mathematics

IMPACT FACTOR 2.3

CITESCORE 4.0

Review

An Overview of Postprocessing in Quantum Key Distribution

Yi Luo, Xi Cheng, Hao-Kun Mao and Qiong Li

MDPI

https://doi.org/10.3390/math12142243

mathematics

MDPI

Review

An Overview of Postprocessing in Quantum Key Distribution

Yi Luo †, Xi Cheng †, Hao-Kun Mao and Qiong Li *

School of Cyberspace Science, Faculty of Computing, Harbin Institute of Technology, Harbin 150001, China; yi_luo@stu.hit.edu.cn (Y.L.); xicheng@stu.hit.edu.cn (X.C.); hkmao@hit.edu.cn (H.-K.M.)
* Correspondence: qiongli@hit.edu.cn
† These authors contributed equally to this work.

Abstract: Quantum key distribution (QKD) technology is a frontier in the field of secure communication, leveraging the principles of quantum mechanics to offer information-theoretically secure keys. Postprocessing is an important part of a whole QKD system because it directly impacts the secure key rate and the security of the system. In particular, with the fast increase in the photon transmission frequency in a QKD system, the processing speed of postprocessing becomes an essential issue. Our study embarks on a comprehensive review of the development of postprocessing of QKD, including five subprotocols, namely, parameter estimation, sifting, information reconciliation, privacy amplification, and channel authentication. Furthermore, we emphasize the issues raised in the implementation of these subprotocols under practical scenarios, such as limited computation or storage resources and fluctuations in channel environments. Based on the composable security theory, we demonstrate how enhancements in each subprotocol influence the secure key rate and security parameters, which can provide meaningful insights for future advancements in QKD.

Keywords: quantum key distribution; postprocessing; information reconciliation; privacy amplification; authentication

MSC: 81P94

Citation: Luo, Y.; Cheng, X.; Mao, H.-K.; Li, Q. An Overview of Postprocessing in Quantum Key Distribution. *Mathematics* **2024**, *12*, 2243. https://doi.org/10.3390/math12142243

Academic Editors: Jonathan Blackledge and Ke-Lin Du

Received: 30 April 2024
Revised: 2 July 2024
Accepted: 12 July 2024
Published: 18 July 2024

1. Introduction

In modern cryptographic theory, the only encryption algorithm that achieves information-theoretic security is the one-time pad (OTP), initially put forward in 1926 and formally established as information-theoretically secure by Shannon in 1949 using information theory [1]. An OTP necessitates that the key be as long as the message itself and that it must be utilized just once. The significant challenge of how to distribute such extensive keys securely, known as the key distribution problem, arises especially in the presence of adversaries. Quantum key distribution (QKD), leveraging principles of the quantum no-cloning theorem [2], emerges as a pivotal solution to achieve information-theoretically secure communication combined with an OTP. As quantum states are inherently non-duplicable due to the no-cloning theorem [3], any eavesdropping attempt by Eve in QKD unavoidably introduces disturbance to the quantum signals (e.g., single-photon) [4].

Several quantum key distribution protocols have been developed to build upon the foundational role of QKD in enhancing communication security, including the seminal Bennett-Brassard-1984 (BB84) [5], Ekert-91 (E91) [6], Bennett-Brassard-Mermin-1992 (BBM92) [7], Grosshans-Grangier2002 (GG02) [8], differential-phase-shift (DPS) [9], decoy-state [10], measurement-device-independent (MDI) [11], twin-field (TF) [12], phase-matching (PM) [13], and mode-pairing (MP) [14] protocols. A much more detailed review of QKD progress can be found in [4,15–20].

Typically, quantum key distribution (QKD) protocols consist of two main components, one involving the transmission and measurement of quantum states and the other focusing

on postprocessing. Postprocessing aims to distill a secure key from the raw data measured in quantum transmission, which includes steps like parameter estimation, sifting, information reconciliation, privacy amplification, and channel authentication. As the implementation of QKD systems advances rapidly, postprocessing has increasingly become a bottleneck in the performance of practical QKD systems. Many studies aim to enhance the performance of QKD postprocessing by optimizing specific steps of the postprocessing protocols. However, when optimizing postprocessing algorithms, it is crucial to address two key considerations. Firstly, designers of QKD systems aim to understand the classical computation and communication required to convert the measurement outcomes of a QKD experiment into a final key. Secondly, it is vital to comprehend the balance between the length of the final key and the security parameter, as it allows for the estimation of the number of initial quantum signals that need to be transmitted to achieve a desired final key length and level of security.

Additionally, addressing the non-ideal factors inherent in each subprotocol and the synergies between various optimization subprotocols are critical aspects that need to be discussed. While standard security proofs provide a method for distilling a final secret key from measurement outcomes, these procedures are based on ideal cases [21]. In the implementation of real-world QKD systems, applying these procedures necessitates further consideration of non-ideal factors, such as hardware constraints, computational resources, and fluctuating error rates. Many proposed optimizations for QKD postprocessing, while theoretically feasible and effective as demonstrated by simulations, may not achieve the expected results. Furthermore, integrating optimizations across different stages poses a significant challenge. It is essential to understand the processing throughput, security, and resource demands of each optimization, along with their impact on the final key rate. Determining whether these elements can be effectively integrated to achieve the anticipated outcomes is crucial.

Currently, there is no comprehensive review of QKD postprocessing that tackles the aforementioned challenges. The final secure key rate and security of QKD are influenced by all postprocessing steps. This article provides a detailed discussion of various optimization strategies and their development and further analyzes the impact of postprocessing optimization algorithms on the final key rate and security parameters under different conditions. Our systematic review covers various optimization strategies and their development in parameter estimation, sifting, information reconciliation, privacy amplification, and channel authentication. Additionally, by employing a universal compositional security framework, we integrate their impacts on QKD systems, offering a holistic understanding of QKD postprocessing improvements and optimization.

2. Foundations of QKD Postprocessing

As shown in Figure 1, the QKD protocol π_A^{QKD}, π_B^{QKD} typically involves two nodes, Alice and Bob, and distributes identical k_A and k_B between them. As shown in Figure 1, there are two types of channels in this setup: an authenticated classical channel $\mathbb{C}$ and a quantum channel $\mathbb{Q}$. The classical channel $\mathbb{C}$ is used for exchanging classical information related to postprocessing. Any information on classical channels can potentially be accessed by an attacker. The quantum channel $\mathbb{Q}$ is used for transmitting quantum states. The attackers can perform any physically possible transformation on the quantum states ρ in the channel.

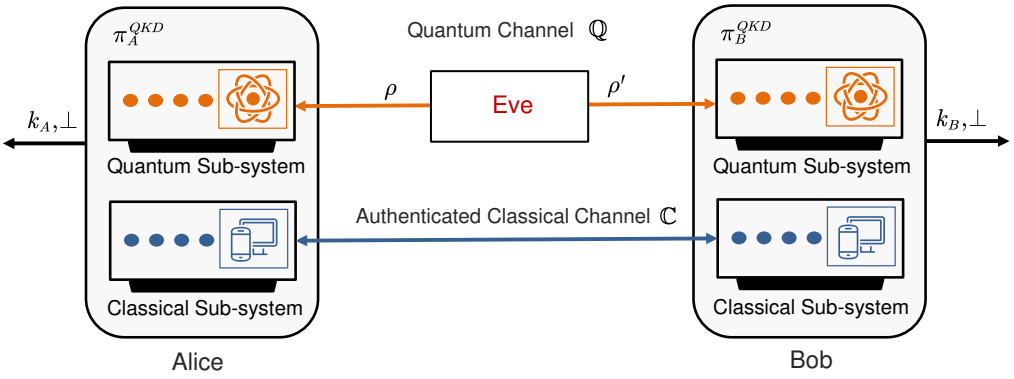

Figure 1. The fundamental principle of the QKD protocol between Alice and Bob. k_A, k_B represent the final QKD keys of Alice and Bob. $\perp$ represents that the protocol failed.

Indeed, a QKD postprocessing protocol consists of multiple subprotocols, each contributing differently to the final secure key rate and overall security. In this paper, we outline five primary steps commonly found in postprocessing protocols for QKD, namely, parameter estimation, sifting, information reconciliation, privacy amplification, and channel authentication. We give the details of the general workflow of QKD postprocessing in Figure 2.

