entropy

IMPACT FACTOR 2.738

Indexed in: PubMed

Article

Asymmetric Adaptive LDPC-Based Information Reconciliation for Industrial Quantum Key Distribution

Nikolay Borisov, Ivan Petrov and Andrey Tayduganov

Special Issue

Quantum Information: From Fundamental Aspects to Practical Applications

Edited by

Dr. Aleksey Fedorov

MDPI

https://doi.org/10.3390/e25010031

entropy

MDPI

Article

Asymmetric Adaptive LDPC-Based Information Reconciliation for Industrial Quantum Key Distribution

Nikolay Borisov †, Ivan Petrov † and Andrey Tayduganov *

Laboratory of Quantum Information Technologies, National University of Science and Technology "MISiS", Moscow 119049, Russia

* Correspondence: a.taiduganov@misis.ru

† These authors contributed equally to this work.

Abstract: We develop a new approach for asymmetric LDPC-based information reconciliation in order to adapt to the current channel state and achieve better performance and scalability in practical resource-constrained QKD systems. The new scheme combines the advantages of LDPC codes, a priori error rate estimation, rate-adaptive and blind information reconciliation techniques. We compare the performance of several asymmetric and symmetric error correction schemes using a real industrial QKD setup. The proposed asymmetric algorithm achieves significantly higher throughput, providing a secret key rate that is close to the symmetric one in a wide range of error rates. Thus, our approach is found to be particularly efficient for applications with high key rates, limited classical channel capacity and asymmetric computational resource allocation.

Keywords: quantum communication; quantum key distribution (QKD); information reconciliation; adaptive error correction; LDPC

Citation: Borisov, N.; Petrov, I.; Tayduganov, A. Asymmetric Adaptive LDPC-Based Information Reconciliation for Industrial Quantum Key Distribution. *Entropy* **2023**, *25*, 31. https://doi.org/10.3390/e25010031

Academic Editor: Aleksey Fedorov

Received: 24 November 2022
Revised: 10 December 2022
Accepted: 19 December 2022
Published: 23 December 2022

1. Introduction

Quantum key distribution (QKD) systems are considered as unconditionally secure trusted couriers for symmetric-key encryption of classical communication. According to the common principle of QKD, the so-called "quantum" part of a protocol is followed by the classical post-processing procedure in order to distill the raw key copies and form a common secret key for both participants. This post-processing procedure consists of the following basic steps: sifting, error correction, parameter estimation, privacy amplification and session authentication [1]. In particular, the error correction (EC) process is executed in order to find and correct all incompatible bits using a classical public channel but still maintaining most of the key data that is unrevealed. This step is thought to be the most computationally complex and time-consuming of the entire procedure [2] and therefore includes the potential for optimization. It is also the most secret-key-reducing part [3,4].

The EC procedure, often referred to as information reconciliation (IR), can be implemented in QKD using various EC techniques [3,5–9]. Among them, the low-density parity-check (LDPC) codes [10] are well studied and widely applied in modern telecommunication systems. The main advantage of the LDPC codes is the possibility to reach information rates that are arbitrarily close to the Shannon limit for a wide variety of channels [11]. That possibility can be implemented by satisfying several basic conditions, such as efficient decoder design, parity check matrix construction and apropos code rate adaptation.

The straightforward LDPC-based EC is asymmetric since the syndrome decoding process is much more computationally complex than the encoding one. In a scheme where the transmitter (Alice) performs encoding and the receiver (Bob) is decoding, Alice's computer is idle most of the time, and the entire throughput is determined by the decoding speed of Bob's computer. Therefore, to avoid this asymmetric and inefficient use of computational resources, some modern industrial point-to-point QKD solutions implement a bi-directional [12,13] or symmetric blind IR approach [14].

The first approach is based on the parallel processing of different sifted key frames by Alice and Bob, achieving a Mbps key throughput. The second one combines the advantages of LDPC and the interactivity of the Cascade IR protocol in the correction of the same frame, achieving fail-resistant performance and high information efficiency simultaneously. These highly-efficient reconciliation schemes, however, remain practical only if both Alice and Bob possess sufficiently powerful computing devices.

Currently, the latest commercially available QKD devices (manufactured by, e.g., ID Quantique, QuantumCTek, Toshiba) are designed as 19-inch rack modules, having the same size specifications for both transmitter and receiver. However, in some practical QKD schemes and applications, one may prefer to minimize the size and cost of the transmitter device and, as a consequence, reduce its computational load. For instance, in an urban star-topology quantum network with one powerful receiver server connecting multiple users, it would be ideal in the future to develop a user's transmitter device of the PCI-e card form factor to be installed inside a normal personal computer. In order to save the processor's computation resources and power consumption, such a transmitter has to execute minimum complex EC operations.

Another example is the satellite QKD in which the satellite is a transmitter playing the role of a trusted node [15]. For the same reasons, such a device requires minimization of the load on its computing module and on the service channel, preserving efficient performance under unstable quantum channel conditions. One can also consider hand-held devices [16]. Therefore, for such applications, one has to reconsider the EC workflow considering the inequality of computational resources of transmitter and receiver. The design must be aimed to provide a real-time post-processing service for such asymmetric QKD systems.

In this work, we consider the decoy-state BB84 protocol [17–20] and revisit the asymmetric LDPC-based reconciliation [12,21–25], in which the syndrome decoding is performed only on Bob's side, by modifying and improving the existing symmetric blind IR scheme [14]. We develop a novel rate-adaptive algorithm that employs a new optimal code rate selection approach based on our a priori quantum bit error rate estimation method. It is shown that the knowledge of the precise error rate value and the proper code rate choice is crucial for high-performance EC.

We also propose a different additional round organization rule that allows a direct code efficiency control without round number limitation. Using the simulated and real experimental data, we demonstrate that the new asymmetric scheme is able to achieve almost the same efficiency as a symmetric one while maintaining the low failure probability and time consumption. The performance of our scheme on data is also compared with two blind asymmetric schemes, proposed in [22,26], that use different bit disclosure rules during additional rounds.

The paper is organized as follows. In Section 2, we review the basics of the IR procedure, particularly focusing on asymmetry-related solutions. In Section 3, we discuss the details of the code rate scheme adaptation changes that have to be made in order to save a satisfactory overall efficiency parameter of the cryptosystem. In Section 4, we compare the asymmetric and symmetric approaches using a set of benchmarks. We summarize our results in Section 5.

2. Information Reconciliation with LDPC Codes

In the BB84 QKD protocol [27] the sifted keys of Alice and Bob, made out of raw keys by rejecting events with incompatible bases, are not 100% identical and contain quantum bit errors that must be found and corrected. After correction and subsequent verification, the key passes to the privacy amplification step—a special contraction of the verified key with 2-universal hash functions into a shorter unconditionally secure secret key in order to minimize information of potential eavesdropper (Eve) to an arbitrarily low value. For practical reasons, the sifted key is accumulated in blocks of fixed size ℓ_{block}.

