Polar-code-based information reconciliation scheme with the frozen-bit erasure strategy for quantum key distribution

Bang-Ying Tang,[1] Chun-Qing Wu,[2] Wei Peng,[1] Bo Liu,[3,*] and Wan-Rong Yu[1,†]

[1] *College of Computer Science and Technology, National University of Defense Technology, Changsha 410073, China*
[2] *School of Electronics and Communication Engineering, Sun Yat-sen University, Shenzhen 518100, China*
[3] *College of Advanced Interdisciplinary Studies, National University of Defense Technology, Changsha 410073, China*

(Received 6 March 2022; accepted 5 January 2023; published 19 January 2023)

Information reconciliation (IR) ensures the correctness of quantum key distribution systems by correcting the error bits that existed in the sifted keys. In this article, we propose a polar-code-based IR scheme with the frozen-bit erasure strategy, where an equivalent transmission of sifted keys is conducted so that each frozen bit in the decoding procedure is erased to zero. Thus, our IR scheme is no longer limited by the assumption of true random numbers and can be implemented simply and efficiently. Furthermore, we implement the proposed IR scheme with the fast simplified successive-cancellation list decoder and its throughput reaches 0.68 Mbps with the yield of 0.8333; when the decoder list size is 16, the block size is 1 Mb and the quantum bit error rate is 0.02.

DOI: 10.1103/PhysRevA.107.012612

I. INTRODUCTION

Quantum key distribution (QKD) can provide information-theoretically-secure keys for distant users [1]. After the quantum communication phase and basis sifting procedure, the users (Alice and Bob) generate the sifted keys (K_s^A and K_s^B). However, these contain errors in realistic QKD systems [2]. Information reconciliation (IR) ensures the correctness of QKD systems by correcting the error bits with exchanged syndrome information via a classical channel and, finally, returns the corrected bit string $K_{\rm IR}$ [3]. IR is widely applied to various secure communication scenarios, such as physical layer security [4–7], underwater acoustic communication [8,9], and so on.

IR schemes mainly contain interactive IR schemes and one-way IR schemes [7]. The interactive IR schemes (BBBSS and Cascade) have limited applications due to the heavy communication latency, although they reach high efficiency [3,10–12]. The one-way IR schemes are based on the forward error correction codes, e.g., Turbo codes, low-density parity-check (LDPC) codes, and polar codes [12–14]. An LDPC-code-based IR scheme is widely applied in the QKD systems and can achieve high efficiency when the error correction matrix corresponding to the quantum bit error rate (QBER) is used. Nevertheless, it is impossible to generate the error correction matrix in real time for arbitrary QBER and the efficiency is limited by the mismatched error correction matrices [12,15]. Recently, polar codes have been applied to IR for the following advantages: The potential to reach the Shannon limit and the low complexity $O(n\log n)$ of the encoding (decoding) procedure [16,17].

The first polar-code-based IR scheme was proposed by Jouguet and Kunz-Jacques and reached the efficiency of 1.121 and the failure probability of 0.08 with the successive-cancellation (SC) decoder when the QBER is 0.02 and the block size is 16 Mb [14]. Then, three configuration strategies were developed to adapt the polar codes into IR schemes: Direct decoding (DD), bits flipping decoding (BFD), and length-adaptive BFD [18]. The DD and BFD strategies, having a higher efficiency than the length-adaptive BFD strategy, are widely used in the polar-code-based IR schemes. Using the DD strategy, the efficiency of 1.176 and the failure probability of 0.001 were achieved by the further improved polar-code-based IR schemes with the successive-cancellation list (SCL) decoder, the list size of 16, and the QBER of 0.02 [18,19]. In our previous work [20], we proposed a polar-code-based feedback IR scheme (with the BFD strategy), which decreased the failure probability to 10^{-8} with the efficiency of 1.055 when the list size of the SCL decoder is 16, the block size is 1 Gb, and the QBER is 0.02. Nevertheless, the throughput of the polar-code-based IR scheme is limited by inefficient implementations. The polar-code-based IR scheme with the BFD strategy can be implemented with the efficient decoder whose frozen bits are constant (usually fixed to zero), such as the simplified SC decoder, the fast simplified SCL (FSSCL) decoder, and so on [18,21]. However, true random numbers (TRNs) are indispensable to the polar-code-based IR scheme with the BFD strategy, which would increase the complexity of the practical systems and might open security loopholes with the inappropriate implementation [22].