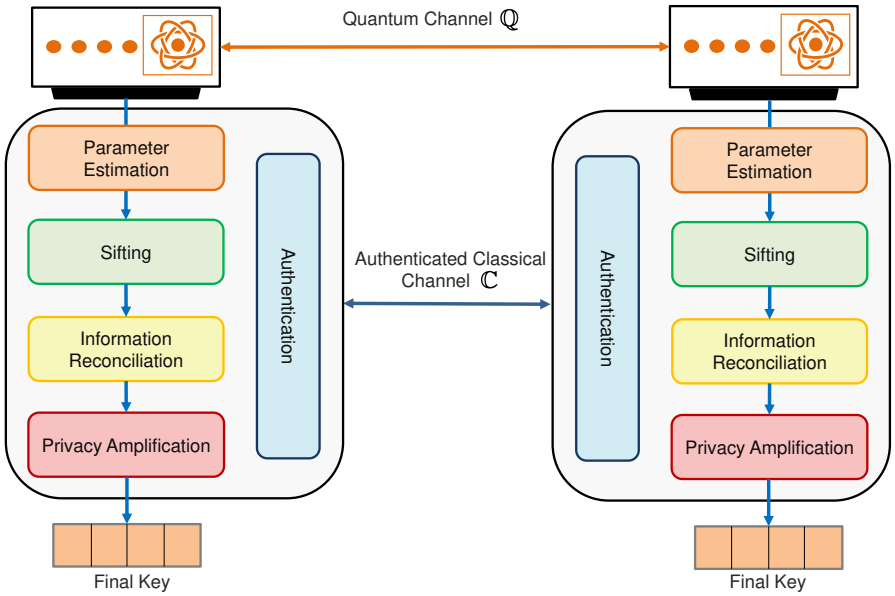

Figure 2. The postprocessing workflow of the QKD protocol.

These steps are crucial for ensuring the security and reliability of the QKD system, as well as for addressing potential errors and eavesdropping attempts. For the QKD postprocessing protocol, the following three factors are crucial:

- Final key rate: The portion of the raw bits that are converted to a secure key. The final key rate in QKD is influenced by various factors including parameter estimation, sifting, information reconciliation, privacy amplification, and channel authentication. One common formula used to calculate the final key rate is as follows:

$$R_{\text{final}} = \eta_{sift} \cdot (1 - FER) \cdot (\beta_{EC} \cdot I_{AB} - \chi_{PE} - \Delta_{finte}) \cdot \gamma_{\text{PA}} - k_{\text{auth}} \quad (1)$$

In Equation (1), R_{final} is the final key rate. η_{sift} is the sifted efficiency, representing the rate of raw keys used to distill the secret key. FER is the frame error rate and β_{EC} is the reconciliation efficiency. I_{AB} is the Shannon mutual information between Alice and Bob, and χ_{PE} represents the amount of information that the attacker Eve might obtain.

Generally, it can be calculated through parameter estimation. In an ideal scenario, it can be computed using the Holevo bound [22]. Δ_{finte} is the finite-size offset factor. γ_{PA} is the compression ratio of privacy amplification. k_{auth} is the key consumption of channel authentication.

- Postprocessing throughput: Postprocessing throughput refers to the speed for practical QKD postprocessing implementations. In most cases, the throughput of the postprocessing phase is primarily determined by the slowest component, which is typically information reconciliation or privacy amplification. The throughput of the postprocessing phase can be expressed by the following equation:

$$T_{\mathrm{final}} = \min(T_{\mathrm{PE}}, T_{\mathrm{sift}}, T_{\mathrm{IR}}, T_{\mathrm{PA}}, T_{\mathrm{Au}}) \tag{2}$$

- Security: Ensuring the protocol is robust against potential attacks, including both passive eavesdropping and active interventions by adversaries. This involves verifying that the key distribution is secure under various quantum cryptography assumptions and attack models.

To better illustrate the relationship between these subprotocols and the overall security of QKD, we employ the composable security framework [23] for analysis. This approach allows for a more comprehensive understanding of how each component within the QKD protocol contributes to its security and efficiency. The composable security framework enables the separate evaluation of each protocol followed by their integration. Within the composable security framework, a QKD protocol is expected to meet several key requirements, including three aspects:

- Correctness: After processing through the QKD protocol, Alice and Bob result in identical keys, noted as $k_A = k_B$. The security parameter for correctness is denoted as ε_{cor}, which satisfies

$$P(k_A \neq k_B) \leq \varepsilon_{cor} \tag{3}$$

- Secrecy: Secrecy refers to the difference between the actual QKD-generated key and an ideal key. Various methods have been used to analyze this, such as statistical distance, information entropy [24], and trace distance of quantum states [25]. In this paper, we use trace distance for analysis because trace distance under quantum states can be converted to statistical distance or information entropy [23]. The security parameter for secrecy is denoted as $\varepsilon_{\mathrm{sec}}$. Here, assume the ideal key τ_K that is perfectly uniform and independent from the adversary's information ρ_E. ρ_{KE} is the joint state of the final key K and the quantum information gathered by an eavesdropper E. The security parameter needs to be greater than or equal to the trace distance in Equation (5).

$$D(\rho_{KE}, \tau_K \otimes \rho_E) \leq \varepsilon_{\mathrm{sec}} \tag{4}$$

- Robustness: The probability that the QKD protocol aborts under non-ideal conditions, which is referred to as robustness. Generally, robustness needs to be discussed in different channel environments and computational resources. These conditions also related to secrecy ε_{cor} and correctness $\varepsilon_{\mathrm{sec}}$. In the study cited as [21], the impact on robustness was analyzed.

The above three points are the requirements for the security of QKD within the theoretical framework of [23]. Generally, the security parameters of QKD are set as $\varepsilon = \varepsilon_{cor} + \varepsilon_{\mathrm{sec}}$ (such as $\varepsilon_{sec} = 10^{-10}$ and $\varepsilon_{cor} = 10^{-15}$ [26]), and ε_{rob} can be discussed separately based on the specific channel environment and computational resources.

The postprocessing subprotocols in Figure 2 contribute to the security parameter ε. There is also one more source of uncertainty based on how much one "smooths" the min-entropy, ε_{min}. Therefore, using the standard security proof [25,27], we wind up with an $\varepsilon = \varepsilon_{PE} + \varepsilon_{min} + \varepsilon_{EC} + \varepsilon_{PA} + \varepsilon_{Au}$ secure protocol which is ε_{EC} correct and $\varepsilon_{PE} + \varepsilon_{min} + \varepsilon_{PA} + \varepsilon_{Au}$ secure. Subsequently, Sections 3–7 will discuss the impact of each protocol on QKD.

3. Parameter Estimation

Parameter estimation is a vital component of any QKD scheme because it is related to the security level and final key rate of QKD [25,28–30]. In standard QKD protocols, the users have to sacrifice part of their raw data to estimate the parameters of the communication channel. Parameter estimation plays a critical role in QKD as it directly affects the security performance and the final key rate of the QKD system. As stated in the previous section, in parameter estimation as presented in the Renner framework [25], Alice and Bob sacrifice a part of the signals to obtain a sequence $Z \in \Sigma^{|Z|}$, for which we refer to the finite set Σ as an alphabet. From the sequence obtained, Alice and Bob construct their frequency distribution F over Σ. If F falls within a preagreed set of distributions Q, they proceed with the protocol; if not, they abort. The term ε_{PE} in the security statement accounts for the exclusion of any state that would result in an accepted frequency distribution with a probability lower than ε_{PE}.

The parameter estimation discussed here is different from error estimation. Error estimation solely focuses on estimating the error rate and is closely related to error correction. Different QKD protocols require the estimation of various parameters, but most QKD protocols have the following key parameters that need to be estimated [28]:

- Block size N: The number of pairs of qubits that Alice and Bob receive.
- Key rate ℓ/N: The ratio of output key size ℓ to block size N. The higher the key rate is, the more efficiently the protocol converts the available quantum resource to a secret key.
- Security level ε: The distance of the output from an ideal secret key. The lower the security level, the better the guarantee that no future evolution of the protocol output and adversary registers will be able to distinguish between the output and an ideal key.
- Robustness: The amount and type of noise that the protocol can tolerate without aborting. In particular, the QKD protocol should be able to tolerate at the very least the imperfections of whatever quantum channel and entanglement source are used to implement the protocol.

