SCIENTIFIC REPORTS
nature research

OPEN

Blind information reconciliation with variable step sizes for quantum key distribution

Zhihong Liu[1], Zhihao Wu[2] & Anqi Huang[2*]

Quantum key distribution (QKD) generates symmetric keys between two authenticated parties with the guarantee of information-theoretically security. A vital step in QKD to obtain fully-matched key between two parties is information reconciliation. The blind reconciliation protocol provides a useful tool that corrects the mismatch in a wide range of qubit error rate (QBER) but without a prior error estimation. However, there is a contradiction between the reconciliation efficiency and the processing time in this protocol. In this work, we propose a blind reconciliation protocol with variable step sizes to relieve this contradiction. The analysis and simulation results show that the improved protocol inherits all the advantages of the original blind reconciliation protocol and can obtain better reconciliation efficiency with less operation time. The improved blind reconciliation protocol enhances the final secret key rate and accelerates the processing speed of a QKD system.

Quantum key distribution (QKD)[1,2] allows two parties, usually called Alice and Bob, to share a pair of secret key via an insecure channel. QKD is proved to be information-theoretically secure owing to the solid foundation of quantum physics without computational assumptions[3–5]. The technology of QKD has been developed quickly in the past three decades and has achieved remarkable milestones. For example, QKD products has been commercialized with growing market[6]; QKD networks has been constructed in several countries around the world[7–9]; a QKD satellite realizes secure communication in global scale[10,11]. Thus, QKD is one of the most mature fields in quantum information.

In the implementation of QKD, a system operates two main phases to establish the shared key – the phase of quantum raw key exchange and the phase of classical post-processing[12]. At the first phase, Alice and Bob share the raw key by transmitting quantum states prepared by Alice through a quantum channel and measuring them by Bob. Then, sifting as the first step of classical post-processing helps Alice and Bob to maintain the cases that they are using the matched bases. The raw key is obtained after this step. However, the raw key shared between Alice and Bob may contain errors due to the channel noise and adversary's attacks. To eliminate the mismatch of the raw key between Alice and Bob, the system runs information reconciliation to guarantee that the same string of key shared at both sides. The reconciled key maybe partially correlated with an adversary, since the adversary can interact with the quantum states during the raw key exchange via quantum channel and listen to the public information during the information reconciliation via the classical channel. Thus, privacy amplification is applied to remove the leaked information, thereby obtaining the final secret key share between Alice and Bob. The sifting, information reconciliation, and privacy amplification are called as the post-processing phase.

In the post-processing, it is obvious that information reconciliation is a vital step to eliminate the mismatch, which is also called error bits, in the raw key to guarantee that Alice and Bob share the same key[13]. Regarding information reconciliation, a commonly used method is Cascade protocol, which identifies the position of errors via dichotomizing search in each block[14]. Although Cascade protocol is simple to be implemented with relative high reconciliation efficiency, this protocol requires many rounds of communication between Alice and Bob. Thus, this information reconciliation protocol is time-consuming and occupies significant amount of communication resources in a QKD system. To reduce the rounds of communication, Winnow protocol is proposed, which uses Hamming code instead of a simple parity check to identify and correct errors[15]. However, Hamming code only can correct 1-bit error in each block, and its efficiency is much lower than the Shannon limit.

[1]College of Intelligence and Technology, National University of Defense Technology, Changsha, 410073, People's Republic of China. [2]Institute for Quantum Information & State Key Laboratory of High Performance Computing, College of Computer, National University of Defense Technology, Changsha, 410073, People's Republic of China. *email: angelhuang.hn@gmail.com

Low-density parity-check (LDPC) code[16,17] is proposed to be used for the information reconciliation in a QKD system to reduce the rounds of communication and achieve high reconciliation efficiency[18,19]. Since LDPC code is able to correct multiple-bit errors, its reconciliation efficiency is close to the Shannon limit. Furthermore, only one round of communication is necessary to transmit the syndrome. Hence, the party (e.g. Alice or Bob) who receives the syndrome can use it to correct the errors. In practice, quantum channel is varying over time, and thus quantum bit error rate (QBER) is also changing[20]. In order to adapt to the different QBER, two techniques, puncturing[21,22] and shortening[23], are applied to the LDPC code to correct errors in one round of communication. This is called rate-adaptive information reconciliation[19,20,24].

Based on the rate-adaptive information reconciliation, blind information reconciliation protocol is suitable to the situation that the QBER is unknown, in which the reconciliation procedure is processed *blindly* without information of QBER[25–28]. Because of no information about the QBER, the blind reconciliation protocol allows multiple rounds of communication to try to correct the errors by assuming different error rate in each round. The specific procedure of the blind reconciliation protocol is as follows. In the first round of communication, Alice assumes the minimal error rate and only transmits the syndrome to Bob, and all the auxiliary bits are punctured. If the reconciliation fails, Alice reveals a small amount of punctured bits, turning them to be shortened bits, which helps Bob to correct errors. With more rounds the protocol operates, more shortened bits are known by Bob. Until Bob successfully corrects all errors or the maximum of rounds reaches, the protocol ends. This protocol does not need the error estimation as prior information and can achieve high average efficiency[26].

