system on the optical fiber with a communication distance of 120 km is usually less than 0.1 (Takemoto et al. 2015). After correcting errors, the corrected bit error rates of the reconstructed schemes all are below 1×10^{-9} while satisfy the practical initial error rate threshold [0,0.1]. On the premise of that the initial error rate is below 0.08, the final error rate of LDPC-based and polar-based schemes is below 1×10^{-7},while the final error rate of our schemes is 1×10^{-9}. Additionally, when the initial error rate is higher than 0.08, the final error rate of LDPC-based and polar-based schemes cannot achieve the level below 1×10^{-7}, while the final error rate of our schemes is still below 1×10^{-9}.

Our organizations. The techniques used in the construction of concatenated IR schemes are introduced in "Preliminaries" section. Some selection criteria of the error correction code in the concatenated method under a certain error rate of the channel is given in "Some selection criteria of concatenated IR schemes" section. The reconstructions of three QKD post-processing schemes based on the concatenated IR method are given in "The construction of concatenated IR schemes" section. Some discussions and the conclusion are given in "Discussions" and "Conclusion" sections, respectively.

Preliminaries

In this section, we review some basic concepts that are necessary for understanding the proposed construction of one-way IR schemes based on the concatenating procedure, including non-interactive IR schemes, wire link permutation, cyclic redundancy code(CRC)-based message authentication code(MAC) and hamming code.

Non-interactive IR schemes

To prevent additional time consumption and communication overheads in interactive communications, we present the one-way IR schemes. There are three kinds of non-interactive IR schemes. The first one is the syndrome IR scheme (Biham et al. 2006). In this scheme, Alice sends syndromes to do error correction. Bob uses the equation $s_A \oplus s_B = H(K_A \oplus K_B)$ to correct his raw key K_B to Alice's raw key K_A. The second one is the IR scheme of Mayers (2001). In this scheme, Alice encodes a local random string x to get the codeword c, and uses her raw key K_A to do one time pad with it to get $c \oplus K_A$. Then she sends it to Bob. Bob adds his raw key K_B to it to get the $(c \oplus K_A) \oplus K_B = c \oplus e$, and decodes it to get the codeword c. Then he adds it to the receiving $c \oplus K_A$ to get K_A. The third one is the key redistribution scheme (Yang et al. 2002). The basic idea of this scheme is: Alice first encodes a local random bit string with an error correcting code, then she uses her raw key to do one time pad with the codeword and transmits it to Bob. Bob adds his raw key to the received bit string and decodes the error correcting code to get Alice's local random bit string, then takes it as the secret key between them. The whole protocol can be summarized as follows.

1. Alice generates a random bit string x.
2. Alice uses a generator matrix g to encode x and gets the code word c, where g is a globe public parameter.
3. Alice uses the raw key K_a to do bitwise XOR operation with the code string c to get $K_a \oplus c$. Then she transmits it to Bob.
4. Bob does the same operation to the received string with K_b and gets $(c \oplus K_a) \oplus K_b = c \oplus e$. He uses checking matrix h and $c \oplus e$ to calculate the syndrome s. Using s, he gets the error vector e and the codeword c. Then he gets the random bit string x by decoding c, and takes it as the secret key between them.

If the generator matrix is kept secret, the key redistribution protocol may generate a secure final key. It can also realize group oriented key distribution, personal identification, and message authentication for non-broadcast channel via key-controlled error-correcting code. Thus the key redistribution protocol may realize the IR and the privacy amplification in one step.

Wire link permutation

In an IR protocol, it is necessary to do a random bit-permutation between any two successive error correction rounds. The permutation used in an IR protocol should be as uniform as possible, that means the bits in a block should be dispersed uniformly into different blocks after a permutation. Wire link permutation(WLP) is also called bit-permutation (Shi and Lee 2000). This digital circuit technology is simple and fast without the help of gate circuits, which is applied to the proposed concatenated schemes. There are many different WLPs. A proper WLP is shown in Fig. 1.

After the permutation, W the first bit of the first block $(a_{11}, a_{12}, \ldots, a_{1n})$ is put in the first position in the new round; The first bit of the second block $(a_{21}, a_{22}, \ldots, a_{2n})$ is put in the second position in the new round, etc.; Go on like this until the last block $(a_{m1}, a_{m2}, \ldots, a_{mn})$: the first bit a_{m1} is put in the m^{th} position in the new round, etc..

The WLP should be done between each pair of successive error correction rounds. The i^{th} permutation W^i is as follows,

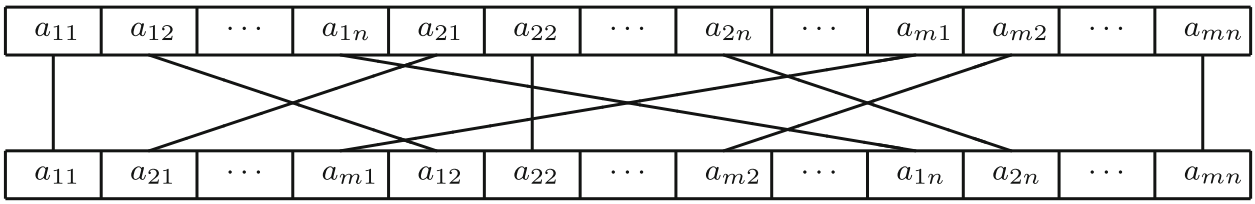

Fig. 1 The wire link permutation W applied in the proposed concatenated schemes

$$\begin{array}{l}(a_{11}^{(i)}, a_{12}^{(i)}, \cdots, a_{1n}^{(i)}, a_{21}^{(i)}, a_{22}^{(i)}, \cdots, a_{2n}^{(i)}, \cdots\cdots, a_{m1}^{(i)}, a_{m2}^{(i)}, \cdots, a_{mn}^{(i)}) \\ \xrightarrow{W^{(i)}} (a_{11}^{(i)}, a_{21}^{(i)}, \cdots, a_{m1}^{(i)}, a_{12}^{(i)}, a_{22}^{(i)}, \cdots, a_{m2}^{(i)}, \cdots\cdots, a_{1n}^{(i)}, a_{2n}^{(i)}, \cdots, a_{mn}^{(i)}).\end{array} \tag{1}$$

We can rearrange the data string $\left(a_{11}^{(i)}, a_{12}^{(i)}, \cdots, a_{1n}^{(i)}, a_{21}^{(i)}, a_{22}^{(i)}, \cdots, a_{2n}^{(i)}, \cdots\cdots, a_{m1}^{(i)}, a_{m2}^{(i)}, \cdots, a_{mn}^{(i)}\right)$ into a matrix as

$$A^{(i)} \triangleq \begin{bmatrix} a_{11}^{(i)} & a_{12}^{(i)} & \cdots & a_{1n}^{(i)} \\ a_{21}^{(i)} & a_{22}^{(i)} & \cdots & a_{2n}^{(i)} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ a_{m1}^{(i)} & a_{m2}^{(i)} & \cdots & a_{mn}^{(i)} \end{bmatrix}. \tag{2}$$

It can be seen that every row is a codeword before the permutation, and every column is a codeword after the permutation. Since the $W^{(i)}$ changes the rows to the columns, it is just a transpose operation of the matrix $A^{(i)}$. Thus, $W^{(1)} = \cdots = W^{(i)} = \cdots \triangleq W$, and $W^{-1} = W$.

