Shannon-limit approached information reconciliation for quantum key distribution

Bang-Ying Tang¹ · Bo Liu² · Wan-Rong Yu¹ · Chun-Qing Wu¹,³

Received: 16 March 2020 / Accepted: 29 October 2020 / Published online: 19 March 2021
© The Author(s) 2021

Abstract
Information reconciliation (IR) corrects the errors in sifted keys and ensures the correctness of quantum key distribution (QKD) systems. Polar codes-based IR schemes can achieve high reconciliation efficiency; however, the incidental high frame error rate decreases the secure key rate of QKD systems. In this article, we propose a Shannon-limit approached (SLA) IR scheme, which mainly contains two phases: the forward reconciliation phase and the acknowledgment reconciliation phase. In the forward reconciliation phase, the sifted key is divided into sub-blocks and performed with the improved block checked successive cancellation list decoder of polar codes. Afterward, only the failure corrected sub-blocks perform the additional acknowledgment reconciliation phase, which decreases the frame error rate of the SLA IR scheme. The experimental results show that the overall failure probability of SLA IR scheme is decreased to $10^{-8}$ and the efficiency is improved to 1.091 with the IR block length of 128 Mb. Furthermore, the efficiency of the proposed SLA IR scheme is 1.055, approached to Shannon limit, when the quantum bit error rate is 0.02 and the input scale of 1 Gb, which is hundred times larger than the state-of-the-art implemented polar codes-based IR schemes.

Keywords Quantum key distribution · Information reconciliation · Shannon-limit · Polar codes

Bang-Ying Tang and Bo Liu have contributed equally to this work.

Bo Liu
liubo08@nudt.edu.cn

Wan-Rong Yu
wlyu@nudt.edu.cn

¹ College of Computer, National University of Defense Technology, Changsha 410073, China
² College of Advanced Interdisciplinary Studies, National University of Defense Technology, Changsha 410073, China
³ Guangdong Tendy Technology Co., Ltd, FoShan 528311, China
1 Introduction

Quantum key distribution (QKD) can generate information-theoretical secure keys between distant communication parties (Alice and Bob) [1–3]. Assume the sifted keys are $K^A$ and $K^B$ with length of $n$ in both sides (Alice and Bob) after the quantum physical communication phase, $K^A \neq K^B$ with the quantum bit error rate $E_\mu$, which is introduced by imperfect implementations of QKD systems and potential attacks. Information reconciliation (IR), a critical procedure of the post-processing phase in QKD systems, aims at reconciling $K^A$ and $K^B$ to an equally weak secure key $K_{IR}$, by exchanging the minimized extra syndrome information [1,4,5]. IR ensures the correctness of QKD systems and is the precondition to generate the final secure keys.

Initially, IR procedure is implemented by performing interactive methods known as BBBSS [5,6] and Cascade [7]. Though high efficiency is achieved by several improvements of Cascade algorithms, multiple rounds of communication are still required, resulting in significant heavy latency and authentication cost of QKD systems. Nowadays, IR is performed with forward error correction (FEC) codes, such as low-density parity-check codes [8,9] and polar codes [10–12], where only one message containing a syndrome is exchanged between Alice and Bob, called as one-way IR scheme. Recently, most IR research focuses on performing with polar codes, for the advantage of the low computational complexity $O(n \log n)$ and high efficiency with potential to reach the Shannon limit, when the block size of a sifted key becomes as large as possible [13–15]. Though several improvements of polar decoders achieve higher IR efficiency with certain input scale ($\sim 10^6$ bits), the $\varepsilon$-correctness of QKD systems is increased to the level of $10^{-3}$ [10–12,16]. The state-of-the-art efficiency of polar codes-based IR scheme reaches 1.176 with the input block size of 1 Mb when $E_\mu = 0.02$, while $\varepsilon$ still stays to 0.001 [11]. Actually, $\varepsilon$ should be decreased as low as possible (usually $< 10^{-6}$), when performing polar codes into the IR procedure of QKD systems.

Therefore, in this article, we propose a Shannon-limit approached (SLA) IR scheme performing improved polar codes, which mainly composes of a forward reconciliation phase and an acknowledgment reconciliation phase. In the forward reconciliation procedure, a novel block checked successive cancellation list (BC-SCL) decoder was proposed to reduce the $\varepsilon$-correctness and error sub-blocks by remaining the successfully decoded sub-blocks with cyclic redundancy check (CRC) values in advance. Meanwhile, existed errors in sub-blocks after the forward reconciliation procedure can be found by calculating the CRC values. For failure corrected sub-blocks, an additional acknowledgment reconciliation procedure is performed to decrease the $\varepsilon$ to the desired level. Finally, the corrected key $K_{IR}$ is achieved. With the advantage of CRC strategy, the BC-SCL decoder determines the corrected decoding path from multiple decoding paths to reduce the $\varepsilon$-correctness and choose the unsuccessfully decoded sub-blocks which are corrected by the acknowledgment reconciliation phase. The experimental results show that our SLA IR scheme achieves correctness $\varepsilon$ to $10^{-8}$ and the reconciliation efficiency is better than 1.091, while the input block size is 128 Mb. In principle, the efficiency and the SLA IR scheme can close to the Shannon limit as the block length increases as large as possible. We achieved an efficiency of 1.055 with the $E_\mu = 0.02$, when the input scale of SLA IR is increased to 1 Gb. Meanwhile,
our SLA IR scheme with large-scale block size will benefit a lot in performing the rigorous statistical fluctuation analysis to remove the finite-size key effects \(^{[17,18]}\) on the final secure key. Thus, SLA IR scheme can be efficiently implemented in practical QKD systems.