However, there is a trade off between the reconciliation efficiency and the time consumption of this protocol. On the one hand, the more rounds of interactivity allowed between Alice and Bob, the higher reconciliation efficiency can achieve. On the other hand, more rounds of interactivity take more time to complete the protocol. Practically, in a QKD system, the time consumption of the post-processing significantly affects the secret key rate. If the post-processing consumes much more time than the raw key exchange phase, the secret key rate will be limited by the speed of post-processing and thus cannot obtain high key rate.

To relieve the contradiction between the reconciliation efficiency and the time consumption, we propose a blind information reconciliation protocol with variable step sizes. Different from the original protocol, the proposed protocol gradually increases the amount of the shortened bits revealed in each round, rather than reveals constant amount of the shortened bits in each round. In this way, the proposed protocol can achieve better reconciliation efficiency while incurring similar or even less time consumption to complete the error correction. More specifically, the simulation results show that the proposed protocol can achieve improvement of the reconciliation efficiency while consuming less iteration time. Besides, by using a decoy-state BB84 QKD system, we demonstrate that the proposed protocol can improve the secret key rate. This is useful in practice when the QBER is not known in advance. In short, this protocol inherits all the advantages of the original blind information reconciliation protocol and can provide better reconciliation efficiency with less operation time than the original one.

The paper is organized as follows. In Sec. 2, we introduce the protocol of blind information reconciliation with variable step sizes. The corresponding simulation results that compared to the original blind information reconciliation protocol are shown in Sec. 3. We further analysis the effect of the improved reconciliation efficiency owing to the variable step sizes on the secret key rate of QKD in Sec. 4. The conclusion is drawn in Sec. 5.

Blind Reconciliation With Variable Step Sizes

Blind reconciliation can cover a wide range of QBER by using only one LDPC code. This is due to the technique of rate-adaptive reconciliation. Thus, in this section, we first describe the working principle of rate-adaptive information reconciliation. Based on this, we introduce the protocol of blind reconciliation with variable step sizes that we propose.

Rate-adaptive information reconciliation. For a given LDPC code $C(n, k)$, there are k symbols that are independent with each other to represent the information. And other $n - k$ symbols are redundant ones that assist to complete the parity check. Thus, its code rate is defined as $R_0 = k/n$. The code rate determines the correction capability, which means the maximum error rate that the LDPC code can correct. It has been shown that a given LDPC code with code rate R only can correct the error in a certain range[16,17]. Therefore, multiple LDPC codes are needed to cover a wide range of error rate. However, this solution may be impractical in the hardware implementation of a QKD system, because it occupies memory space to store copies of the LDPC codes. Thus, an ideal solution would be using a single LDPC code whose code rate can be adjusted in order to adapt to a wide range of error rate. This solution is called rate-adaptive information reconciliation, in which the adaptable code rate is realized by the techniques of puncturing and shortening[19,20,24].

Puncturing deletes p symbols from the code words, and thus the LDPC code becomes $C(n - p, k)$[21,22]. The code rate is increased to be $R(p) = k/(n - p)$. The puncturing technique can be used in the information reconciliation to adapt the code rate as follows. The bit string X with length (i.e. $n - p$) is hold by Alice. According to the error rate, Alice and Bob determine the number of puncturing symbols, the value of p. Then Alice randomly fills p bits into her bit string X, constructing the code word with length n. The syndrome of the constructed code word is calculated by Alice and sent to Bob to help him correct his bit string. At Bob side, Bob also randomly fills p bits into his bit string Y and operates the decoding procedure. Thus, if the new code rate under puncturing technique, $R(p)$, can adapt to the error rate, Bob is able to correct the mismatch in his bit string with a high success rate. For a time-varying channel, the value of p should be changed according to the different error rate over time. Thus, the length of Alice's and Bob's bit strings ($n - p$) also needs to be adapted to the changed value of p. This is inconvenient in practice.

In contrary to puncturing that increases the code rate via reducing the redundant bits, the technique of shortening decreases the code rate by increasing the ratio of redundant bits in a code word[23]. Specifically, shortening

means that Alice tells the Bob the values of s symbols in the k symbols, which reduces unknown information. Thus, the code $C(n, k)$ turns to be $C(n - s, k - s)$, and the code rate is decreased to be $R(s) = (k - s)/(n - s)$. During the information reconciliation, Alice and Bob share the values of the shortened bits and their positions. Then Alice constructs a code word with length n that contains s bits of the shortened ones and $n - s$ bits of raw key. At Bob side, he also builds a string with $n - s$ bits of the raw key and the s-bit shortened part. Shortening indeed also changes the code rate by adjusting the amount of shortened bits. However, there is an issue similar to the puncturing technique. Regarding a time-varying channel, the value of s also has to be changed over time due to the variable error rate, which causes the same problem of modifying the bit length of Alice's and Bob's strings.