Cyclic redundancy code(CRC)-based message authentication code(MAC)

CRC-based MAC (Krawczyk 1994a, b) designed for stream ciphers is a scheme with information-theoretic security based on CRC. LFSR can be used to realize rapid polynomial division in a CRC authentication scheme. This kind of authentication schemes can authenticate large amount of messages by consuming a few bits of the key. It is used to authenticate the classical channel of QKD in the proposed schemes. The CRC based the authentication scheme is as follows.

Denote the n bits message to be authenticated as M. Make $M = M_{n-1} \ldots M_1 M_0$ and the polynomial $M(x) = \sum_{i=0}^{n-1} M_i x^i$ associated. Denote the CRC hash function as h, and the MAC value as *aut*. The output of h is an m bit string.

1. Alice and Bob secretly preshare a binary irreducible polynomial $p(x)$ of degree m, and a m-bit random string K as their one time pad key.
2. Alice calculates $h(M) = coef\,(M(x) \cdot x^m \ mod\ p(x))$.
3. Alice gets the m-bit *aut* of M by calculating $h(M) \oplus K$.
4. Alice sends *aut* and M to Bob
5. Bob uses the received M' to calculate a aut'', and checks whether it is equal to the aut' he received.

The successful attack probability is $\frac{n+m}{2^{m-1}}$(Krawczyk 1994b) for any n and $m > 1$.

Hamming code

Hamming code is a linear debugging code in the field of telecommunications, which inserts validation codes into the transmitted message stream. When the data bit error occurs, the validation bit detects and corrects a single bit error. $[n, n-k, 3]$Hamming code over F_2 with $n = 2^k - 1$ has a special structure (Hamming 1950) and is a fast error correction algorithm. Considering of the fast decoding algorithm of Hamming code, we choose it as the error-correcting code to be concatenated in our concatenated IR scheme.

For a code word of $[n, n-k, 3]$Hamming code, let a serial number from 1 to n denote the position of each bit. The codes include the validation bitsand the information bits. The validation bits are inserted into $2^l th (0 \le l < k)$ positions. The information bits take up the left positions. Its generating matrix is obtained by exchanging the $2^l th$ column with the corresponding systematic code's $(n-l)th$ column, respectively. The decoding method is multiplying the receiving bit-string with the parity check matrix to get the syndrome $s = (s_1, \ldots, s_k)$, then the binary number $(s_1 \ldots s_k)_2$ indicates just the position of an error bit in the code word.

Some selection criteria of concatenated IR schemes

In order to solve the problem of high communication delay and system complexity caused by frequent interactions while to achieve actual acceptable error key rate, it is necessary to choose the selection criteria of the error correcting rounds and error correcting code under the premise of the given error rate required for actual communication. In this section, we rigorously demonstrate some selection criteria for choosing the number of round and the error correcting code under a given error rate of the channel.

Definition 1 (Lint 1999) *Let C denote a linear code of length n and let A_i denote the number of codewords of weight i, then the weight enumerator of C is*

$$A(z, n) := \sum_{i=0}^{n} A_i z^i. \tag{3}$$

The sequence $(A_i)_{i=0}^n$ *is called the weight distribution of C. If C is linear and* $\vec{c} \in C$*, then the number of codewords at distance i from* $\vec{c}$ *equals* A_i*.*

For binary Hamming code of length n, the weight enumerator is

$$A(z,n) = \sum_{i=0}^{n} A_i z^i = \frac{1}{n+1}(1+z)^n + \frac{n}{n+1}(1+z)^{\frac{n-1}{2}}(1-z)^{\frac{n+1}{2}}. \tag{4}$$

From Eq. (4), compare the polynomial coefficients of the two sides of Eq. (4), we get that $A_1 = A_2 = A_{n-2} = A_{n-1} = 0$, and all other coefficients are non-zero integers. For example, for the code $[7,4,3]$, $n = 7$, we get $A(z,7) = 1 + 7z^3 + 7z^4 + z^7$. For the code $[15,11,3]$, $n = 15$, we get $A(z,15) = 1 + 35z^3 + 105z^4 + 168z^5 + 280z^6 + 435z^7 + z^{15} + 35z^{12} + 105z^{11} + 168z^{10} + 280z^{19} + 435z^8$.

According to Eq. (4), we calculate the weight distribution $(A_i)_{i=0}^n$ of Hamming code of length n.

$$\begin{aligned}
A(z,n) &= \frac{1}{n+1}(1+z)^n + \frac{n}{n+1}(1+z)^{\frac{n-1}{2}}(1-z)^{\frac{n+1}{2}} \\
&= \frac{1}{n+1}\sum_{k=0}^{n} C_n^k z^k + \frac{n}{n+1}(1-z)\sum_{i=0}^{\frac{n-1}{2}} C_{\frac{n-1}{2}}^i (-1)^i z^{2i} \\
&= \frac{1}{n+1}\sum_{k=0}^{n} C_n^k z^k + \frac{n}{n+1}\sum_{i=0}^{\frac{n-1}{2}}\left[(-1)^i C_{\frac{n-1}{2}}^i z^{2i}\right. \\
&\quad \left. +(-1)^{i+1} C_{\frac{n-1}{2}}^i z^{2i+1}\right] \\
&= \frac{1}{n+1}\sum_{k=0}^{n} C_n^k z^k + \frac{n}{n+1}\sum_{k=0}^{n}(-1)^{\lceil\frac{k}{2}\rceil} C_{\frac{n-1}{2}}^{\lfloor\frac{k}{2}\rfloor} z^k \\
&= \sum_{k=0}^{n}\left(\frac{1}{n+1}C_n^k + \frac{n}{n+1}(-1)^{\lceil\frac{k}{2}\rceil} C_{\frac{n-1}{2}}^{\lfloor\frac{k}{2}\rfloor}\right) z^k
\end{aligned} \tag{5}$$

Comparing the coefficients with $A(z,n) = \sum_{k=0}^{n} A_k z^k$, we get

$$A_k = \frac{1}{n+1}C_n^k + \frac{n}{n+1}(-1)^{\lceil\frac{k}{2}\rceil} C_{\frac{n-1}{2}}^{\lfloor\frac{k}{2}\rfloor}.$$

Definition 2 (Lint 1999) *Let* $C \subseteq Q^n$ *denote a code with M words. We define*

$$A_i := M^{-1}|\{(\vec{x},\vec{y})|\vec{x} \in C, \vec{y} \in C, d(\vec{x},\vec{y}) = i\}|. \tag{6}$$

The sequence $(A_i)_{i=0}^n$ *is the distance distribution or inner distribution of C.*

If C is linear, the distance distribution is weight distribution. Thus, for Hamming code, the weight distance and the distance distribution are the same. With the weight distribution of Hamming code calculated in Eq. (3), we get that its distance distribution is $(A_k)_{k=0}^n$, here $A_k = \frac{1}{n+1}C_n^k + \frac{n}{n+1}(-1)^{\lceil\frac{k}{2}\rceil} C_{\frac{n-1}{2}}^{\lfloor\frac{k}{2}\rfloor}, k = 0,1,\cdots,n$. This means, for any Hamming code $\vec{c}$ of length n, the number of the codewords at distance i from $\vec{c}$ is $A_i, i = 0,1,\cdots,n$.

Assuming that a Hamming code with a length of n is used and that the bit error probability is $p(p \in [0,100\%])$, then the expected number of errors per block before decoding is np.