2 Related work

2.1 Information reconciliation

Information reconciliation (IR), as the critical post-processing procedure of QKD systems, corrects the errors in the sifted keys introduced by the implementation imperfection and various attacks \(^{[1,19,20]}\), so as to ensure the correctness of QKD systems \(^{[21]}\). Assume the sifted key is \(K_A^S\) \((K_B^S)\) with length of \(n\) on Alice’s (Bob’s) side, the quantum bit error rate (QBER) is \(E_\mu\), and the error corrected key is \(K_{IR}^A\) and \(K_{IR}^B\), then the \(\varepsilon\)-correctness is equivalent to the requirement that the outputs of IR procedure, \(K_{IR}^A\) and \(K_{IR}^B\), differ only with small probability \(^{[21]}\),

\[
\Pr \left[ K_{IR}^A \neq K_{IR}^B \right] \leq \varepsilon. \tag{1}
\]

Assume the key information learned by eavesdroppers is \(S\), then the reconciliation efficiency is defined as

\[
f (E_\mu) = 1 - \min \left\{ \frac{H_2 \left( K_{IR}^A | S \right)}{H_2 (E_\mu)}, H_2 \left( K_{IR}^B | S \right) \right\}, \tag{2}
\]

where \(H_2(x)\) is the binary Shannon entropy, calculated by

\[
H_2 (x) = -x \log_2 (x) - (1 - x) \log_2 (1 - x). \tag{3}
\]

The average yield of IR scheme is given by

\[
\gamma = (1 - \varepsilon) \min \left\{ H_2 \left( K_{IR}^A | S \right), H_2 \left( K_{IR}^B | S \right) \right\} = (1 - \varepsilon) \left[ 1 - f (E_\mu) \right] H_2 (E_\mu). \tag{4}
\]

2.2 Polar codes-based IR schemes

Given any binary-input discrete memoryless channel (B-DMC), E. Arikan first proposed a Shannon-limit approached information reconciliation scheme with complexity \(O (N \log N)\), named as polar codes in 2009 \(^{[13,14]}\). In 2014, P. Jouguet and S. Kunz-Jacques performed the polar codes in the IR procedure in QKD systems; furthermore, they showed that polar codes have an equivalent efficiency below 1.12 for given upper bound \(\varepsilon = 0.1\) and block length starting from 64 Kb to 16 Mb \(^{[10]}\). Afterward, A. Nakassis and A. Mink described flexible polar codes-based IR approaches for QKD systems and showed the potential to approach the Shannon limit with a more efficient
decoder when the location and values of the frozen bits were known at the design time [12]. Yan et al. [11] improved the polar codes-based IR scheme with successive cancellation list (SCL) decoding and optimized coding structures, which decreased the $\varepsilon$-correctness to the level of $10^{-3}$ and the equivalent efficiency reached to 1.176. The detailed performance of the above IR schemes and partial experimental results of our SLA IR scheme are described in Table 1.

### 3 Shannon-limit approached IR scheme

In principle, lower $\varepsilon$-correctness and Shannon-limit $f$ of polar codes-based IR schemes can be approached with increased input block size and improved decoders [22–29]. Moreover, IR schemes with large-scale input block size benefit much in performing the rigorous statistical fluctuation analysis to remove the finite-size key effects on the final secure keys. However, $\varepsilon$-correctness of state-of-the-art polar codes-based IR schemes still stays on the level of $10^{-3}$, which reduces the final secure key rates of QKD systems.

In this article, we propose an improved Shannon-limit approached (SLA) IR scheme for QKD, and the schematic diagram is shown in Fig. 1. The proposed SLA IR scheme

---

**Table 1** The performance of polar codes-based IR schemes

| Author                        | QBER | $n$   | $f$   | $\varepsilon$ | $\gamma$ |
|-------------------------------|------|-------|-------|----------------|----------|
| Jouguet and Kunz-Jacques [10] | 0.02 | 64 Kb | 1.395 | 0.090         | 0.731    |
|                               |      | 1 Mb  | 1.225 | 0.110         | 0.736    |
|                               |      | 16 Mb | 1.121 | 0.080         | 0.774    |
| Nakassis and Mink [12]        | 0.02 | 64 Kb | 1.425 | 0.073         | 0.740    |
|                               |      | 1 Mb  | 1.243 | 0.027         | 0.802    |
|                               | 0.04 | 64 Kb | 1.344 | 0.015         | 0.664    |
|                               |      | 1 Mb  | 1.188 | 0.031         | 0.690    |
| Yan et al. [11]               | 0.02 | 64 Kb | 1.261 | 0.002         | 0.820    |
|                               |      | 1 Mb  | 1.176 | 0.001         | 0.833    |
| Our scheme                    | 0.02 | 1 Mb  | 1.146 | $10^{-8}$     | 0.838    |
|                               |      | 16 Mb | 1.085 | $10^{-8}$     | 0.847    |
|                               |      | 128 Mb| 1.073 | $10^{-8}$     | 0.848    |
|                               | 0.04 | 1 Mb  | 1.116 | $10^{-8}$     | 0.730    |
|                               |      | 16 Mb | 1.072 | $10^{-8}$     | 0.740    |
|                               |      | 128 Mb| 1.059 | $10^{-8}$     | 0.743    |
|                               | 0.06 | 1 Mb  | 1.099 | $10^{-8}$     | 0.640    |
|                               |      | 16 Mb | 1.062 | $10^{-8}$     | 0.652    |
|                               |      | 128 Mb| 1.049 | $10^{-8}$     | 0.657    |
mainly contains two phases: the forward reconciliation phase and the acknowledgment reconciliation phase. In the forward reconciliation phase, Alice constructs the encoding vector $U$ with true random numbers and the optimal frozen vector $V$, chosen from the frozen vector library with the quantum bit error rate $E_\mu$. Then, Alice calculates the syndrome $Z$ of $K^A_s$ with the polar codes encoder and, meanwhile, divides the vector $U$ to $m$ sub-blocks and calculates the cyclic redundancy check (CRC) value of each block. Afterward, the syndrome $Z$ and combined CRC value vector $T$ are transmitted to Bob via classical channel. Bob performs the same operations to select the frozen vector $V$ and then performs the improved BC-SCL decoder (detail described in Sect. 3.3) to get the corrected vector $U'$ and the status vector $\sigma$, indicating which sub-block is failure corrected. In the acknowledgment reconciliation phase, Alice and Bob perform a low-density parity-check (LDPC) error correction procedure to correct the error bits in the failure corrected sub-blocks. Afterward, Alice and Bob obtain the uniform key $K_{IR}$, respectively.