In this article, we propose the polar-code-based IR scheme with the frozen-bit erasure (FBE) strategy, which can be implemented efficiently without the TRNs. The proposed IR scheme mainly contains two phases: The equivalent transmission of sifted keys with FBE strategy and the error bits correction of the equivalent sifted keys. In the former, Alice distills the syndrome vector W and sends W to Bob via the

[*] liubo08@nudt.edu.cn
[†] wlyu@nudt.edu.cn

classical channel. Alice and Bob both conduct the "XOR" operation between the sifted keys and the encoded vector of W to generate a new couple of vectors (X and X'). In the latter, Alice extracts the key K_{IR}^{A} by encoding X and sends the cyclic redundancy check (CRC) value of K_{IR}^{A} to Bob. Bob decodes the generated vector X' to U' with the received CRC value and the frozen bits of zero. Afterwards, Bob extracts the key K_{IR}^{B} from U'. Compared with the existing IR schemes performing the DD and BFD strategies, our proposed polar-code-based IR scheme with the FBE strategy can adapt the low-computational-complexity decoder and remove the assumption of TRN simultaneously. Furthermore, we implemented our IR scheme with the FSSCL decoder on a commercial computer. The implementation reaches the throughput of 0.68 Mbps and the yield of 0.8333 (efficiency of 1.176 and failure probability of 0.0004) with the decoder list size of 16, the block size of 1 Mb, and the QBER of 0.02.

II. RELATED WORKS

A. Information reconciliation

In quantum key distribution (QKD) systems, the communication parties (Alice and Bob) gain the sifted keys (K_s^A and K_s^B) of length n after the quantum communication and key and basis sifting procedures [23–25]. However, the imperfection of the QKD systems causes the error bits between the sifted keys in the quantum communication procedure [26–29]. Assume the quantum bit error rate is E.

Alice and Bob exchange the syndrome string S via the classical channel and correct the sifted keys to the weak secure keys (K_{IR}^{A} and K_{IR}^{B}) in the information reconciliation (IR) procedure [3,29]. The failure probability ε represents the correctness of IR as [14]

$$\varepsilon \geqslant \Pr\left(K_{\mathrm{IR}}^{A} \neq K_{\mathrm{IR}}^{B}\right). \tag{1}$$

Assume $K_{\mathrm{IR}} = K_{\mathrm{IR}}^{A} = K_{\mathrm{IR}}^{B}$, when the IR procedure is conducted successfully. The syndrome S through the classical channel discloses partial information of the key and decreases the secure key rate. The leaked information is represented by the efficiency of IR, defined as [7]

$$f(E) = \frac{I(S;K_{\mathrm{IR}})}{nH_2(E)}, \tag{2}$$

where $I(S;K_{\mathrm{IR}})$ is the mutual information between S and K_{IR}, and $H_2(x)$ is the binary Shannon entropy as

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

Furthermore, the yield γ of each sifted bit evaluates the performance of the IR scheme and is calculated as [18,20]

$$\gamma = (1-\varepsilon)[1 - f(E)H_2(E)]. \tag{4}$$

B. Polar codes

Polar codes, invented by Arikan in 2008, have the potential to reach the Shannon limit of binary discrete memoryless channels (B-DMC) in theory [16,17]. In polar codes, transmitting the n-bit vector in the B-DMC is regarded as transmitting the bits in n copies of B-DMC, respectively ($n = 2^m, m \in \mathbf{N}^+$). The n copies of B-DMC are polarized to a new set of bit channels composed of k error-free ("good") channels and $n-k$ noisy ("bad") channels. The bits at the error-free (noisy) channels are called information (frozen) bits. The positions of the frozen bits can be determined according to the channel capacity, the Bhattacharyya parameter, or the error probability of each polarized channel [17,30]. Frozen vector $V = [v_0, v_1, \ldots, v_{n-1}]$ is usually used to represent the positions of the frozen bits, where $v_i = 0$ ($v_i = 1$) means the position i is the information (frozen) bit.

In the encoding procedure of the polar codes, k information bits and $n-k$ preshared frozen bits are filled into error-free positions and noisy positions of an n-length vector U, respectively. Usually, the frozen bits are set to zero. Then, U is encoded to a codeword X as

$$X = UG_n = UF^{\otimes m}B_n, \tag{5}$$

where G_n is the generation matrix of polar codes, $F = \left[\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right]$, $F^{\otimes m}$ represents the m-fold Kronecker product of F, and B_n is the permutation matrix for bit-reversal operation. G_nG_n is an identity matrix I_n [31]. In the encoding, the calculations are Boolean calculations. Afterwards, the codeword X is sent through the B-DMC.

The receiver gets the measured codeword as X' from B-DMC. The received codeword X' can be decoded to U with the preshared frozen bits.

Arikan *et al.* first proposed the successive-cancellation (SC) decoder, whose complexity is $O(n\log n)$ [17]. Then, the successive-cancellation list (SCL) decoder was proposed to decrease the frame error rate with the complexity of $O(Ln\log n)$, where L is the list size [32]. In the SC and SCL decoding, the recursion decoding of the constituent code can be simplified with the constant frozen bits [33,34]. And some efficient decoders are developed from SC and SCL decoders with the same correction performance, e.g., simplified successive-cancellation decoder [33], simplified successive-cancellation list decoder [34], and fast simplified successive-cancellation list (FSSCL) decoder [21]. In addition, the hardware-based decoders of polar codes with constant frozen bits were improved to reach the throughput of 237 Gbps [35].