Remark 1 *We regard the bit error in the channel as a single event. Because the adversary can artificially eavesdrop to change the error rate in the channel. He can not get a stable channel. And in each transmission channel the bit error rate may change. Under this premise, the probability p of bit error rate belongs to [0,100%]. The specific example is as follows: when hamming code is used to correct error, for the check bit of 7 bits, the correct case is that all 7 bits are 0, while the 7 bits that are actually transmitted through the channel are all 1. We consider the error rate in this case to be 100%.*

(1) If one error occurs, the number of errors corrected is 0.
(2) If k, $(2 \le k \le n-1)$ errors occur, there are two cases when error correction is performed:

- The k errors turn one code word into another codeword. In this situation, we cannot use error-correcting code to correct any bit of errors. There are still k errors after error correction. For any Hamming codeword $\vec{c}$ of length n, the number of the code words at distance k from $\vec{c}$ is A_k. Thus, the probability of this case is $A_k p^k (1-p)^{n-k}$. Namely, there are still k errors after correcting the error, and the probability is $A_k p^k (1-p)^{n-k}$.
- The k errors do not turn the code into another code. In this case, the error correction can only correct one error to reduce the number of errors to $k-1$. However, it may also lead to a new error that increases the number of errors to $k+1$. Namely, we obtain a new code word at distance $k-1$ from the code word $\vec{c}$ or a new code word at distance $k+1$ from code word $\vec{c}$. For any codeword $\vec{c}$, the number of codewords with a distance of $k-1$ from $\vec{c}$ is A_{k-1} and the number of codewords with a distance of $k+1$ from $\vec{c}$ is A_{k+1}. So, after correcting the errors, we can get one of $A_{k-1} + A_{k+1}$ codewords. It is assumed that each codeword has the same probability in error correction. After correcting the errors, the probability of reducing the number of errors to $k-1$ is $\frac{A_{k-1}}{A_{k-1}+A_{k+1}}$, and the probability of increasing the number of errors to $k+1$ is $\frac{A_{k+1}}{A_{k-1}+A_{k+1}}$. The probability that the k error does not convert the codeword $\vec{c}$ to another codeword is $\left(C_n^k - A_k\right) p^k (1-p)^{n-k}$, since A_k is the number of the codewords at distance k from $\vec{c}$.

Therefore, the probability that k errors cannot turn a codeword to another codeword and the number of errors is reduced to $k-1$ is $\left(C_n^k - A_k\right)\frac{A_{k-1}}{A_{k-1}+A_{k+1}}p^k(1-p)^{n-k}$. The probability that k errors cannot turn a codeword to another codeword and the number of errors is increased to $k-1$ is $\left(C_n^k - A_k\right)\frac{A_{k+1}}{A_{k-1}+A_{k+1}}p^k(1-p)^{n-k}$.

(3) If n errors occur, 1 is the number of the codewords at distance n with $\vec{c}$, namely $A_n = 1$. The length of the codeword is n, so if all the n bits are wrong, then the case is only $C_n^n = 1$. Thus n errors can only turn a codeword to another codeword. Namely, there are still n errors after correcting the error. And the probability is p^n.

Let the bit error probability denote p_1 after correcting errors. Therefore, after error correction, the mathematical expectation of the error in each block is

$$\begin{aligned} np_1 &= \sum_{k=2}^{n-1}\Bigg[kA_kp^k(1-p)^{n-k} + (k-1)\left(C_n^k - A_k\right) \\ &\quad \frac{A_{k-1}}{A_{k-1}+A_{k+1}}p^k(1-p)^{n-k} + (k+1)\left(C_n^k - A_k\right) \\ &\quad \frac{A_{k+1}}{A_{k-1}+A_{k+1}}p^k(1-p)^{n-k}\Bigg] + np^n \\ &= \sum_{k=2}^{n-1}\left[kA_k + \left(C_n^k - A_k\right)\frac{(k-1)A_{k-1}+(k+1)A_{k+1}}{A_{k-1}+A_{k+1}}\right] \\ &\quad p^k(1-p)^{n-k} + nA_np^n \\ &= \sum_{k=0}^{n}\left[kA_k + \left(C_n^k - A_k\right)\left(k + \frac{A_{k+1}-A_{k-1}}{A_{k-1}+A_{k+1}}\right)\right] \\ &\quad p^k(1-p)^{n-k}. \end{aligned} \tag{7}$$

Here, denote $A_{-1} = 0, A_{n+1} = 0$. When $A_{k+1} = A_{k-1} = 0$, denote $\frac{A_{k+1}-A_{k-1}}{A_{k-1}+A_{k+1}} = 0$.

From the above equation, we can get

$$np_1 = \sum_{k=0}^{n}\left[\left(C_n^k - A_k\right)\frac{A_{k+1}-A_{k-1}}{A_{k-1}+A_{k+1}} + kC_n^k\right]p^k(1-p)^{n-k} \tag{8}$$

$$= \sum_{k=0}^{n}\left(C_n^k - A_k\right)\frac{A_{k+1}-A_{k-1}}{A_{k-1}+A_{k+1}}p^k(1-p)^{n-k} + np. \tag{9}$$

Thus, $p_1 < p$ equals the following equation

$$\sum_{k=0}^{n}\left(C_n^k - A_k\right)\frac{A_{k+1}-A_{k-1}}{A_{k-1}+A_{k+1}}p^k(1-p)^{n-k} < 0. \tag{10}$$

We present the derivation of Eq. (10) in Appendix A.

For the Hamming code of length $n = 7$, we have

$$7p_1 = 63p^2 - 182p^3 + 210p^4 - 84p^5. \tag{11}$$

We can simplify Eq. (11) to get the following:

$$p_1 = 9p^2 - 26p^3 + 30p^4 - 12p^5. \tag{12}$$

From $p_1 < p$, we get

$$0 < p < \frac{1}{6}(3-\sqrt{3}), \text{or } \frac{1}{2} < p < \frac{1}{6}(3+\sqrt{3}). \tag{13}$$

This means we can use error-correcting code to reduce the error rate if and only if the bit error probability p satisfies $0 < p < \frac{1}{6}(3-\sqrt{3})$ or $\frac{1}{2} < p < \frac{1}{6}(3+\sqrt{3})$.

The Fig. 2 shows that the error rate after error-correction p_1 varies with the inial error rate p when $n = 7$. According to Fig. 2, there are five points of intersection between the curve and X-axis. They are $0, \frac{1}{6}(3-\sqrt{3}), \frac{1}{2}, \frac{1}{6}(3+\sqrt{3}), 1$. If the p is in the interval

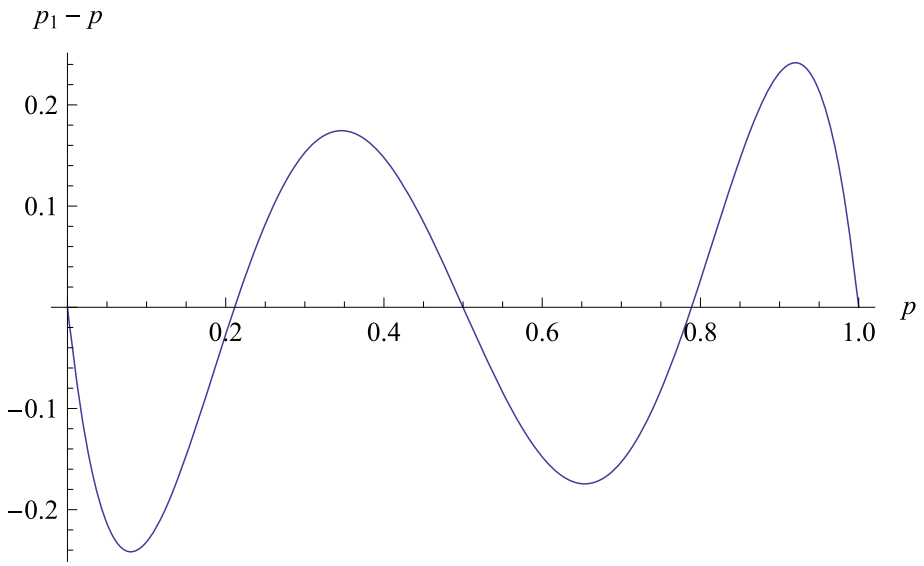

Fig. 2 The error rate after error-correction p_1 varies with the inial error rate p when $n = 7$

