



CHORUS

This is the accepted manuscript made available via CHORUS. The article has been published as:

Symmetric Blind Information Reconciliation for Quantum Key Distribution

E. O. Kiktenko, A. S. Trushechkin, C. C. W. Lim, Y. V. Kurochkin, and A. K. Fedorov

Phys. Rev. Applied **8**, 044017 — Published 27 October 2017

DOI: [10.1103/PhysRevApplied.8.044017](https://doi.org/10.1103/PhysRevApplied.8.044017)

Symmetric blind information reconciliation for quantum key distribution

E.O. Kiktenko,^{1,2,3,*} A.S. Trushechkin,³ C.C.W. Lim,^{4,5,†} Y.V. Kurochkin,¹ and A.K. Fedorov^{1,2,‡}

¹*Russian Quantum Center, Skolkovo, Moscow 143025, Russia*

²*QApp, Skolkovo, Moscow 143025, Russia*

³*Steklov Mathematical Institute of Russian Academy of Sciences, Moscow 119991, Russia*

⁴*Department of Electrical and Computer Engineering,
National University of Singapore, 117583, Singapore*

⁵*Quantum Information Science Group, Computational Sciences and Engineering Division,
Oak Ridge National Laboratory, Oak Ridge, Tennessee 37831-6418, USA*

Quantum key distribution (QKD) is a quantum-proof key exchange scheme which is fast approaching the communication industry. An essential component in QKD is the information reconciliation step, which is used for correcting the quantum channel noise errors. The recently suggested blind reconciliation technique, based on low-density parity-check (LDPC) codes, offers remarkable perspectives for efficient information reconciliation without an a priori error rate estimation. In the present work, we suggest an improvement of the blind information reconciliation protocol allowing significant increase the efficiency of the procedure and reducing its interactivity. The proposed technique is based on introducing symmetry in operations of parties, and the consideration of results of unsuccessful belief propagation decodings.

I. INTRODUCTION

QKD is the art of distributing provably-secure cryptographic keys in an insecure communication network [1–4]. Unlike conventional cryptography, the security of QKD is based on the laws of quantum physics and thus is guaranteed to be secure against any unforeseen technological and algorithmic developments, *e.g.*, quantum computing. For this reason, QKD has attracted an enormous amount of interest since its discovery, and is now one of the most widely studied research field in quantum information science. In fact, provably-secure commercial QKD systems are now available at retail [5].

A QKD system is carried out in two consecutive phases, namely a quantum key establishment phase and a classical post-processing phase [6]. In the first phase, the users first create an unprocessed (raw) key pair by performing local measurements on quantum signals which are exchanged via an untrusted quantum channel. At this point, the pair of raw keys are weakly correlated—due to noise in the quantum channel—and are partially secure. To correct the errors and remove the adversary’s information about the raw key pair, the users run an information reconciliation step and a privacy amplification step. The former requires the user to exchange a certain amount of public information about the key pair, which is then compensated for in the privacy amplification step. Finally, after the classical post-processing phase, the users are left with a correct and secure key pair (for details, see Refs. [6–9]).

It is clear that information reconciliation is an important step of QKD, for it is necessary to correct the errors

introduced by the quantum channel (or the adversary). In practice, the information reconciliation step is typically implemented using an iterative method known as Cascade [10]. The Cascade method is based on the random shuffling and the dichotomic search of discrepancies based on announcements of sub-block parities via communication over the authenticated channel. A number of possible improvements have been proposed, but most of them are very expensive in terms of communication [11]. That is, despite the fact that different sub-blocks can be treated in parallel [12], the Cascade method is still a highly interactive algorithm as the dichotomic search requires multiple rounds of communication between users.

Interactivity of Cascade-based information reconciliation procedure can cost significant amount of authentication resources together with time delays and workload in QKD systems. Another popular information reconciliation scheme is forward error correction with LDPC codes [13, 14], which uses a single message containing syndrome calculated for particular block of sifted key [15–19]. However, this scheme could fail and penalize the secret key throughput due to its inability to perform the syndrome decoding procedure. Such failures appear if the syndrome decoding, based on iterative belief propagation algorithm, does not converge in the predefined number of iterations (*e.g.* it could be caused by an inappropriate choice of the code rate relative to actual number of discrepancies in raw keys).

The problem with convergence differs the traditional LDPC code-based error correction methods [13, 14] from the Cascade, where the dichotomic search is performed as long as all the sub-blocks in all the shuffling rounds will contain odd numbers of errors. Then Cascade can be considered as a *guaranteed convergence* method (see Fig. 1). It is important to note that guaranteed convergence does not imply *guaranteed reconciliation*. In the case of Cascade some of sub-blocks still can contain positive numbers of undetected error after implementation

* e.kiktenko@rqc.ru

† elelimc@nus.edu.sg

‡ akf@rqc.ru

		Efficiency	Typical number of communication rounds	Guaranteed convergence
	Cascade	Depends on particular realization	>30	
LDPC code-based	Straightforward	Typically better than Cascade (for QBER>2%)	1	
	Rate-adaptive	Better than straightforward	1	
	Blind	Better than rate-adaptive	< 10	
	Symmetric	Better than blind	< 10, less than or equal to blind	

Figure 1. Comparison of three parameters (efficiency, typical number of communication rounds, and convergence guarantee) for different approaches to information reconciliation for QKD systems: the cascade method [11], straightforward implementation of LDPC codes [16], rate-adaptive implementation of LDPC codes [18], blind reconciliation implementation of LDPC codes [21], and our proposed solution (symmetric blind information reconciliation). We note that the typical number of communication rounds for blind and symmetric blind protocols is considered in the assumption that both the protocols are running until a convergence of syndrome decoding.

of the reconciliation procedure [11]. The analogous problem remains for all the LDPC code-based reconciliation protocols, where belief propagation decoding sometimes could converge to inappropriate codeword. In order to solve this problem, an additional step of verification with universal hashing is usually considered [8, 20].

Therefore, an important task for optimizing the workflow of QKD is to provide a regime with guaranteed convergence of the information reconciliation scheme, but without significant expenditure of authentication and time resources. This can be achieved by combining the key advantages of the aforementioned schemes and by introducing some interactivity into error correction with LDPC codes. This technique is known as blind information reconciliation [18, 21, 22] and can operate without an a priori estimation of the quantum bit error rate (QBER).

In this work, we demonstrate further improvements of error correction combining LDPC codes and interactivity. We show that the use of interactivity — by introducing symmetry in operations of parties and the consideration of results of unsuccessful belief propagation decodings — allows one to perform an efficient and convergence guaranteed information reconciliation procedure. For practical QKD parameters, simulation results show an average of about 10% improvement in the efficiency and an average of about 30% improvement in the number of information requests. We refer to our proposed method as the symmetric blind information reconciliation. For a comparison of the proposed information reconciliation procedure with existing solutions, see Fig. 1.

The paper is organized as follows. In Sec. II, we explain concepts of the information reconciliation procedure. In Sec. III, we present an improvement of blind information reconciliation with LDPC codes. We summarize our results and consider an illustrative example in Sec. IV.

II. BASIC CONCEPTS OF ERROR CORRECTION

The goal of the information reconciliation procedure is to correct the errors between Alice’s and Bob’s raw keys by disclosing some key information over a public (authenticated) channel. Each bit value of the Bob’s string is a result of a transmission of the corresponding bit from the Alice’s string through a binary symmetric channel (BSC). The crossover probability q of the channel is also known as the quantum bit error rate (QBER).

One of the ways to perform error correction is to use a LDPC code which is a linear code with a sparse $m \times n$ binary parity check matrix [13, 14]. Alice multiplies the parity-check matrix by a block of the raw key of length n to obtain a syndrome of length m , which is then sent to Bob. Then, Bob performs syndrome decoding operation on his side using his raw key, the same sparse matrix and estimated level of QBER, which comes from the preceding procedures.