To overcome the problem of varying string length mentioned above but also take the advantage of the adaptive rate, we can combine the techniques of puncturing and shortening. The total symbols of puncturing and shortening are set to be $d = p + s$, which is a fixed value. Thus, the length of Alice's and Bob's bit strings are also fixed to be $m = n - d$. To modify the code rate to adapt to different error rates, the values of p and s are flexible to be changed. Since the puncturing technique increases the code rate but the shortening technique decreases the code rate, a proper code rate can be achieved by balancing the values of p and s. The range of code rate that can be covered by the rate-adaptive LDPC code is

$$R_{min} = \frac{k - d}{n - d} \leq R \leq \frac{k}{n - d} = R_{max}. \tag{1}$$

Therefore, the rate-adaptive reconciliation protocol can use one LDPC code to adapt to a wide range of code rate with help of puncturing and shortening.

The design of the proposed protocol. The blind reconciliation protocol inherits the core idea of rate-adaptive information reconciliation. Instead of deciding the values of p and s at the beginning of the protocol when the error rate is estimated, the blind reconciliation starts without error estimation and thus does not fix the values of p and s[25–27]. At the beginning, all d bits are regarded as punctured bits. If Bob is not able to correct the error bits according to the syndrome that Alice sends to him, a fixed amount of bits will be revealed as shortened bits in the next round. That is, $\Delta_i = \Delta,\ \ i \in [1, t]$. Here, Δ_i is the number of the shortened bits revealed in the ith round, and it is also named as the step size in the ith round. Thus, in each round, Bob gains more information than last round to correct the errors. This protocol can achieve relative high reconciliation efficiency with the cost of operation time due to multiple communication rounds.

To keep the advantage of high reconciliation efficiency and also speed up its operation, we propose a blind reconciliation protocol with variable step sizes as follows. In the protocol, Alice and Bob assume that the error rate is minimum at the beginning, and Alice only sends syndrome to Bob (Set $p = d, s = 0$). That is, Bob tries to correct the error bits with minimal help from Alice. The increased number of rounds indicates that the error rate is higher than that Bob can correct and more help from Alice (i.e. the information of the shortened bits) is needed. Thus, to provide more help, instead of revealing a fixed number of shortened bits in each round, Alice can reveal an increased amount of shortened bits $\Delta_i = \Delta_{i-1} + \delta$ ($\delta \in \mathbb{R}$) to Bob. It is notable that the amount of shortened bits is related to the number of rounds. When the number of round i is larger, the amount of shortened bits revealed in this round also becomes greater. In this way, Bob can receive more help from Alice, thereby accelerating the speed of Bob's error correction. Thus, variable step sizes in the reconciliation protocol mean that revealed shortened bits $\Delta_i = \Delta_{i-1} + \delta$ in the ith round is more than Δ_{i-1} in the $i - 1$ th round.

The specific procedure of the blind reconciliation protocol with variable step sizes is as follows.

Step 1: Preparation. Assume $C(n, k)$ is a LDPC code. Alice/Bob prepares a bit string X/Y with length $m = n - d$ from the raw key, which will be reconciled during this protocol. Set $p = d, s = 0$ and $\Delta_0 = 0$ as initialization.

Step 2: Encoding. Alice constructs an n-bit code word X' that consists of m-bit raw key and d-bit random symbols as punctured bits. Alice then calculates the syndrome of X' and sends it to Bob. Also, Alice informs Bob the positions of the punctured bits but not their values.

Step 3: Error correction. Bob builds another n-bit string Y' that consists of m-bit raw key at his side, s-bit shortened symbols, and p-bit puncturing symbols. Then Bob runs the error correction algorithm. If the syndrome calculated from the corrected string matches to that sent by Alice, Bob successfully recovers X and the protocol stops. Otherwise, goes to Step 4.

Step 4: Information disclosure. If $s = d$, the protocol fails. Otherwise, Alice discloses $\Delta_i = \Delta_{i-1} + \delta$ symbols to Bob, and the total shortened bits are $s = s + \Delta_i$. Then turn back to Step 3 for the ith iteration of information reconciliation.

In this protocol, assume the maximum iterations is t and the step size in ith iteration is Δ_i, then $\sum_{i=1}^{t} \Delta_i = s$.