C. Polar-code-based information reconciliation strategies

IR is essentially the same as Slepian-Wolf compression, which can be implemented with polar codes [36,37]. Then, the polar-code-based IR schemes were proposed with three configuration strategies [14,18]. These strategies guide how to adopt polar codes into IR schemes and comprise the direct decoding (DD) strategy, the bits flipping decoding (BFD) strategy, and the length-adaptive BFD strategy [18]. The length-adaptive BFD strategy is suitable for any input length, but has a lower efficiency than the DD and BFD strategies. In QKD systems, the input length of IR can be fixed to 2^m ($m \in \mathbf{N}^+$), so that the polar-code-based IR schemes are mainly based on the DD strategy and the BFD strategy to achieve high efficiency. Figure 1 shows the diagram of the DD and BFD strategies.

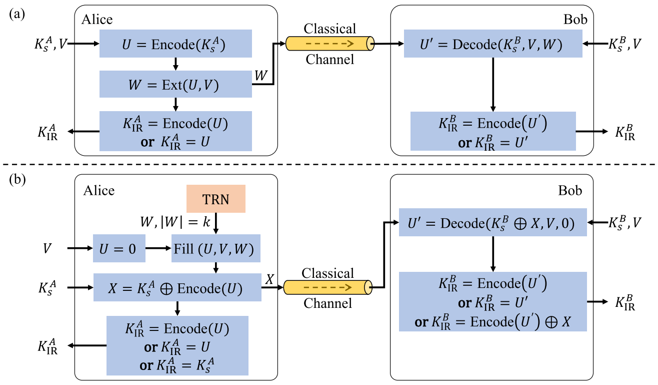
(a)
Alice
K_s^A, V
$U = \text{Encode}(K_s^A)$
$W = \text{Ext}(U,V)$
W
$K_{\text{IR}}^A = \text{Encode}(U)$ or $K_{\text{IR}}^A = U$
K_{IR}^A
Classical
Channel
Bob
$U' = \text{Decode}(K_s^B, V, W)$
K_s^B, V
$K_{\text{IR}}^B = \text{Encode}(U')$ or $K_{\text{IR}}^B = U'$
K_{IR}^B
(b)
Alice
TRN
$W, |W| = k$
V
$U = 0$
Fill (U,V,W)
K_s^A
$X = K_s^A \oplus \text{Encode}(U)$
X
$K_{\text{IR}}^A = \text{Encode}(U)$ or $K_{\text{IR}}^A = U$ or $K_{\text{IR}}^A = K_s^A$
K_{IR}^A
Classical
Channel
Bob
$U' = \text{Decode}(K_s^B \oplus X, V, 0)$
K_s^B, V
$K_{\text{IR}}^B = \text{Encode}(U')$ or $K_{\text{IR}}^B = U'$ or $K_{\text{IR}}^B = \text{Encode}(U') \oplus X$
K_{IR}^B

FIG. 1. The diagram of polar-code-based IR schemes with (a) DD strategy and (b) BFD strategy. The block size is n and the length of information bits is k. V is the frozen vector precalculated according to QBER E. TRN means true random number. Encode(U) represents encoding U to UG_n. $U = \text{Decode}(X, V, Y)$ represents decoding X to U with the frozen vector of V and the frozen bits value of Y. In (a), $W = \text{Ext}(U, V)$ represents extracting a vector W from U, W is composed of the elements u_i when $v_i = 1$, $U = [u_0, u_1, \dots, u_{n-1}]$, and $V = [v_0, v_1, \dots, v_{n-1}]$. In (b), W is composed of the k random bits. Fill(U, V, W) means filling W into the information bits of U when V is the frozen vector.

In the DD strategy, the frozen vector is preshared by the communication parties (Alice and Bob), and the length of the sifted keys n is 2^m, $m \in \mathbf{N}^+$. Alice encodes K_s^A to U and sends the frozen bits of U to Bob. Bob directly decodes K_s^B to U' with the received frozen bits. Alice (Bob) chooses U (U') or K_s^A ($U'G_n$) as K_{IR}, respectively. When K_{IR} is U (U'), the frozen bits of U (U') can be discarded directly. The frozen bits in decoding are determined by K_s^A and vary in each run. Thus, the DD strategy cannot adapt the improved efficient decoders that require constant frozen bits.

In the BFD strategy, the input length n is 2^m and the frozen vector is V. Alice generates a vector U whose frozen bits are zero and information bits are true random bits. Afterwards, Alice calculates X as Encode(U) $\oplus K_s^A$ and sends X to Bob. Bob decodes the vector $X \oplus K_s^B$ to U' with the frozen bits zero. Alice (Bob) has three choices of K_{IR}: U (U'), UG_n ($U'G_n$), and K_s^A ($U'G_n \oplus X$). The BFD strategy can be accelerated by the efficient decoders and is widely used in the recent polar-code-based IR schemes [20,38]. However, the generation of true random numbers (TRNs) would increase the complexity of systems and might open security loopholes with inappropriate implementation. In addition, n syndrome bits are transmitted via a public channel, which increases the overload of the public channel.