$\left[\frac{1}{6}(3-\sqrt{3}),\frac{1}{2}\right],\left[\frac{1}{6}(3+\sqrt{3}),1\right]$, $p_1 > p$ after error correction. In this situation we cannot correct the errors. In practical QKD protocol, the channel's initial bit error rate threshold is $[0,0.1]$. The interval of p where we can use this code is $[0,\frac{1}{6}(3-\sqrt{3})]$.

The error rate after error-correction p_1 varying with the inial error rate p when $n = 15$ is as Fig. 3.The analysis of available intervals where we can use this code is the same as above.

Comparing Fig. 3 with Fig. 2, the effective interval of Hamming code $[15,11,3]$ is less than that of Hamming code $[7,4,3]$. Under the premise that the initial bit error rate threshold of the practical QKD channel is $[0,0.1]$, both of them satisfy the actual situation. So, we can select the appropriate error correction code.

Lemma 1 *Let C denote the $[n,n-k,3]$ Hamming code over F_2, where $n=2^k-1$. Suppose the upper bound of the average number of errors within per block after one error correction round with C is χ, then*

$$\chi = 1 + np - 2p^n - (1-p+2np)(1-p)^{n-1}, \quad (14)$$

where p is the bit error rate of the channel.

This lemma is proved in Appendix B in detail.

Lemma 2 (See the proof of lemma 2 in Appendix C.)

$$\chi < n(n-1)p^2\left[1+\frac{1}{2}(1-p)^{n-2}\right]. \quad (15)$$

Theorem 1 (See the proof of Theorem 1 in Appendix D.) *When C is used as the error correcting code, if bit error rate p satisfies the condition $p < \frac{1}{(n-1)[1+\frac{1}{2}(1-p)^{n-2}]}$, then the concatenated error correction scheme can achieve any given error rate level.*

Corollary 1 (See the proof of Corollary 1 in Appendix E.) *If bit error rate $p < p_{th} = \frac{2}{3(n-1)}$, the concatenated error correction scheme can reduce the error rate to any given level.*

Tables 1 and 2 show the concatenating results based on Eq. (10), which are useful for choosing the proper error correcting code and the concatenating depth l. Parameter η is the information rate of the concatenated IR algorithm. α is the final error rate of the concatenated IR algorithm. It is required that after l rounds error correction the final error rate α should be below 1×10^{-9}. According to this criterion, the required error correction round l and the final left bit rate are determined. The results based on Hamming code $[15,11,3]$ and $[7,4,3]$ are given in Tables 1 and 2, respectively.

Through the above series of demonstrations, based on the channel error rate p, we can choose the appropriate concatenating depth l and error correction code to achieve the ultimate actual communication acceptance error rate α. Specifically, according to the initial bit error rate of the pactical channel([0,0.1]), the final bit error rate is reduced to 1×10^{-9} after l round error correction.

The construction of concatenated IR schemes

In "Introduction" section, we have discussed that the necessary interactive communication makes the efficiency of these protocols decreased. The original schemes of Biham et al. (2006), Mayers (2001) and key redistribution (Yang et al. 2002) employ only one-round error correction,

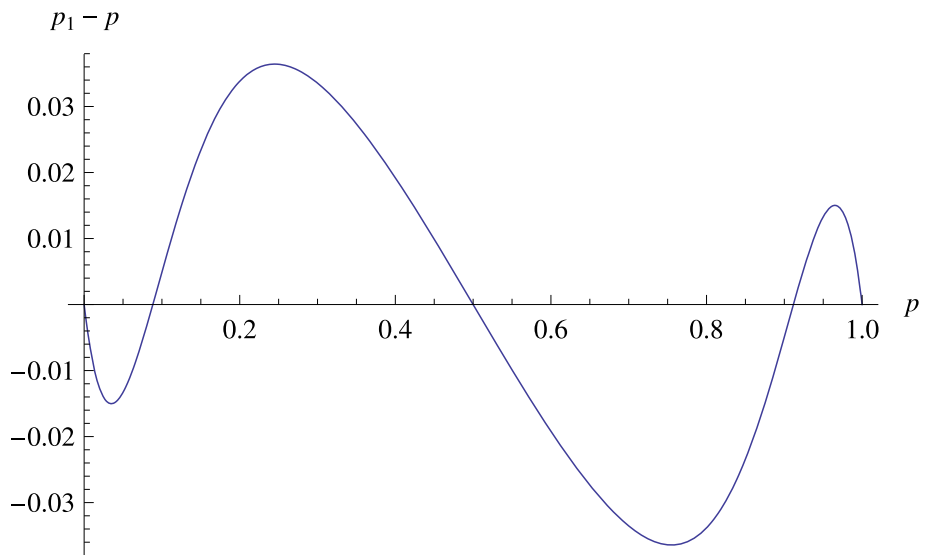

Fig. 3 The error rate after error-correction p_1 varies with the inial error rate p when $n = 15$

Table 1 Concatenated IR based on [15, 11, 3] code

p	0.01	0.02	0.04	0.05	0.06	0.07	0.08
l	4	5	6	7	8	9	11
η	0.289	0.212	0.156	0.114	0.084	0.061	0.024
α	3.58×10^{-13}	2.59×10^{-15}	1.77×10^{-12}	2.72×10^{-14}	8.86×10^{-15}	2.35×10^{-11}	2.04×10^{-11}

p represents the channel error rate. l represents the needed error correction rounds. α represents the final error rate. η represents the left bit rate

which cannot reduce the error rate to an acceptable level in practical system. In order to realize both one time one-way communication and an acceptable error rate level simultaneously, we present the specific reconstructions of three QKD post-processing schemes (Biham et al. 2006; Mayers 2001; Yang et al. 2002), which requires only one time one-way communication. Based on the selection criteria given in "Some selection criteria of concatenated IR schemes" section, we can choose the appropriate choices of error correction code and concatenated depth of the reconstruction schemes, so that they can achieve a more reliable error rate required by the actual QKD communication.

I. The reconstruction of Biham's syndrome error correction protocol

Firstly we consider the reconstruction of Biham's syndrome error correction protocol. The protocol is as follows.