3.1 Forward reconciliation

Before Alice and Bob start the SLA IR scheme, optimized multi-rate frozen vectors of polar codes and parity-check matrix of LDPC codes are shared between each other. First of all, Alice and Bob will calculate the required CRC length $d$ and choose the appropriate number of sub-blocks $m$ to achieve the expected $\varepsilon$-correctness. Given $E_\mu$, Alice selects the optimized frozen vector $V$ of polar codes, where the elements representing frozen bits are set to “0” and the rest are set to “−1”. Then, $k$ bits of true random numbers are used to replace the elements of $V$, whose value equals to “−1”, marked as the vector $U$. Then, split $U$ to $m$ sub-blocks with length $n' = n/m$. For \textcircled{S}pringer
each sub-block $U_i$, $i \in [0, m)$ and $i \in \mathbb{N}$, calculate the CRC tag value $T_i = \text{CRC}(U_i)$ and combined to $T$, $T = (T_0|T_1| \ldots |T_{m-1})$.

Meanwhile, the vector $U$ is encoded to $Z$ by

$$Z = UG_n \oplus K_s^A,$$

where $G_n$ is the bit-reversal invariant matrix, defined as $G_n = BF^{\otimes \log n}$, $B$ is the permutation matrix for bit-reversal operation and $F \triangleq \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ [13]. Afterward, Alice sends $T$ and $Z$ to Bob via the classical channel.

At Bob’s side, with Bob’s sifted key $K_s^B$, received $T$ and $Z$, we can get the decoded vector $U'$ with failure probability $\varepsilon_f$ by performing our improved novel block checked (BC) SCL decoder, detailed described in Sect. 3.3. Additionally, a status vector $\sigma$ also given for indicating which sub-block $U'_i$ is failure decoded. Each element of $\sigma$ is defined as

$$\sigma_i = \begin{cases} 1 & \text{CRC} (U'_i) \neq T_i \\ 0 & \text{else} \end{cases}.$$

Thus, in total $r$ sub-blocks are failure decoded, $r = \sum \sigma_i$. The position vector of these failure corrected sub-blocks is defined as $E \triangleq \{i|\sigma_i = 1\}$.

### 3.2 Acknowledgment reconciliation

After the forward reconciliation phase, we have to perform the acknowledgment reconciliation phase to correct the remained errors in partial sub-blocks.

Here, Bob distinguishes two cases according to the value of $r$.

**Case I.** If $r \neq 0$, Bob performs the permutation operation to $K_s^B$,

$$Y = K_s^B B,$$

and then, divide $Y$ to $m$ sub-blocks with length $n' = n/m$. Then, Bob calculates the syndrome $\mathcal{S}$ from $Y_E$ by performing the LDPC encoding scheme with chosen optimized parity-check matrix, where $Y_E \triangleq \{Y_{ei}|e_i \in E\}$. Then, Bob sends $\sigma$ and $\mathcal{S}$ to Alice. Alice performs the bit-reversal operation to $K_s^A$,

$$X = K_s^A B,$$

and then, divide $X$ into $m$ sub-blocks with length $n' = n/m$. Alice corrects the error bits in $X_E$ with $\mathcal{S}$, where $X_E \triangleq \{X_{ei}|e_i \in E\}$. 
In the end of acknowledgment reconciliation phase, Bob gets the error corrected key $K_{IR}^B$ with failure probability $\varepsilon$, whose $i$th sub-block can be represented by

$$K_{IR,i}^B \triangleq \begin{cases} U_i' \sigma_i = 0 \\ Y_i \sigma_i \neq 0. \end{cases}$$

(9)

Alice performs similar procedure shown in Eq. (9) to the identical and weak secure key $K_{IR}^A$.

**Case II.** If $r = 0$, Bob sets $S = \emptyset$. Then, $\sigma$ and $S$ are transmitted to Alice. Afterward, Alice and Bob gets $K_{IR}^A = U$ and $K_{IR}^B = U'$ as the error corrected key, respectively.

### 3.3 Block checked SCL decoder

In the article, we improve the successive cancellation list (SCL) decoder to reduce the $\varepsilon$-correctness by performing cyclic redundancy check (CRC) to divided sub-blocks, called as block checked (BC) SCL decoder [22].