In order to minimize the effect of statistical fluctuations on the final secret key length evaluation and consequently obtain a less conservative result, ℓ_{block} has to be of the order of 10^6 and larger. Since such bit string size is too large for high-speed and efficient LDPC-based

EC; the block is split into a number of smaller subblocks of length $\ell_{\text{subblock}} \sim 10^3$–$10^5$ bits and EC is performed on each subblock separately.

Each subblock correction starts with an a priori quantum bit error rate (QBER) estimation. The straightforward approach is to disclose and publicly compare a random sample of the sifted key. The disclosed bits have to be discarded by Alice and Bob. To avoid such excessive key consumption, the estimation can be done by analyzing only indirect information about errors, such as the polarization drift [28] for polarization-encoding protocol or LDPC syndrome [29,30] for general discrete variable QKD protocol.

Originally, the LDPC codes were designed for a one-way EC scheme [11]. In this scheme, Alice selects an appropriate code of rate R that fits the quantum channel capacity, determines the corresponding sparse parity-check matrix H_R, calculates the syndrome $\boldsymbol{s}_A$ of length $(1-R)\ell_{\text{subblock}}$ from her message (key) $\boldsymbol{x}_A$,

$$\boldsymbol{s}_A = H_R \boldsymbol{x}_A \pmod 2 \tag{1}$$

and sends it to Bob via a classic authenticated channel. Bob, in turn, computes the syndrome $\boldsymbol{s}_B = H_R \boldsymbol{x}_B$ from their sifted bit string $\boldsymbol{x}_B$ and performs Alice's syndrome decoding that can be interpreted as searching for error pattern $\boldsymbol{e}$ such that

$$H_R\, \boldsymbol{e} \pmod 2 = \boldsymbol{s}_A \oplus \boldsymbol{s}_B\,. \tag{2}$$

Solving (2), Bob corrects their bit string: $\boldsymbol{x}_B \to \boldsymbol{x}_B \oplus \boldsymbol{e} \equiv \boldsymbol{x}_A$. If the solution is not found within a limited period of time, the decoding fails.

The efficiency of LDPC algorithms can be further increased using the rate-adaptive [4,21] and blind reconciliation [22] methods. To adapt the code rate R more precisely to the current quantum channel state, we use the puncturing (and shortening) technique [31,32]. This is based on the idea of extending subblock (payload data) to a new EC unit, hereafter called *frame*, by inserting additional noise (punctured bits) into $\boldsymbol{x}_{A,B}$. Then, the blind IR can be applied to increase the EC success probability. In this approach, an accurate a priori QBER estimation and initial choice of R are considered to be unnecessary.

Instead, if Bob reports their basic round decoding failure, during additional rounds, Alice discloses some fraction of her punctured bit values and Bob makes another decoding attempt, this time with more information about the frame. The resulting efficiency deteriorates with the number of disclosed bits and the number of additional rounds. Consequently, the frame correction running time and the load on the classical channel increase, and the EC success probability increases.

The number of additional rounds is limited by the amount of information to be revealed and the revealing strategy. In the original blind reconciliation scheme [22], during every additional round, Alice discloses the fixed number of punctured bits, $d_k = p/N_{\text{add}}^{\max}$, where $p = \alpha \ell_{\text{frame}}$ is the total number of punctured bits in the frame, defined by empiric code rate adaptation parameter α, and $N_{\text{add}}^{\max}$ is the maximum allowed number of additional rounds. Another method, proposed in an attempt to make the decoder converge faster, is the linearly increasing with iteration number k step $d_k = k\delta$ ($k \geq 1$) where δ is determined empirically [26].

In symmetrically organized reconciliation [14], Alice and Bob share their syndromes and both perform belief-propagation decoding of (2). In the case of failure, they compute the log-likelihood ratio (LLR) for every bit in the frame and then disclose to each other only the bits with minimal LLR. To increase the decoding success probability, both punctured and payload bits are allowed to be disclosed (of course, such payload bits are excluded from the final secret key). Then, Alice and Bob refresh their EC frames using new data and perform another decoding attempt. In [14], the following heuristic rule is used to determine the disclosed data amount: $d_k(R) = \lceil \ell_{\text{frame}}(0.028 - 0.02R)\beta \rceil$, $\beta \in \{0.5, 1\}$.

In the case of unsuccessful decoding, the process is stopped if all bits are disclosed, or the frame correction time budget is over. The authors of [14] compared the blind approach with

the rate-adaptive regime under the assumption that the QBER level is known and performed a simulation that showed better efficiency and number of iterations.

The symmetric strategy shows itself to be highly efficient; however, for the asymmetric scheme, Alice has no intermediate decoder parameters, such as positions of bits with minimal LLR, and thus she cannot disclose this auxiliary data to Bob blindly anymore. Using different ideas, some solutions were proposed in Refs. [24,25]. In this work, we step aside from the blind reconciliation principle and develop further the additional rounds' organization strategy that preserves the efficiency of symmetric IR in the presence of limited computational resources.

IR Performance Metrics

Since Eve can, in principle, extract some partial useful information from syndromes and other data, exchanged via the classic channel during the IR communication rounds, this potential leakage has to be subtracted and considered in the final key length estimation. In order to quantify the EC efficiency and estimate the amount of disclosed information about the key, the following metric is introduced [21]:

$$f_{\text{ec}} = \frac{\ell_{\text{syndrome}} - p + d}{(\ell_{\text{frame}} - p - s) h_2(E_\mu)} \tag{3}$$

with $\ell_{\text{syndrome}} = (1 - R)\ell_{\text{frame}}$ and $p + s = \ell_{\text{frame}} - \ell_{\text{subblock}} = \alpha \ell_{\text{frame}}$ where

- E_μ—the average signal pulse QBER of a subblock.
- p—the number of punctured bits in a frame.
- s—the number of shortened bits in a frame.
- $d = \sum_k d_k$—the total number of disclosed bits in additional rounds.
- $h_2(x) = -x \log_2 x - (1 - x) \log_2 (1 - x)$—the Shannon binary entropy.

This metric represents the ratio of the information content used to reconcile one data frame over the minimal information theoretically required [4]. Thus, a large f_{ec} implies less efficient EC. A large f_{ec} also indicates the process interactivity. Note that f_{ec} cannot approach values less than 1 due to Shannon's limit. In this way, for purely theoretical studies, the average information leakage per successfully corrected subblock can be estimated as $\ell_{\text{subblock}} f_{\text{ec}} h_2(E_\mu)$.

Another important code quality metric that also affects the secret key generation rate is the frame error rate (FER)—the frame decoding failure probability. Considering FER, the modified formula for the average secret key length from [20] can be written as follows,

$$\ell_{\text{sec}} \simeq \ell_{\text{block}} (1 - \text{FER}) \left\{ \kappa_1^l [1 - h_2(E_1^u)] - f_{\text{ec}} h_2(E_\mu) \right\} \tag{4}$$

where κ_1^l is a lower bound on the fraction of bits in the verified key obtained from single-photon pulses, and E_1^u is an upper bound on the fraction of errors in such positions in the sifted keys (for their estimations, see, e.g., [20,33]). The trade-off between low (high) f_{ec} and high (low) FER is the main objective of this IR research.