In the best case scenario, the syndrome decoding procedure outputs the same key as it is on the Alice’s side. Nevertheless, there is still a probability of undetected frame error. To ensure that the error correction procedure was performed properly, an additional stage of error verification is applied [8, 20]. It can be done using a universal hashing technique [23, 24], which guarantees correctness with a probability depending on the length of the hash code. There is also a possibility that the syndrome decoding based on belief propagation procedure does not converge in the specified number of iterations. Then the parties have to discard the processed blocks of the raw key and go to the next ones.

An important figure of merit for a reconciliation protocol is its efficiency f . It is given by the redundancy

of disclosed information to the theoretical limit necessary for successful reconciliation [25]. For a given BSC it is characterized by the Shannon binary entropy of the QBER [26]:

$$h_b(q) = -q \log_2 q - (1 - q) \log_2(1 - q). \quad (1)$$

Thus, the efficiency of the considered information reconciliation with LDPC code can be represented as

$$f = \frac{m}{nh_b(q)} = \frac{1 - R}{h_b(q)}, \quad (2)$$

where $R = 1 - m/n$ is a rate of the given LDPC code. The importance of the efficiency f is based on a fact that the value of disclosed information have to be removed from the key in the stage of privacy amplification. We also note that the efficiency larger than unity does not guarantee successful decoding. In fact, it depends on the specific parity-check matrix, the maximal number of iteration in decoding procedure and other factors.

A. Rate-adaptive scheme

The straightforward implementation of the LDPC error correction suffers from the following drawback. The efficiency parameter f is fixed by the dimension of the parity check matrix and the current level of the QBER, according to Eq. (2). A naive way to perform information reconciliation with the desired efficiency is to choose or construct another parity-check matrix with a new rate, *i.e.*, m/n ratio.

Two elegant ways known as shortening and puncturing have been proposed to adjust the rate of the LDPC code to the desirable efficiency by modification of encoding and decoding vectors rather than through the parity check matrix [18, 19]. The main idea is to perform syndrome coding and decoding with extended keys of length n obtained from the original raw keys of length $n - s - p$, by padding them with s shortened and p punctured bits. The shortened symbols are the ones which have values exactly known by Alice and Bob, as well as by the adversary. The values of punctured bits come from true random number generators (TRNG), independently of the both sides. In this way, the shortened (punctured) bits serve for lowering (raising) the average discrepancy between the extended keys. The positions for shortened and punctured bits could be chosen using a synchronized pseudo-random number generator (PRNG), or depending on a particular parity-check matrix (for example, via the untainted puncturing method [27]).

After the construction of the extended keys, the parties perform information reconciliation in the same way as discussed above. The difference is that in the case of a successful decoding, Bob excludes shortened and punctured bits from the result of decoding procedure to obtain a corrected version of his raw key. The efficiency of the

described scheme is defined in the following form:

$$f = \frac{m - p}{[n - p - s] h_b(q)}. \quad (3)$$

Thus, the artificial reduction (increasing) of discrepancies between extended keys by shortened (punctured) bits allows one to implement fine-tuning of efficiency in order to keep a tradeoff between a probability of failure for belief propagation decoding and information leakage.

B. Blind reconciliation

The above scheme implies a single message sent from Alice to Bob only. This is a crucial advantage as compared to the cascading method, which is highly interactive [11]. However, the cascading method demonstrates rather good efficiency, particularly at low values of the QBER [11, 16]. Also, cascade methods do not suffer from the inability to perform the error correction, *i.e.*, it always converges to some result. Therefore, the cascading method is widely used as an important benchmark for comparison of information reconciliation protocols [22].

To combine “the best of two worlds” by linking interactivity and LDPC codes, a blind information reconciliation technique was suggested [18, 21, 22]. Its title comes from the fact that it can operate without an a priori estimation of the QBER (a rough estimation of the QBER for the belief propagation decoding one can be obtained directly from syndromes [28]). Blind reconciliation is based on the hybrid automatic repeat request technique [29] with the LDPC codes with an essential presence of punctured symbols. The crucial difference is that, in the case of a decoding failure, parties try to implement the decoding procedure again by turning a number of punctured symbols into shortened ones instead of discarding their blocks. The values of these bits are transferred via the classical channel after a corresponding Bob’s request. Once the punctured bits have been exhausted it is possible to continue revealing of additional information with sifted key bits. The efficiency of the procedure after n_{add} number of additional communication rounds is given by [21]:

$$f = \frac{m - p_0 + n_{\text{add}}d}{[n - p_0 - s_0] h_b(q)}, \quad (4)$$

where s_0 and p_0 are the initial number of punctured and shortened bits, d is the number of disclosed bits in each additional round of blind reconciliation. The meaning of expression (4) in comparison with expression (3) is as follows: if the decoding procedure according to the rate adaptive scheme with efficiency (3) does not converge, then the parties increase f in each additional communication round of the blind reconciliation to increase the probability of convergence.

The main advantage of the blind reconciliation over rate-adaptive scheme is that it allows one to adjust the

efficiency to the actual error ratio, which can significantly fluctuate around the average QBER. In Refs. [21, 22] it was shown the gradual disclosing of information can notably lower the mean value of f together with frame error rate (FER). These are benefits obtained by price of introducing of additional interactivity (see Fig. 1).

III. SYMMETRIC BLIND RECONCILIATION

We suggest an improvement of blind information reconciliation with LDPC codes. The proposed technique allows one to overcome the drawbacks of the aforementioned information reconciliation schemes by providing guaranteed belief propagation-based decoding with decreased information leakage and decreased number of communication rounds. Our approach is based on applying information reconciliation with LDPC codes in a symmetric way. In particular, it consists of the following general steps (the detailed description of the procedure is given in Methods). First, in analogy to the rate-adaptive scheme, the parties choose the numbers and positions of the shortened and punctured bits and extend their blocks of raw keys. Second, both Alice and Bob compute the syndrome of their extended raw keys and share them with each other. Then they perform belief propagation decoding. In the case of success, one party, say Bob, correct the errors, and the procedure proceeds to the verification stage. In the case of a failure, the parties exchange the values of the fixed number of bits having maximal uncertainty according to log-likelihood ratio (LLR). After that, Alice and Bob repeat the belief propagation decoding procedure with the updated list of shortened and punctured positions. In this respect, the proposed symmetric blind reconciliation is similar to the standard blind reconciliation. The novel ingredient is that the positions of additionally disclosed bits come not from the punctured positions but are decidedly indicated by unsuccessful belief propagation decoding algorithm. This removes the restrictions on a number of additionally disclosed bits and also makes it possible to perform interactive LDPC code-based reconciliation even in the absence of punctured bits. The latter allows the adjustment of current sets of LDPC codes to a broad range of QBER values (see Appendix A). We also note that that in contrast to the standard blind reconciliation protocol, where the parties use two consecutive messages in each of communication rounds (the request and the corresponding answer), in the symmetric blind reconciliation the messages between parties are transferred simultaneously.

The convergence of proposed method is formally guaranteed by the fact that, in the worst case scenario, the parties reveal the entire extended key. Clearly, in this case the block will be useless for the secret key distillation. In practice, the convergence takes place after a relatively small number of additional communication rounds. The efficiency of the suggested method like in the blind reconciliation is given by Eq. (4).

The security analysis for rate-adaptive information reconciliation has been considered in details in Ref. [32]. It turns out that the symmetric blind reconciliation due to its inherent symmetry has a lot in common with the Cascade method, and the security analysis, developed for a class of adaptive symmetric error correction methods (including the Cascade method) given in Ref. [31], is applicable to our proposed scheme as well. We refer the reader to Appendix C for the details.