In the BC-SCL decoder, we assume the list size is $l$, $P$ is the list of decoded vectors, $\mathcal{P} \in P$ with length of $n$, $\mathcal{P}_i^k$ is a sub-vector of $\mathcal{P} \in P$, where $\mathcal{P}_i^k = [P[j], \ldots, P[k]]$, $0 \leq j \leq k < n$ and the outcome of the decoder is $U$ which can be split into the sub-blocks $U_i$ of length $n'$, $0 \leq i < m$.

**Definition 1** $\mathcal{M}(\mathcal{P}, i)$ is the path metric of the decoded vector $\mathcal{P}_0^i$, calculated as [30]

$$\mathcal{M}(\mathcal{P}, i) = -\ln \Pr \left( \mathcal{P}_0^i | K_{s}^B \oplus Z \right),$$

(10)

where $i \in [0, n)$.

**Definition 2** $\mathcal{M}_{\text{min}}^l(P, i)$ is the $l$th minimum path metric of $\mathcal{M}(P, i)$, where $\mathcal{M}(P, i) = \{ \mathcal{M}(\mathcal{P}, i) | \mathcal{P} \in P \}$ and $i \in [0, n)$.

**Definition 3** $\text{For}(P, i)$ is defined as assume $P' = P$, for $\forall \mathcal{P} \in P'$, set $\mathcal{P}[i] = 1$ and $P \leftarrow P \cup \mathcal{P}$, where $i \in [0, n)$ [22].

**Definition 4** $\text{Prune}(P, i, l)$ is defined as the operation that when $|P| > l$, for $\forall \mathcal{P} \in P$ and $\mathcal{M}(\mathcal{P}, i) > \mathcal{M}_{\text{min}}^l(P, i)$, set $P \leftarrow P \backslash \mathcal{P}$ [30].

The detailed description of the decoding procedure of BC-SCL decoder is shown in Algorithm 1.

### 3.4 Performance of the SLA IR scheme

Let $\mathcal{W}_i$ be the corresponding bit channel of polar codes performed in our forward reconciliation phase of the SLA IR scheme, $P_e(\mathcal{W}_i)$ is the probability of error on the $i$th bit channel, where $i = 0, 1, \ldots, n - 1$. The union upper bound of correctness $\varepsilon_f$ of forward reconciliation phase is estimated as [31]
Algorithm 1 BC-SCL Decoder decoding procedure

Require: \( l, n, m, T, V, \) and \( K^B \oplus Z \)
Ensure: \( U, \sigma \)
1: \( n' = n/m, U = 0^n\)
2: \( P = \{0^n\} \)
3: for \( i = 0 \) to \( m - 1 \) do
   4:      for \( j = 0 \) to \( n' - 1 \) do
      5:         if \( v_{in'+j} = -1 \) then \( \text{Fork}(P, in'+j) \)
      6:         \( \text{Prune}(P, in'+j, l) \)
      7:   end for
      8:   if \( \exists P \in P, \text{CRC}(P_{in'+1}^{(i)\#-1}) = T_i \) then \( U_i = P_{in'+1}^{(i)\#-1}, \sigma_i = 0 \)
      9:      else \( \sigma_i = 1 \)
   10: end for
11: if \( \exists P \in P, \forall i \in [0, m), \text{CRC}(P_{in'+1}^{(i)\#-1}) = T_i \) then \( U = P \)

\[
\epsilon_f \leq \sum_{i=0}^{n-1} -v_i P_e (W_i) . \tag{11}\]

Then, we analyze the total correctness of the SLA IR scheme in two cases.

\textbf{Case I.} \( r \neq 0 \). In this case, the total \( \epsilon \)-correctness \( \epsilon_I \) can be calculated as

\[
\epsilon_I \leq \epsilon_f \sum_{i=1}^{m} \Pr (r = i) \left[ 1 - \left(1 - \frac{l}{2^d}\right)^{m-i} + \epsilon_a \right] , \tag{12}\]

where \( \epsilon_a \) is the failure probability of the acknowledgment reconciliation phase and \( 1 - \left(1 - \frac{l}{2^d}\right)^{m-i} \) is the probability of error on \( i \) sub-blocks which passed the CRC check in the forward reconciliation phase.

\textbf{Case II.} \( r = 0 \). In this case, all outcome sub-blocks of the BC-SCL decoder will pass the CRC check in the forward reconciliation phase, and the total correctness \( \epsilon_{II} \) can be calculated as

\[
\epsilon_{II} \leq \epsilon_f \Pr (r = 0) \left[ 1 - \left(1 - \frac{l}{2^d}\right)^m \right] . \tag{13}\]

Thus, the total \( \epsilon \)-correctness of SLA IR scheme can be calculated as

\[
\epsilon \leq \epsilon_f \Pr (r = 0) \left[ 1 - \left(1 - \frac{l}{2^d}\right)^m \right] + \sum_{i=1}^{m} \epsilon_f \Pr (r = i) \left[ 1 - \left(1 - \frac{l}{2^d}\right)^{m-i} + \epsilon_a \right] . \tag{14}\]

\[
< \epsilon_f \left[ 1 - \left(1 - \frac{l}{2^d}\right)^m + \epsilon_a \right] .
\]
Fig. 2 The $\varepsilon$-correctness of the SLA IR scheme versus $d$ with $l = 16, m = 1, 8, 32, 128$ and $d \geq \log_2 l$

With optimized construction of polar codes and LDPC codes [8,31], we set $\varepsilon_a \leq 10^{-6}$ and $\varepsilon_f \leq 10^{-2}$. The analyzed results of $\varepsilon$ versus $d$ of the SLA IR scheme is shown in Fig. 2, according to Eq. (14), here $l = 16, m = 1, 8, 32, 128$ and $d \geq \log_2 l$. As shown in Fig. 2, the value of $\varepsilon$ becomes higher with larger $m$ and approaches to the lower bound of $10^{-8}$ when $d \geq 36$.