1. Alice divides the raw key string into 15-bit length blocks and then performs the permutation W on it. Alice calculates the syndromes $s_{Ai}^{(j)}$, and discards the check bits of each block, here i is the serial number of the block, and j is the serial number of the round. Alice repeats above operations from $j=1$ to $j=l$, to get the syndromes $s_{Ai}^{(1)},\ldots,s_{Ai}^{(l)}, i=1,\cdots,n$, where l is the predetermined number of the correction rounds. The Alice's final bit-string is the common random string to be privacy amplified.
2. Alice takes the syndromes $s_{Ai}^{(1)}, s_{Ai}^{(2)},\ldots,s_{Ai}^{(l)}$ $(i=1,\cdots,n)$ as her message to be sent. She uses CRC authentication algorithm to calculate the MAC of the message and sends the MAC and the message to Bob.
3. After receiving the sequence $s_{Ai}^{(1)}, s_{Ai}^{(2)},\ldots,s_{Ai}^{(l)}$, Bob uses the CRC authentication algorithm and the one time pad key K to check whether the message comes from Alice and has not been changed. If the authentication is passed, Bob uses the wire link permutation W to transform his raw key and calculates the syndrome $s_{Bi}^{(1)}$ of every block. Then he calculates the i^{th} syndrome $s_i^{(1)}=s_{Ai}^{(1)}\oplus s_{Bi}^{(1)}$, and does error correction to the i^{th} block, $i=1,\cdots,n$. After the error correction of the first round he discards all the check bits. Bob repeats above operation to get the syndromes $s_i^{(j)}, i=1,\cdots,n$ and performs error correction from $j=1$ to $j=l$. Finally he gets Alice's key after l rounds error correction.

Analysis result. Currently a typical error rate for a QKD IR protocol to deal with is less than 10%. Suppose the initial error rate is 3%. According to the criteria in "Some selection criteria of concatenated IR schemes" section, we get the upper bound of the final error rate and the final bit rate after each error correction round, as shown in Table 3. According to Theorem 1, we can choose [15, 11, 3] Hamming code as the basic code, whose error correction ability is 6.7%. The concatenating depth l in the protocol is determined by a given final error rate. Table 3 shows that when the concatenating depth l is 5, we can get an error rate under 1.0×10^{-9} with a left bit rate 0.212.

II. The reconstruction of key redistribution protocol

The original key redistribution protocol is also used [15, 11, 3] Hamming code to executing error correction. The specific reconstruction is as follows.

1. Alice randomly generates a string $r_A^{(1)}$, which is divided into blocks in length 11, $r_A^{(1)}=\left(r_1^{(1)},\cdots,r_{n_1}^{(1)}\right)$. The [15, 11, 3] Hamming code is also used to encode each block. Then Alice obtains $c^{(1)}=\left(c_1^{(1)},\cdots,c_{n_1}^{(1)}\right)$, and rearranges $c^{(1)}$ with WLP W. It is divided into blocks in length 11 again, $r_A^{(2)}=\left(r_1^{(2)},\cdots,r_{n_2}^{(2)}\right)$. After repeated l-round operations, she obtains the codeword string

Table 2 Concatenated IR based on [7, 4, 3] code

p	0.05	0.07	0.09	0.10	0.12	0.13	0.14
l	5	5	6	6	7	7	8
η	0.061	0.061	0.035	0.035	0.020	0.011	0.011
α	5.22×10^{-14}	5.93×10^{-10}	1.20×10^{-12}	1.74×10^{-10}	1.66×10^{-12}	6.96×10^{-10}	1.04×10^{-13}

p represents the channel error rate. l represents the needed error correction rounds. α represents the final error rate. η represents the left bit rate

Table 3 The upper bound of error rate based on Lemma 1 and the left bit rate after each error correction round

Round	1	2	3	4	5	6
Error Rate	1.53×10^{-2}	4.40×10^{-3}	3.93×10^{-4}	3.23×10^{-6}	2.20×10^{-10}	5.92×10^{-17}
Left Rate	0.733	0.538	0.394	0.289	0.212	0.156

Suppose channel error rate is 3%. The chosen code is Hamming code [15, 11, 3]. The data in this table are the upper bound of error rate and left bit rate after i rounds error correction, $1 \le i \le 6$.

$c^{(l)} = \left(c_1^{(l)}, \cdots, c_{n_l}^{(l)}\right)$. In the last round, there is no need to execut permutation. The above process can be written as $C_l\Big[P_{l-1}\Big[C_{l-1}\cdots\Big[C_2\Big[P_1\Big[C_1\left(r_A^{(1)}\right)\Big]\Big]\Big]\cdots\Big]\Big] = c^{(l)}$, where P_i is the i^{th} round wire link permutation W, C_i is the i^{th} round encoding with [15, 11, 3] code.

2. Alice uses her raw key K_A to execute XOR operation bit by bit on the codeword string to get $K_A \oplus c^{(l)}$. She computes the corresponding MAC based on the CRC authentication algorithm. Then Alice transmits the string and the corresponding MAC to Bob.
3. Bob verifies whether the string has been tempered with based on the CRC authentication algorithm. If the authentication is successful, Bob uses his raw key K_B to execute XOR operation bit by bit on the received codeword string to obtain $\left(K_A \oplus c^{(l)}\right) \oplus K_B = c^{(l)} \oplus e$. Bob can decode it with the inverse WLP $W^{-1} = W$. After repeated operations round by round, Bob obtains $r_B^{(1)}$.

Analysis result. Similarly, supposing that the initial error rate is 3%. According to the criteria in "Some selection criteria of concatenated IR schemes" section, we get the upper bound of the final error rate and the final bit rate after each error correction round, as shown in Table 3. It shows that the concatenating depth l is also 5 according to Table 3. It can also achieve that the final error rate is under 1.0×10^{-9}. Additionally, the improved key redistribution scheme based on the concatenated method of IR scheme can realize authentication, privacy amplification and IR simultaneously.

III. The reconstruction of Mayer's ECC-based IR protocol

Mayer's ECC-based IR protocol is similar to the reconstruction of key redistribution protocol. The first three steps of reconstruction of Mayer's ECC-based IR protocol and that protocol are the same. Additionally it needs to be implemented one more step. The reconstruction of Mayer's ECC-based IR protocol is as follows.

1-3. The same as that of the key redistribution protocol.

4. Bob uses the $r_B^{(1)}$ to do concatenated encoding just as Alice has done to get

$$c'^{(l)} = C_l\left[P_{l-1}\left[C_{l-1}\cdots\left[C_2\left[P_1\left[C_1\left(r_B^{(1)}\right)\right]\right]\right]\cdots\right]\right],$$

and gets the K'_A by calculating $(K_A \oplus c^{(l)}) \oplus c'^{(l)}$.

Analysis result. Assuming that the initial error rate is 3%, the final error rate after correcting errors is also below 1.0×10^{-9} and the concatenating depth l is also 5. In addition, through the reconstruction of the above schemes, we can analyze that the key redistribution protocol is more suitable than the ECC based IR protocols for being reconstructed into a concatenated form. The step 4 shows that the concatenated ECC-based IR protocol needs to do an extra concatenated encoding. In step 3, Bob uses his raw key K_B to do xor bit by bit with the received sequence and gets $\left(K_A \oplus c^{(l)}\right) \oplus K_B = c^{(l)} \oplus e$. He gets gradually all the vectors $e^{(l)}, e^{(l-1)} \ldots, e^{(1)}, c_B^{(l)}, c_B^{(l-1)}, \ldots, c_B^{(1)}$, and $r_B^{(1)}$ in the end. His purpose is getting K_A, so he should get e and then get $c'^{(l)}$, because he can get K_A by adding it to the receiving string $K_A \oplus c^{(l)}$. However, using $e^{(l)}, e^{(l-1)} \ldots, e^{(1)}$ to reconstruct e is too complicated to be finished generally. Thus he has to do the step 4 to get the $c'^{(l)}$, and then to get the K'_A.