In order to demonstrate the improvements on the efficiency of the information reconciliation procedure, we perform a numerical simulation. In particular, we compare the proposed procedure to the standard blind reconciliation, as in most progressive LDPC based method for information reconciliation in the QKD systems. We use a set of four standard LDPC codes [33] with the rates

$$\mathcal{R} = \{5/6, 3/4, 2/3, 1/2\}, \quad (5)$$

with the block length fixed to $n = 1944$. For each of these codes, we obtain a list of bit positions according to the untainted puncturing technique [27] containing $p_{\max} = 154, 221, 295$ and 433 symbols, correspondingly. These codes are currently used in industrial QKD systems [8, 9].

We simulate standard blind and symmetric blind reconciliation procedures with the absence of initially shortened bits and p_{\max} initially punctured bits for a range of QBER values from 1% up to 10.5% (typical range for BB84 implementations). In addition, we fix the FER to less than 10%.

The number of bits to be disclosed in each additional round of the procedure is chosen according to a particular code rate R and the heuristic expression

$$d(R) = \lceil n \cdot (0.0280 - 0.02R) \cdot \alpha \rceil, \quad (6)$$

where n is the block length, α is the auxiliary parameter, and $\lceil \cdot \rceil$ is the standard ceiling operation. This expression was constructed in order to keep the mean number of additional communication rounds approximately on the same level for all the considered values of the QBER. The larger the value of the parameter α , the wider the step over the possible values of the efficiency f , for which the syndrome decoding process is tried (see Eq. (4)), and the less iterations are required to perform reconciliation. The pay for a small amount of communication rounds is that the resulting value of f becomes higher, than in the case with shorter step d . Therefore, the parameter α allows realizing a trade-off between the mean number of additional communication rounds and the mean efficiency of the information reconciliation.

The simulation results for $\alpha = 1$ and 0.5 are presented in Fig. 2. First, one can see that symmetric reconciliation improves both efficiency f . This comes from the fact that the decoding procedure in the symmetric scheme has a faster convergence rate. Moreover, it requires a smaller number of additional communication rounds.

From this data, we identify an average of 10% improvement in the efficiency (10.4% for $\alpha = 1$, and 11.4% for

$\alpha = 0.5$) and an average of 30% improvement in the number of information requests (28% for $\alpha = 1$, and 33% for $\alpha = 0.5$). Moreover, the scheme does not suffer from the frame errors coming from unsuccessful belief propagation decodings.

Next we compare two sets of codes in the rate-adaptive regime under the assumption that the level of the QBER is known. The first set of codes is the previously considered one with rates (5) and block length fixed to $n = 1944$. The second set of codes has rates in the range

$$\mathcal{R}' = \{0.5, 0.55, \dots, 0.9\} \quad (7)$$

with block length fixed to $n=4000$. It is constructed with the use of the improved edge growth algorithm [30] with the degree distribution polynomials given by Ref. [16]. The initial numbers of shortened and punctured bits are chosen to obtain initial decoding efficiency $f_{\text{start}} = 1$ (see Appendix B). For each code we also constructed a set of untainted puncturing positions [27] and use them if possible.

The results of simulation for two sets of codes and two values of α (0.5 and 1) are presented in Fig. 3. It is clearly seen that the use of codes with block length $n = 1944$ and $\alpha = 0.5$ gives roughly the same efficiency as the codes with the block length $n = 4000$ and $\alpha = 1$. This observation suggests that the symmetric blind reconciliation procedure is able to perform a trade-off between the number of required communication rounds and information leakage.

IV. DISCUSSION AND CONCLUSION

We have proposed an approach which significantly improves the blind information reconciliation technique — the most progressive LDPC codes-based method for information reconciliation in the QKD systems. The gain comes from employing information from unsuccessful decodings and making the whole information reconciliation process in a symmetric form.

Specifically, we have proposed to disclose a number of bits with the positions corresponding to maximal uncertainty of the values upon finishing of decoding procedure rather than certain bits in the punctured positions. We note that the shortcoming of the presented method is that it occupies computational resources on the both sides and make it impossible to parallelize two opposite one-way information reconciliation processes. The ability of symmetric blind reconciliation to obtain rather low values of efficiency with short-length codes is expected to realize an efficient throughput with hardware implemented syndrome decoding.

We note that short-length LDPC codes have been used to show the results of our method. The fact is that a small block length leads to high fluctuations of actual number of discrepancies in raw keys even in the case of a constant QBER. In turn, these fluctuations are crucial for successful belief propagation decoding. The feature

of blind reconciliation is that it can treat fluctuations by disclosing adequate amount of information via public channel.

The suggested method of information reconciliation can be essentially used for LDPC codes with large block lengths (say, 10^4 or 10^5). In the case of an adjustment to a proper level of initial efficiency, it can be used for the complete elimination of belief propagation decoding failures via relatively rare request of additional bit values. Nevertheless, these requests could appear to be very useful in the case of fluctuations of the QBER and especially in the case when error estimation is performed after the error correction (similar to that in Ref. [8]).

In order to evaluate the performance of our proposed scheme in the context of industrial QKD systems, we consider an illustrative example based on the results of Ref. [8]. In this particular setup, the information reconciliation was performed with a straightforward implementation of the standard $n = 1944$ LDPC code [33] with $R = 3/4$ using QBER $q \approx 1.9\%$. According to the results presented in Fig. 3, an implementation of symmetric blind reconciliation may lead to a decrease of efficiency down to $f \approx 1.3$ with approximately six additional communication rounds. It provides a 10% increase of secure key rate (we note that Cascade implementation of the information reconciliation procedure in the same conditions requires about 50 communication rounds [11]).

Moreover, in this QKD system an estimated level of QBER was calculated via the comparison of a number of key blocks before and after error correction (unverified blocks were conservatively assumed to have 50% error rate). Verification errors, resulted from unsuccessful belief propagation decodings and convergences to improper vectors, led to an overly pessimistic estimation of the QBER: $q_{\text{est}} \approx 3.4\%$. Thus, the suggested approach opens a way for QBER estimation in a more accurate way together with a more economical utilization of generated raw keys.

Our source code for a proof-of-principle realization of the symmetric blind information reconciliation procedure for Python 2.7 is freely available under GNU general public license (GPL) [34]. A proof-of-principle realization of the suggested post-processing procedure is also available [35].

Finally we would like to emphasize that in the current contribution we have considered the information ordering, inherent for QKD scheme: (i) the sifted quantum keys are generated using consistent preparing and measuring events, (ii) the information reconciliation for removing discrepancies in the sifted keys is applied, (iii) the privacy amplification, based on the estimated quantum channel parameters and information leakage in information reconciliation step, is performed for obtaining the pair of secret identical keys. Then, this pair of keys could be used for information-theoretically secure information transfer with one-time pad encryption (Vernam cipher) or other applications [37]. The above scheme differs from the another important protocol of quantum