III. POLAR-CODE-BASED IR SCHEME WITH THE FBE STRATEGY

Polar codes are employed in IR for the following advantages: The potential to achieve Shannon-limit efficiency, and low complexity $O(n \log n)$ of the encoding and decoding procedure [16,17]. However, the previous polar-code-based IR schemes cannot be accelerated by efficient decoders without TRNs. In this article, we propose the frozen-bit erasure (FBE) strategy to address this issue and design an IR scheme based on the FBE strategy.

TABLE I. Feature comparison of the DD, BFD, and FBE strategies.

Strategy	Complexity	Syndrome bits	Frozen bits	With TRNs?
DD	$O(n \log n)$	$n - k$	Variable	No
BFD	$O(n \log n)$	n	Constant	Yes
FBE	$O(n \log n)$	$n - k$	Constant	No

Before the IR procedure, Alice and Bob generate the sifted keys (K_s^A and K_s^B) of length n ($n = 2^m$, $m \in \mathbf{N}^+$), respectively, estimate the QBER as E, and preshare the frozen vector V, which represents the positions of k information bits and $n - k$ frozen bits. The following calculations are Boolean calculations.

Definition 1. Ext(U, V) represents the vector composed of the elements u_i when $v_i = 1$, $U = [u_0, u_1, \dots, u_{n-1}]$, and $V = [v_0, v_1, \dots, v_{n-1}]$.

A. Frozen-bit erasure strategy

In our proposed FBE strategy, Alice calculates syndrome vector W as

$$W = \text{Encode}\big(K_s^A\big) \wedge V = K_s^A G_n \wedge V. \tag{6}$$

Then, Alice sends the vector W to Bob via the classical channel. Afterwards, Alice generates a novel codeword X as

$$X = K_s^A \oplus W G_n. \tag{7}$$

Bob receives the syndrome vector W. Then, Bob encodes the vector W and generates a codeword X' with error bits as

$$X' = K_s^B \oplus W G_n. \tag{8}$$

According to Eqs. (6) and (7), the codeword X can be further calculated as

$$\begin{aligned} X &= K_s^A \oplus \big(K_s^A G_n \wedge V\big) G_n = K_s^A G_n G_n \oplus \big(K_s^A G_n \wedge V\big) G_n \\ &= \big[\big(K_s^A G_n\big) \oplus \big(K_s^A G_n \wedge V\big)\big] G_n = \big(K_s^A G_n \wedge \neg V\big) G_n. \end{aligned} \tag{9}$$

Assume $U = \text{Encode}(X)$. According to Eq. (9), U equals $K_s^A G_n \wedge \neg V$ for $G_n G_n = I_n$ and the frozen bits of U are zero.

The positions of error bits between X and X' are the same as K_s^A and K_s^B. Thus, the errors between X and X' can be corrected by decoding X' with the frozen bits zero of U. Assume the decoded vector is U'. U' equals U when the decoding procedure is conducted successfully.

The users can choose the information bits of U and U' as the output weak secure keys.

In the realistic implementation, Alice only needs to transmit $n - k$ frozen bits of W via the classical channel and Bob can reconstruct W with the received $n - k$ bits and the frozen vector V. Table I shows the feature comparison of the DD, BFD, and FBE strategies.

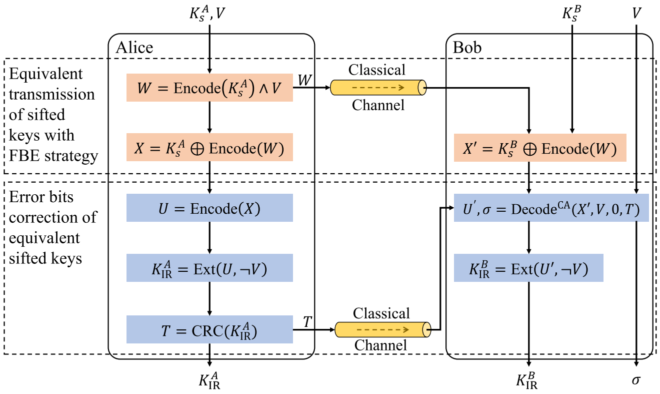
K_s^A, V
K_s^B
V
Alice
Bob
Equivalent transmission of sifted keys with FBE strategy
$W = \text{Encode}(K_s^A) \wedge V$
W
Classical
Channel
$X = K_s^A \oplus \text{Encode}(W)$
$X' = K_s^B \oplus \text{Encode}(W)$
Error bits correction of equivalent sifted keys
$U = \text{Encode}(X)$
$U', \sigma = \text{Decode}^{\text{CA}}(X', V, 0, T)$
$K_{\text{IR}}^A = \text{Ext}(U, \neg V)$
$K_{\text{IR}}^B = \text{Ext}(U', \neg V)$
$T = \text{CRC}(K_{\text{IR}}^A)$
T
Classical
Channel
K_{IR}^A
K_{IR}^B
σ