Finally, the last important factor is the CPU load. As already mentioned above, the LDPC decoder complexity essentially depends on the frame length ℓ_{frame}. Hence, the processing time consumption is linearly dependent on the total number of decoding iterations that can be used to analyze the load of Bob's module. Therefore, for practical QKD applications, even more crucial performance criterion is the average secret key generation rate, which can be estimated as

$$R_{\text{sec}} = \frac{\ell_{\text{sec}}}{\tau} \tag{5}$$

where τ is the time needed to produce a secret key of length ℓ_{sec} or equivalently the overall block generation and post-processing time. In this way, Equations (4) and (5) can be used as the main benchmarks when comparing various EC schemes with different f_{ec}, FER and number of additional EC rounds.

3. Adaptive Code Rate Method for Asymmetric Blind Reconciliation

In this section, we describe the proposed asymmetric algorithm, schematically shown in Figure 1, which contains three key steps explained below. Before going into detail, let us first list the used basic IR parameters and tools.

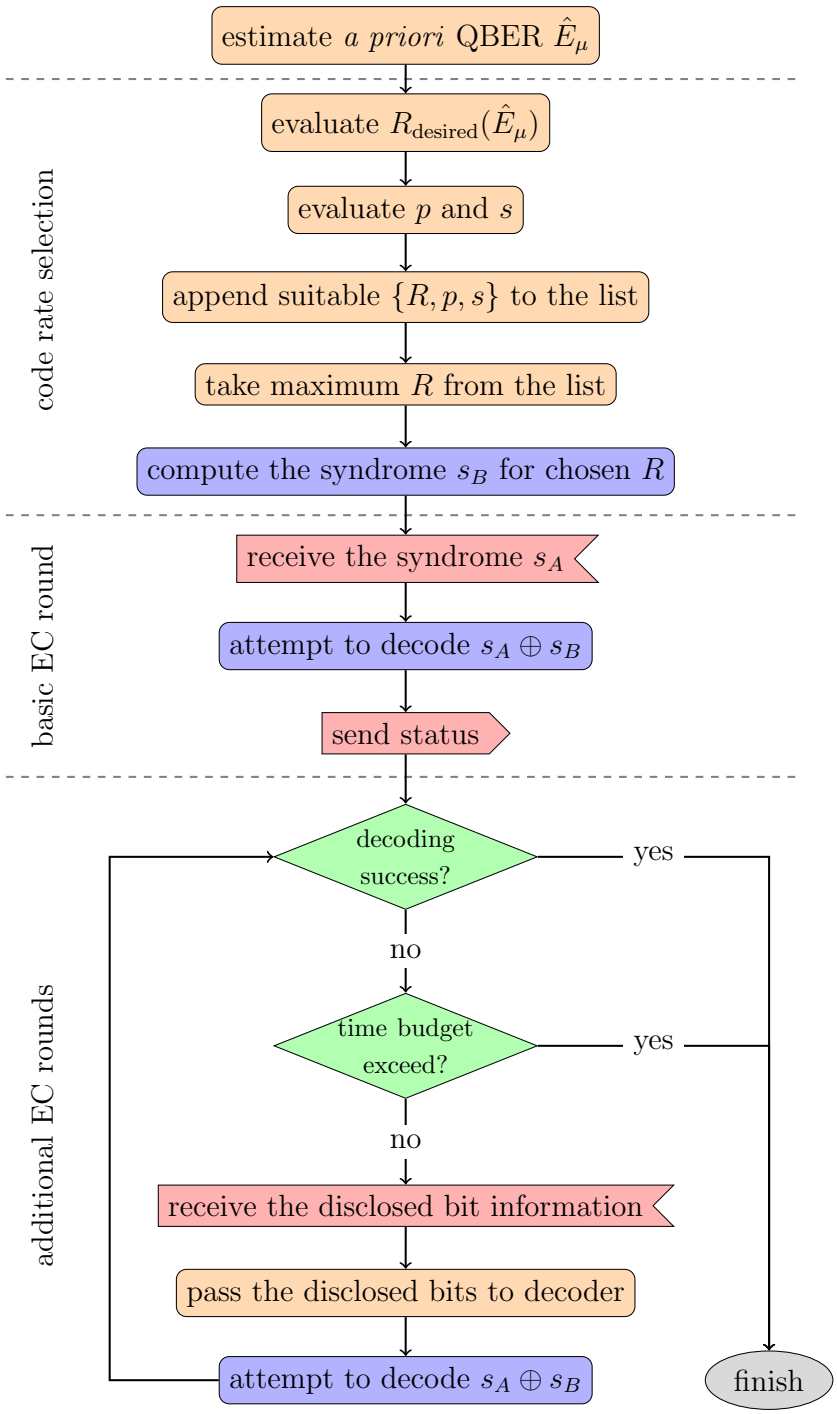

Figure 1. Activity diagram of the asymmetric information reconciliation process on Bob's side.

In our study, the appropriate frame length is chosen to be $\ell_{\text{frame}} = 32{,}000$ bits. Then, the key subblock length is computed as

$$\ell_{\text{subblock}} = \ell_{\text{frame}}(1 - \alpha)\,. \tag{6}$$

Using $\alpha = 0.15$ [8], one obtains ℓ_{subblock} = 27,200 bits. Since the post-processing block size has to be at least of the order of 10^6, we take $\ell_{\text{block}} = 50\ell_{\text{subblock}} = 1.36 \times 10^6$.

In order to reduce the impact of error bursts on the decoding process and to randomize the locations of errors, we apply the interleaving technique [2]. Alice and Bob simultaneously reorder bits in the subblock according to the permutation law, determined by two synchronized pseudo-random number generators based on Mersenne Twister.

The LDPC matrices $\{H_R\}$ are generated for the code pool $R \in \{0.5, 0.55, \ldots, 0.9\}$ with the Progressive Edge-Growth algorithm [34] and Tanner graph node degree distributions described in [7]. The values of shortened and punctured bits are defined by pseudo-random and true number generators, respectively (see [14] for detailed information). The untainted puncturing technique of the proper punctured bit position choice is also used [35].

The Sum-Product decoder [11] is the popular belief propagation LDPC syndrome decoder. However, it employs rather heavy computational operations and thus is not efficient enough for high-speed data processing. Therefore, we apply its effective approximation—the variable-scaled Min-Sum decoder [36] with the scaling parameter step equal to 12.5, which is chosen empirically and gives the best efficiency in our tests.

3.1. A Priori QBER Estimation

The EC of a new frame starts with the LDPC code rate choice based on the a priori error rate estimation. Although the blind rate-adaptive reconciliation is supposed to work without exact knowledge of QBER [22], it remains rather sensitive to the initial code rate value. The main idea of the blind reconciliation is to use an LDPC code of fixed rate that can be adapted by iterative disclosure of punctured bits. Therefore, in order to choose the optimal code rate, in this work, we propose to estimate the current a priori QBER using the a posteriori QBER information from the previously corrected and verified frames. We also consider the non-zero frame error rate (FER), caused by either LDPC code imperfections or unexpected QBER fluctuations and propose a simple feedback loop.