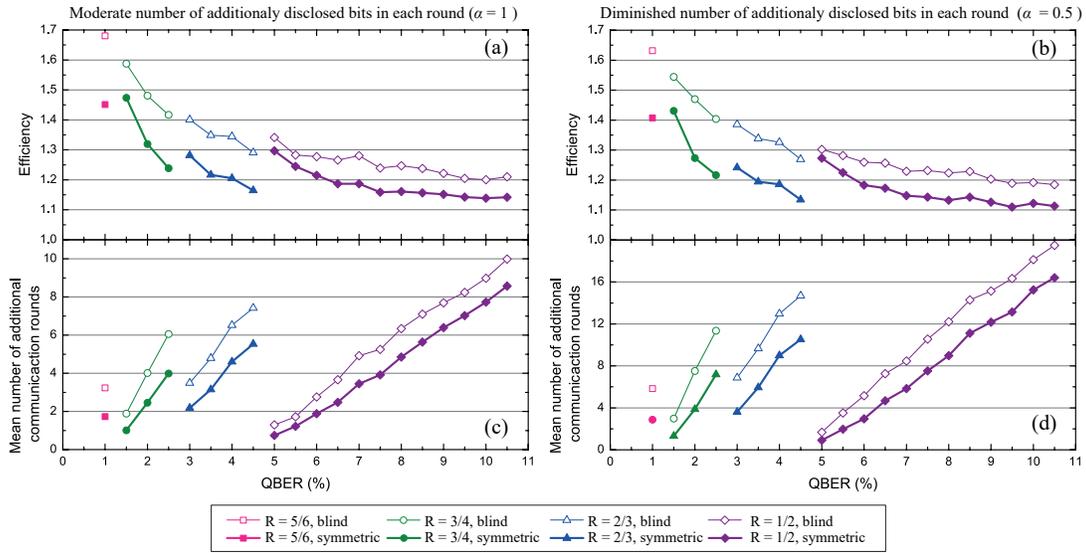


Figure 2. Comparison of the standard blind and symmetric blind information reconciliation protocols for two modes of disclosed bit number calculation (6): $\alpha = 1$ (left column) and $\alpha = 0.5$ (right column). Thin lines and empty symbols stand for blind information reconciliation, bold lines and filled symbols stand for the suggested approach (symmetric blind information reconciliation). In (a) and (b) the efficiencies, *i.e.* ratios of disclosed information to theoretical limit, are shown as functions of the QBER for the four standard LDPC codes [33] with block length $n = 1944$. In (c) and (d) the mean numbers of communication rounds are shown as function of the QBER. Changes of the codes (corresponding to different R) were performed according to the requirement that the probability of convergence for the blind reconciliation using only the punctured bits is larger than 90%. The convergence probability for the symmetric blind reconciliation is always 100%

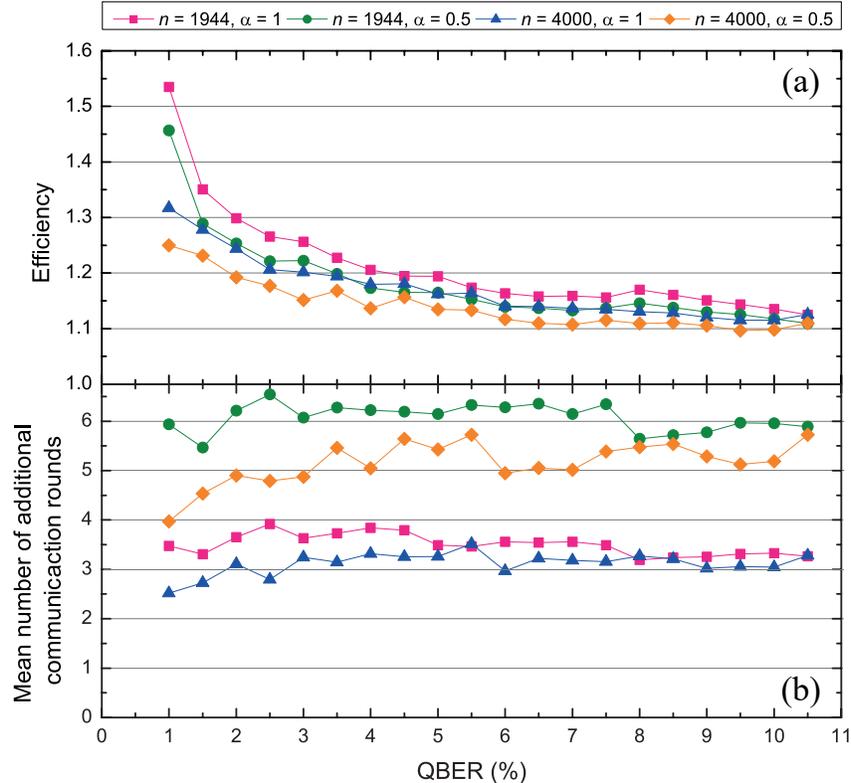


Figure 3. In (a) the efficiency of rate-adaptive symmetric blind reconciliation for two sets of codes and two modes of disclosed bit number is shown as a function of QBER. In (b) mean numbers of additional communication round of rate-adaptive symmetric blind reconciliation for two sets of codes and two modes of disclosed bit number is shown as function of QBER. The first set of codes is the standard one with block length $n = 1944$ [33] and the second set of codes consists of nine codes with rates (7) and block length $n = 4000$. The disclosed bit number chose according to (6) with $\alpha = 1$ (moderate) and $\alpha = 0.5$ (diminished).

cryptography, namely quantum secure direct communication (QSDC), where the information is directly transmitted through quantum channel without preliminary key generation stage (*e.g.* see Ref. [38] for the first theoretical proposal, and Ref. [39, 40] for recent experimental demonstrations). In the case of QSDC, there is also a need in the error correction, but usually it is more appropriate to perform it by means of some noisy-channel coding techniques: that is by adding redundancy in the transmitting message, rather than by employing public discussion after the message has been transmitted.

ACKNOWLEDGMENTS

We thank N. Gisin for a number of useful discussions and valuable comments. We thank J. Martínez-Mateo for numerous of important remarks and comments helping us to improve the manuscript. We acknowledge fruitful discussions with N. Pozhar, M. Anufriev, D. Kronberg, and D. Elkouss. We thank M. Galchenkova for invaluable input in the initial phase of the project. The research leading to these results has received funding from Russian Science Foundation under project 17-71-20146. C.C.W.L. acknowledges support from ORNL laboratory directed research and development program (LDRD), the U.S. Department of Energy Cybersecurity for Energy Delivery Systems (CEDs) program program under contract M614000329.

APPENDIX A: WORKFLOW OF THE SYMMETRIC BLIND RECONCILIATION

Here we give a detailed description of the workflow of the proposed symmetric blind reconciliation. The general scheme is presented in Fig. 4(a).

First, we assume that Alice and Bob have an estimated value of QBER q_{est} , which comes from preceding error estimation step or previous rounds of post-processing procedure. Parties start with choosing of the optimal code among set (pool) of available LDPC codes according to q_{est} and desired starting efficiency f_{start} (in all our discussions it was set to unity). For each code, specified by its $m \times n$ parity matrix \mathbf{H} (with $m < n$), parties calculate the number of shortened (s) or punctured (p) symbols that is required to obtain desired efficiency f_{start} from not adaptable efficiency $f_0 = m/[n h_b(q_{\text{est}})]$ as follows:

$$\begin{aligned} p &= \lfloor (m - n h_b(q_{\text{est}}) f_{\text{start}}) / (1 - h_b(q_{\text{est}}) f_{\text{start}}) \rfloor, \\ s &= 0, \end{aligned} \quad (\text{A1})$$

for $f_0 > f_{\text{start}}$, and

$$\begin{aligned} s &= \lceil n - m / h_b(q_{\text{est}}) f_{\text{start}} \rceil, \\ p &= 0, \end{aligned} \quad (\text{A2})$$

for $f_0 < f_{\text{start}}$.

The particular code among the set is then chosen in such way that it has the maximal number of raw key bits in the extended key. We note that in our approach we use only shortened *or* punctured bits to obtain the desired efficiency f_{start} [see also Fig. 4(b)]. This method is quite different from the commonly used approach [18, 19], where the sum of numbers of shortened and punctured bits remains constant.