Typically, robustness requires special consideration. As for the key rate and security level, there is a trade-off between them. Increasing security requirements will reduce the key rate. We can use the theorem from [29] to describe this trade-off.

Theorem 1. *Assuming an i.i.d. collective attack, the QKD protocol is* $\varepsilon_{PE} + \varepsilon_{min} + \varepsilon_{PA} + \varepsilon_{EC}$ *secure. When the protocol does not abort, the output key is of length* ℓ *and satisfies*

$$\ell \leqslant N\big(H_{\mu}(X \mid E) - \delta(\bar{\varepsilon})\big) - \ leak\ _{\varepsilon_{\mathrm{EC}}} - 2\log_2(2/\varepsilon_{\mathrm{PA}}) \tag{5}$$

where $H_{\mu}(X \mid E)$ represents the min-entropy of the key sequence X with respect to the attacker E, with a variation bound μ. $\delta\ (\bar{\varepsilon})$ is a correction term, for which a more detailed calculation method can be found in [29]. $leak_{\varepsilon_{\mathrm{EC}}}$ is an upper bound on the amount of information leaked during the error-correction step.

Discussing the robustness of QKD systems is a complex issue that involves various components within the QKD system. According to [31], the security requirements and security parameters of the QKD communication model are segmented into five parts, covering the source, encoder, channel, decoder, and detector. Then, ref. [31] discusses the basic security requirements and quantum hacking strategies for each module. Additionally, the relationship between quantum hacking and security parameters is detailed in [31].

In addition to using random sampling methods, parameter estimation can also employ other methods to achieve higher accuracy. For example, the fine-graining method proposed in [29] provides a reliable, efficient, tight, and generic numerical method for calculating the asymptotic key rate of QKD. Some of the literature has proposed other methods for parameter estimation instead of random sampling, such as those based on universal hashing [28], Bayesian estimation [32], compressive sensing [33], and artificial

neural networks [34]. Moreover, there are many studies focused on parameter estimation for continuous-variable quantum key distribution (CV-QKD) [32–39] that also discuss various channel conditions [33,36,38,40].

4. Sifting

The function of the sifting module is to filter out invalid data. Upon receiving the raw key material from the quantum channel, this module removes invalid data caused by system loss and basis inconsistency through bit sifting and basis sifting. Alice and Bob compare a subset of their measurement bases or positions (without revealing the actual measurement outcomes) to identify which bits are likely to be correlated. The sifting module is illustrated in Figure 3.

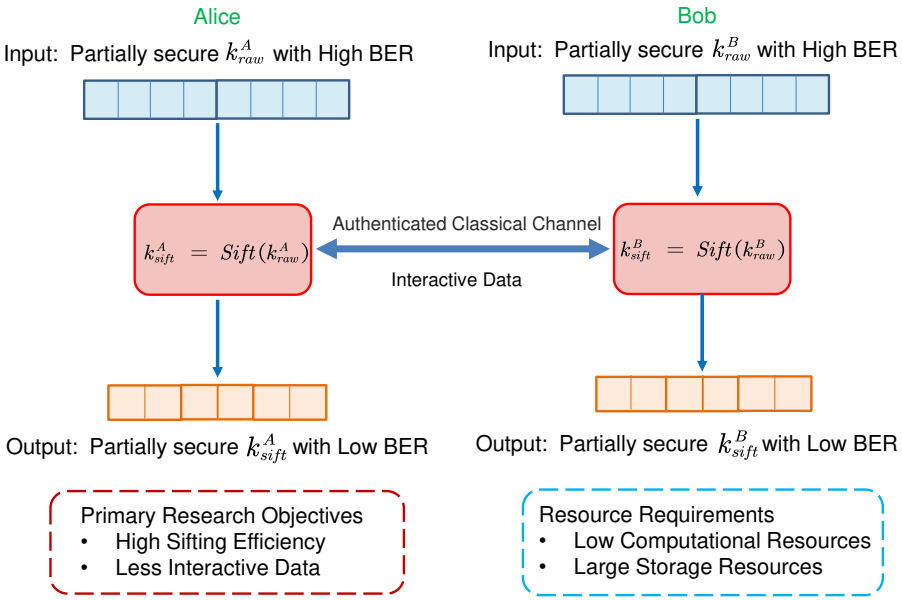

Figure 3. An overview of the sifting module in QKD postprocessing. k_{raw} denotes the raw key input to the sifting module, and k_{sift} represents the sifted key output from the sifting module.

Sifting includes bit sifting and basis sifting. The function of bit sifting is to eliminate unresponsive raw codes, while the purpose of basis sifting is to filter out raw codes with inconsistent bases. In the seminal BB84 quantum key distribution protocol, information is encoded utilizing two orthogonal polarization bases, specifically the rectilinear basis (also referred to as the Z basis) and the diagonal basis (referred to as the X basis). These bases operate within the polarization dimension of photons. To enhance the sifting efficiency, Alice and Bob employ a modified approach to the standard BB84 protocol, featuring a biased selection of bases. In this optimized scheme, the Z basis is predominantly utilized (with a probability $P_Z > 0.5$) for key distillation purposes. As a result of this strategic basis biasing, the counting rates for the Z and X bases exhibit asymmetry.

Security proofs for QKD were predominantly developed under the asymptotic assumption. This assumption posits the availability of an infinite dataset, thereby enabling the theoretical determination of QKD parameters with boundless precision [41]. While this assumption is valuable for theoretical investigations, it deviates considerably from practical situations where datasets are naturally limited, and measurements are always influenced by statistical fluctuations caused by finite sample sizes. To correct this, ref. [42] introduced the T12 protocol, which features composable security against collective attacks in the finite-size scenario and provides high key distribution rates. On another security aspect, ref. [43] pointed out a security issue of iterative sifting and proposed a more secure sifting protocol based on [44]. It does not require an additional random seed for the sample and at the same time allows for asymmetric basis choice probabilities. This enhancement leads to higher sifting efficiency.

Data exchanged during the sifting phase must undergo authentication, and expanding data size will escalate the usage of authentication keys. To optimize the ultimate key rate, reducing the volume of interaction information in the sifting stage is crucial. Since a significant portion of the signals transmitted between Alice and Bob consists of invalid empty signals (related to the response rate), it was proposed by [44] that compression algorithms could be used to compress information related to bit sifting, effectively reducing the amount of interaction required and thus reducing the consumption of authentication keys. In 2015, the MZRLFL encoding algorithm was proposed [45], which can effectively reduce the amount of interaction information in the bit-sifting part while reducing authentication key consumption. Experimental results show that it can reduce authentication key consumption by 26%.

5. Information Reconciliation

5.1. Preliminaries of Information Reconciliation

The function of the information reconciliation module is to correct errors in the input-sifted codes while minimizing information leakage. In this paper, both error estimation and correction are considered components of the reconciliation module. Error estimation impacts error correction by determining the accuracy of the initial error rate, which in turn influences the selection of parameters in the error correction process. The information reconciliation module is crucial for determining the correctness of the final QKD key, and the success rate of information reconciliation also influences the overall robustness and correctness of the QKD protocol. The input and output of the information reconciliation module are illustrated in Figure 4. Input k_{sift} containing a small number of errors is transformed into an error-free reconciled key k_{EC} after processing by the information reconciliation module. To enhance the final secure key rate as much as possible, it is imperative to minimize the amount of information leaked during the information reconciliation process. Information reconciliation involves two main tasks as follows:

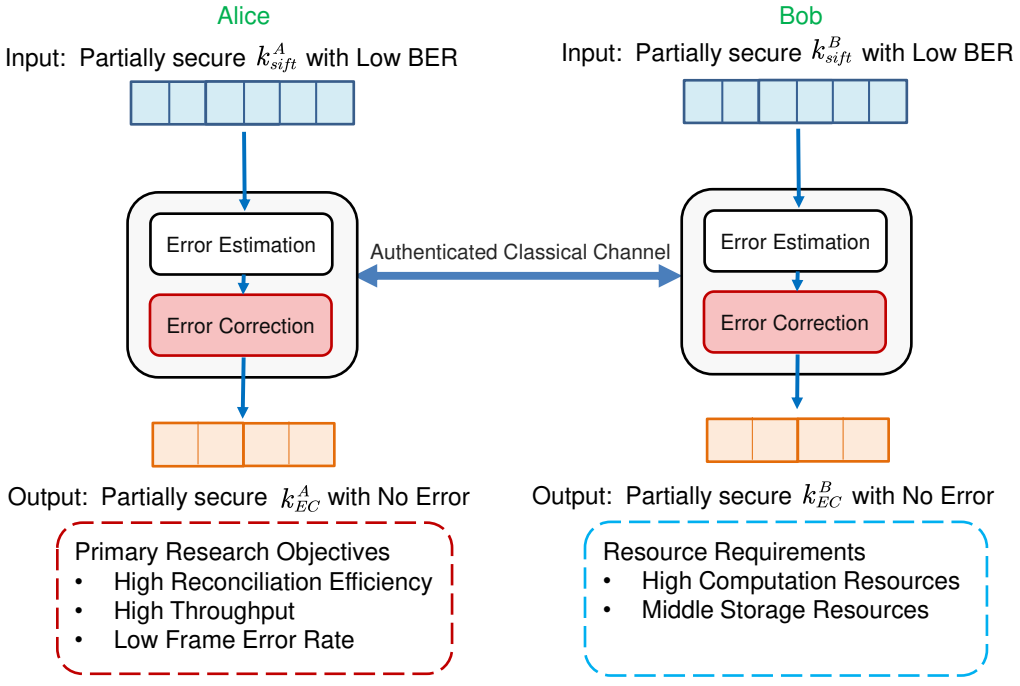

Figure 4. An overview of information reconciliation module in QKD postprocessing. k_{sift} denotes the sifted key input to the information reconciliation module, and k_{EC} represents the reconciled key output from the information reconciliation module.

Error estimation is the process by which the parties estimate the error rate in the key bits they have, respectively, measured. This step is crucial for determining the parameters that will be used in the error correction process to maximize the reconciliation efficiency.

Error correction involves the actual correction of errors in the quantum key. It ensures that any discrepancies between the keys of the communicating parties due to quantum channel noise or potential eavesdropping are resolved. This process is vital for the security and reliability of QKD systems, as it directly influences the final secure key rate and overall security parameters.

The performance of information reconciliation is typically characterized by three parameters: reconciliation efficiency, frame error rate (FER), and throughput. Reconciliation efficiency measures how close the process comes to the theoretical limit of information that needs to be exchanged for successful reconciliation. FER quantifies the frequency of erroneous frames within the data stream that cannot be successfully reconciled, which directly impacts the robustness. Throughput refers to the volume of keys that can be processed per unit of time, which is crucial for high-performance QKD systems where quick key generation is necessary. They are all vital for enhancing the security and performance of QKD systems.

There are currently two equivalent definitions of reconciliation efficiency, both of which encapsulate the discrepancy between the actual and theoretical amount of leaked information during the error correction, albeit focusing on different specific aspects.

The theoretical lower bound for the amount of interactive information required for information reconciliation is defined by the Slepian–Wolf bound $H(A|B)$, where $A \in \{0,1\}^n$ and $B \in \{0,1\}^n$, respectively, denote the output sequences k_{est} from Alice's and Bob's error estimation modules. Alice and Bob need to exchange at least $H(A|B)$ amount of information for error correction. Consider a BSC channel with QBER e_u, in this case, $H(A|B) = nh(e_u)$, where the binary entropy $h(e_u) = -e_u \log_2(e_u) - (1-e_u)\log_2(1-e_u)$.

Let m be the length of the message exchanged between Alice and Bob, and the reconciliation efficiency can be defined as the ratio of the actual amount of secure keys to the theoretical maximum amount of secure keys, denoted as β:

$$\beta = \frac{n-m}{n(1-h(e_u))} \leq 1 \tag{6}$$

Conversely, the reconciliation efficiency can also be defined as the ratio of the actual information leaked for the error correction to the theoretical minimum quantity of information leaked, denoted as f_{EC}:

$$f_{EC} = \frac{m}{nh(e_u)} \geq 1 \tag{7}$$

so that

$$1 - f_{EC} \cdot h(e_u) = \beta(1-h(e_u)) \tag{8}$$

The theoretical limits for both β and f_{EC} are 1. The closer to 1 the reconciliation efficiency approaches, the more closely the information reconciliation protocol approximates an ideal state.

Some studies indicated that the leaked information should be considered when the reconciliation fails [46,47]. To take the influence of FER into consideration, the modified reconciliation $f_{EC}^{'}$ can be given as [47]

$$f_{EC}^{'} = \frac{(1-FER)(1-R)+FER}{h(e_u)} \tag{9}$$

where $R = 1 - m/n$ is the ratio of information transmitted.

Furthermore, the approaches and challenges in information reconciliation can differ significantly between continuous-variable QKD (CV-QKD) and discrete-variable QKD (DV-QKD) systems. The difference stems from the distinct approaches each employs in processing quantum information:

- In DV-QKD, information is encoded in the discrete states of quantum systems, such as the polarization states of photons. The primary challenge in DV-QKD is the discrete nature of errors, which typically arise due to the presence of noise in the quantum channel and potential eavesdropping activities. Information reconciliation in DV-QKD often involves interactive protocols such as Cascade, which work through multiple rounds of information exchange to pinpoint and correct errors. These protocols are designed to minimize the leakage of information to potential eavesdroppers and are characterized by their high efficiency in terms of the fraction of the key that remains secure after reconciliation.
- CV-QKD mainly uses continuous quantum variables, such as the quadrature amplitudes of light, to encode information. The main challenge here arises from the continuous nature of quantum measurements, which leads to a different error profile characterized by Gaussian noise. Reconciliation methods in CV-QKD typically involve non-interactive protocols that convert the continuous variables into discrete bits using slicing or quantization techniques before applying error correction. These methods require sophisticated statistical strategies to deal with the Gaussian distribution of errors and often employ multidimensional reconciliation techniques to enhance the correction process.

Both DV-QKD and CV-QKD strive to balance the trade-off between reconciliation throughput and efficiency, but their different physical implementations and error characteristics necessitate tailored approaches.

5.2. Error Estimation in Information Reconciliation

Information reconciliation involves two main steps: error rate estimation and error correction. Error rate estimation assesses the error rate of the filtered key sequence, while error correction aims to rectify these errors through public channels. Subsequently, a data verification process follows to confirm the coherence of the ultimate key sequences maintained by both Alice and Bob.

The a priori error rate can be directly inferred from historical information for QKD systems with relatively stable quantum bit error rates (QBERs). However, for QKD systems operating in practical environments, especially free-space QKD systems, the QBER often exhibits significant fluctuations. When the estimated a priori error rate deviates significantly from the true QBER, it can lead to a decline in the performance of information reconciliation. Therefore, for these QKD systems with large QBER fluctuations, the approach to obtain a more accurate a priori error rate with minimal information leakage is crucial. This process is known as error estimation.

For systems with significant fluctuations in the QBER, it is necessary to estimate the error rate before information reconciliation. In 2011, Calver et al. found that an error sampling rate of 25% provides optimal Cascade performance when using variable block sizes [48]. In 2015, Li et al. proposed an error estimation approach based on parity-check bit comparison. Simulation results indicate that this approach offered improved estimation accuracy compared to previous random sampling approaches. Specifically, it could achieve relatively higher accuracy with fewer communication overheads under conditions of low error rates [49]. In 2017, Lu et al. analyzed the impact of the sampling rate on the final secure key rate (SKR) in resource-limited decoy-state QKD systems using a random sampling approach. When the number of transmitted pulses is equal to 7×10^{-9}, the greatest sampling rate is 27.74%, and as the number of pulses increases, the greatest sampling rate decreases. This provided guidance for selecting the appropriate sampling rate in error estimation for practical QKD systems [50]. In summary, a sampling rate of 25% is considered reasonable. In systems with stable QBERs, the sampling rate can be appropriately reduced as the number of transmitted pulses increases.