In our scheme, the a priori QBER for arbitrary i-th frame $\hat{E}_\mu^{(i)}$ is estimated by the exponential moving average of the previous verified frame, $\text{EMA}^{(i-1)}$, defined iteratively as

$$\text{EMA}^{(j)} = \begin{cases} E_\mu^{(i-6)} & j = i-6 \\ \gamma E_\mu^{(j)} + (1-\gamma)\text{EMA}^{(j-1)} & i-5 \le j \le i-1 \end{cases} \tag{7}$$

with the empirical smoothing factor $\gamma = 0.33$. The exponential weights lead to a more optimal code rate choice from the pool in the case of gradual QBER variation, while the average value smooths possible sporadic error bursts and, therefore, results in stable EC performance.

Nevertheless, the EMA method does not allow to detect and quickly adapt R to a sudden significant leap of QBER level. Therefore, we check the presence of error bursts by analyzing the set of weak decoy pulse QBERs of the block, $\{E_{\nu_1}^{(1)}, \ldots E_{\nu_1}^{(50)}\}$. Since decoy pulses are not used for the key formation, Alice can safely send a string of decoy bit values to Bob who compares it with their own one and computes decoy QBERs straightforwardly.

We set the following condition: if $|E_{\nu_1}^{(i)} - \mathbb{E}[E_{\nu_1}]| \ge 3\sigma[E_{\nu_1}]$, where $\mathbb{E}[E_{\nu_1}]$ and $\sigma[E_{\nu_1}]$ are the mean value and the standard deviation, respectively, the sporadic error burst is detected. Using the simplest theoretical model for QBER prediction, e.g., from Ref. [19], one can show that E_μ and E_{ν_1} have very similar behavior and that $\mathbb{E}[E_\mu] \le \mathbb{E}[E_{\nu_1}]$ due to the $\mu > \nu$ condition. Thus, we can use $\hat{E}_\mu^{(i)} = E_{\nu_1}^{(i)}$ as an upper bound for the signal a priori QBER instead of the EMA estimation.

After the i-th frame correction the verification step is performed, where we propose a simple performance control rule: in the case of frame verification failure, the EMA is calculated with penalty value $\hat{E}_\mu^{(i)} = 0.5$. Such a feedback loop provides a temporal decrease of the algorithm efficiency, increasing the probability of successful EC of the next frame.

The workflow of our a priori QBER estimation is shown in Figure 2. One can observe high consistency of E_μ and its estimation $\hat{E}_\mu$ even in the presence of the error burst from 2% up to 8% values of E_μ (frames 200–250).

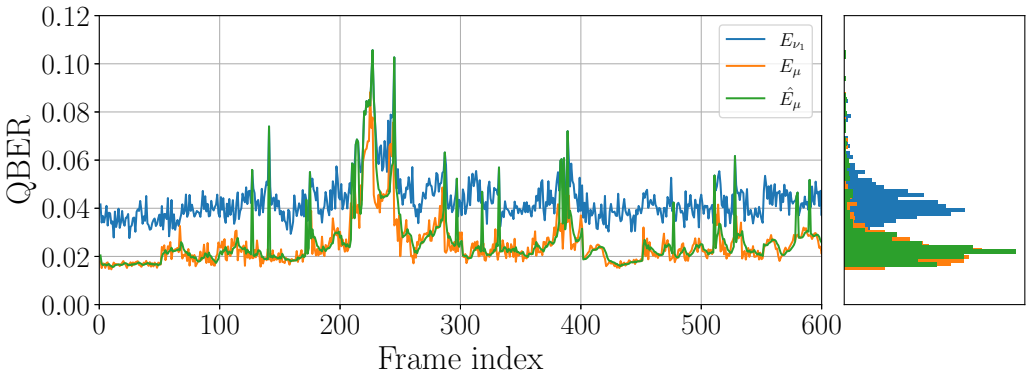

Figure 2. Example of experimental weak decoy (E_{ν_2}), real (E_μ) and estimated a priori ($\hat{E}_\mu$) signal QBER. The data was generated with QKD devices by QRate for the 20 dB quantum channel.

3.2. Code Rate Selection

It is crucial for the entire algorithm to set up a proper initial efficiency value of f_{ec} before the code rate is chosen. We use $f_{\text{start}} = 1.15$ as an empirical optimum. In this way, we can directly control the reconciliation scheme efficiency. Considering the LDPC code's imperfection, the desired code rate is defined by Shannon's capacity of the binary symmetric channel,

$$R_{\text{desired}} = 1 - f_{\text{start}} h_2(\hat{E}_\mu)\,. \tag{8}$$

If $0.5 \leq R_{\text{desired}} \leq 0.9$, then, for every code rate R from the pool $\{0.5, 0.55, \ldots, 0.9\}$, the total numbers of punctured (p) and shortened (s) bits are estimated as

$$\begin{aligned} p &= \ell_{\text{frame}} \lceil 1 - R - (1-\alpha) f_{\text{start}} h_2(\hat{E}_\mu) \rceil \\ s &= \alpha \ell_{\text{frame}} - p\,. \end{aligned} \tag{9}$$

This list of sets $\{R, p, s\}$ is sifted considering the following conditions:

$$p, s \geq 0 \quad p \leq p_R \quad \hat{E}_\mu < t_R\,. \tag{10}$$

Here, t_R is the error rate threshold defined in [7], p_R is the maximum amount of punctured bits calculated by the untainted puncturing technique [35]. The rest of appropriate sets $\{R, p, s\}$ forms a list, from which the algorithm chooses the one with maximum R. A similar rule to calculate p, s values was proposed in [7]; however, with no proper QBER estimation and pool of codes, it appears to be ineffective compared to blind schemes.

For very high/low QBER, the list is found to be empty. In this case, the algorithm chooses either $\{0.5, 0, \alpha\ell_{\text{frame}}\}$ if $R_{\text{desired}} \leq R_{\min} = 0.5$, or $\{0.9, p_{R_{\max}}, \alpha\ell_{\text{frame}} - p_{R_{\max}}\}$ if $R_{\text{desired}} \geq R_{\max} = 0.9$.

3.3. Additional Correction Rounds

Next, we modify the scheme of additional rounds organization. If the basic decoding round does not converge successfully, Bob reports to Alice about the occurred fail, and Alice, in return, begins disclosing punctured node values. Since the punctured nodes are generated true-randomly, their values' disclosure eliminates rather a high amount of uncertainty for Bob's decoder, and hence, with high probability, these nodes have the smallest LLR values. If all punctured bits are already disclosed but the decoding is still unsuccessful, Alice continues additional rounds by disclosing pseudo-randomly chosen payload bits.