In short, there are two main advantages in the proposed protocol. During the first few rounds, Alice reveals less shortened bits to Bob than the original blind reconciliation protocol. If Bob still can recover the correct code word, the reconciliation efficiency of the improved protocol with variable step sizes is better than the original one because of less disclosed information. If the error rate is relative high, Bob has to run more rounds of reconciliation with more help from Alice. In the improved protocol, the shortened bits revealed in each round are increased gradually, which can provide more information to Bob for his reconciliation. Thus, under the situation of high error rate, less rounds of communication are needed for the improved protocol with variable step sizes than that of the original one, which saves the operation time. The simulation results in the next section also verify these advantages.

It is noted that although we only use linear function to increase the step sizes gradually in this paper, the change pattern of the step size is not restricted. For instance, exponential and logarithmic functions can also be used according to the error rate.

Protocol Simulation Results

To show the improved performance of the blind reconciliation protocol with variable step sizes, we compare the reconciliation efficiency and the number of iterations between the proposed protocol and the original blind reconciliation protocol in the simulation. In the experiments, 64800-bit LDPC codes with code rate $R_0 = 0.8, 0.6, 0.5$ are chosen to cover the error range of [1%, 10%]. 10% of code bits are used for adapting the code rate. That it, $d = 6480$. Regarding the original blind reconciliation protocol, we set the maximum number of iterations $N = 3, 6, 10$, which means, $\Delta = 2160, 1080, 648$ shortened bits are revealed in every iteration, respectively. Under the same LDPC code setting, we simulate two types of the improved blind reconciliation protocol with variable step sizes. In the first case, Alice reveals $\Delta_i = 648 \times i$ shortened bits in ith iteration, and in the second case, Alice reveals $\Delta_1 = 590$ and $\Delta_i = 589 \times (i-1)$ shortened bits in ith iteration. As an important parameter, the reconciliation efficiency f is calculated as follows in the simulation[26].

$$f = \frac{1-R}{h(\varepsilon)} = \frac{1-\frac{k-s}{n-p-s}}{h(\varepsilon)} = \frac{n-p-k}{(n-d)h(\varepsilon)}, \tag{2}$$

where ε is the error rate, and $h(\varepsilon)$ is the binary Shannon entropy. The best information reconciliation is to reach $f = 1$. We run each reconciliation protocol for 30 times and take the averaged values of reconciliation efficiency and iteration number for each case.

The simulation results are shown in Fig. 1. We can see that for the relative low error rates in Fig. 1(a,c,e), the improved blind reconciliation protocol with variable step sizes $\Delta_i = 648 \times i$ and $\Delta_i = 589 \times (i-1)$ can achieve a better reconciliation efficiency than the original one with $\Delta = 1080$ and $\Delta = 2160$ bits revealed in every iteration. The reconciliation efficiency of the protocol with the variable step sizes $\Delta_i = 589 \times (i-1)$ is close to the original one with small step of $\Delta = 648$ bits revealed in every iteration. Thus, the better reconciliation efficiency achieved by the improved protocol discloses less information to the public, which helps Alice and Bob preserve more secret information. When the error rate is relative high in Fig. 1(a,c,e), the efficiency of the proposed blind reconciliation protocol may be slightly worse than that of the original protocol. However, in this range of high error rate, as shown in Fig. 1(b,d,f), the improved protocol with $\Delta_i = 648 \times i$ or $\Delta_i = 589 \times (i-1)$ operates less iterations than the original one with steps $\Delta = 1080$ and $\Delta = 648$ and also achieves similar reconciliation efficiency. This shows the improved protocol consumes much less time to process the phase of information reconciliation. This strategy accelerates the speed of post-processing especially for the cases of high error rate, which also saves hardware resources. In the application of the blind information reconciliation where the QBER is not known in advance, the advantages of our proposed protocol are obvious. Therefore, the improved blind reconciliation protocol with variable step sizes relieves the conflict of reconciliation efficiency and operation time by gradually revealing more number of shortened bits instead of a fixed number of shortened bits in each iteration.

Secret Key Rate Analysis for QKD

To further shown the better reconciliation efficiency acheived by the improved blind reconciliation protocol can helps Alice and Bob generate higher secret key rate, we simulate the decoy-state BB84 QKD protocol with the reconciliation efficiency obtained by the simulation. According to the analysis of Gottesman-Lo-Lütkenhaus-Preskill (GLLP)[29], the secret key rate of QKD with the weak coherent source can be written as