Then the parties take blocks of their raw keys \mathbf{x} and \mathbf{y} of length $n - p - s$ and pad them with shortened and punctured symbols obtaining extended keys \mathbf{x}_{ext} and \mathbf{y}_{ext} of code block length n . In Fig. 4(a) we denote this operation as $E(\cdot, S, P)$, where S and P are list of positions for shortened and punctured symbols of length s and p correspondingly. If it is possible, parties choose P using position from special list, generated in advance with untainted puncturing technique [27]. Otherwise, the parties choose P as well as S with a synchronized PRNG. All shortened symbols obtains zero values, while the values of the punctured bits come from the TRNG (independently on each side). The party that modifies its raw key (in our case it is Bob) also keeps original positions of shortened and punctured symbols as S_0 and P_0 . These position are used in the final stage of the procedure.

The subsequent part of the procedure aims at reconstruction of a vector \mathbf{e}_{dec} , that we call an error pattern, such that

$$\mathbf{x}_{\text{ext}} = \mathbf{y}_{\text{ext}} + \mathbf{e}_{\text{dec}} \pmod{2}. \quad (\text{A3})$$

In order to cope with this task, both Alice and Bob initialize supposed error pattern \mathbf{e} as the zero vector, calculate the syndromes $\mathbf{s}_{\mathbf{x}}$ and $\mathbf{s}_{\mathbf{y}}$ of their extended keys \mathbf{x}_{ext} and \mathbf{y}_{ext} , and share the obtained syndromes with each other. Then each party performs belief propagation decoding with the relative syndrome

$$\mathbf{s} = \mathbf{s}_{\mathbf{x}} + \mathbf{s}_{\mathbf{y}} \pmod{2}. \quad (\text{A4})$$

We use an updated belief propagation decoding algorithm (see below), which returns not only a resulting decoded vector \mathbf{e}_{dec} (that is ‘None’ in the failure case), but also a set of bit positions D of the fixed length d which have the lowest log-likelihood (LLR) values upon finishing of decoding. In other words, the updated decoding procedure returns d positions of symbols with the most uncertainty in their values.

Due to the fact the both parties perform the same operation, they obtain the same output \mathbf{e}_{dec} and D . In the case of a failure ($\mathbf{e}_{\text{dec}} = \text{None}$), the parties share the values of bits in the positions of D , update their supposed error pattern \mathbf{e} in the positions form D according to received values:

$$\mathbf{e}[D] = \mathbf{x}_{\text{ext}}[D] + \mathbf{y}_{\text{ext}}[D] \pmod{2}, \quad (\text{A5})$$

and try to perform the decoding process again marking positions in D as shortened, that is crucial for the subsequent decoding procedure. This sequence of operations is

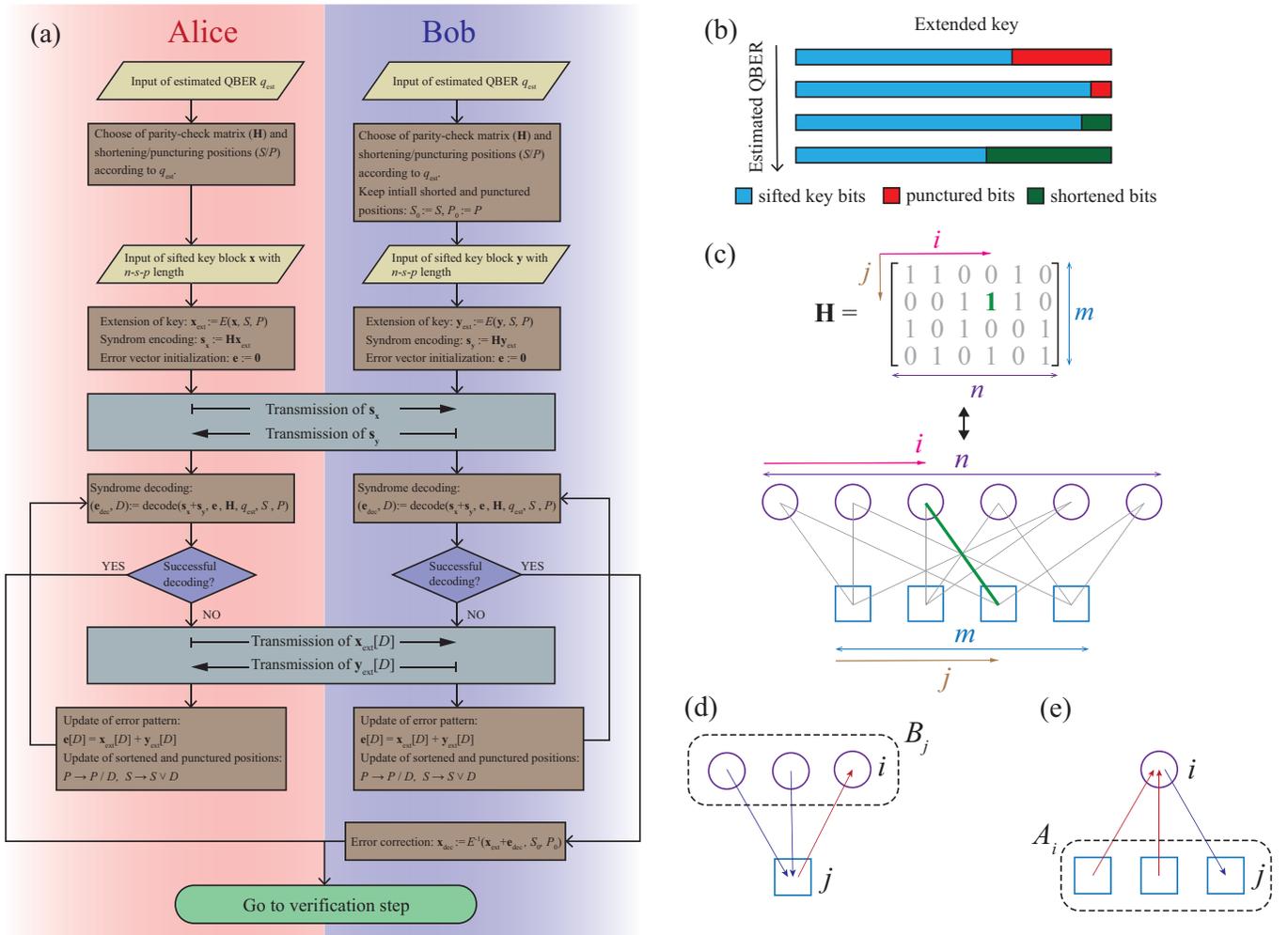


Figure 4. In (a) block scheme of symmetric blind reconciliation procedure workflow is presented. Note that all summations are assumed to be performed by modulo 2. In (b) visual representation of choosing of numbers for shortened and punctured symbols in an extending key according to estimated level of QBER for particular code is shown. In (c) the correspondence between parity-check matrix and the bipartite Tanner graph is presented. In (d) and (e) the principles of construction of messages from check node to symbol node and symbol node to check node are shown.

repeated until a convergence of belief propagation decoding. Then Bob applies error correction according to the obtained error pattern \mathbf{e}_{dec} by modulo 2 summation with his extended key \mathbf{y} . Finally, Bob excludes the symbols with initially shortened S_0 and punctured P_0 positions to obtain the corrected key \mathbf{x}_{dec} [we denote this operation as E^{-1} in Fig. 4(a)], and parties move to the verification step with the original raw key \mathbf{x} on Alice's side and its corrected version \mathbf{x}_{dec} on the Bob's one.

APPENDIX B: BELIEF PROPAGATION DECODING

We use belief propagation sum-product algorithm [14] based on a use of log-likelihood ratios (LLRs) with some updates necessary for our implementation. For a given

random bit variable X , its LLR is defined as

$$\text{LLR}(X) \equiv \log \frac{\text{Prob}(X = 0)}{\text{Prob}(X = 1)}. \quad (\text{B1})$$

One can see that sign of LLR corresponds to the most likely value of X (0 for positive LLR and 1 for negative), and its absolute value exhibits confidence level of this particular value.