Another kind of error estimation approach utilizes the interactive information during information reconciliation for error estimation. This kind of approach differs from the pre-reconciliation error estimator in that it does not affect the secure key rate and is suitable

for QKD systems with relatively stable QBERs. In 2014, Treeviriyanupab et al. used the syndrome information to estimate QBER instead of the traditional key sampling approach. However, this estimation approach is only suitable for regular LDPC codes and does not take into account the influence of punctured and shortened bits [51]. Based on this research, Kiktenko et al. proposed an improved error estimation approach based on a single LDPC matrix in 2018. This approach is applied to irregular LDPC codes and takes into account the influence of punctured and shortened bits. Additionally, the protocol also considers the results of the previous round's actual QBER to further enhance the accuracy of error estimation [52]. In 2019, Gao et al. proposed an error estimation approach based on multiple LDPC matrices, pointing out that due to the introduction of multiple matrices, this approach offers better estimation performance compared to previous error estimation protocols [53].

5.3. Error Correction in Information Reconciliation

The fundamental principles in QKD systems are equal, transforming information bits into longer codewords and employing specific algorithms to detect and correct transmission errors, ensuring that the receiver can accurately recover the sender's original information. During the encoding process, information bits (data bits) are transformed into redundant codewords, which include additional parity bits for error detection and correction. In the decoding process, the receiver uses decoding algorithms to detect and correct transmission errors.

5.3.1. Discrete-Variable QKD Error Correction

In DV-QKD, error correction deals specifically with discrete data, as opposed to continuous data handled in continuous-variable QKD (CV-QKD). The error correction process in DV-QKD typically involves turning a sequence of discrete bits into codewords. These codewords are then processed using different error-correcting codes to identify and correct errors. Two primary approaches are utilized in DV-QKD error correction: interactive error correction, which involves multiple rounds of communication between the parties to iteratively correct errors, and forward error correction, which theoretically allows it to be performed with a single round of communication, thus significantly reducing latency and communication overhead.

Interactive error correction: The earliest QKD systems mainly adopted interactive reconciliation protocols. In 1992, Bennett et al. [54] proposed the first error correction protocol for DV-QKD systems, known as the BBBSS protocol, which utilized block parity checks and binary search for error correction.

Cascade: Building upon the BBBSS protocol, Bennett et al. proposed the Cascade protocol in 1994 [55], improving the error correction capability per round and reducing the amount of interaction information required on the public channel.

The Cascade protocol is a widely adopted error correction protocol in QKD postprocessing. It operates by segmenting the key bits and applying parity checks on each segment to identify and correct errors through multiple rounds of interactive communication. Cascade's primary advantage lies in its high error correction efficiency, making it suitable for environments with high error rates. However, the protocol requires several rounds of communication, which increases both latency and communication overhead. With the advancement of QKD system speeds, optimizing the complexity and processing time of the Cascade protocol has become a critical point of research.

The process of the Cascade protocol is presented in Figure 5. For an example of direct reconciliation, Alice and Bob divide their key sequence into sub-blocks; for each block, Alice computes the parity (i.e., the sum modulo 2 of all bits in the block) and transforms it to Bob through an authenticated classical channel. Bob then computes the parity of their corresponding block and compares it to the parity received from Alice. If the parties differ, this indicates the presence of an odd number of errors within the block. Alice and Bob then perform a binary search within the block to locate the error. This process involves dividing

the block into two blocks, exchanging parities for each block, and narrowing down the location of the error based on the parity discrepancies. Once an error is localized to a specific position, Bob corrects their bit to match Alice's corresponding bit. After correcting errors in the initial blocks, Alice and Bob shuffle their keys randomly. This process terminates when the corrected keys are identical with high probability or Cascade reaches the predefined maximum number of error correction rounds.

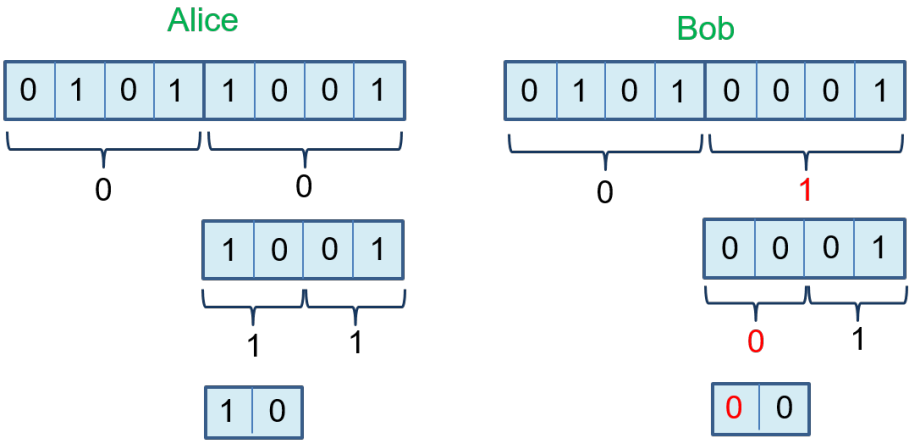

Figure 5. The schematic of the Cascade protocol. Red numbers mark the positions of detected errors.

In the standard Cascade protocol, fixed block sizes are used throughout the error correction process. This approach often faces several issues:

- Inefficiency in high error rates: Fixed large block sizes can be inefficient in high-error-rate environments because they may not accurately localize errors, leading to multiple iterations and excessive communication overhead.
- Overhead in low error rates: Conversely, fixed small block sizes in low-error-rate environments can lead to unnecessary fine-grained corrections, increasing the number of required iterations and reducing overall efficiency.
- Uniform strategy: The uniform application of fixed block sizes does not account for the varying distribution of errors, leading to suboptimal performance.

The adaptive Cascade protocol enhances the standard Cascade protocol by dynamically adjusting its parameters based on real-time error conditions, thereby improving its efficiency and effectiveness.

Instead of using a fixed block size, the adaptive Cascade protocol adjusts the block size based on the various error rates. Higher error rates necessitate smaller blocks for more precise error localization, while lower error rates allow for larger blocks to improve efficiency. The number of iterations and the strategies used in each iteration are also adjusted dynamically. Initial iterations may use smaller block sizes for fine-grained error detection, and subsequent iterations use larger blocks to consolidate corrections. The protocol analyzes the distribution of errors after each iteration to refine the error correction process, which helps in identifying patterns and adjusting the error correction strategy accordingly.

Dynamic adjustments in block sizes and iteration strategies make the adaptive Cascade protocol more efficient than the standard version, particularly in varying error conditions. Furthermore, optimizing communication rounds makes the protocol more practical for real-world applications.

In 2003, Lo et al. [56] proved the unconditional security of the Cascade protocol in practical QKD systems. After the introduction of the Cascade protocol, numerous research proposals [57–62] analyzed the length of the first and subsequent blocks in the Cascade protocol, leading to improvements in the reconciliation efficiency of the protocol. Additionally, modifications to the Cascade protocol [47,63,64] have also been an important direction for improvement. In terms of practical implementation of the Cascade protocol [65–67], there have been numerous studies on optimizing the algorithm's parameters and hardware im-

plementations. The Cascade protocol is easy to implement and has excellent reconciliation efficiency. Considering implementation costs, it performs well in practical QKD systems and remains one of the most widely used error correction protocols today.

Winnow: In 2003, Buttler et al. [68] modified the Cascade protocol and proposed the Winnow protocol. The Winnow protocol replaced the BISECT binary search operation with error correction based on Hamming codes, significantly reducing the number of interactions required between Alice and Bob.

This approach minimizes the number of communication rounds required, maintaining a high error-correction capability. The Winnow protocol is particularly effective in low-error-rate environments, offering higher efficiency and lower communication overhead compared to Cascade. Although it still requires some communication rounds, the overall communication volume and computational complexity are significantly reduced, making it an effective choice for QKD postprocessing.

Unlike the Cascade protocol, the Winnow protocol utilizes Hamming codes to correct errors within sub-blocks. By exchanging syndromes, Alice and Bob can identify and correct single-bit errors in their respective blocks. After correcting these single-bit errors, the protocol can be repeated with different block sizes to detect and correct any remaining errors. The main process of the Winnow protocol is illustrated in Figure 6.