Table 3 is based on Lemma 1, which shows the upper bound of error rates and the left bit rates after each error correction round when the initial error rate is 3%. Currently a typical error rate for a QKD IR protocol to deal with is less than 10%. We can select the error correction code according to the practical channel error rate. It depends on the actual cases. Additionally, we can also come to a specific conclusion to select accurate concatenating depth based on the different initial error rates and error correction codes according to Lemma 1, and can reduce the final bit error rate to a more relaible level.

Discussions

Concatenated IR scheme can reduce the error rate to any given level if and only if every error correction round makes the error rate lower. Thus, if the error rate of the channel satisfies Eq. (10), after a few error correction round, we can arrive at an error rate less than the given value. We choose the complete Hamming code $[2^k - 1, 2^{k-1} - 1 - k, 3]$ to do this because of their rapid decoding algorithm. The result shows that the error rate decreases exponentially with the concatenated depth.

Error rate estimation via public channel is another basic step of QKD. It is usually an interactive process. We can leave it out by using concatenating IR scheme. For a given error rate of the raw key, after the first round syndrome calculating, the rate of non-zero syndromes should be less

than a threshold. e.g., if the given error rate is p, the non-zero rate of syndromes of the first error correction round is less than $(1-p)^n$. If the rate is beyond this threshold, Bob simply notifies Alice to give up this packet. Otherwise, Bob continues his process. In QKD, after the base sifting step, the classical data post-processing, together with error estimation using our method, can be constructed into a single protocol with almost one-way classical communication.

There are at least three interactions in a BB84 QKD protocol. The first one is quantum signal transmission from Alice to Bob. The second one is measurement information transmission from Bob to Alice: Bob informing Alice the positions of qubits received and the bases of his measurement. The third one is a classical packet from Alice to Bob: a bit string representing the positions of raw key bits she selected, and a sequence of syndromes, Alice puts them in a packet and sends it to Bob. Then Bob does the error rate check and the post-processing described above. If Bob finds the non-zero rate of syndrome is bigger than $(1-p)^n$, he has to do the fourth interaction to inform Alice abandoning that packet.

The concatenated IR method cannot reduce the information leakage rate. Because the adversary cannot predict the positions of his eavesdropped bits in the raw key, the eavesdropped bits are uniformly located in both the information digits and the check digits of the raw key's codewords. After each error correction round, the left bit string is permuted by wire link permutation. Thus the left leaking bits will be uniformly distributed in both the information digits and the check digits of the next round's blocks. Supposing that the eavesdropping rate of the adversary is η. After abandoning the check bits in each error correction round, the length of the block is decreased from n bits to k bits. After l rounds error correction, there are $(\frac{k}{n})^l \eta n$ bits information leakage left. Thus, after l rounds reconciliation, the final information leakage rate is still η, and the parameters of privacy amplification remain the same.

Conclusion

In this paper, we propose a concatenated method of IR schemes which can achieve any given error rate level without the need of interactions. Under the premise of the given error rate level, we present the selection criteria of the concatenating depths and error correcting code. Additionally, we can choose the appropriate choices of error correction code and concatenated depth for the reconstruction scheme. We improve three QKD post-processing schemes based on the concatenated method of IR scheme. The reconstructed schemes designed based on this idea can achieve an error rate below 1×10^{-9} after correcting erros while meet the requirement of one-way communication, thus may achieve the pratical error rate level, reduce the post-processing delay and system complexity of QKD. Compared with the one-way IR schems based on LDPC codes and polar codes, the IR schemes based on the proposed concatenated method can get lower bit error rates after error correction.

Appendix

A The derivation of Eq. (10)

In this section we present the derivation of Eq. (10), which is as follows.

$$\begin{aligned} C_n^k - A_k &= C_n^k - \frac{1}{n+1}C_n^k - \frac{n}{n+1}(-1)^{\lceil \frac{k}{2} \rceil} C_{\frac{n-1}{2}}^{\lfloor \frac{k}{2} \rfloor} \\ &= \frac{n}{n+1}\left(C_n^k - (-1)^{\lceil \frac{k}{2} \rceil} C_{\frac{n-1}{2}}^{\lfloor \frac{k}{2} \rfloor} \right). \end{aligned} \tag{16}$$

$$\begin{aligned} &\frac{A_{k+1}-A_{k-1}}{A_{k-1}+A_{k+1}} \\ &= \frac{\frac{1}{n+1}C_n^{k+1} + \frac{n}{n+1}(-1)^{\lceil \frac{k+1}{2} \rceil} C_{\frac{n-1}{2}}^{\lfloor \frac{k+1}{2} \rfloor} - \frac{1}{n+1}C_n^{k-1} - \frac{n}{n+1}(-1)^{\lceil \frac{k-1}{2} \rceil} C_{\frac{n-1}{2}}^{\lfloor \frac{k-1}{2} \rfloor}}{\frac{1}{n+1}C_n^{k+1} + \frac{n}{n+1}(-1)^{\lceil \frac{k+1}{2} \rceil} C_{\frac{n-1}{2}}^{\lfloor \frac{k+1}{2} \rfloor} + \frac{1}{n+1}C_n^{k-1} + \frac{n}{n+1}(-1)^{\lceil \frac{k-1}{2} \rceil} C_{\frac{n-1}{2}}^{\lfloor \frac{k-1}{2} \rfloor}} \\ &= \frac{C_n^{k+1} - C_n^{k-1} + n(-1)^{\lceil \frac{k+1}{2} \rceil} \left(C_{\frac{n-1}{2}}^{\lfloor \frac{k+1}{2} \rfloor} + C_{\frac{n-1}{2}}^{\lfloor \frac{k-1}{2} \rfloor} \right)}{C_n^{k+1} + C_n^{k-1} + n(-1)^{\lceil \frac{k+1}{2} \rceil} \left(C_{\frac{n-1}{2}}^{\lfloor \frac{k+1}{2} \rfloor} - C_{\frac{n-1}{2}}^{\lfloor \frac{k-1}{2} \rfloor} \right)} \\ &= \frac{A+B}{C+D}, \end{aligned} \tag{17}$$

Here,

$$\begin{aligned} A &= (n-1)!\left(\frac{1}{(k+1)!\,(n-k-1)!} - \frac{1}{(k-1)!\,(n-k+1)!} \right) \\ &= C_{n-1}^{k+1} \frac{n^2+n-4k}{(n-k-1)(n-k)(n-k+1)}, \end{aligned} \tag{18}$$

$$\begin{aligned} B &= (-1)^{\lceil \frac{k+1}{2} \rceil} (\frac{n-1}{2})! \frac{1}{\lfloor \frac{k+1}{2} \rfloor! \, (\frac{n-1}{2} - \lfloor \frac{k-1}{2} \rfloor)!} (\frac{n-1}{2}) \\ &= (-1)^{\lceil \frac{k+1}{2} \rceil} C_{\frac{n+1}{2}}^{\lfloor \frac{k+1}{2} \rfloor}, \end{aligned} \tag{19}$$

$$\begin{aligned} C &= (n-1)!\left(\frac{1}{(k+1)!\,(n-k-1)!} + \frac{1}{(k-1)!\,(n-k+1)!} \right) \\ &= C_{n-1}^{k+1} \frac{n^2+n+2k^2-2k}{(n-k-1)(n-k)(n-k+1)}, \end{aligned} \tag{20}$$

$$\begin{aligned} D &= (-1)^{\lceil \frac{k+1}{2} \rceil} (\frac{n-1}{2})! \frac{\frac{n+1}{2} - \lfloor \frac{k+1}{2} \rfloor - \lfloor \frac{k+1}{2} \rfloor}{\lfloor \frac{k+1}{2} \rfloor! \, (\frac{n+1}{2} - \lfloor \frac{k+1}{2} \rfloor)!} \\ &= (-1)^{\lceil \frac{k+1}{2} \rceil} \left(C_{\frac{n+1}{2}}^{\lfloor \frac{k+1}{2} \rfloor} - 2C_{\frac{n-1}{2}}^{\lfloor \frac{k-1}{2} \rfloor} \right) \\ &= (-1)^{\lceil \frac{k+1}{2} \rceil} C_{\frac{n+1}{2}}^{\lfloor \frac{k+1}{2} \rfloor} \left(1 - \frac{4}{n+1} \lfloor \frac{k+1}{2} \rfloor \right). \end{aligned} \tag{21}$$