Assume $P^U_j$ is error probability of the decoded sub-block in the forward reconciliation and the error probability threshold of a sub-block is $\varepsilon$, where $j = 0, 1, \cdots, m-1$. Thus, the upper bound of $P^U_j$ can be estimated by $P_e(W_i)$ as

$$P^U_j \leq \sum_{i=jd^m}^{(j+1)d^m-1} -v_i P_e(W_i),$$

(15)

and the upper bound of the decoded sub-blocks with error bits in forward reconciliation $r$ can be estimated as

$$r = \left| \left\{ P^U_j \mid j \in [0, m), P^U_j > \varepsilon \right\} \right|.$$  

(16)

With the implementation of upgrading and degrading channel construction of polar codes [31,32], the upper bound of $P_e(W_j)$ is calculated, and the estimated upper bound of $r$ is shown in Fig. 3 with different $m$ when $\varepsilon = 10^{-3}$, $E_\mu = 0.02$, $d = 32$ and $md < nH(E_\mu)$.

Assume the efficiency of polar codes as $f_1$ and the efficiency of the LDPC codes as $f_II$. After the acknowledgment reconciliation, the total efficiency of SLA IR scheme is

$$f = f_1 H_2(E_\mu) + md + m + \varepsilon_f n' f_II H_2(E_\mu) + \frac{m (d + 1)}{nH_2(E_\mu)} + \varepsilon_f \frac{r}{m},$$

(17)

where $md$ is the upper bound of leaked information to Eve from the transmitted CRC tag values, extra $m$ bits information may leaked to Eve from the vector $\sigma$ and
Fig. 3 The upper bound of $r$ with different $m$ when QBER is 0.02 and $md < nH(E_μ)$.

$\varepsilon_f n' f_{II} H_2(E_μ)$ is the syndrome information leaked in the acknowledgment reconciliation.

In the proposed SLA IR scheme, we divide the error correction block to $m$ subblocks, which will increase the overall efficiency. Without block partition strategy, we have $m = 1$ and the efficiency $f_{m=1}$ can be calculated as

$$f_{m=1} = f_1 + \frac{(d + 1)}{nH_2(E_μ)} + \varepsilon_f f_{II}. \quad (18)$$

Thus, given the fixed $f_1$, the increased efficiency yield $\mathcal{Y}(m)$ of SLA IR scheme with divide the error correction block into $m$ subblocks can be calculated as

$$\mathcal{Y}(m) = f_{m=1} - f = -\frac{(m - 1) (d + 1)}{nH(E_μ)} + \varepsilon_f f_{II} \frac{m - r}{m}. \quad (19)$$

The estimation results of $\mathcal{Y}(m)$ are shown in Fig. 4, where $E_μ = 0.02$, $m = 32$. The yield of efficiency increases as block length and $\varepsilon_f$ increase and approaches to 0.01 when $\varepsilon_f$ equals 0.1 and block length is larger than $10^8$. According to Eq. (4), the yield of efficiency will lead to higher final secure key rates of QKD systems.

4 Results

We have implemented the Shannon-limit approached (SLA) IR scheme with the BC-SCL decoder. Afterward, a series of experiments have been conducted to evaluate the efficiency of the SLA IR scheme with the limitation of $\varepsilon_f \leq 0.01$. In the experiments, the upgrading and degrading channel construction of polar codes [31,32] is used to determine the frozen vector of polar codes. The number of sub-blocks $m$ and length of CRC $d$ are both set as 32 and the list size of BC-SCL decoder $l$ is set as 16, so
that $\varepsilon$-correctness of SLA scheme is calculated as the level of $10^{-8}$ with $\varepsilon_{II} = 10^{-6}$. Meanwhile, the correction threshold of LDPC codes [8] is directly used to evaluate the efficiency of the acknowledgment reconciliation. We collected the sifted key from the QKD network [33], and extended the collected data with the targeted length and QBER as the sifted key used in experiment.

The sifted key used in the experiment is collected from the QKD network experiment [33], and extended to the targeted length and QBER.

The SLA IR scheme is tested for 10,000 times each round with QBER ranging from 0.01 to 0.12 with interval of 0.01, block length of 1 Mb, 16 Mb, 128 Mb. The experimental results of the $\varepsilon_f$, the reconciliation efficiency $f$ and average yield $\gamma$ are shown in Table 2. In particular, the leaked information used for calculating the efficiency is accumulated from all tests instead of one test for the different error sub-blocks in the forward reconciliation. Meanwhile, we have tested the SLA IR scheme for three practical cases [33–35] and the performance is shown in Appendix section.

The efficiency $f$ of the SLA IR scheme is 1.205, 1.114, 1.091 when the block length is 1 Mb, 16 Mb, 128 Mb, respectively. When the block length increases to 128 Mb, the $f$ and $\gamma$ of our SLA IR scheme are much more efficient than the previous polar codes-based IR schemes shown in Table 1. Meanwhile, the efficiency increases and the $\varepsilon_f$ decreases as block length is increased to 1 Mb, 16 Mb and 128 Mb. Moreover, the SLA IR scheme runs around 167 h on a personal computer with the block length $n = 1$ Gb, $E_{\mu} = 0.02$, resulting the efficiency of 1.055 and $\varepsilon_f$ less than $10^{-2}$. As shown in Table 2, performance of polar codes-based IR schemes can be improved by increasing the block lengths; however, the implementation of large-scale decoders will result in huge computational complexity, which may destroy the system availability. Therefore, with limited block lengths, our SLA IR scheme can be performed to further improve both the reconciliation efficiency and the correctness of QKD systems.