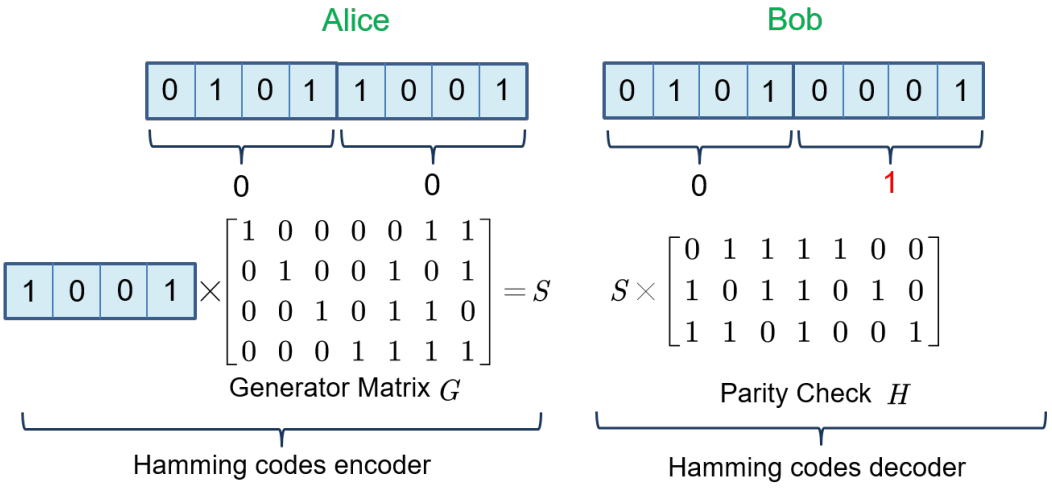

Figure 6. Theschematic of the Winnow protocol. Red numbers mark the positions of detected errors.

A few studies [69–73] have further improved the performance of the Winnow protocol. However, a drawback of the Winnow protocol is that Hamming codes can only correct a single error within a data block. When the number of errors in a data block exceeds one, the protocol is not only unable to correct the errors but may also introduce new ones. This is the reason why the Winnow protocol has consistently exhibited lower reconciliation efficiency.

Research studies about interactive error correction in DV-QKD are listed in Table 1. Due to the constraints imposed by the dimensions of the table, some data presented herein represent only a subset of the full experimental results.

Our data selection adheres to the following criteria:

- For discrete data in tables or figures, we select one to three data points that show the best performance in aspects such as reconciliation efficiency, throughput, and FER. The QBER or SNR and other relevant parameters correspond to the values at which the best performance was achieved.
- For continuous experimental data presented in the figures, we display the best-performing range.
- Data obtained from graphs using extraction tools rather than directly reported numbers are marked with an asterisk (*).

This criterion applies equally to Tables 2–5.

Table 1. Interactive error correction schemes in DV-QKD. Data extracted from graphs by tools are marked with an asterisk (*). Reconciliation efficiencies using the form of Equation (9) are marked with an hash ($^{\#}$).

Reference	Year	Method	QBER	β	f_{EC}	FER	Throughput (Mbps)
Bennett et al. [54]	1992	BBBSS	-	-	-	-	-
Brassard et al. [55]	1994	Cascade	-	-	-	-	-
Yan et al. [61]	2008	Cascade	0.01	91.43%	-	-	-
Ma et al. [62]	2010	Cascade	0.01	91.33%	-	-	-
Martinez et al. [47]	2015	Cascade	0.01	99.63%	1.043 $^{\#}$	8×10^{-5}	-
Pedersen et al. [65]	2015	Cascade	0.01	98.9%	-	-	83.49
Pacher et al. [64]	2015	Cascade	0.03	99.55%	1.019	1×10^{-4}	-
Li et al. [66] *	2019	Cascade	0.01	91%	-	0.019	-
Mao et al. [67]	2022	Cascade	0.01	-	1.038 $^{\#}$	-	570
Buttler et al. [68]	2003	Winnow	-	-	-	-	-
Zhao et al. [69]	2007	Winnow	-	-	-	-	-
Yan et al. [70]	2009	Winnow	-	-	-	-	-
Cui et al. [71] *	2012	Winnow	(0, 0.1)	-	(1.39, 1.67)	-	10.5
Li et al. [72] *	2015	Winnow	(0.01, 0.05)	-	(1.26, 1.34)	-	-

The most common formula for reconciliation efficiency is given by Equations (6) and (7). However, in Table 1, several papers use the formula of Equation (9). To better distinguish them, we add a marker (#) after references using the form of Equation (9).

Forward error correction: To address the issue of excessive interaction times in interactive information reconciliation protocols, researchers have proposed forward error correction (FEC) protocols. Theoretically, FEC protocols require only one interaction (although it may take several interactions in practice) to complete error correction. For FEC protocols, the AFF3CT toolbox is valuable for simulating and implementing various FEC codes, emphasizing high throughput and low latency for both simulations and real-world applications [74]. Currently, there are mainly two types of forward error correction information reconciliation protocols based on LDPC codes and polar codes.

LDPC: LDPC codes were first proposed in 1962 [75], but they did not receive much attention due to the weak computing and storage capabilities of hardware devices at that time. They were rediscovered in 1999 [76], and studies have shown that they have advantages such as low decoding complexity and error correction capabilities approaching Shannon's limit [77].

LDPC information reconciliation protocols predominantly use binary domain LDPC codes based on $GF(2)$. Here, n denotes the code length, k represents the length of the information bits, and the check bits have a length $m = n - k$. An LDPC code can be uniquely defined by a parity-check matrix H of size $m \times n$. For an LDPC code of the form (n, k), the code rate R satisfies $R \geq k/n$, with equality holding only when H is a full-rank matrix.

This matrix can be visually represented using a Tanner graph. Figure 7 depicts a typical Tanner graph representation and corresponding LDPC parity-check matrix of a standard LDPC code, where V and C represent variable nodes and check nodes, respectively.

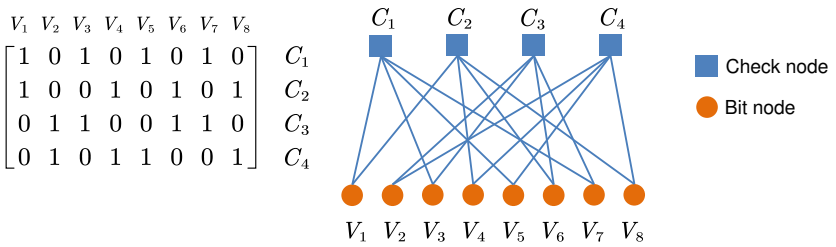

Figure 7. The Tanner representation of the LDPC parity-check matrix.

Decoding LDPC codes involves inferring a sequence X that satisfies the set of parity-check equations $HX = S$. In classical communication systems, S is typically a zero vector. However, in QKD error reconciliation, S represents the syndrome information, which must be computed by the encoder and transmitted to the decoder via an authenticated classical channel.

In 2004, Pearson et al. [78] first implemented an LDPC information reconciliation protocol on a CPU platform. Experiments showed that when the QBER was 3%, the LDPC information reconciliation protocol outperformed the Cascade protocol in terms of the number of interactions and the amount of communication data. In 2009, Elkouss et al. [79] optimized the degree distribution of LDPC matrices in QKD systems, greatly improving their performance. In 2011, Elkouss et al. proposed an adaptive LDPC information reconciliation protocol [80], which successfully achieved dynamic rate adjustment of a single LDPC matrix by introducing tuning bits, allowing it to adapt well to fluctuations in QBERs.

A rigorous security analysis of its impact on the final secure key rate was presented in 2013 [81]. The study [82] improved the selection strategy for tuning bits. In 2012, Martinez et al. proposed a blind LDPC information reconciliation protocol [83], which does not require prior estimation of the QBER. By increasing a certain amount of interaction, the code length was reduced from 200 kb to 2 kb, resulting in a significant reduction in computation and an increase in reconciliation efficiency. In 2017, Kiktenko et al. [84] introduced a symmetric decoding mechanism and selected additional interaction bits for each round based on the confidence level after each round of decoding. Compared to the blind LDPC information reconciliation protocol, it not only reduced the number of interactions but also further improved reconciliation efficiency. In 2020, Liu et al. [85] improved reconciliation efficiency to a certain extent by dynamically adjusting the number of additional interaction bits per round in case of decoding failure. In 2021, the protocol proposed by Mao et al. [86] improved reconciliation efficiency and reduced the number of communication rounds by placing the check bits of some data frames into the puncture positions of other data frames, fully utilizing previously wasted information. In 2022, Borisov et al. [87] proposed an asymmetric adaptive algorithm based on LDPC codes, which can be effectively used in the BB84 protocol with large fluctuations in QBER and asymmetric allocation of computing resources.