The decoding algorithm is based on the representation of parity check matrix \mathbf{H} in the bipartite graph [see Fig. 4(c)]. It consists of n symbol nodes and m check nodes that corresponds to rows and columns of parity check matrix \mathbf{H} . The i -th symbol node is connected by edge with the j -th check node if and only if the corresponding element of parity check matrix is nonzero: $\mathbf{H}[i, j] = 1$. Process of a decoding can be described as exchanging of messages about symbol nodes.

We consider the decoding procedure as follows:

$$\mathbf{e}_{\text{dec}}, D := \text{decode}(\mathbf{s}, \mathbf{e}, \mathbf{H}, q_{\text{est}}, S, P), \quad (\text{B2})$$

where \mathbf{s} is syndrome, \mathbf{e} is the vector of length n have to be corrected, \mathbf{H} is the $m \times n$ parity-check matrix, q_{est} is the estimated level of crossover probability (QBER), S and P are positions of shortened and punctured bits, \mathbf{e}_{dec} is the corrected version of \mathbf{e} , D is list of positions for d symbols with the lowest LLR values, where d is considered as an external constant.

The workflow of the procedure is as follows. We start from calculation of initial LLRs for all symbol nodes. The corresponding vector is denoted as $\mathbf{r}^{(0)}$ and its elements are given by

$$\mathbf{r}^{(0)}[i] := \begin{cases} (-1)^{\mathbf{e}[i]} r_{\mathbf{k}}, & i \in K \\ (-1)^{\mathbf{e}[i]} r_{\mathbf{s}}, & i \in S \\ 0, & i \in P \end{cases}, \quad (\text{B3})$$

where K consists raw key positions, such that

$$K \cup S \cup P = \{1, 2, \dots, n\}. \quad (\text{B4})$$

Here $r_{\mathbf{k}}$ is calculated using estimated value of QBER ϵ_{est} :

$$r_{\mathbf{k}} = \log \frac{1 - q_{\text{est}}}{q_{\text{est}}}. \quad (\text{B5})$$

The LLR value for shortened symbols $r_{\mathbf{s}} \gg 1$ and in our implementation we used $r_{\mathbf{s}} := 100$. The LLR for punctured symbols is zero as there is no information about their values, since they come from independent true RNG

The initial messages from check nodes to symbol nodes are given by the initial values of corresponding LLRs as follows:

$$\mathbf{M}_{i \rightarrow j}^{(1)} := \mathbf{r}^{(0)}[i]. \quad (\text{B6})$$

Here $i \in \mathcal{N}$ and $j \in A_i$, where A_i is a set of symbol nodes connected with i -th symbol node.

Check nodes form messages back to symbol node is realized in the following way:

$$\mathbf{M}_{i \leftarrow j}^{(k)} := 2 \tanh^{-1} \left[\prod_{i' \in B_j/i} \frac{\mathbf{M}_{i' \rightarrow j}^{(k)}}{2} \right] (-1)^{\mathbf{s}[j]}, \quad (\text{B7})$$

where $j \in \mathcal{M} \equiv \{1, 2, \dots, m\}$ and $i \in B_j$ with B_j being a set of symbol nodes connected to j -th check node. We note that $\mathbf{M}_{i \leftarrow j}$ does not taking into account $\mathbf{M}_{i \rightarrow j}$. Actually $\mathbf{M}_{i \leftarrow j}$ is LLR of i -th bit value based on satisfying parity equation of j -th row of parity check matrix \mathbf{H} , and LLRs of all other symbol nodes taking part in this equation [see Fig. 4(d)].

Symbol node updates its LLR using all the messages coming from its check nodes:

$$\mathbf{r}^{(k)}[i] := \mathbf{r}^{(0)}[i] + \sum_{j \in A_i} \mathbf{M}_{i \leftarrow j}^{(k)} \quad (\text{B8})$$

and calculates current estimates of bit values

$$\mathbf{z}^{(k)}[i] := \begin{cases} 0, & \mathbf{r}^{(k)}[i] \geq 0 \\ 1, & \mathbf{r}^{(k)}[i] < 0 \end{cases}. \quad (\text{B9})$$

If this estimate satisfies all parity equations,

$$\mathbf{H}\mathbf{z}^{(k)} = \mathbf{s} \pmod{2}, \quad (\text{B10})$$

than the algorithm stops and returns decoded vector \mathbf{z}

As a stopping criteria, we consider behavior of averaged magnitude LLRs for symbols in non shortened positions:

$$\hat{\mathbf{r}}^{(k)} := \frac{1}{n-s} \sum_{i \in K \cup P} |\mathbf{r}^{(k)}[i]|. \quad (\text{B11})$$

We stop the decoding and return ‘None’ as decoded vector if for the current step k the following inequality holds

$$\hat{\mathbf{r}}^{(k)} \leq \frac{1}{\mathcal{N}} \sum_{j=k-\mathcal{N}}^{k-1} \hat{\mathbf{r}}^{(j)}, \quad (\text{B12})$$

where we used $\mathcal{N} := 5$. It can be interpreted as stop of a trend growth of our confidence in bits values. The algorithm also returns D that is a list d positions of symbols, which has minimal values of LLR magnitude:

$$D = \{i \mid |\mathbf{r}^{(k)}[i]| \leq |\mathbf{r}^{(k)}[j]| \forall j \notin D\}, \quad |D| = d. \quad (\text{B13})$$

Otherwise, algorithm goes to the next step.

According to new LLRs, we updated messages from symbol nodes to check nodes:

$$\begin{aligned} \mathbf{M}_{i \rightarrow j}^{(k+1)} &:= \mathbf{r}^{(0)}[i] + \sum_{j' \in A_i/j} \mathbf{M}_{i \leftarrow j'}^{(k)} \\ &= \mathbf{r}^{(k)}[i] - \mathbf{M}_{i \leftarrow j}^{(k)} \end{aligned} \quad (\text{B14})$$

counter of iterations is incremented: $k := k + 1$ [see Fig. 4(e)], and algorithm goes to the step with check nodes form messages back to symbol node [see Eq. (B8)].

It is important to note that the most computationally expensive calculation (B7) can be optimized by using a technique suggested in Ref. [36]. We also point out that Eq. (B7) allows revealing some peculiarity of punctured symbols. Zero LLR of punctured symbol $i \in B_j$ on the first step ‘deactivates’ the j -th check node making all messages $\mathbf{M}_{i' \leftarrow j}$ ($i' \in B_j$, $i' \neq i$) to other symbol nodes to be zero. If there are no punctured bits in B_j/i then $|\mathbf{M}_{i \leftarrow j}| > 0$ and i th node become ‘rescued’ after the first iteration and then participates in decoding procedure. However, if there are a least of two punctured nodes connected to given j -th check node, then all messages $\mathbf{M}_{i \leftarrow j}$, $i \in B_j$ are zero. There still a possibility that the punctures symbols will be ‘rescued’ via another check nodes, but nonetheless such behavior indicates the importance of choosing a set of punctured symbols. To avoid this situation the special technique of untainted puncturing is used [27].

APPENDIX C: SECURITY OF SYMMETRIC BLIND RECONCILIATION

Here we consider a security issue of the presented symmetric blind reconciliation protocol. Particularly, we show that the amount of information leakage have to be taken into account in the privacy amplification step in accordance with Eq.(4) is given by

$$\text{leak}_{\text{ec}} = m - p_0 + n_{\text{add}} d, \quad (\text{C1})$$

where recall m is the syndrome length, p_0 is the initial number of punctured symbols, n_{add} is number of additional communication rounds, and d is the number of bits disclosed in each of these rounds.