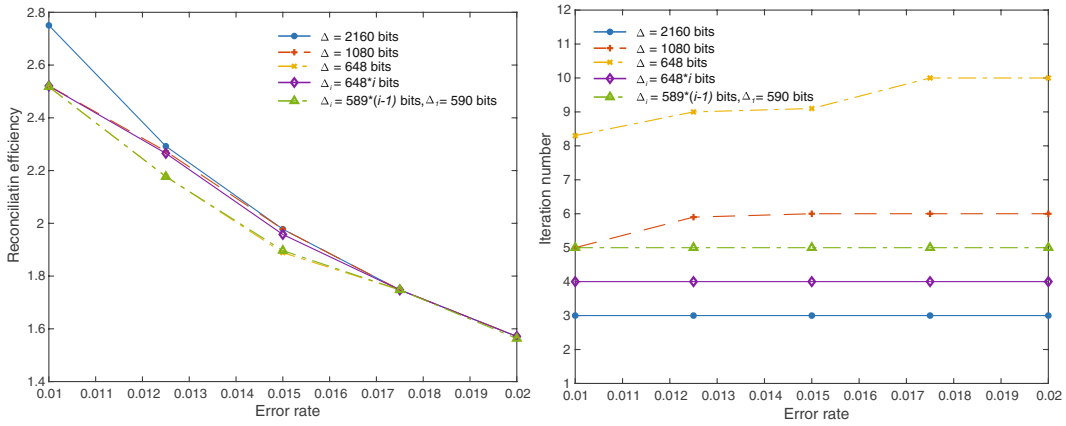
$$R \geq q\{-Q_\mu H_2(E_\mu) f(E_\mu) + P_1^\mu Y_1^\mu [1 - H_2(e_1^\mu)]\}, \tag{3}$$

where $q = 1/2$ for BB84 protocol, μ is the intensity of a signal state, Q_μ/E_μ is the total gain/error rate of the signal state, Y_1^μ and e_1^μ are the yield and error rate of single-photon pulses in the signal states, P_1^μ is the probability of single-photon pulses in the signal states, $f(x)$ is the reconciliation efficiency, and $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon information entropy. In the decoy-state protocol, Y_1^μ and e_1^μ are estimated as follows[30].

$$\begin{aligned} Y_1^L &= \frac{\mu}{\mu\nu - \nu^2}\left(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2-\nu^2}{\mu^2} Y_0\right), \\ e_1^U &= \frac{E_\nu Q_\nu e^\nu - e_0 Y_0}{Y_1^L \nu}. \end{aligned} \tag{4}$$

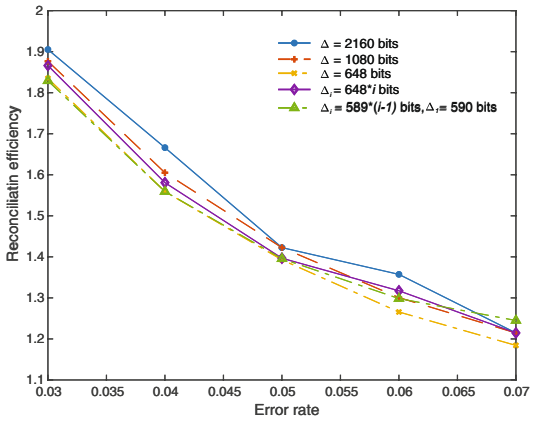
Here ν is the intensity of a decoy state, Q_ν/E_ν is the total gain/error rate of the decoy state, Y_0 is the dark count rate of a single-photon detector, and e_0 is the error rate of the background noise.

In order to show the effect of the improved efficiency provided by the modified blind reconciliation protocol on a QKD system, we simulate the final secret key rate of a decoy-state BB84 QKD system with the typical reconciliation efficiency obtained from the blind reconciliation protocol with shortened bits $\Delta_1 = 590$ and $\Delta_i = 589 \times (i-1)$. As a comparison, we also show the secret key rate with the reconciliation efficiency of the original blind reconciliation protocol with $\Delta = 1080$ shortened bits revealed in each iteration. In the simulation, we assume $\mu = 0.6, \nu = 0.2$, and $e_0 = 0.5$. All the detection parameters are taken from the Gobby-Yuan-Shields