In general, provided that the previous $k-1$ rounds failed, in the next k-th round, the number of disclosed punctured/payload bits is calculated according to our rule,

$$d_k = \left| \frac{\ell_{\text{syndrome}} - p + \sum_{l=0}^{k-1} d_l}{(\ell_{\text{frame}} - p - s) h_2(\hat{E}_\mu)} - f_k \right| \ell_{\text{frame}} \hat{E}_\mu \quad k \geq 1 \tag{11}$$

with $d_0 = 0$ and $f_k = f_{\text{start}} + 0.03k$. The additional rounds take place until the successful decoding result, or in the case of continuous fails, either the frame correction time budget or the maximum allowed number of iterations ($N_{\text{add}}^{\max}$) exceeds its limit. In the latter case, Bob reports their failure status to Alice, and both sides discard the corresponding subblock from the block. We evaluate the time budget out of timeouts for data transfer operations, i.e., based on the Quality of Service (QoS) of the classic channel (main factor), sifted key generation rate and hardware computational resources, which results in a value of the order of milliseconds.

4. Simulation and Experimental Results

In order to analyze the proposed asymmetric error correction (AEC) algorithm and compare it with the improved symmetric (SEC) approach and other asymmetric schemes as well, we first generate numerous bit strings of raw key for various average signal QBER values, $E_\mu \in \{0.005, 0.01, \ldots, 0.105\}$, using a theoretical model of the decoy-state BB84 protocol with the parameters listed in Table 1. The results of our simulations are presented in Figure 3 where we plot the efficiency f_{ec} (3) and the average number of decoding iterations as functions of the average QBER.

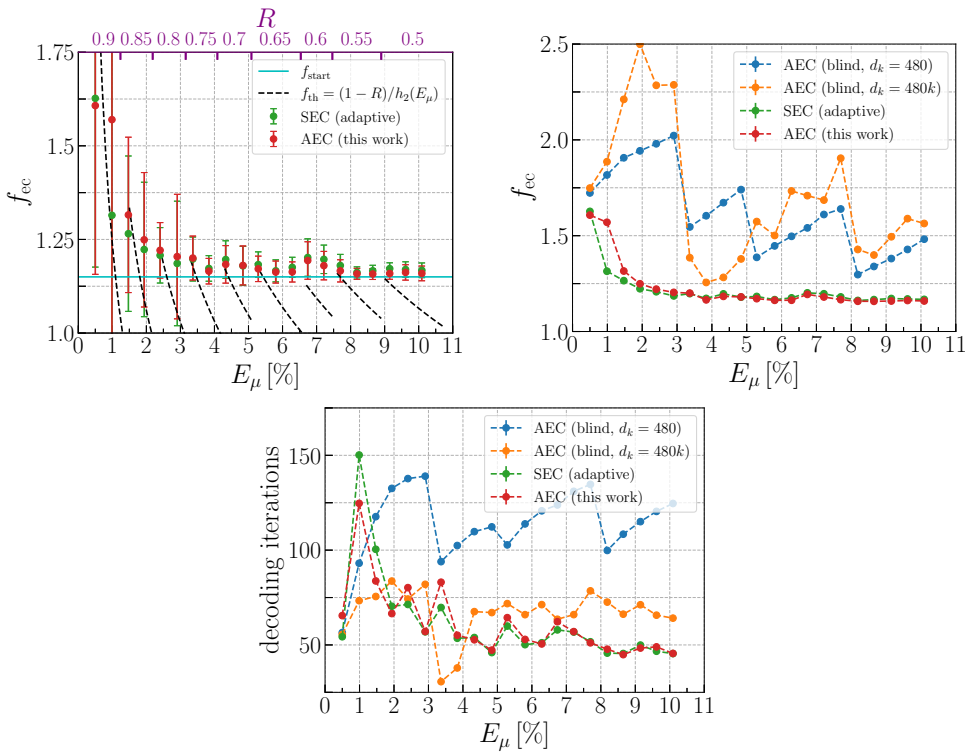

Figure 3. The dependencies of f_{ec} and the average number of iterations elapsed by the LDPC-decoder during one frame correction on average signal pulse QBER E_μ for symmetric (SEC) and asymmetric error correction (AEC) approaches based on the simulated data analysis. Key differences between the compared approaches are listed in Tables 2 and 3. The top axis on the upper-left plot represents the most frequently chosen LDPC code rate for the given QBER interval.

Table 1. The decoy-state BB84 setup parameters, used in both simulated and experimental data analysis: the mean photon number per pulse of signal (μ), week (ν_1) and vacuum (ν_2) decoy states, corresponding state generation probabilities $\{p_\mu, p_{\nu_1}, p_{\nu_2}\}$, single-photon detector quantum efficiency η, dark count probability p_{dc}, dead time τ_{dead} and optical error probability p_{opt}.

μ	ν_1	ν_2	p_μ	$p_{\nu_{1,2}}$	η	p_{dc}	τ_{dead}	p_{opt}
0.30	0.09	0.003	0.50	0.25	0.13	10^{-6}	5 µs	0.02

For reference, on the upper-left plot, we also used the theoretical efficiency of a code with a fixed rate for a given E_μ interval, $f_{\text{th}} = (1 - R)/h_2(E_\mu)$, which is the best efficiency that an EC scheme without rate-adaptive technique can achieve without frame correction failure. Note that, in our scheme, f_{ec} cannot be smaller than the initial value f_{start} due to additional EC rounds. The important result of this work is that the proposed AEC scheme closely approaches the SEC efficiency for error rates $E_\mu \gtrsim 2\%$. On the contrary, in the lower QBER region, the AEC efficiency increases faster than SEC but still does not exceed by more than 5%. Furthermore, one can notice the increase of the f_{ec} variance due to significant error fluctuations that induce the instability in the performance of any scheme with fast LDPC codes ($R \geq 0.75$).

Therefore, the fast codes have more strict requirements for the compliance of the selected set $\{R, p, s\}$ to an actual QBER of the frame, particularly in an asymmetric scheme. In particular, this implies more precise a priori QBER estimation for low E_μ. In terms of the number of decoding iterations, AEC performs slightly better than SEC in the lower range $E_\mu < 2\%$, while, for $E_\mu \gtrsim 2\%$, they demonstrate nearly the same results.

The basic principle of our method is a union of adaptive code rate selection and strategy of additional rounds organization. This could be potentially applied to the code represented by arbitrary parity check matrix (PCM) with any ℓ_{frame} and α values. We compare our EC with two asymmetric blind IR schemes that use different data disclosure rules for additional reconciliation rounds using common codes pool with fixed ℓ_{frame} = 32,000 bits in order to provide fair comparison. Key features of the compared approaches are summarized in Table 2.

Table 2. Key features of various EC schemes. Both AEC schemes with fixed and variable step d_k are conceptually blind, using no precise a priori QBER estimation and payload bits disclosure. The adaptive AEC proposed in this work is described in Section 3. The adaptive SEC scheme is based on the original one [14] but with the proposed a priori QBER estimation and code rate selection method.

EC Scheme	A Priori QBER Estimation	Code Rate Adaptation	Payload Bits Disclosure	d_k
AEC (blind, fixed d_k)	✗	✓	✗	480
AEC (blind, variable d_k)	✗	✓	✗	$480k$
AEC (this work)/SEC (adaptive)	✓	✓	✓	Equation (11)

In the AEC scheme, proposed in [22,37], in each additional round, the number of disclosed bits is equal and fixed, $d_k = \delta$. In another AEC scheme from Ref. [26], it is increased with iterations, $d_k = d_{k-1} + \delta$. In both schemes, no initial shortened bits are generated, and only punctured bits are used in additional rounds. Thus, in these two schemes, $s = 0$ and $p = \alpha\ell_{\text{frame}}$. The results obtained with these two methods are highly dependent on initial settings, such as the LDPC code frame length, the quality of parity check matrices and the amount of punctured bits.