During the symmetric blind reconciliation Alice and Bob exchange

$$\mathcal{L} = 2(m + n_{\text{add}} d) \quad (\text{C2})$$

bits of information: each party transfers m -bit syndrome and $n_{\text{add}} d$ bits in additional communication rounds. Obviously, the information leakage could not be larger than \mathcal{L} . Nevertheless, the actual leakage turns out to be lower (and given by Eq.(C1)) for two reasons. The first is that the p_0 punctured symbols due to their inherent uncertainty decrease the leakage from each of the syndromes from m to $m - p_0$; and the second is that the factor 2 in (C2) could be omitted due to the fact that each pair of parity bits (one transferring from Alice to Bob, and the other – in the opposite direction) can bring only one bit of valuable information to the eavesdropper. Next we would like to focus on these two points.

Let us consider a symmetric blind reconciliation protocol for $m \times n$ parity-check matrix, $(n - s_0 - p_0)$ -bit sifted keys, s_0 shortened, and p_0 punctured bits. Recall that the punctured symbols are the bits with values coming from independent TRNGs on both sides. The consideration of puncturing technique is greatly simplified in untainted puncturing [27], that is employed in our scheme. In the untainted puncturing each of the check nodes of the Tanner graph (corresponding the employed parity-check matrix) is connected with at most one punctured symbol. This implies that it is possible to split all the syndrome bits' positions $\{1, 2, \dots, m\}$ into the subsets F and \bar{F} where F contains p_0 check nodes' indices of those which are connected with the punctured bits, and the subset $\bar{F} \equiv \{1, 2, \dots, m\}/F$ contains all the remaining syndrome bit positions. Since each of the syndromes' bit values $\mathbf{s}_{\mathbf{x}}[F]$ and $\mathbf{s}_{\mathbf{y}}[F]$ is obtained as their result of modulo-2 summation of non-punctured symbols and a single punctured bit (which is completely random at each side), the disclosure of $\mathbf{s}_{\mathbf{x}}[F]$ and $\mathbf{s}_{\mathbf{y}}[F]$ in the public channel does not bring any valuable information to the eavesdropper. One can imagine that bits of $\mathbf{s}_{\mathbf{x}}[F]$ and $\mathbf{s}_{\mathbf{y}}[F]$ are transferred separately from all the other public communication that is considered further. Thus, the information leakage does not exceed $2(m - p_0 + n_{\text{add}} d)$ bits. We would like to remark that the case of random

puncturing, where the *positions* for punctured symbols are chosen with synchronised PRNGs, could be treated in a similar way, but in this case an additional information about the Tanner graph construction method have to be taken into account. One have to show that it is always possible to chose p_0 syndrome bits whose values are statistically independent from the $n - p_0$ values of symbols that are not punctured.

The second statement about the factor 2 in (C2) is closely related to a similar question regarding to the one of the first information reconciliation protocols – Cascade [10], where Alice and Bob also exchange with parity bits of some blocks of their keys in the symmetrical way. A rigorous examination of this question related to the BB84 protocol is considered by H.-K. Lo in Ref. [31]. In his work Lo considers the *adaptive symmetric method for error correction* (which we will refer as *adaptive symmetric error correction*) — the generalized information reconciliation protocol which includes Cascade and the symmetric blind reconciliation. Next, we provide its definition.

Definition (adapted from Ref. [31]). Adaptive symmetric error correction is an iterative procedure applied to the Alice's n -bit string \mathbf{x} and Bob's n -bit string \mathbf{y} (which is a corrupted version of \mathbf{x}). where the rounds of operations given below are performed.

- Round 1. Alice picks an n -bit string \mathbf{a}_1 , broadcasts \mathbf{a}_1 and the parity $p_{\mathbf{x},1} = \mathbf{a}_1 \cdot \mathbf{x} \pmod{2}$. Bob broadcasts the parity $p_{\mathbf{y},1} = \mathbf{a}_1 \cdot \mathbf{y} \pmod{2}$. Alice and Bob compute the relative parity $r_1 = p_{\mathbf{y},1} - p_{\mathbf{x},1} \pmod{2}$.
- Round i ($i > 1$). Alice picks an i -bit string \mathbf{a}_i , where the choice of \mathbf{a}_i may depend on the strings $\{\mathbf{a}_j | j < i\}$ and the relative parities $\{r_j | j < i\}$ (but not on the individual parities, $\{p_{\mathbf{x},j} | j < i\}$ and $\{p_{\mathbf{y},j} | j < i\}$). Then Alice broadcasts \mathbf{a}_i and the parity $p_{\mathbf{x},i} = \mathbf{a}_i \cdot \mathbf{x} \pmod{2}$. Bob broadcasts the parity $p_{\mathbf{y},i} = \mathbf{a}_i \cdot \mathbf{y} \pmod{2}$. Alice and Bob compute the relative parity $r_i = p_{\mathbf{y},i} - p_{\mathbf{x},i} \pmod{2}$.

After some number N of necessary rounds, Bob corrects the errors in his string \mathbf{y} by applying a recovery operator

$$\mathbf{z} := \text{Recover}(\mathbf{y}, \{r_i\}_{i=1}^N). \quad (\text{C3})$$

Ideally, $\mathbf{z} = \mathbf{x}$ and Alice and Bob will now share the same string \mathbf{x} .

One can see that in the described protocol Alice and Bob exchange with $2N$ bits of information: N bits goes from Alice to Bob, and N bits – in the opposite direction. In Ref. [31] it is proven that the procedure of adaptive symmetric error correction is secure for purposes of the BB84 QKD protocol in the case where both parity bits $p_{\mathbf{x},i}$ and $p_{\mathbf{y},i}$ are one-time pad encrypted with the *same* secret bit. That is, Alice and Bob exchange with the messages $p_{\mathbf{x},i} + \mathbf{w}[i] \pmod{2}$ and $p_{\mathbf{y},i} + \mathbf{w}[i] \pmod{2}$, where \mathbf{w} is an n -bit string of the secret key possessed by Alice and Bob. From an overall key generation balance

point of view, this scenario is equivalent to the situation, where the information leakage in the adaptive symmetric error correction is equal to N .

Now we return to the symmetric blind reconciliation. As it was shown, the communication of $\mathbf{s}_x[F]$ and $\mathbf{s}_y[F]$ can be considered separately since all these bits do not bring any valuable information to the eavesdropper. The exchange of the remaining syndromes' bits $\mathbf{s}_x[\overline{F}]$ and $\mathbf{s}_y[\overline{F}]$ can be regarded as the first $m - p_0$ rounds of the adaptive symmetric error correction: for each syndrome bit, the string \mathbf{a}_i from the definition is the corresponding row of the employed parity-check matrix. The syndrome decoding algorithm (B2) either converges and allows Bob to perform recover of \mathbf{x} , or returns a set of positions D for the new communication round. Note that the set D is obtained as a result of the syndrome decoding executed for the relative syndrome \mathbf{s} . By its definition (see (A4)),

the relative syndrome consists of relative parities, therefore the choice of positions for the set D is in agreement with the definition of adaptive symmetric error correction. Each of the additional communication rounds of the symmetric blind reconciliation, in respect to the set D , can be regarded as $|D| = d$ of communication rounds in the definition of the adaptive symmetric error correction. Namely, the string \mathbf{a}_i has all zeros except of single one at the position D_j (here i is number of the round in the general sequence, and j is the index of the element inside the set D of length d).

Thus, the completion of the symmetric blind reconciliation with n_{add} additional rounds corresponds to the adaptive symmetric error correction with $N = m - p_0 + n_{\text{add}}d$ rounds, and the information leakage given by expression (C1).