![Fig. 4](image_url) The yield of efficiency $\mathcal{Y}(\epsilon)$ when QBER is 0.02
### Table 2  The experimental result of the SLA IR scheme

| $E_{\mu}$ | $n=1$ Mb |       |       | $n=16$ Mb |       |       | $n=128$ Mb |       |
|----------|----------|-------|-------|----------|-------|-------|------------|-------|
|         | $f$      | $\varepsilon_f$ | $\gamma$ | $f$      | $\varepsilon_f$ | $\gamma$ | $f$      | $\varepsilon_f$ | $\gamma$ |
| 0.01     | 1.205    | 0.0164 | 0.903 | 1.114    | 0.0032 | 0.910 | 1.091 | $\leq 10^{-4}$ | 0.912 |
| 0.02     | 1.146    | 0.0050 | 0.838 | 1.087    | 0.0138 | 0.847 | 1.073 | $\leq 10^{-4}$ | 0.848 |
| 0.03     | 1.124    | 0.0163 | 0.782 | 1.087    | 0.0005 | 0.789 | 1.062 | 0.0011 | 0.794 |
| 0.04     | 1.116    | 0.0072 | 0.730 | 1.072    | 0.0048 | 0.740 | 1.059 | 0.0033 | 0.743 |
| 0.05     | 1.107    | 0.0046 | 0.683 | 1.070    | 0.0022 | 0.694 | 1.055 | $\leq 10^{-4}$ | 0.698 |
| 0.06     | 1.099    | 0.0040 | 0.640 | 1.062    | 0.0050 | 0.652 | 1.049 | 0.0067 | 0.657 |
| 0.07     | 1.101    | 0.0012 | 0.597 | 1.066    | 0.0004 | 0.610 | 1.050 | $\leq 10^{-4}$ | 0.616 |
| 0.08     | 1.104    | 0.0026 | 0.556 | 1.064    | 0.0001 | 0.572 | 1.048 | $\leq 10^{-4}$ | 0.579 |
| 0.09     | 1.092    | 0.0037 | 0.523 | 1.056    | 0.0007 | 0.539 | 1.044 | 0.0015 | 0.544 |
| 1.0      | 1.083    | 0.0064 | 0.492 | 1.062    | $\leq 10^{-4}$ | 0.502 | 1.042 | $\leq 10^{-4}$ | 0.511 |
| 0.11     | 1.079    | 0.0024 | 0.461 | 1.057    | $\leq 10^{-4}$ | 0.472 | 1.039 | 0.0050 | 0.481 |
| 0.12     | 1.072    | 0.0043 | 0.433 | 1.056    | $\leq 10^{-4}$ | 0.441 | 1.037 | 0.0013 | 0.451 |

### 5 Conclusion

In this article, we propose a Shannon-limit approached (SLA) information reconciliation (IR) scheme based on polar codes in quantum key distribution (QKD) systems, which achieves high reconciliation efficiency and decreases the overall IR failure probability to $10^{-8}$. The proposed SLA IR scheme mainly consists of two phases: the forward reconciliation phase and the acknowledgment reconciliation phase. In the forward reconciliation phase, the sifted key is divided into sub-blocks and performed with the improved block checked successive cancellation list decoder, where errors can be efficient located and corrected in each sub-block. Afterward, the additional acknowledgment reconciliation phase is performed to the failure corrected sub-blocks. The experimental results show that the overall failure probability of the SLA IR scheme is decreased to $10^{-8}$ and the efficiency is improved to 1.091 with the IR block length of 128 Mb. Therefore, with limited block lengths, our SLA IR scheme can be performed to further improve both the reconciliation efficiency and the correctness of QKD systems. The SLA IR scheme achieves the efficiency of 1.055 with quantum bit error rate of 0.02, when the input scale length increased to 1 Gb, which is hundred times larger than the state-of-the-art implemented polar codes-based IR schemes.

**Acknowledgements**  This work was supported in part by the National Natural Science Foundation of China under Grant No. 61972410 and the research plan of National University of Defense Technology under Grant No. ZK19-13.

**Author contributions**  BYT and BL proposed the scheme, performed the experiments, wrote the paper and contributed equally. This work was conceived by BL and WRY, supervised by WRY and co-supervised by CQW. All authors reviewed the manuscript.
Compliance with ethical standards

Conflict of interest The authors declare no competing interests.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article’s Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article’s Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

Appendix

Our SLA IR scheme can be directly adapted into the practical QKD systems. And we tested the performance of the SLA IR scheme for three practical cases [33–35].

In article [34], the QKD system generated keys with the length of about 0.5Mb and the QBER of 0.005. Thus, we tested our SLA IR scheme with QBER of 0.005 and input length of 0.5Mb, and the reconciliation efficiency reaches to 1.315. Meanwhile, our SLA IR scheme reaches the efficiency of 1.273, 1.168 and 1.084 with the input length of 1Mb, 16Mb and 128Mb, respectively, when the QBER is 0.005. Table 3 shows the experimental results of the SLA IR scheme when the QBER is 0.005.