FIG. 2. The diagram of the polar-code-based IR scheme with FBE strategy. $Y = \text{Ext}(U, V)$ represents extracting the vector Y, which is composed of the elements u_i when $v_i = 1$, $U = [u_0, u_1, \ldots, u_{n-1}]$, and $V = [v_0, v_1, \ldots, v_{n-1}]$. $T = \text{CRC}(X)$ represents calculating the CRC value T of vector X. $U, \sigma = \text{Decode}^{\text{CA}}(X, V, 0, T)$ represents conducting the CRC-aided decoding procedure on the codeword X with the CRC value of T, the frozen vector of V, and the frozen bits of zero, and output the decoded vector U and the decoding flag σ, which represents whether X is decoded successfully.

B. The IR Scheme with FBE strategy

Based on the proposed FBE strategy, we designed a polar-code-based IR scheme, which contains two phases: Equivalent transmission of sifted keys with FBE strategy and error bits correction of equivalent sifted keys. In the scheme, the cyclic redundancy check (CRC) [39] is used to check whether the errors are corrected successfully. The diagram of this IR scheme is shown in Fig. 2. Before the IR procedure, Alice and Bob preshare the CRC length d and the frozen vector V via the classical channel.

Equivalent transmission of sifted keys with FBE strategy. Alice distills the syndrome vector W according to Eq. (6) and calculates the codeword vector X as Eq. (7). Then, Alice sends the syndrome vector W to Bob via the classical channel. Bob receives the vector W and calculates the codeword X' as Eq. (8).

Error bits correction of equivalent sifted keys. Alice encodes codeword X to vector U and extracts the information bits of X as K_{IR}^A. Then, Alice calculates the CRC value T of K_{IR}^A and sends T to Bob through the classical channel. Bob performs a CRC-aided (CA) decoding procedure to decode X' to U' and output the decoding flag σ with the CRC value T and frozen vector V [40]. Afterwards, Bob extracts the information bits of U' as K_{IR}^B and notifies Alice whether the IR procedure is conducted successfully via the classical channel.

In the CA decoding procedure, the decoder generates multiple temporary decoded vectors. The temporary vectors are CRC checked one by one until one of them passes the CRC checking. If there is a temporary vector U' that passes the CRC checking, then the output is vector U' and decoding flag $\sigma = 1$. If no temporary vectors pass the CRC checking, then the output $U' = \varnothing$ and $\sigma = 0$ [40].

In the realistic implementation, the procedures at Alice's side can be simplified as (1) encode K_s^A to vector Y, (2) generate the syndrome vector $W = Y \wedge V$ and send W to Bob, (3) extract the information bits of Y as $K_{\text{IR}}^A = \text{Ext}(Y, \neg V)$, and (4) calculate the CRC value $T = \text{CRC}(K_{\text{IR}}^A)$ and send to Bob.

TABLE II. Experimental environment settings.

	Parameters	Value
Polar codes	Block size	1 Mb
	CRC length	32
	Decoder	FSSCL decoder [21]
	Construction	Upgrading and degrading method [30]
Computer	Operation System	Windows 10
	CPU	Intel I5-9300H
	Cores per CPU	4
	Treads per core	2
	Memory	16 GB
	Programming language	C++
	Compiler	VISUAL STUDIO 2019

In our IR scheme, the leakage syndrome information S contains the CRC value T and the frozen bits of W (the information bits of W are zero). The mutual information $I(K_{\text{IR}}; S)$ is less than the Shannon entropy $H(S)$. And $H(S) \leqslant n - k + d$ because the total length of S is $n - k + d$. Thus, the reconciliation efficiency of our scheme is calculated as

$$f(E) = \frac{I(S; K_{\text{IR}})}{nH_2(E)} \leqslant \frac{n - k + d}{nH_2(E)}. \tag{10}$$

IV. PERFORMANCE ANALYSIS

In this article, we proposed a polar-code-based IR scheme with FBE strategy, which can be implemented efficiently without TRNs. We implemented the IR scheme on a commercial computer. Then, a series of experiments is conducted to evaluate its performance. In the experiments, the decoder is the FSSCL decoder, the block size n is 1 Mb, the length of CRC is 32, and the locations of the frozen bits are determined by the optimized upgrading and degrading channels' construction [30,41]. The sifted keys are collected from our reference-frame-independent QKD experiment and are extended to the targeted length and QBER [42]. Table II shows the experimental environment settings.

A. Yield of IR

The yield γ of each sifted key bit represents the performance of IR schemes and is calculated from the failure probability ε and the efficiency f according to Eqs. (1)–(4). The lower bound of the efficiency value is determined by the failure probability ε.

To evaluate the optimal yield of IR, we tested our IR scheme with $L \in \{1, 2, 8, 16, 32, 64\}$, $E = 0.02$, and ε from 10^{-4} to about 10^{-1} for 10 000 times each round.