-
- [1] C.H. Bennet and G. Brassard, Quantum cryptography: public key distribution and coin tossing, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing Bangalore, India* (IEEE, New York, 1984), p. 175.
- [2] C.H. Bennett, F. Bessette, L. Salvail, G. Brassard, and J. Smolin, Experimental quantum cryptography, *J. Cryptol.* **5**, 3 (1992).
- [3] For a review, see N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, *Rev. Mod. Phys.* **74**, 145 (2002).
- [4] For a review, see V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, *Rev. Mod. Phys.* **81**, 1301 (2009).
- [5] Characteristics of commercial devices from ID Quantique (Switzerland), SeQureNet (France), and the Austrian Institute of Technology (Austria) are available.
- [6] R. Renner, Security of quantum key distribution, *Int. J. Quantum Inform.* **6**, 1 (2008); *Security of Quantum Key Distribution*, PhD thesis, ETH Zurich; arXiv:0512258 (2005).
- [7] M. Peev et al., The SECOQC quantum key distribution network in Vienna, *New J. Phys.* **11**, 075001 (2009).
- [8] N. Walenta, A. Burg, D. Caselunghe, J. Constantin, N. Gisin, O. Guinnard, R. Houlmann, P. Junod, B. Korzh, N. Kulesza, M. Legré, C.C.W. Lim, T. Lunghi, L. Monat, C. Portmann, M. Soucarros, P. Trinkler, G. Trollet, F. Vannel, and H. Zbinden, A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing, *New J. Phys.* **16** 013047 (2014).
- [9] E.O. Kiktenko, A.S. Trushechkin, Y.V. Kurochkin, and A.K. Fedorov, Post-processing procedure for industrial quantum key distribution systems, *J. Phys. Conf. Ser.* **741**, 012081 (2016).
- [10] G. Brassard and L. Salvail, Secret-key reconciliation by public discussion, *Lect. Notes Comput. Sc.* **765**, 410 (1994).
- [11] J. Martínez-Mateo, C. Pacher, M. Peev, A. Ciurana, and V. Martin, Demystifying the information reconciliation protocol Cascade, *Quant. Inf. Comp.* **15**, 453 (2015).
- [12] T. Pedersen and M. Toyran, High performance information reconciliation for QKD with cascade, *Quantum. Inf. Comput.* **15**, 419 (2015).
- [13] R. Gallager, Low density parity check codes, *IRE Trans. Inf. Theory* **8**, 21 (1962).
- [14] D.J.C. MacKay, Good error-correcting codes based on very sparse matrices, *IEEE Trans. Inf. Theory* **45**, 399 (1999).
- [15] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, Current status of the DARPA quantum network, *Proc. SPIE* **5815**, 138 (2005).
- [16] D. Elkouss, A. Leverrier, R. Alleaume, and J.J. Boutros, Efficient reconciliation protocol for discrete-variable quantum key distribution, in *Proceedings of the IEEE International Symposium on Information Theory*, Seoul, South Korea, (2009), p. 1879
- [17] A Mink and A. Nakassis, LDPC for QKD reconciliation, *Comput. Sci. Technol. Int. J.* **2**, 2162 (2012).
- [18] D. Elkouss, J. Martínez-Mateo, and V. Martin, Information reconciliation for quantum key distribution, *Quant. Inf. Comp.* **11**, 226 (2011).
- [19] D. Elkouss, J. Martínez-Mateo, and V. Martin, Secure rate-adaptive reconciliation, in *Proceedings of the IEEE International Symposium on Information Theory and its Applications (ISITA)*, Taichung, Taiwan (IEEE, 2010), p. 179.
- [20] C.-H. F. Fung, X. Ma, and H. F. Chau, Practical issues in quantum-key-distribution postprocessing, *Phys. Rev. A* **81**, 012318 (2010).
- [21] J. Martínez-Mateo, D. Elkouss, and V. Martin, Information reconciliation for quantum key distribution, *Quant. Inf. Comp.* **12**, 791-812 (2012).
- [22] J. Martínez-Mateo, D. Elkouss, and V. Martin, Key reconciliation for high performance quantum key distribution, *Sci. Rep.* **3**, 1576 (2013).
- [23] J.L. Carter, and M.N. Wegman, New hash functions and their use in authentication and set equality, *J. Comput. Syst. Sci.* **18**, 143 (1977).
- [24] M.N. Wegman and L.J. Carter, Universal classes of hash functions, *J. Comput. Syst. Sci.* **22**, 265 (1981).

- [25] D. Slepian, and J. Wolf, Noiseless coding of correlated information sources, *IEEE Trans. Inf. Theory* **19**, 471-480 (1973).
- [26] C.E. Shannon and W. Weaver, *The Mathematical Theory of Communication* (University of Illinois Press, 1963).
- [27] D. Elkouss, J. Martínez-Mateo, and V. Martin, Untainted puncturing for irregular low-density parity-check codes, *IEEE Wireless Comm. Lett.* **1**, 585 (2012).
- [28] G. Lechner and C. Pacher, Estimating channel parameters from the syndrome of a linear code, *IEEE Comm. Lett.* **17**, 2148 (2013).
- [29] R. Comroe and D. Costello, ARQ schemes for data transmission in mobile radio systems, *IEEE J. Sel. Area Comm.* **2**, 472 (1984).
- [30] J. Martínez-Mateo, D. Elkouss, and V. Martin, Improved construction of irregular progressive edge-growth Tanner graphs, *IEEE Comm. Lett.* **14**, 1155 (2010).
- [31] H.-K. Lo, Method for decoupling error correction from privacy amplification, *New J. Phys.* **5**, 6 (2003).
- [32] D. Elkouss, J. Martinez-Mateo, and V. Martin, Analysis of a rate-adaptive reconciliation protocol and the effect of leakage on the secret key rate, *Phys. Rev. A* **87**, 042334 (2013).
- [33] *IEEE Standard for Information Technology*, 802.11n-2009.
- [34] E.O. Kiktenko, M.N. Anufriev, N.O. Pozhar, and A.K. Fedorov, Symmetric information reconciliation for the QKD post-processing procedure (source code), DOI: 10.5281/zenodo.164953.
- [35] E.O. Kiktenko, A.S. Trushechkin, M.N. Anufriev, N.O. Pozhar, and A.K. Fedorov, Post-processing procedure for quantum key distribution systems (source code), DOI: 10.5281/zenodo.200365.
- [36] X.-Y. Hu, E. Eleftheriou, D.-M. Arnold, and A. Dholakia, Efficient implementations of the sum-product algorithm for decoding LDPC codes, in *Proceedings of Global Telecommunications Conference, San Antonio, TX, USA (IEEE, 2001)*, p. 1879.
- [37] R. Alléaume, C. Branciard, J. Bouda, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Länger, N. Lütkenhaus, C. Monyk, P. Painchault, M. Peev, A. Poppe, T. Pornin, J. Rarity, R. Renner, G. Ribordy, M. Riguidel, L. Salvail, A. Shields, H. Weinfurter, and A. Zeilinger, Using quantum key distribution for cryptographic purposes: A survey, *Theor. Comput. Sci.* **560**, 6281 (2014).
- [38] G. L. Long and X. S. Liu, Theoretically efficient high-capacity quantum-key-distribution scheme, *Phys. Rev. A* **65**, 032302 (2002).
- [39] J.-Y. Hu, B. Yu, M.-Y. Jing, L.-T. Xiao, S.-T. Jia, G.-Q. Qin, and G.-L. Long, Experimental quantum secure direct communication with single photons, *Light Sci. Appl.* **5**, e16144 (2016).
- [40] W. Zhang, D.-Sh. Ding, Y.-B. Sheng, L. Zhou, B.-S. Shi, and G.-C. Guo, Quantum secure direct communication with quantum memory, *Phys. Rev. Lett.* **118**, 220501 (2017).