Therefore, we set our implementations of these methods maintaining the original number of additional rounds (or larger), which defines the maximum f_{ec} and FER for any blind method. We set the maximum number of additional rounds equal to 10 and 4 for AEC with fixed and variable steps, respectively. This, in turn, results to $\delta = 480$ bits. The parameter list of the original works and our adaptation to our LDPC setup is presented

in Table 3. One can see from Figure 3 that our AEC efficiency performs significantly better compared with both blind AEC schemes in the entire QBER region.

Table 3. The list of parameters for blind AEC schemes with fixed ($d_k = \delta$) and increased ($d_k = k\delta$) number of disclosed bits during additional rounds. In this work, we slightly modify some QBER intervals from Refs. [22,26] to cover the entire QBER range and use the maximum total number of reconciliation rounds $N_{\text{add}}^{\max}$, which is expected to show better f_{ec}. For fixed d_k, doubled $N_{\text{add}}^{\max}$ is used. The code rates and ℓ_{frame} in Ref. [37] insignificantly differ from those in Ref. [22].

	EC Scheme	ℓ_{frame}	α	$R : [E_\mu^{\min}, E_\mu^{\max}]$	$N_{\text{add}}^{\max}$	δ
$d_k = \delta$	[22,37]	2000	0.1	$0.8 : [0.01, 0.035]$, $0.7 : [0.02, 0.06]$, $0.6 : [0.04, 0.09]$, $0.5 : [0.07, 0.12]$	1–5	$\frac{\alpha \ell_{\text{frame}}}{N_{\text{add}}^{\max}}$
	this work	32,000	0.15	$0.8 : [0, 0.03]$, $0.7 : [0.03, 0.05]$, $0.6 : [0.05, 0.08]$, $0.5 : [0.08, 0.11]$	10	480
$d_k = k\delta$	[26]	64,800	0.1	$0.8 : [0.01, 0.02]$, $0.6 : [0.03, 0.07]$, $0.5 : [0.08, 0.1]$	4	648
	this work	32,000	0.15	$0.8 : [0, 0.03]$, $0.6 : [0.03, 0.08]$, $0.5 : [0.08, 0.11]$	4	480

Although the efficiency metric (3) is informative when comparing different EC schemes, one has to consider another critical quantity of practical IR process—the decoding time consumption that is proportional to the total number of decoder iterations. On the bottom plot in Figure 3, we show the average total number of iterations depending on the QBER level. This number evaluation includes both basic and additional reconciliation rounds. We have to mention that all results are obtained on a single-processor setup without parallel computing. One can see that the proposed adaptive AEC method is approximately two-times faster than AEC with fixed step and slightly faster than AEC with a variable step for $E_\mu \gtrsim 4\%$.

Finally, we tested the real EC performance on experimental data, obtained with industrial QKD devices manufactured by QRate [38] for various losses in the quantum channel up to 20 dB (100 km@0.2 dB/km). Our results are presented in Figure 4. The upper plots show similar behavior as in Figure 3: the proposed AEC and SEC are very close in terms of efficiency, and SEC is slightly faster than AEC in terms of decoder iterations. The AEC scheme with a fixed step is less efficient and slower in the entire loss range. Although AEC with variable step is a bit faster for losses up to 7 dB; however, it has much worse efficiency.

Having a great deal of experimental data at our disposal (45,000 frames per dot), we also studied the frame correction failure probability. One can see, from Figure 4, that the FER of our AEC scheme is less than 10^{-3}, which is about one order of magnitude smaller than the FER of AEC with fixed/increased step, which can reach 10% at 20 dB. Furthermore, the failure probability of the AEC scheme is slightly better than of SEC for losses starting from 5 dB.

For a practical QKD setup, the IR throughput has to be analyzed as well [37]. The throughput defines how many bits per second the EC algorithm can proceed and depends on two basic factors. The first is the decoder's iteration cost, i.e., the time spent on one belief propagation algorithm execution, determined by CPU performance, number of threads and chosen code rate. The second factor is the total number of iterations in all rounds, which increases with additional rounds.