Figure 3 shows the yield γ against the failure probability ε. The increase of list size improves the yield of IR by improving the correction performance. The yield γ first slowly increases to the maximum with the increase of ε because f is improved

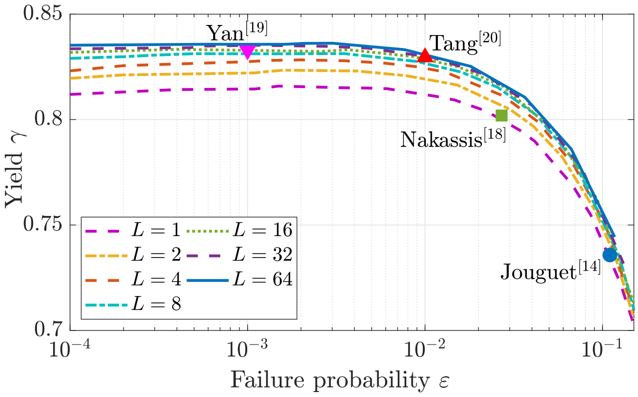

FIG. 3. The yield of the polar-code-based IR schemes with FBE strategy against the failure probability, when the decoder is the FSSCL decoder, QBER equals 0.02, the list size is in $\{1, 2, 8, 16, 32, 64\}$, and the block size is 1 Mb. The data of Tang's scheme are from the forward reconciliation phase [20].

(the value decreases) by the increase of ε. Then, as the failure probability ε increases, the discard failure cases increase and the yield γ decreases rapidly. Figure 4 shows the yield γ against the efficiency f.

The efficiency and the failure probability are shown in Table III when the optimal yield is achieved and the list size $L \in \{1, 2, 8, 16, 32, 64\}$. The performance of polar-code-based IR schemes could be further improved by appending the feedback procedure or improving the decoders, such as the scheme in Ref. [20].

B. Throughput of IR

The "bottleneck" of IR is the decoding procedure at Bob's side. In this article, we use the throughput of the IR scheme at Bob's side to represent the whole IR scheme.

We implemented the polar-code-based IR scheme in Ref. [20] (forward reconciliation) with the FSSCL decoder. Meanwhile, the IR scheme in Ref. [19] is also implemented with the SCL decoder because the scheme cannot adapt the FSSCL decoder. The throughput of the implementations is evaluated with $n = 1$Mb, $E = 0.02$, and $L \in \{1, 2, 4, 8, 16, 32, 64\}$. The efficiencies of the schemes are set as Table III by adjusting the size of information bits to ensure the same amount of decoding calculation. Figure 5 shows the evaluated throughput result, and the detailed throughput of our scheme is shown in Table III. The increase of list size improves the efficiency, but decreases the throughput. Tang's scheme and our scheme reach 60% higher throughput than the implementation of Yan's scheme for adapting the efficient FSSCL decoder. Although our scheme reaches a slightly lower throughput than Tang's scheme for one more encoding procedure, our scheme does not require TRNs. Furthermore, the polar-code-based IR scheme with FBE strategy can also apply state-of-the-art decoders to reach higher throughput and efficiency without TRNs.

TABLE III. The optimal yield and the throughput of our polar-code-based IR scheme with the FBE strategy. $n = 1$Mb, $L \in \{1, 2, 4, 8, 16, 32, 64\}$ and $E = 0.02$.

L	f	ε	γ	Throughput (Mbps)
1	1.293	0.0015	0.8159	8.60
2	1.239	0.0016	0.8234	4.46
4	1.202	0.0020	0.8283	3.26
8	1.172	0.0035	0.8313	1.66
16	1.176	0.0004	0.8333	0.68
32	1.158	0.0011	0.8353	0.33
64	1.140	0.0030	0.8362	0.14

V. CONCLUSION

In this article, we propose the polar-code-based information reconciliation (IR) scheme with the frozen-bit erasure (FBE) strategy, where an equivalent transmission of the sifted keys is conducted so that each frozen bit in the decoding procedure is erased to zero. Compared with the existing IR schemes, our proposed polar-code-based IR scheme with the FBE strategy can be implemented with the low-computational-complexity decoder and removes the

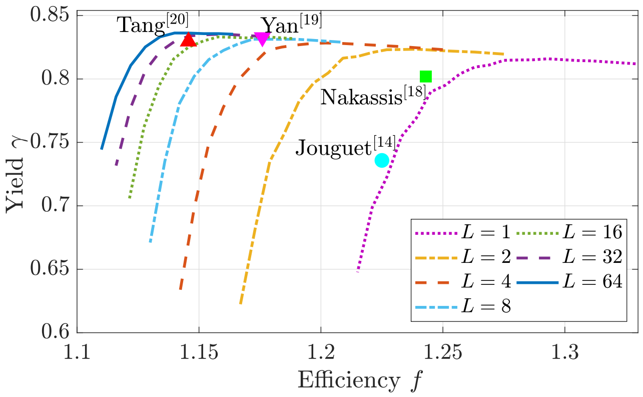

FIG. 4. The yield of the polar-code-based IR schemes with FBE strategy against the corresponding efficiency. The data of Tang's scheme are from the forward reconciliation [20].