Thus,

$$\frac{A_{k+1}-A_{k-1}}{A_{k-1}+A_{k+1}} = \frac{C_n^{k+1}-C_n^{k-1}+n(-1)^{\lceil\frac{k+1}{2}\rceil}C_{\frac{n+1}{2}}^{\lfloor\frac{k+1}{2}\rfloor}}{C_n^{k+1}+C_n^{k-1}+n(-1)^{\lceil\frac{k+1}{2}\rceil}C_{\frac{n+1}{2}}^{\lfloor\frac{k+1}{2}\rfloor}\left(1-\frac{4}{n+1}\lfloor\frac{k+1}{2}\rfloor\right)}, \tag{22}$$

Here,

$$C_n^{k+1}+C_n^{k-1} = C_{n+1}^{k+1}\frac{n^2+n-2nk+2k^2}{n^2+2n+1-k}, \tag{23}$$

$$\begin{aligned} &C_n^{k+1}-C_n^{k-1} \\ &= \frac{n!}{(k+1)!\,(n-k-1)!}-\frac{n!}{(k-1)!\,(n-k+1)!} \\ &= \frac{n!}{(k+1)!\,(n-k+1)!}[\,(n-k+1)(n-k)-(k+1)k] \\ &= C_{n+1}^{k+1}\frac{n-2k}{n-k+1}. \end{aligned} \tag{24}$$

B The proof of Lemma 1

Proof 1 *In "Some selection criteria of concatenated IR schemes" section, Lemma 1 is presented. Here, we prove it in detail.Hamming code can correct one-bit error without failure. When there are more errors, the correction process may add 1 bit error. Here we consider the upper bound of the average number of errors, thus we assume the number of errors will increase by 1 after error correcting. When there are n bits errors, the number of errors will be reduced by 1 after error correction. Then*

$$\begin{aligned} \chi &= \sum_{k=2}^{n-1}(1+k)C_n^k p^k(1-p)^{n-k}+(n-1)C_n^n p^n \\ &= \sum_{k=2}^{n}(1+k)C_n^k p^k(1-p)^{n-k}-2p^n \\ &= \sum_{k=0}^{n}(1+k)C_n^k p^k(1-p)^{n-k}-2p^n-(1-p)^n-2np(1-p)^{n-1}. \end{aligned} \tag{25}$$

By the identity $\sum_{k=0}^{n} kC_n^k p^k(1-p)^{n-k} = np$, *we have*

$$\chi = 1+np-2p^n-(1-p)^{n-1}(1-p+2np). \tag{26}$$

□

Now let us consider the upper bound of χ.

C The proof of Lemma 2

Proof 2 *In "Some selection criteria of concatenated IR schemes" section, Lemma 2 is also presented. Here, we prove it in detail. From the Eq. (26), we have*

$$\begin{aligned} \chi &< \sum_{k=2}^{n-1}(1+k)C_n^k p^k(1-p)^{n-k} \\ &= \sum_{k=3}^{n}(1+k)C_n^k p^k(1-p)^{n-k}+3C_n^2p^2(1-p)^{n-2}. \end{aligned} \tag{27}$$

By the inequality (Lint 1999) $(1+k)C_n^k \le n(n-1)C_{n-2}^{k-2}$ $(k\ge 3)$, *it holds that*

$$\begin{aligned} \sum_{k=3}^{n}(1+k)C_n^k p^k(1-p)^{n-k} &\le n(n-1)\sum_{k=3}^{n}C_{n-2}^{k-2}p^k(1-p)^{n-k} \\ &= n(n-1)p^2\sum_{k=3}^{n}C_{n-2}^{k-2}p^{k-2}(1-p)^{n-k} \\ &= n(n-1)p^2\sum_{k=1}^{n-2}C_{n-2}^{k}p^{k}(1-p)^{n-2-k} \\ &= n(n-1)p^2\left[1-(1-p)^{n-2}\right]. \end{aligned} \tag{28}$$

Thus we obtain

$$\begin{aligned} \chi &< 2C_n^2p^2\left[1-(1-p)^{n-2}\right]+3C_n^2p^2(1-p)^{n-2} \\ &= n(n-1)p^2\left[1+\frac{1}{2}(1-p)^{n-2}\right]. \end{aligned} \tag{29}$$

□

From the Lemma 2, it holds that

$$\chi < \frac{3n(n-1)}{2}p^2 < \frac{3}{2}(np)^2. \tag{30}$$

D The proof of Theorem 1

Proof 3 *Here, we present the proof of Theorem 1 stated in "Some selection criteria of concatenated IR schemes" section. Denote* p_1 *as the error rate after one error correction round. From the definition of* χ, *we know* $p_1 < \frac{\chi}{n}$. *It is clear that the concatenated error correction scheme can reduce the error rate to any given level, if and only if* $p_1 < p$. *Because* $p_1 < \frac{\chi}{n}$, $p_1 < p$ *holds if* $\frac{\chi}{n} < p$. *From Lemma 2,* $\frac{\chi}{n} < p$ *holds if* $n(n-1)p^2\left[1+\frac{1}{2}(1-p)^{n-2}\right] < np$. *That is*

$$p < \frac{1}{(n-1)\left[1+\frac{1}{2}(1-p)^{n-2}\right]}. \tag{31}$$

□

E The proof of Corollary 1

Proof 4 *Here, we present the proof of Corollary 1 stated in "Some selection criteria of concatenated IR schemes" section.*

$$\frac{2}{3(n-1)} < \frac{1}{(n-1)\left[1+\frac{1}{2}(1-p)^{n-2}\right]} < \frac{1}{n-1}. \tag{32}$$

Thus, when $p < \frac{2}{3(n-1)}$, *the condition* 31 *holds. Let* $p_{th} = \frac{2}{3(n-1)}$. *Thus if* $p < p_{th}$, *according to Theorem* 1, *the concatenated error correction scheme can reduce the error rate to any given level.* □

Abbreviations

BB84: Bennett and Brassard's protocol in 1984; BBBSS: Bennett and Brassard's protocol in 1992; BCH: The abbreviation of Bose, Ray-Chaudhuri and Hocquenghem; CRC: Cyclic redundancy code; ECC: Error correcting code; IR: Information reconciliation; LDPC: Low-density Parity-check; MAC: Message authentication code; QKD: Quantum key distribution; WLP: Wire link permutation

Acknowledgement

We thank Gang Yao for his discussion on the theory of correcting error code, and reviewers for their comments and suggestions.

Funding

This research was funded by National Natural Science Foundation of China under Grant No. 61672517 and National Cryptography Development Fund under Grant No. MMJJ20170108.