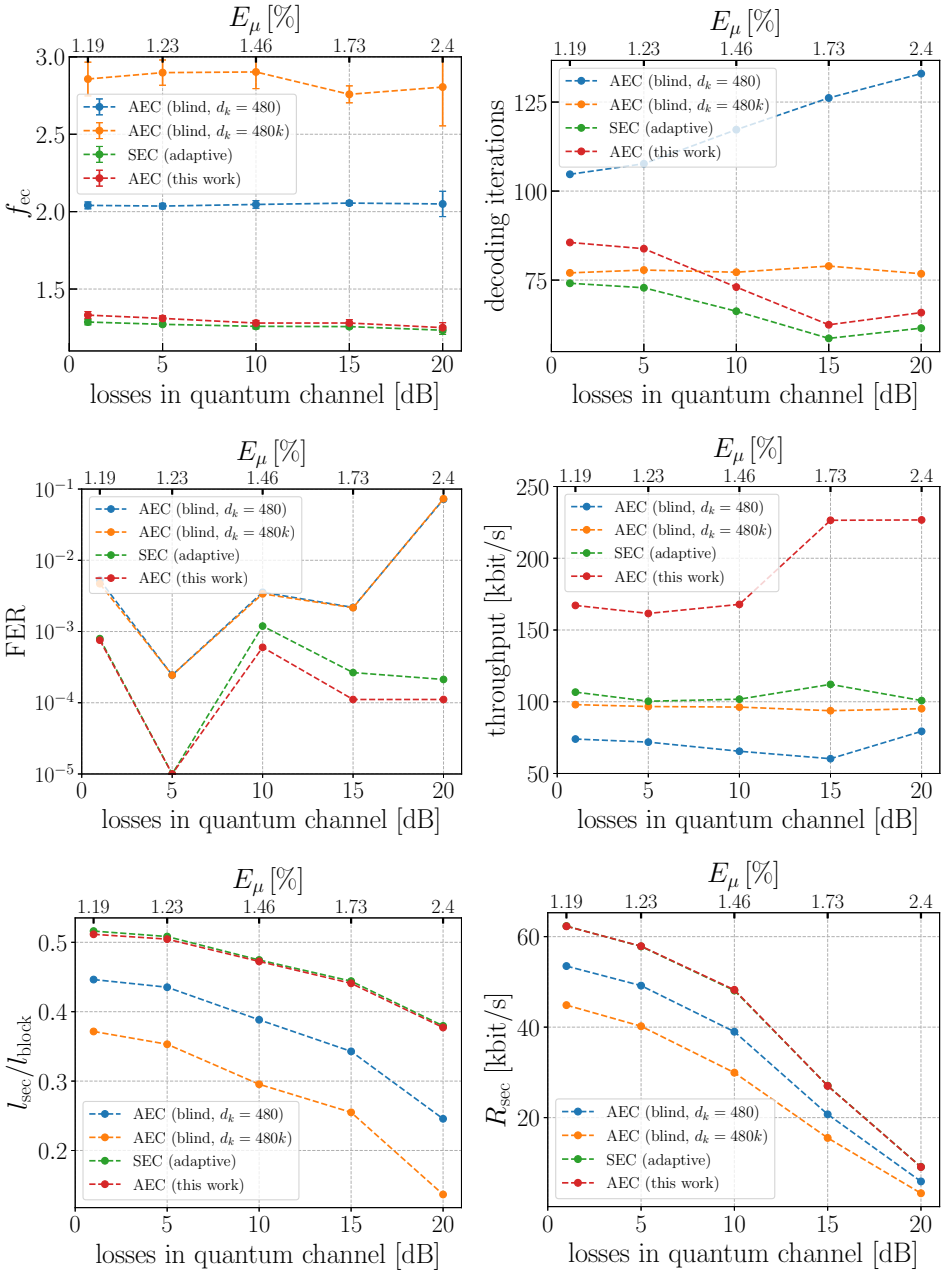

Figure 4. Performance of various error correction schemes on the real experimental data obtained with the industrial QKD devices by QRate.

Both blind AEC approaches have the lowest throughput because of their high number of iterations and FER. The SEC approach needs a smaller number of additional rounds since the knowledge of the smallest LLR positions leads to faster convergence of the decoder. However, the cost of each decoder iteration overweights the number of rounds and leads to lower throughput in comparison to our AEC approach. For these reasons, the developed AEC scheme demonstrates about two-times better throughput with respect to the three other schemes.

On the bottom plots in Figure 4, we present the overall result of all previously discussed metrics and effects—the normalized secret key length and generation rate. One observes that AEC and SEC have almost identical results and gain enhancement of about 20% (40%) in ℓ_{sec} and R_{sec} with respect to AEC with fixed (variable) step. This fact clearly confirms the advantage of our AEC approach over the previously studied blind AEC ver-

sions. Another important conclusion is that the introduced AEC algorithm demonstrates practically the same or sometimes even better performance compared with SEC.

5. Discussion

In this work, we suggested a new approach to asymmetric error correction that could be used in practical QKD systems with limited computational resources on one side. We took the symmetric blind information reconciliation [14] as a basis and proposed improvements, such as a priori QBER estimation, different code rate selection and the punctured bits disclosure rule. In particular, using the exponential moving average QBER of the previous verified frame together with decoy-state QBER allows the algorithm to detect gradual error rate changes and sudden bursts as swells and quickly adapt the code.

Novel a priori error estimation methods were efficiently applied together with a slightly changed rate-adaptive technique and blind-like interactive information reconciliation. Then, for the first time, we applied these features in an asymmetric approach. To compare various schemes, we studied several EC performance metrics and the secret key length/rate as final benchmarks on simulated and real data. We found that the improved symmetric and new asymmetric schemes demonstrated close efficiencies and average numbers of decoding iterations in rather wide QBER range ($E_\mu \gtrsim 2\%$).

Thus, a crucial result of this work is that our asymmetric scheme was found to be not inferior to the symmetric one regarding either the efficiency or in the secret key generation rate. We also made a comparison with two asymmetric blind schemes with the fixed and variable steps of the number of disclosed bits per additional round. We found that both proposed non-blind interactive approaches demonstrated a clear advantage over the blind ones. In this way, we conclude that the developed adaptive error correction approach can be efficiently used in decoy-state BB84 setups with fluctuating QBER levels and asymmetric computational resource allocation.

Author Contributions: Conceptualization, N.B., I.P. and A.T.; methodology, N.B., I.P. and A.T.; formal analysis, I.P.; visualization, I.P.; investigation, N.B. and I.P.; project administration, A.T.; software, N.B. and I.P.; supervision, A.T.; validation, I.P. and A.T.; writing—original draft preparation, N.B. and I.P.; writing—review and editing, A.T.; funding acquisition, A.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the Priority 2030 program at the National University of Science and Technology "MISIS" under the project K1-2022-027.

Institutional Review Board Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

Abbreviations

The following abbreviations are used in this manuscript:

QKD	Qunatum Key Distribution
QBER	Quantum Bit Error Rate
LDPC	Low-Density Parity Check
LLR	Log-Likelihood Ratio
EC	Error Correction (AEC/SEC—Asymmetric/Symmetric EC)
IR	Information Reconciliation
FER	Frame Error Rate
CPU	Central Processing Unit
EMA	Exponential Moving Average