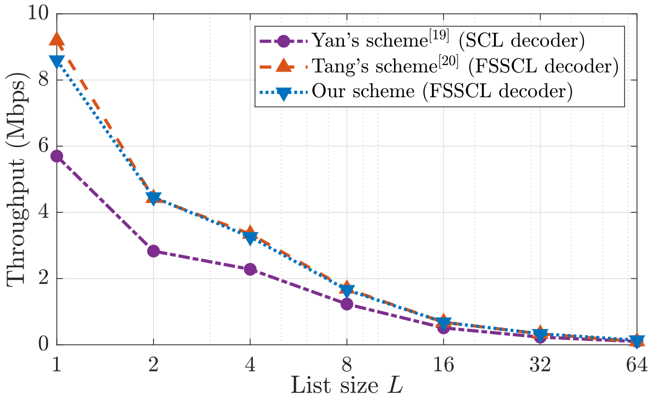

FIG. 5. Throughput comparison of the polar-code-based IR schemes with FSSCL and SCL decoders. The block size is 1 Mb and the QBER is 0.02.

assumption of true random numbers simultaneously. Furthermore, we implemented the scheme with the fast simplified successive-cancellation list decoder on a commercial computer. The implementation reaches the throughput of 0.68 Mbps and the yield of 0.8333 (efficiency of 1.176 and failure probability of 0.0004) with the decoder list size of 16, the block size of 1 Mb, and QBER of 0.02.

ACKNOWLEDGMENTS

This work was supported by the National Natural Science Foundation of China under Grant No. 61972410, the Research Plan of National University of Defense Technology under Grants No. ZK19-13 and No. 19-QNCXJ-107, and the Postgraduate Scientific Research Innovation Project of Hunan Province under Grant No. CX20200003.

[1] H.-K. Lo, M. Curty, and K. Tamaki, Secure quantum key distribution, Nat. Photon. **8**, 595 (2014).

[2] F. Zhao, M. Fu, F. Wang, Y. Lu, C. Liao, and S. Liu, Error reconciliation for practical quantum cryptography, Optik **118**, 502 (2007).

[3] G. Brassard and L. Salvail, Secret-key reconciliation by public discussion, *Advances in Cryptology—EUROCRYPT '93* (Springer, Berlin, 1994), pp. 410–423.

[4] Y. Liu, H. Chen, and L. Wang, Physical layer security for next generation wireless networks: Theories, technologies, and challenges, IEEE Commun. Surv. Tutor. **19**, 347 (2017).

[5] K. Moara-Nkwe, Q. Shi, G. M. Lee, and M. H. Eiza, A novel physical layer secure key generation and refreshment scheme for wireless sensor networks, IEEE Access **6**, 11374 (2018).

[6] M. F. Awan, K. Kansanen, S. Perez-Simbor, C. Garcia-Pardo, S. Castelló-Palacios, and N. Cardona, RSS-based secret key generation in wireless in-body networks, *2019 13th International Symposium on Medical Information and Communication Technology (ISMICT)* (IEEE, Piscataway, 2019).

[7] C. Huth, R. Guillaume, T. Strohm, P. Duplys, I. A. Samuel, and T. Güneysu, Information reconciliation schemes in physical-layer security: A survey, Comput. Networks **109**, 84 (2016).

[8] Y. Huang, S. Zhou, Z. Shi, and L. Lai, Channel frequency response-based secret key generation in underwater acoustic systems, IEEE Trans. Wireless Commun. **15**, 5875 (2016).

[9] Y. Luo, L. Pu, Z. Peng, and Z. Shi, RSS-based secret key generation in underwater acoustic networks: Advantages, challenges, and performance improvements, IEEE Commun. Mag. **54**, 32 (2016).

[10] Y. Watanabe, W. Matsumoto, and H. Imai, Information reconciliation in quantum key distribution using low-density parity-check codes, *Proc. of International Symposium on Information Theory and its Applications, ISITA2004* (ISITA, Tokyo, 2004).

[11] T. Pedersen and M. Toyran, High performance information reconciliation for QKD with cascade, Quantum Inf. Comput. **15**, 419 (2015).

[12] D. Elkouss, A. Leverrier, R. Alleaume, and J. J. Boutros, Efficient reconciliation protocol for discrete-variable quantum key distribution, *2009 IEEE International Symposium on Information Theory* (IEEE, Piscataway, 2009).

[13] Y. Sungsik and H. Jun, Efficient information reconciliation with turbo codes over the quantum channel, *2013 International Conference on ICT Convergence (ICTC)* (IEEE, Piscataway, 2013).

[14] P. Jouguet and S. Kunz-Jacques, High performance error correction for quantum key distribution using polar codes, Quantum Inf. Comput. **14**, 329 (2014).