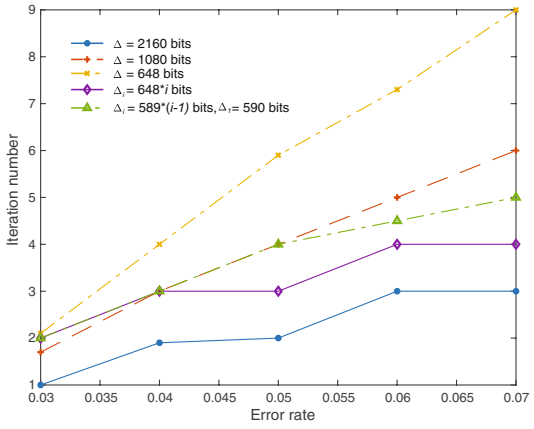


(a) Efficiency comparison with $R_0 = 0.8$

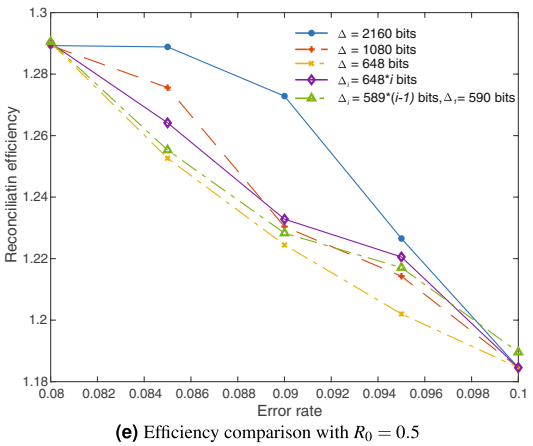
(b) Iteration num. comparison with $R_0 = 0.8$



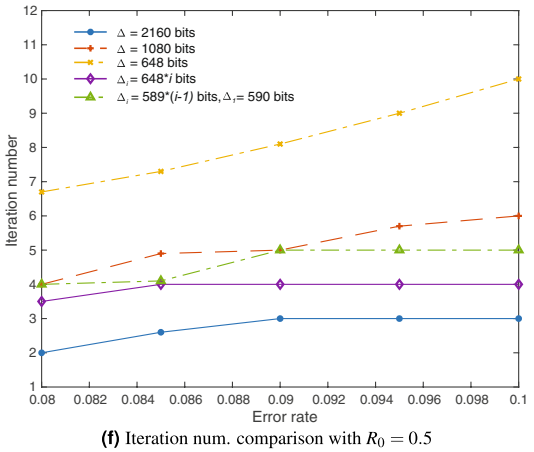
(c) Efficiency comparison with $R_0 = 0.6$



(d) Iteration num. comparison with $R_0 = 0.6$



(e) Efficiency comparison with $R_0 = 0.5$



(f) Iteration num. comparison with $R_0 = 0.5$

Figure 1. The simulated reconciliation efficiency and iteration number of the original blind reconciliation protocol (with $\Delta = 2160, \Delta = 1080, \Delta = 648$ shortened bits revealed in every iteration) and the proposed blind reconciliation protocol (with $\Delta_i = 648 \times i, \Delta_i = 589 \times (i-1)$ shortened bits revealed in every iteration). To cover the error rate in the range [1%, 10%], we simulate (**a**) the efficiency and (**b**) iteration number of the LDPC code with $R_0 = 0.8$, (**c**) the efficiency and (**d**) iteration number of the LDPC code with $R_0 = 0.6$, and (**e**) the efficiency and (**f**) iteration number of the LDPC code with $R_0 = 0.5$.

(GYS) experiment[31]. The dark count rate $Y_0 = 1.7 \times 10^{-6}$, the transmittance in Bob's device $\eta_{Bob} = 4.5\%$, and the misalignment error rate $e_{detector} = 3.3\%$.

The simulation results are shown in Fig. 2. From Fig. 2 we can see that the secret key rate with the reconciliation efficiency obtained from the reconciliation protocol with variable step sizes is higher than that with reconciliation efficiency got from the original blind reconciliation protocol. This is because the modified protocol with variable step sizes can achieve a higher reconciliation efficiency than the original one. The fluctuation points

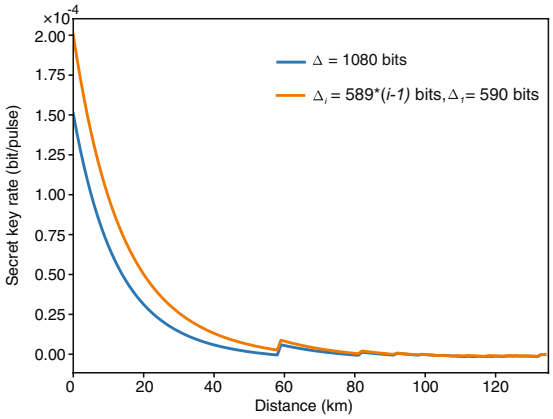


Figure 2. The simulated secret key rates of a decoy-state BB84 QKD system with the reconciliation efficiency obtained from the original blind reconciliation protocol ($\Delta = 1080$) and the blind reconciliation protocol with variable step sizes ($\Delta_1 = 590$ and $\Delta_i = 589 \times (i-1)$), respectively. The detection parameters are taken from the GYS experiment. The dark count rate $Y_0 = 1.7 \times 10^{-6}$, the transmittance in Bob's device $\eta_{Bob} = 4.5\%$, and the misalignment error rate $e_{detector} = 3.3\%$.

are the places where the reconciliation efficiency changed due to our simulation data of different error rates. The simulation results prove that the modified blind reconciliation protocol contributes to a higher secret key rate for the decoy-state BB84 QKD system than the original blind reconciliation protocol.