In Ref. [35], the length of the sifted key is about 7Mb, the reconciliation efficiency is set as 1.16 and the final secure key rate is calculated as 1.29 × 10⁻⁷ bits/pulse when QBER is about 0.028 and the total loss is 28.0 dB. We tested the reconciliation efficiency of the SLA IR scheme with the QBER of 0.028 and the input length of 1Mb. The SLA IR scheme improves the efficiency to 1.141, so that the final secure key rate is improved to 1.3038 × 10⁻⁷ bits/pulse with the same parameter used in Ref. [35].

Table 3 The experimental results of the SLA IR scheme when the QBER is 0.005

|  | n   | 0.5Mb | 1Mb  | 16Mb | 128Mb |
|---|-----|-------|------|------|-------|
| f | 1.315 | 1.273 | 1.168 | 1.084 |

Table 4 QBER between each pair of users in Ref. [33]

| $E_{\mu}$ | Bob  | Chloe | Dave | Feng  | Gopi  | Heidi | Ivan |
|----------|------|-------|------|-------|-------|-------|------|
| Alice    | 0.045| 0.066 | 0.085| 0.042 | 0.075 | 0.034 | 0.043|
| Bob      | 0.059| 0.044 | 0.035| 0.034 | 0.040 | 0.044 |      |
| Chloe    |      | 0.076 | 0.039| 0.073 | 0.051 | 0.070 |      |
| Dave     |      |       | 0.078| 0.071 | 0.087 | 0.071 |      |
| Feng     |      |       |     | 0.042 | 0.048 | 0.049 |      |
| Gopi     |      |       |     |       | 0.055 | 0.055 |      |
| Heidi    |      |       |     |       |       | 0.040 |      |
Afterward, we performed the SLA IR scheme to correct the sifted key with the length of 16 Mb and the QBER shown in Table 4, which is collected from the QKD network experiment [33]. In our experiments, the frozen vectors are optimized for the IR block size of 16 Mb and the constant QBER (upper thresholds) with the interval of 0.01. In practical QKD systems, the sifted key with the measured QBER $E_\mu$ is corrected by the polar code optimized with the closest upper threshold.

Table 5 shows the reconciliation efficiency results between each pair of users. Partial pairs of users suffer worse reconciliation efficiency than the experimental results shown in Table 2. For example, the reconciliation efficiency between Alice and Feng drops to 1.2190 when the QBER of the sifted key is 0.042 and the frozen vector used has the correction threshold of 0.05. Thus, the reconciliation efficiency can be further improved by the frozen vectors for constant QBER with smaller intervals.

### References

1. Lo, H.K., Curty, M., Tamaki, K.: Secure quantum key distribution. Nat. Photonics 8, 595 (2014). https://doi.org/10.1038/nphoton.2014.149
2. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N.J., Duek, M., Ltenhaus, N., Peev, M.: The security of practical quantum key distribution. Rev. Mod. Phys. 81(3), 1301 (2009). https://doi.org/10.1103/RevModPhys.81.1301
3. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Quantum cryptography. Rev. Mod. Phys. 74(1), 145 (2002). https://doi.org/10.1103/RevModPhys.74.145
4. Martinez-Mateo, J., Elkouss, D., Martin, V.: Key reconciliation for high performance quantum key distribution. Sci. Rep. 3, 1576 (2013). https://doi.org/10.1038/srep01576
5. Brassard, G., Salvail, L.: Secret-key reconciliation by public discussion. In: Workshop on the Theory and Application of of Cryptographic Techniques. Springer, pp. 410–423 (1993)
6. Bennett, C.H., Bessette, F., Brassard, G., Salvail, L., Smolin, J.: Experimental quantum cryptography. J. Cryptol. 5(1), 3 (1992)
7. Yan, H., Ren, T., Peng, X., Lin, X., Jiang, W., Liu, T., Guo, H.: Information reconciliation protocol in quantum key distribution system. In: 2008 Fourth International Conference on Natural Computation, vol. 3, pp. 637–641. IEEE (2008)
8. Elkouss, D., Leverrier, A., Alloatme, R., Bourots, J.J.: Efficient reconciliation protocol for discrete-variable quantum key distribution. In: 2009 IEEE International Symposium on Information Theory, pp. 1879–1883 (2009). https://doi.org/10.1109/ISIT.2009.5205475
9. Li, Q., Wen, X., Mao, H., Wen, X.: An improved multidimensional reconciliation algorithm for continuous-variable quantum key distribution. Quantum Inf. Process. 18(1), 25 (2018). https://doi.org/10.1007/s11128-018-2126-0
10. Jouguet, P., Kunz-Jacques, S.: High performance error correction for quantum key distribution using polar codes. Quantum Info. Comput. 14(3–4), 329 (2014)

11. Yan, S.L., Wang, J.D., Fang, J.B., Jiang, L., Wang, X.: An improved polar codes-based key reconciliation for practical quantum key distribution. Chin. J. Electron. 27(2), 250 (2018). https://doi.org/10.1049/cje.2017.07.006

12. Nakassis, A., Mink, A.: Polar codes in a QKD environment. In: SPIE Sensing Technology + Applications, vol. 9123. SPIE (2014). https://doi.org/10.1117/12.2050919

13. Arikan, E.: Channel polarization: a method for constructing capacity-achieving codes. In: 2008 IEEE International Symposium on Information Theory, pp. 1173–1177 (2013). https://doi.org/10.1109/ISIT.2008.4595172