Availability of data and materials

Not applicable.

Authors' contributions

Idea and formula direvation, LY; writing— original draft preparation, LY and ZL; new literature investigation and writing— new draft preparation, HD. All authors read and approved the final manuscript.

Competing interests

The authors declare that they have no competing interests.

Publisher's Note

Received: 22 March 2019 Accepted: 26 April 2019
Published online: 22 May 2019

References

Bennett CH, Brassard G (1984) Quantum cryptography: public-key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers Systems and Signal Processing. pp 175–179

Bennett CH, Brassard G, Robert JM (1988) Privacy amplification by public discussion. SIAM J Comput 17(2):210–229

Bennett CH, Bessette F, Brassard G, Salvail L, Smolin J (1992) Experimental quantum cryptography. J Cryptol 5(1):3–28

Biham E, Boyer M, Boykin PO, Mor T, Roychowdhury V (2006) A proof of the security of quantum key distribution. J Cryptol 19(4):381–439

Blundo C, De Santis A, Herzberg A, Kutten S, Vaccaro U, Yung M (1992) Perfectly-secure key distribution for dynamic conferences. In: Annual international cryptology conference. Springer, Heidelberg, Berlin. pp 471–486

Brassard G, Salvail L (1993) Secret-key reconciliation by public discussion. In: Workshop on the Theory and Application of of Cryptographic Techniques. Springer, Berlin Heidelberg. pp 410–423

Buttler WT, Lamoreaux SK, Torgerson JR, Nickel GH, Donahue CH, Peterson CG (2003) Fast, efficient error reconciliation for quantum cryptography. Phys Rev A 67(5):052303

Cachin C, Maurer UM (1997) Linking information reconciliation and privacy amplification. J Cryptol 10(2):97–110

Cui K, Wang J, Zhang HF, Luo CL, Jin G, Chen TY (2013) A real-time design based on FPGA for expeditious error reconciliation in QKD system. IEEE Trans Inf Forensic Secur 8(1):184–190

Elkouss D, Leverrier A, Alleaume R, Boutros JJ (2009) Efficient reconciliation protocol for discrete-variable quantum key distribution. In: 2009 IEEE International Symposium on Information Theory. IEEE. pp 1879–1883

Elkouss D, MartinezMateo J, Martin V (2011) Information reconciliation for quantum key distribution. Quantum Inf Comput 11(3):226–238

Gong CQ, Zhou HY, Feng JL (2009) An improvement of protocol binary in reconciliation of quantum key distribution. In: 2009 International Conference on Management and Service Science. IEEE. pp 1–4

Gong CQ, Zhou HY, Feng JL (2009) Research on reconciliation algorithm in quantum key distribution. In: 2009 Ninth International Conference on Hybrid Intelligent Systems. IEEE Vol. 1. pp 496–498

Hamming RW (1950) Error detecting and error correcting codes. Bell Sys Tech J 29(2):147–160

Jouguet P, Kunzjacques S (2014) High performance error correction for quantum key distribution using polar codes. Quantum Inf Comput 14(3-4):329-388. arXiv: 1204.5882

Jouguet P, Elkouss D, KunzJacques S (2014) High-bit-rate continuous-variable quantum key distribution. Phys Rev A 90(4):042329

Kiktenko EO, Trushechkin AS, Lim CCW, Kurochkin YV, Fedorov AK (2017) Symmetric blind information reconciliation for quantum key distribution. Phys Rev Appl 8(4):044017

Krawczyk H (1994) New hash function for message authentication, Advances in Cryptology-EUROCRYPT '95 (LNCS 809). Springer-Verlag

Krawczyk H (1994) LFSR-based hashing and authentication. In: Annual International Cryptology Conference. Springer, Berlin Heidelberg. pp 129–139

Li J, Jiang I, Lin X, Fang J (2019) Polar Codes-based One-step Post-processing for Quantum Key Distribution(in Chinese). https://doi.org/doi:10.6054.jscnun.2019015

Li Q, Wen X, Mao H, Wen X (2019) An improved multidimensional reconciliation algorithm for continuous-variable quantum key distribution. Quantum Inf Process 18(1):25

Lint JV (1999) Introduction to coding theory. Springer

Liu S, van Tilborg HCA (2002) Privacy amplification over a non-authentic public channel. In: Proceedings IEEE International Symposium on Information Theory. IEEE. p 322

Martinez-Mateo J, Elkouss D, Martin V (2010) Interactive reconciliation with low-density parity-check codes. In: 2010 6th International Symposium on Turbo Codes & Iterative Information Processing. IEEE. pp 270–274

Maurer UM (1991) Perfect cryptographic security from partially independent channels. In: STOC Vol. 91. pp 561–571

Maurer UM (1993) Secret key agreement by public discussion from common information. IEEE Trans Inf Theory 39(3):733–742

Maurer U, Wolf S (1997) Privacy amplification secure against active adversaries. In: Annual International Cryptology Conference. Springer, Berlin Heidelberg. pp 307–321

Mayers D (2001) Unconditional security in quantum cryptography. J ACM (JACM) 48(3):351–406

Nakassis A, Mink A (2014) Polar codes in a QKD environment. SPIE.9123:912305

Pearson D (2004) High-speed QKD Reconciliation using Forward Error Correction. In: AIP Conference Proceedings Vol. 734. pp 299–302

Renes JM, Dupusi F, Renner R (2012) Efficient polar coding of quantum information. Phys Rev Lett 109(5):050504

Shi Z, Lee RB (2000) Bit permutation instructions for accelerating software cryptography. In: Proceedings IEEE International Conference on Application-Specific Systems, Architectures, and Processors. IEEE. pp 138–148

Takemoto K, Nambu Y, Miyazawa T, Sakuma Y, Yamamoto T, Yorozu S, Arakawa Y (2015) Quantum key distribution over 120 km using ultrahigh purity single-photon source and superconducting single-photon detectors. Sci Rep 5:14383

Tomamichel M, Martinez-Mateo J, Pacher C, Elkouss D (2017) Fundamental finite key limits for one-way information reconciliation in quantum key distribution. Quantum Inf Process 16(11):280

Traisilanun W, Sripimanwat K, Sangaroon O (2007) Secret key reconciliation using BCH code in quantum key distribution. In: 2007 International Symposium on Communications and Information Technologies. IEEE. pp 1482–1485

Xiao H, Shi P, Zhao SM (2015) A reconciliation protocol with delayed error correction for quantum key distribution(in Chinese). Sci Sin Tech 45:843–848

Yamamura A, Ishizuka H (2001) Error detection and authentication in quantum key distribution. In: Australasian Conference on Information Security and Privacy. Springer, Berlin Heidelberg. pp 260–273

Yan H, Ren T, Peng X, Lin X, Jiang W, Liu T, Guo H (2008) Information reconciliation protocol in quantum key distribution system. In: 2008 Fourth International Conference on Natural Computation. IEEE Vol. 3. pp 637–641

Yang L, Wu LA, Liu SH (2002) On the Breidbart eavesdropping problem of the extended BB84 QKD protocol(in Chinese). Acta Phys Sin 51(5):961–965
Zhao F, Fu M, Wang F, Lu Y, Liao C, Liu S (2007) Error reconciliation for practical quantum cryptography. Opt Int J Light Electron Opt 118(10):502–506
Zhao YB, Gui YZ, Chen JJ, Han ZF, Guo GC (2008) Computational complexity of continuous variable quantum key distribution. IEEE Trans Inf Theory 54(6):2803–2807