Discussion and Conclusions

Information reconciliation is an important step in the post-processing of QKD. The information reconciliation protocol based on LDPC codes is becoming popular because of its strong capability of error correction. As required by practice, blind reconciliation protocol can correct the error without estimating the QBER but still obtain good reconciliation efficiency. However, the blind reconciliation protocol runs multiple rounds of communication between Alice and Bob to correct all errors, which consumes large amount of communication resources. Thus, reconciliation efficiency is a key parameter in QKD, and the speed of reconciliation is the bottleneck of the system's repetition rate. In this work, we propose an improved blind reconciliation protocol with variable step sizes that reveals more shortened bits than that in the last round, increasing the information of the code word to help Bob correct his errors. The major modification of the improved reconciliation protocol is to set the number of shortened bits Δ_i disclose to Bob in the ith iteration is related to i instead of a fixed number as in the original protocol. This indicates the idea of variable step sizes.

The variable step sizes relieve the conflict of the reconciliation efficiency and the processing time. As shown by the analysis and simulation results in above sections, in the range of relative low error rate for a LDPC code, the improved blind reconciliation protocol discloses less shortened bits in the first several iterations, thus reaching better reconciliation efficiency than the original blind reconciliation protocol. In the range of relative high error rate, the proposed blind reconciliation protocol with variable step sizes reveals the shortened bits within less iterations than the original one to help Bob reconcile his bit strings, which takes less operation time and accelerates the speed of post-processing. In the application of the blind information reconciliation where the QBER is not known in advance, the advantages of our proposed protocol are obvious. We also show that the modified blind reconciliation protocol can provide a better reconciliation efficiency in QKD system, which enhances the final secret key rate of a decoy-state BB84 QKD system. To further achieve a even better reconciliation efficiency for the improved protocol, a protocol that can choose the size of step (Δ_i) according to the error correction conditions of previous rounds in a more sophisticated way may be needed. This optimized protocol can be our future work. Moreover, the blind information reconciliation protocol with variable sizes may combine with the methodology of symmetric blind information reconciliation proposed in ref. [28] that improves the reconciliation efficiency by disclosing the positions of additional shortened bits decidedly indicated by unsuccessful belief propagation decoding algorithm. The reconciliation efficiency may be further improved by leveraging these two ways of the information leakage reduction. The investigation of this methodological combination can also be an interesting future work.

Received: 26 August 2019; Accepted: 18 October 2019;
Published online: 13 January 2020

References

1. Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In *Proc. IEEE International Conference on Computers, Systems, and Signal Processing (Bangalore, India)*, 175–179, https://doi.org/10.1016/j.tcs.2014.05.025 (IEEE Press, New York, 1984).
2. Bennett, C. H. Quantum cryptography using any 2 nonorthogonal states. *Phys. Rev. Lett.* **68**, 3121–3124, https://doi.org/10.1103/PhysRevLett.68.3121 (1992).
3. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145–195, https://doi.org/10.1103/RevModPhys.74.145 (2002).