Many studies have conducted targeted optimizations for LDPC reconciliation protocols in practical QKD systems. In 2014, Dixon et al. [88] implemented an adaptive LDPC information reconciliation protocol in a practical QKD system, relying on both CPU and GPU platforms. In 2019, Mao et al. [89] designed a quantized LDPC decoder that achieved high throughput and reconciliation efficiency on low-cost CPUs. Furthermore, in 2019, Gao et al. [53] proposed an LDPC information reconciliation protocol based on multiple check matrices, which simultaneously decoded the same data frame using multiple interrelated LDPC check matrices, thereby improving reconciliation efficiency to a certain extent. In 2021, they implemented the protocol using a GPU [90]. Additionally, many practical QKD systems [41,91–93] have employed LDPC codes for error correction.

Research studies about LDPC code-based forward error correction in DV-QKD are listed in Table 2.

Table 2. LDPC-based forward error correction schemes in DV-QKD. Data extracted from graphs by tools are marked with an asterisk (*).

Reference	Year	Method	Code Length	QBER	f_{EC}	FER	Throughput (Mbps)
Pearson et al. [78]	2004	LDPC	$4096 \approx 4 \times 10^3$	0.03	-	-	-
Elkouss et al. [79] *	2009	LDPC	10^6	0.1	1.04	-	-
Elkouss et al. [94]	2010	LDPC	2×10^5	0.092	1.0836	-	-
Elkouss et al. [80] *	2011	LDPC	2×10^5	(0.05, 0.11)	<1.1	-	-
Elkouss et al. [82]	2012	LDPC	10^4	-	-	-	-
Martinez et al. [83] *	2012	Blind LDPC	2×10^3	0.09	1.2	5.4×10^{-2}	-
		Blind LDPC	2×10^4	0.024	1.2	5.8×10^{-3}	-
Dixon et al. [88] *	2014	LDPC	10^5	0.01	1.645	-	46.7
		LDPC	10^5	0.04	1.1	-	15.4
		LDPC	10^5	-	2	-	120
Kiktenko et al. [84] *	2017	Blind LDPC	1944	0.019	1.3	-	-
		Blind LDPC	1944	0.1	1.13	-	-
		Blind LDPC	4×10^3	0.1	1.1	-	-
C.Gao et al. [53]	2019	LDPC	10^4	-	-	-	-
Mao et al. [89]	2019	LDPC	10^5	-	1.108	-	122.17
Liu et al. [85] *	2020	Blind LDPC	6.48×10^4	0.1	1.18	-	-
Guo et al. [90]	2021	LDPC	$2^{12} \approx 4 \times 10^3$	-	1.4	-	85.67
		LDPC	$2^{12} \approx 4 \times 10^3$	0.04	-	0	102.084
Mao et al. [86]	2021	LDPC	10^5	0.05	1.09	-	-
		LDPC	1944	0.05	1.14	-	-
Borisov et al. [87] *	2022	LDPC	3.2×10^4	20 db	1.19	10^{-4}	225
Tarable et al. [95] *	2024	LDPC	2×10^3	0.11	1.12	-	-
		LDPC	10^5	0.11	1.08	-	-

Polar: The polar code-based protocol is another common forward error correction-based information reconciliation protocol.

Polar codes operate by transforming a set of identical channels into two sets: highly reliable channels and highly unreliable channels. This transformation is accomplished using a process known as channel polarization. Information bits are transmitted over the reliable channels, while the unreliable channels are assigned predetermined values known as frozen bits. The specific assignment of information and frozen bits is determined by the polarization effect, which ensures that the capacity of the channel is maximized.

Polar codes are applied in QKD postprocessing due to their excellent error correction performance and lower complexity. The encoding and decoding processes of polar codes can be efficiently implemented using recursive structures, making them well suited for hardware implementation and high-speed communication systems. Compared to LDPC codes, polar codes exhibit superior performance in low-error-rate environments, though their performance might not be as robust in high-error-rate scenarios. Overall, polar codes present a promising error correction solution for QKD systems, particularly in contexts demanding high-speed and efficient quantum communication networks.

In 2009, Arikan et al. [96] proposed a novel channel coding algorithm based on channel polarization theory, which has been proven to achieve the limit of channel capacity with relatively low decoding complexity. In 2012, Jouguet et al. [97] first introduced polar codes into the field of QKD, achieving significant performance improvements. Both processing speed and reconciliation efficiency were higher than those of LDPC-based error correction protocols implemented on GPUs. In 2014, Nakassis et al. [98] continued to investigate the application of polar codes in QKD and proposed various application modes. In 2018, Yan et al. [99] introduced the successive cancellation list (SCL) decoding algorithm into QKD, further reducing the amount of leaked information and frame error rate (FER). In the same year, Lee et al. [100] proposed an error correction algorithm using a soft-output decoder, achieving a certain improvement in reconciliation efficiency.

In 2020, Kiktenko et al. [101] proposed a blind polar information reconciliation protocol, which outperforms blind LDPC protocols when the QBER fluctuates significantly. In 2021, Tang et al. [102] proposed a polar reconciliation protocol integrated with a feedback mechanism, greatly improving reconciliation efficiency and reducing the failure probability. However, its excessively long code length increased computational and storage burdens. In 2022, Fang et al. [103] designed a polar code-based codeword structure, enabling the simultaneous completion of error correction and privacy amplification during a single encoding-and-decoding process. Furthermore, in 2022, Zhou et al. [104] proposed a novel error correction algorithm based on polar codes. Compared to previous algorithms, this algorithm achieves higher reconciliation efficiency and lower failure probability under the same block size and QBER. Tang et al. [105] proposed an error reconciliation algorithm based on polar codes using frozen bit erasure. Implemented on commercial CPUs, this algorithm achieved a throughput of 0.88 Mbps with a QBER of 0.02 and a reconciliation efficiency of 1.760, making it suitable for QKD systems with poor link conditions. Guo et al. [106] proposed a dedicated error correction algorithm based on polar codes and achieved a throughput of over 15 Mbps and a block length of 2^{12} bits using FPGA, meeting the real-time requirements of error correction in high-repetition QKD systems.

Research studies about polar code-based forward error correction in DV-QKD are listed in Table 3.

Table 3. Polar-based forward error correction schemes in DV-QKD. Data extracted from graphs by tools are marked with an asterisk (*).

Reference	Year	Method	Code Length	QBER	β	f_{EC}	FER	Throughput (Mbps)
Jouguet et al. [97]	2012	Polar	2^{24}	0.02	98%	-	0.08	8.3
		Polar	2^{16}	0.02	93.5%	-	0.09	10.9
Nakassis et al. [98]	2014	Polar	2^{20}	0.02	96.2%	-	0.086	-
			2^{16}	0.02	93.0%	-	0.073	-
Yan et al. [99]	2018	Polar	2^{20}	0.02	97.1%	-	1×10^{-3}	-
		Polar	2^{16}	0.02	95.7%	-	2×10^{-3}	-
Lee et al. [100] *	2018	Polar	2^{11}	0.05	-	1.55	10^{-3}	-
Kiktenko et al. [101] *	2020	Blind Polar	-	0.1	-	1.22	-	-
		Blind Polar	-	0.09	-	1.18	-	-
Tang et al. [102]	2021	Polar	2^{20}	0.02	-	1.055	-	-
		Polar	2^{17}	0.01	-	1.091	$\leq 10^{-4}$	-
		Polar	2^{10}	0.02	-	1.146	5×10^{-3}	-
Fang et al. [103]	2022	Polar	2^{10}	0.01	-	-	$\approx 10^{-4}$	-
Zhou et al. [104]	2022	Polar	2^{20}	0.02	-	1.046	$\approx 10^{-8}$	-
Tang et al. [105]	2023	Polar	2^{10}	0.02	-	1.293	1.5×10^{-3}	8.60
		Polar	2^{10}	0.02	-	1.176	4×10^{-4}	0.68
Guo et al. [106]	2023	Polar	2^{12}	(0.02, 0.1)	-	-	-	18.07

In summary, considering interactive error correction protocols, the Cascade protocol has been extensively researched due to its high reconciliation efficiency, achieving practical efficiency values close to the theoretical limit of 1.0. However, its requirement for hundreds of interactive rounds to complete a high-efficiency reconciliation process poses significant limitations on its applicability. Another notable protocol is the Winnow protocol, which reduces the number of interactive rounds to at least three. Despite this reduction, its lower reconciliation efficiency significantly impacts the secure key rate and maximum transmission distance of QKD systems. Consequently, the application of interactive protocols has diminished in recent years due to the excessive number of interactions required.