14. Arikan, E.: Channel polarization: a method for constructing capacity-achieving codes for symmetric binary-input memoryless channels. IEEE Trans. Inf. Theory 55(7), 3051 (2009). https://doi.org/10.1109/TIT.2009.2021379

15. Mori, R., Tanaka, T.: Performance and construction of polar codes on symmetric binary-input memoryless channels. In: 2009 IEEE International Symposium on Information Theory, pp. 1496–1500 (2009). https://doi.org/10.1109/ISIT.2009.5205857

16. Lee, S., Heo, J.: Efficient reconciliation protocol with polar codes for quantum key distribution. In: 2018 Tenth Conference on Ubiquitous and Future Networks (ICUFN), pp. 40–43 (2018). https://doi.org/10.1109/ICUFN.2018.8436787

17. Tang, B.Y., Liu, B., Zhai, Y.P., Wu, C.Q., Yu, W.R.: High-speed and large-scale privacy amplification scheme for quantum key distribution. Sci. Rep. 9(1), 15733 (2019). https://doi.org/10.1038/s41598-019-50290-1

18. Cai, R.Y., Scarani, V.: Finite-key analysis for practical implementations of quantum key distribution. New J. Phys. 11(4), 045024 (2009)

19. Pedersen, T.B., Toyran, M.: High performance information reconciliation for QKD with CASCADE. arXiv preprint arXiv:1307.7829 (2013)

20. Mateo, J.M.: Efficient information reconciliation for quantum key distribution = reconciliacin eficiente de informacin para la distribucin cuntica de claves. Doctoral thesis, Universidad Politcnica de Madrid (2011). http://oa.upm.es/9717/

21. Miller-Quade, J., Renner, R.: Composability in quantum cryptography. New J. Phys. 11(8), 085006 (2009). https://doi.org/10.1088/1367-2630/11/8/085006

22. Tal, I., Vardy, A.: List decoding of polar codes. In: 2011 IEEE International Symposium on Information Theory Proceedings, pp. 1–5 (2011). https://doi.org/10.1109/ISIT.2011.6033904

23. Niu, K., Chen, K.: CRC-aided decoding of polar codes. IEEE Commun. Lett. 16(10), 1668 (2012). https://doi.org/10.1109/LCOMM.2012.090312.121501

24. Wang, T., Qu, D., Jiang, T.: Parity-check-concatenated polar codes. IEEE Commun. Lett. 20(12), 2342 (2016). https://doi.org/10.1109/LCOMM.2016.2607169

25. Hashemi, S.A., Condo, C., Gross, W.J.: Fast simplified successive-cancellation list decoding of polar codes. In: 2017 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), pp. 1–6 (2017). https://doi.org/10.1109/WCNWC.2017.7919044

26. Hashemi, S.A., Condo, C., Gross, W.J.: Simplified successive-cancellation list decoding of polar codes. In: 2016 IEEE International Symposium on Information Theory (ISIT), pp. 815–819 (2016). https://doi.org/10.1109/ISIT.2016.7541412

27. Hashemi, S.A., Condo, C., Gross, W.J.: Fast and flexible successive-cancellation list decoders for polar codes. IEEE Trans. Signal Process. 65(21), 5756 (2017). https://doi.org/10.1109/TSP.2017.2740204

28. Chen, K., Li, B., Shen, H., Jin, J., Tse, D.: Reduce the complexity of list decoding of polar codes by tree-pruning. IEEE Commun. Lett. 20(2), 204 (2016). https://doi.org/10.1109/LCOMM.2015.2506568

29. Chen, J., Fan, Y., Xia, C., Tsui, C., Jin, J., Chen, K., Li, B.: Low-complexity list successive-cancellation decoding of polar codes using list pruning. In: 2016 IEEE Global Communications Conference (GLOBECOM), pp. 1–6 (2016). https://doi.org/10.1109/GLOCOM.2016.7841969

30. Balatsoukas-Stimming, A., Parizi, M.B., Burg, A.: LLR-based successive cancellation list decoding of polar codes. IEEE Trans. Signal Process. 63(19), 5165 (2015). https://doi.org/10.1109/TSP.2015.2439211

31. Tal, I., Vardy, A.: How to construct polar codes. IEEE Trans. Inf. Theory 59(10), 6562 (2013). https://doi.org/10.1109/TIT.2013.2272694

32. Tang, B.Y.: The implementation of upgrading channels for construction of polar code. https://github.com/cfxtby/PolarCodeForQKD. Accessed 2 Jan (2020)
33. Joshi, S.K., Aktas, D., Wengerowsky, S., Lonari, M., Neumann, S.P., Liu, B., Scheidl, T., Samec, K.L., Qiu, A.: A trusted-node-free eight-user metropolitan quantum communication network. arXiv preprint arXiv:1907.08229 (2019)

34. Liu, Y., Chen, T.Y., Wang, L.J., Liang, H., Shentu, G.L., Wang, J., Cui, K., Yin, H.L., Liu, N.L., Li, L., Ma, X., Pelc, J.S., Fejer, M.M., Peng, C.Z., Zhang, Q., Pan, J.W.: Experimental measurement-device-independent quantum key distribution. Phys. Rev. Lett. 111(13), 130502 (2013). https://doi.org/10.1103/PhysRevLett.111.130502

35. Wei, K., Li, W., Tan, H., Li, Y., Min, H., Zhang, W., Li, H., You, L., Wang, Z., Jiang, X.: High-speed measurement-device-independent quantum key distribution with integrated silicon photonics. arXiv: Quantum Physics (2019)

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