4. Scarani, V. *et al*. The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301–1350, https://doi.org/10.1103/RevModPhys.81.1301 (2009).
5. Lo, H.-K., Curty, M. & Tamaki, K. Secure quantum key distribution. *Nat. Photonics* **8**, 595–604, https://doi.org/10.1038/nphoton.2014.149 (2014).
6. Commercial QKD systems are available from at least three companies: ID Quantique (Switzerland), http://www.idquantique.com; QuantumCTek (China), http://www.quantum-info.com/en.php; Qasky (China), http://www.qasky.com/en/.
7. Peev, M. *et al*. The SECOQC quantum key distribution network in Vienna. *New J. Phys.* **11**, 075001, https://doi.org/10.1088/1367-2630/11/7/075001 (2009).
8. Sasaki, M. *et al*. Field test of quantum key distribution in the Tokyo QKD Network. *Opt. Express* **19**, 10387–10409, https://doi.org/10.1364/OE.19.010387 (2011).
9. Quantum secure communication "Beijing-Shanghai backbone" project, http://www.quantum-info.com/English/case/2017/0901/339.html (visited 22 August 2019).
10. Liao, S.-K. *et al*. Satellite-to-ground quantum key distribution. *Nature* **549**, 43, https://doi.org/10.1038/nature23655 (2017).
11. Liao, S.-K. *et al*. Satellite-relayed intercontinental quantum network. *Phys. Rev. Lett.* **120**, 030501, https://doi.org/10.1103/PhysRevLett.120.030501 (2018).
12. Renner, R. Security of quantum key distribution. *Int. J. Quantum Inf.* **6**, 1–127, https://doi.org/10.1142/S0219749908003256 (2008).
13. Van Assche, G. *Quantum cryptography and secret-key distillation* (Cambridge University Press, 2006).
14. Brassard, G. & Salvail, L. Secret-key reconciliation by public discussion. In *Workshop on the Theory and Application of of Cryptographic Techniques*, 410–423, https://doi.org/10.1007/3-540-48285-7_35 (Springer, 1993).
15. Buttler, W. T. *et al*. Fast, efficient error reconciliation for quantum cryptography. *Phys. Rev. A* **67**, 052303, https://doi.org/10.1103/PhysRevA.67.052303 (2003).
16. Gallager, R. Low-density parity-check codes. *IEEE Trans. Inf. Theory* **8**, 21–28, https://doi.org/10.1109/TIT.1962.1057683 (1962).
17. MacKay, D. J. Good error-correcting codes based on very sparse matrices. *IEEE Trans. Inf. Theory* **45**, 399–431, https://doi.org/10.1109/18.748992 (1999).
18. Elkouss, D., Leverrier, A., Alléaume, R. & Boutros, J. J. Efficient reconciliation protocol for discrete-variable quantum key distribution. In *2009 IEEE International Symposium on Information Theory*, 1879–1883, https://doi.org/10.1109/ISIT.2009.5205475 (IEEE, 2009).
19. Elkouss, D., Martnez-Mateo, J. & Martin, V. Secure rate-adaptive reconciliation. In *2010 International Symposium On Information Theory & Its Applications*, 179–184, https://doi.org/10.1109/ISITA.2010.5650099 (IEEE, 2010).
20. Wang, X. *et al*. Efficient rate-adaptive reconciliation for continuous-variable quantum key distribution. *Quantum Inf. Comput.* **17**, 1123–1134 (2017).
21. Ha, J., Kim, J. & McLaughlin, S. W. Rate-compatible puncturing of low-density parity-check codes. *IEEE Trans. Inf. Theory* **50**, 2824–2836, https://doi.org/10.1109/TIT.2004.836667 (2004).
22. Pishro-Nik, H. & Fekri, F. Results on punctured low-density parity-check codes and improved iterative decoding techniques. *IEEE Trans. Inf. Theory* **53**, 599–614, https://doi.org/10.1109/TIT.2006.889701 (2007).
23. Tian, T. & Jones, C. R. Construction of rate-compatible ldpc codes utilizing information shortening and parity puncturing. *Eurasip. J. Wirel. Comm* **2005**, 692121, https://doi.org/10.1155/WCN.2005.789 (2005).
24. Elkouss, D., Martinez-Mateo, J. & Martin, V. Analysis of a rate-adaptive reconciliation protocol and the effect of leakage on the secret key rate. *Phys. Rev. A* **87**, 042334, https://doi.org/10.1103/PhysRevA.87.042334 (2013).
25. Elkouss, D., Martinez-mateo, J. & Martin, V. Information reconciliation for quantum key distribution. *Quantum Inf. Comput.* **11**, 226–238 (2011).
26. Martinez-Mateo, J., Elkouss, D. & Martin, V. Blind reconciliation. *Quantum Inf. Comput.* **12**, 791–812 (2012).
27. Martinez-Mateo, J., Elkouss, D. & Martin, V. Key reconciliation for high performance quantum key distribution. *Sci. Rep.* **3**, 1576, https://doi.org/10.1038/srep01576 (2013).
28. Kiktenko, E. O., Trushechkin, A. S., Lim, C. C. W., Kurochkin, Y. V. & Fedorov, A. K. Symmetric blind information reconciliation for quantum key distribution. *Physical Review Applied* **8**, 044017, https://doi.org/10.1103/PhysRevApplied.8.044017 (2017).
29. Gottesman, D., Lo, H.-K., Lütkenhaus, N. & Preskill, J. Security of quantum key distribution with imperfect devices. *Quantum Inf. Comput.* **4**, 325–360 (2004).
30. Ma, X., Qi, B., Zhao, Y. & Lo, H.-K. Practical decoy state for quantum key distribution. *Phys. Rev. A* **72**, 012326, https://doi.org/10.1103/PhysRevA.72.012326 (2005).
31. Gobby, C., Yuan, Z. L. & Shields, A. J. Quantum key distribution over 122 km of standard telecom fiber. *Appl. Phys. Lett.* **84**, 3762–3764, https://doi.org/10.1063/1.1738173 (2004).

Acknowledgements

We thank David Elkouss and Xingtong Liu for very useful discussions. This work was funded by the National Natural Science Foundation of China (Grants 61901483, 61601476 and 61632021) and the National Key Research and Development Program of China (Grant 2019QY0702).

Author contributions

A.H. and Z.L. conceived the improved blind reconciliation protocol with variable step sizes, Z.L. conducted the simulation of improved blind reconciliation protocol, Z.W. conducted the simulation of the secret key rate, Z.L. and A.H. wrote the manuscript, and A.H. supervised the study. All authors reviewed the manuscript.

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to A.H.

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

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