References

1. Kiktenko, E.O.; Trushechkin, A.S.; Kurochkin, Y.V.; Fedorov, A.K. Post-processing procedure for industrial quantum key distribution systems. *J. Phys. Conf. Ser.* **2016**, *741*, 012081. [CrossRef]
2. Mehic, M.; Niemiec, M.; Siljak, H.; Voznak, M. Error Reconciliation in Quantum Key Distribution Protocols. In *Reversible Computation: Extending Horizons of Computing*; Springer: Cham, Switzerland, 2020; pp. 222–236. [CrossRef]
3. Brassard, G.; Salvail, L. Secret-Key Reconciliation by Public Discussion. In *Advances in Cryptology—EUROCRYPT'93*; Springer: Berlin/Heidelberg, Germany, 1994; pp. 410–423.
4. Elkouss, D.; Martínez-Mateo, J.; Martín, V. Secure rate-adaptive reconciliation. In Proceedings of the International Symposium on Information Theory and Its Applications, Kapolei, HI, USA, 24–27 October 2010; pp. 179–184. . [CrossRef]
5. Martinez-Mateo, J.; Pacher, C.; Peev, M.; Ciurana, A.; Martin, V. Demystifying the Information Reconciliation Protocol Cascade. *Quantum Info. Comput.* **2015**, *15*, 453–477. [CrossRef]
6. Vatta, F.; Romano, R.; Alizo, M. Turbo codes for quantum key distribution (QKD) applications. In Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL'11), Barcelona, Spain, 26–29 October 2011; Association for Computing Machinery: New York, NY, USA, 2011; pp. 1–5. [CrossRef]
7. Elkouss, D.; Leverrier, A.; Alleaume, R.; Boutros, J. Efficient reconciliation protocol for discrete-variable quantum key distribution. In Proceedings of the 2009 IEEE International Symposium on Information Theory, Seoul, Republic of Korea, 28 June–3 July 2009; pp. 1879–1883. [CrossRef]
8. Kiktenko, E.; Malyshev, A.; Fedorov, A. Blind information reconciliation with polar codes for quantum key distribution. *IEEE Commun. Lett.* **2020**, *25*, 79–83. [CrossRef]
9. Niemiec, M. Error correction in quantum cryptography based on artificial neural networks. *Quantum Inf. Process.* **2019**, *18*, 174. [CrossRef]
10. Gallager, R. Low-density parity-check codes. *IRE Trans. Inf. Theory* **1962**, *8*, 21–28. [CrossRef]
11. MacKay, D.J. Good error-correcting codes based on very sparse matrices. *IEEE Trans. Inf. Theory* **1999**, *45*, 399–431. [CrossRef]
12. Dixon, A.; Sato, H. High speed and adaptable error correction for megabit/s rate quantum key distribution. *Sci. Rep.* **2014**, *4*, 7275. [CrossRef]
13. Yuan, Z.; Plews, A.; Takahashi, R.; Doi, K.; Tam, W.; Sharpe, A.W.; Dixon, A.R.; Lavelle, E.; Dynes, J.F.; Murakami, A.; et al. 10-Mb/s Quantum Key Distribution. *J. Light. Technol.* **2018**, *36*, 3427–3433. [CrossRef]
14. Kiktenko, E.; Trushechkin, A.; Lim, C.; Kurochkin, Y.; Fedorov, A. Symmetric Blind Information Reconciliation for Quantum Key Distribution. *Phys. Rev. Appl.* **2017**, *8*, 044017. [CrossRef]
15. Liao, S.K.; Cai, W.Q.; Liu, W.Y.; Zhang, L.; Li, Y.; Ren, J.G.; Yin, J.; Shen, Q.; Cao, Y.; Li, Z.P.; et al. Satellite-to-ground quantum key distribution. *Nature* **2017**, *549*, 43–47. [CrossRef]
16. Vest, G.; Freiwang, P.; Luhn, J.; Vogl, T.; Rau, M.; Knips, L.; Rosenfeld, W.; Weinfurter, H. Quantum key Distribution with a Hand-Held Sender Unit. *Phys. Rev. Appl.* **2022**, *18*, 024067. [CrossRef]
17. Hwang, W.Y. Quantum Key Distribution with High Loss: Toward Global Secure Communication. *Phys. Rev. Lett.* **2003**, *91*, 057901. [CrossRef] [PubMed]
18. Lo, H.K.; Ma, X.; Chen, K. Decoy State Quantum Key Distribution. *Phys. Rev. Lett.* **2005**, *94*, 230504. [CrossRef] [PubMed]
19. Ma, X.; Qi, B.; Zhao, Y.; Lo, H.K. Practical decoy state for quantum key distribution. *Phys. Rev. A* **2005**, *72*, 012326. [CrossRef]
20. Trushechkin, A.; Kiktenko, E.; Fedorov, A. Practical issues in decoy-state quantum key distribution based on the central limit theorem. *Phys. Rev. A* **2017**, *96*, 022316. [CrossRef]
21. Elkouss, D.; Martinez-Mateo, J.; Martin, V. Information reconciliation for quantum key distribution. *Quantum Inf. Comput.* **2011**, *11*, 226–238. [CrossRef]
22. Martínez-Mateo, J.; Elkouss, D.; Martín, V. Blind Reconciliation. *Quantum Inf. Comput.* **2012**, *12*, 0791–0812. [CrossRef]
23. Mao, H.K.; Li, Q.; Han, Q.; Guo, H. High-throughput and low-cost LDPC reconciliation for quantum key distribution. *Quantum Inf. Process.* **2019**, *18*, 232. [CrossRef]
24. Mao, H.K.; Qiao, Y.C.; Li, Q. High-Efficient Syndrome-Based LDPC Reconciliation for Quantum Key Distribution. *Entropy* **2021**, *23*, 1440. [CrossRef]
25. Gao, C.; Jiang, D.; Guo, Y.; Chen, L. Multi-matrix error estimation and reconciliation for quantum key distribution. *Opt. Express* **2019**, *27*, 14545–14566. [CrossRef]
26. Liu, Z.; Wu, Z.; Huang, A. Blind information reconciliation with variable step sizes for quantum key distribution. *Sci. Rep.* **2020**, *10*, 171. [CrossRef]
27. Bennett, C.H.; Brassard, G. Quantum cryptography: Public-key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 10–12 December 1984; pp. 175–179. [CrossRef]
28. Muga, N.J.; Ferreira, M.F.S.; Pinto, A.N. QBER Estimation in QKD Systems with Polarization Encoding. *J. Light. Technol.* **2011**, *29*, 355–361. [CrossRef]
29. Treeviriyanupab, P.; Phromsa-ard, T.; Zhang, C.M.; Li, M.; Sangwongngam, P.; Ayutaya, T.S.N.; Songneam, N.; Rattanatamma, R.; Ingkavet, C.; Sanor, W.; et al. Rate-adaptive reconciliation and its estimator for quantum bit error rate. In Proceedings of the 2014 14th International Symposium on Communications and Information Technologies (ISCIT), Incheon, Republic of Korea, 24–26 September 2014; pp. 351–355. [CrossRef]

30. Kiktenko, E.O.; Malyshev, A.O.; Bozhedarov, A.A.; Pozhar, N.O.; Anufriev, M.N.; Fedorov, A.K. Error Estimation at the Information Reconciliation Stage of Quantum Key Distribution. *J. Russ. Laser Res.* **2018**, *39*, 558–567. [CrossRef]
31. Ha, J.; Kim, J.; McLaughlin, S. Rate-compatible puncturing of low-density parity-check codes. *IEEE Trans. Inf. Theory* **2004**, *50*, 2824–2836. [CrossRef]
32. Yazdani, M.; Banihashemi, A. On construction of rate-compatible low-density parity-check codes. In Proceedings of the 2004 IEEE International Conference on Communications (IEEE Cat. No.04CH37577), Paris, France, 20–24 June 2004; Volume 1, pp. 430–434. [CrossRef]
33. Zhang, Z.; Zhao, Q.; Razavi, M.; Ma, X. Improved key-rate bounds for practical decoy-state quantum-key-distribution systems. *Phys. Rev. A* **2017**, *95*, 012333. [CrossRef]
34. Hu, X.Y.; Eleftheriou, E.; Arnold, D.M. Progressive edge-growth Tanner graphs. In Proceedings of the GLOBECOM'01, IEEE Global Telecommunications Conference (Cat. No. 01CH37270), San Antonio, TX, USA, 25–29 November 2001; Volume 2, pp. 995–1001. [CrossRef]
35. Elkouss, D.; Martínez-Mateo, J.; Martín, V. Untainted puncturing for irregular low-density parity-check codes. *IEEE Wirel. Commun. Lett.* **2012**, *1*, 585–588. [CrossRef]
36. Emran, A.; Elsabrouty, M. Simplified variable-scaled min sum LDPC decoder for irregular LDPC codes. In Proceedings of the IEEE 11th Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA, 10–13 January 2014; pp. 518–523. [CrossRef]
37. Martinez-Mateo, J.; Elkouss, D.; Martin, V. Key Reconciliation for High Performance Quantum Key Distribution. *Sci. Rep.* **2013**, *3*, 1576. [CrossRef] [PubMed]
38. Kiktenko, E.; Pozhar, N.; Duplinskiy, A.; Kanapin, A.; Sokolov, A.; Vorobey, S.; Miller, A.; Ustimchik, V.; Anufriev, M.; Trushechkin, A.; et al. Demonstration of a quantum key distribution network in urban fibre-optic communication lines. *Quantum Electron.* **2017**, *47*, 798–802. [CrossRef]