[15] H. Mao, Q. Li, Q. Han, and H. Guo, High-throughput and low-cost LDPC reconciliation for quantum key distribution, Quantum Inf. Proc. **18**, 232 (2019).

[16] E. Arikan, Channel polarization: A method for constructing capacity-achieving codes, *2008 IEEE International Symposium on Information Theory* (IEEE, Piscataway, 2008).

[17] E. Arikan, Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels, IEEE Trans. Inf. Theor. **55**, 3051 (2009).

[18] A. Nakassis and A. Mink, *Polar Codes in a QKD Environment*, Vol. 9123 of SPIE Sensing Technology + Applications (SPIE, Bellingham, 2014).

[19] S. Yan, J. Wang, J. Fang, L. Jiang, and X. Wang, An improved polar codes-based key reconciliation for practical quantum key distribution, Chin. J. Electron. **27**, 250 (2018).

[20] B.-Y. Tang, B. Liu, W.-R. Yu, and C.-Q. Wu, Shannon-limit approached information reconciliation for quantum key distribution, Quantum Inf. Proc. **20**, 113 (2021).

[21] S. A. Hashemi, C. Condo, and W. J. Gross, Fast simplified successive-cancellation list decoding of polar codes, *2017 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)* (IEEE, Piscataway, 2017).

[22] A. Kuznetsov, O. Nariezhnii, I. Stelnyk, T. Kokhanovska, O. Smirnov, and T. Kuznetsova, Side channel attack on a quantum random number generator, *2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)* (IEEE, Piscataway, 2019).

[23] C.-H. F. Fung, X. Ma, and H. F. Chau, Practical issues in quantum-key-distribution postprocessing, Phys. Rev. A **81**, 012318 (2010).

[24] X. Ma, C.-H. F. Fung, J.-C. Boileau, and H. F. Chau, Universally composable and customizable post-processing for practical quantum key distribution, Comput. Secur. **30**, 172 (2011).

[25] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, Piscataway, 1984).

[26] H.-K. Lo, X. Ma, and K. Chen, Decoy State Quantum Key Distribution, Phys. Rev. Lett. **94**, 230504 (2005).

[27] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Practical decoy state for quantum key distribution, Phys. Rev. A **72**, 012326 (2005).

[28] D. Gottesman, H. K. Lo, N. Lutkenhaus, and J. Preskill, Security of quantum key distribution with imperfect devices, *International Symposium on Information Theory* (IEEE, Piscataway, 2004).

[29] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, Experimental quantum cryptography, J. Cryptology **5**, 3 (1992).

[30] I. Tal and A. Vardy, How to construct polar codes, IEEE Trans. Inf. Theory **59**, 6562 (2013).

[31] O. Gazi, *Polar Codes*, Springer Topics in Signal Processing (Springer, Singapore, 2019).

[32] I. Tal and A. Vardy, List decoding of polar codes, *2011 IEEE International Symposium on Information Theory* (IEEE, Piscataway, 2011).

[33] A. Alamdar-Yazdi and F. R. Kschischang, A simplified successive-cancellation decoder for polar codes, IEEE Commun. Lett. **15**, 1378 (2011).

[34] S. A. Hashemi, C. Condo, and W. J. Gross, Simplified successive-cancellation list decoding of polar codes, *2016 IEEE International Symposium on Information Theory (ISIT)* (IEEE, Piscataway, 2016).

[35] P. Giard, G. Sarkis, C. Thibeault, and W. J. Gross, 237 Gbit/s unrolled hardware polar decoder, Electron. Lett. **51**, 762 (2015).

[36] E. A. Bilkent, Polar coding for the Slepian-Wolf problem based on monotone chain rules, *2012 IEEE International Symposium on Information Theory* (IEEE, Piscataway, 2012).

[37] S. B. Korada and R. Urbanke, Polar codes for Slepian-Wolf, Wyner-Ziv, and Gelfand-Pinsker, *2010 IEEE Information Theory Workshop on Information Theory* (IEEE, Piscataway, 2010).

[38] E. O. Kiktenko, A. O. Malyshev, and A. K. Fedorov, Blind information reconciliation with polar codes for quantum key distribution, IEEE Commun. Lett. **25**, 79 (2021).

[39] W. W. Peterson and D. T. Brown, Cyclic codes for error detection, Proc. IRE **49**, 228 (1961).

[40] K. Niu and K. Chen, CRC-aided decoding of polar codes, IEEE Commun. Lett. **16**, 1668 (2012).

[41] B.-Y. Tang, The implementation of upgrading channels for construction of polar code, https://github.com/cfxtby/PolarCodeForQKD (unpublished).

[42] B.-Y. Tang, H. Chen, J.-P. Wang, H.-C. Yu, L. Shi, S.-H. Sun, W. Peng, B. Liu, and W.-R. Yu, Free-running long-distance reference-frame-independent quantum key distribution, npj Quantum Inf. **8**, 117 (2022).