Forward error correction (FEC) protocols have gained considerable attention in recent years due to their ability to perform error correction with theoretically only a single round of

communication, thereby expanding their range of applications. Among FEC protocols, the polar protocol can surpass the reconciliation efficiency of LDPC protocols under large code lengths. However, this improvement substantially increases computational and storage resource consumption, thereby impacting their throughput. Therefore, LDPC protocols, which achieve high reconciliation efficiency with shorter code lengths, remain the most competitive among FEC protocols.

5.3.2. Continuous-Variable QKD Error Correction

In the DV-QKD system, the data exchanged between the two communicating parties are inherently discrete. Therefore, the information reconciliation primarily focuses on error correction. However, in the Gaussian-modulated coherent-state CV-QKD protocol, continuous random variables satisfying a Gaussian distribution are employed. Before error correction, these continuous random variables need to be quantized, and then classical error-correction algorithms are utilized to correct errors in the data.

In addition, reverse reconciliation is more widely used than direct reconciliation in CV-QKD systems, due to a significant constraint known as the 3 dB limit [107]. This constraint significantly restricts the achievable transmission distance. To overcome this limitation, Grosshans et al. proposed an alternative approach known as reverse reconciliation [108]. In reverse reconciliation, Bob encodes their data, and Alice decodes them, reversing the roles compared to direct reconciliation. This method has been proved to be more secure through information-theoretic analysis, as it reduces the amount of information an eavesdropper Eve can obtain by intercepting Bob's data compared to Alice's.

Information reconciliation in CV-QKD primarily encompasses two approaches: slice reconciliation and multidimensional reconciliation. Due to the significant impact of noise on the quantization performance of slice reconciliation protocols, most existing slice reconciliation protocols are tailored for high signal-to-noise ratio (SNR) channels. In contrast, multidimensional reconciliation protocols are suitable for low-SNR CV-QKD systems with an SNR of less than 1.

Slice reconciliation: Slice reconciliation is a widely used error correction scheme, which is particularly suited for environments with high SNRs. The main steps of slice reconciliation are listed as follows:

Data slicing: The continuous-variable data, represented by real numbers, are divided into several discrete intervals or "slices". Each slice corresponds to a specific range of values. This discretization process converts the continuous-variable data into a format suitable for classical error-correction techniques.

Error correction within slices: Once the data are sliced, traditional error-correcting codes, such as LDPC or polar codes, are applied to each slice independently.

Combining corrected slices: After error correction, the corrected slices are recombined to reconstruct the original continuous-variable data. This step ensures that any discrepancies introduced by noise or other errors during transmission are effectively mitigated, resulting in a high-fidelity shared key.

In 2004, G.V. Assche and their team proposed the slice reconciliation protocol. Its main idea is that Alice and Bob utilize a quantization function to map the original data into multiple-bit strings. With the assistance of binary error correction algorithms and low-level bit information, error correction is performed on high-level bit information. The high-level bit information is adopted as the reconciled code. Although the slice reconciliation protocol can convert original data into reconciled codes with multiple bits, its quantization performance for low signal-to-noise ratio (SNR) data is poor, limiting its application to high-SNR, short-distance CV-QKD systems [109]. In 2006, Bloch et al. built upon the slice reconciliation protocol by incorporating LDPC codes as the fundamental error-correcting codes and employing multilevel coding/multistage decoding (MLC/MSD) techniques to achieve data reconciliation (known as the Bloch scheme). This approach achieved a reconciliation efficiency of 88.7% [110]. In 2008, Lodewyck et al. applied the Bloch scheme to a practical system, achieving a transmission distance of 25 km with a key rate of 2 kbps.

The system had an SNR of 3 and similarly achieved a reconciliation efficiency of 88.7% [111]. In 2010, Lu et al. fully utilized optimization techniques such as vector quantization and iterative decoding. By adopting LDPC codes, they conducted a simulation experiment for reverse reconciliation in a CV-QKD system, achieving a reconciliation efficiency of 89% and a key generation rate of 2.2 kbps [112]. In 2014, Jouguet et al. achieved a slice reconciliation scheme with a reconciliation efficiency of approximately 94% by increasing the number of quantization levels and designing LDPC codes with outstanding performance [113]. In 2016, Qian et al. employed polar codes as the error-correcting codes for the slice reconciliation protocol and conducted data reconciliation for a backward-selection CV-QKD simulation system. They achieved a reconciliation efficiency of 90% at an SNR of 3 [114]. In the same year, Pacher et al. presented an information reconciliation method for CV-QKD using non-binary LDPC codes, achieving an efficiency between 0.94 and 0.98 with an SNR between 4 dB and 24 dB [115]. Later in 2016, Bai et al. used LDPC codes to achieve an SEC reconciliation scheme with a reconciliation efficiency of approximately 93% under an SNR of 3 [116]. In 2017, Bai et al. further optimized this scheme, achieving a reconciliation efficiency exceeding 95% [117]. In 2020, Yang et al. proposed a high-speed implementation scheme for the slice reconciliation protocol on an FPGA hardware platform. By designing an LDPC decoder with excellent decoding performance and high throughput, they achieved a data reconciliation processing rate of up to 100.9M symbols/s at an SNR of 3 [118]. In 2021, Mani et al. introduced a method for information reconciliation in continuous-variable quantum key distribution (CV-QKD) using multi-edge-type low-density parity-check (LDPC) codes, achieving efficiencies greater than 97% for channel coding rates from 0.01 to 0.1 across SNRs from -20 dB to 10 dB [119]. In 2021, Wen et al. proposed an improved rotated slice reconciliation protocol, which significantly improved both the reconciliation efficiency of reconciliation and the secure transmission distance of the CV-QKD system. For CV-QKD systems with a signal-to-noise ratio range of (3, 10), this protocol could achieve a reconciliation efficiency of up to 95.6% [120]. In 2022, Ai et al. conducted an analysis and experimental verification of the hierarchical information reconciliation protocol for CV-QKD, examining the impact of large-scale parallelization of information coordination in satellite communications on the final secure key rate [121]. Furthermore, in 2022, Wang et al. introduced polar codes into hierarchical reconciliation, proposing a hierarchical reconciliation scheme with a simple structure, effective execution, and adaptability to a wide range of signal-to-noise ratio systems. Simulation results showed that for CV-QKD systems with a signal-to-noise ratio range of (1, 10), the reconciliation efficiency of this scheme exceeded 95%, reducing complexity while improving the secure key rate of CV-QKD [122].

Research studies about slice reconciliation in CV-QKD are listed in Table 4.

Slice reconciliation for CV-QKD has been well summarized in the review article [123], and we cite Table 6 from [123], with two additional papers included in Table 4.

Multidimensional reconciliation: Multidimensional reconciliation is an effective scheme for low-SNR environments, thereby extending the key distribution distance.

The process of multidimensional reconciliation involves mapping the continuous-variable data into a higher-dimensional space, where the correlations between different dimensions can be exploited to improve error correction. This mapping allows for more robust detection and correction of errors, even in noisy environments. By leveraging these correlations, multidimensional reconciliation can achieve higher reconciliation efficiencies, which are crucial for maintaining the integrity of the distributed key over longer distances.

Table 4. Slice reconciliation schemes in CV-QKD.

Reference	Year	Method	Code Length	SNR	β	FER	Throughput (Msymbols/s)
Assche et al. [109]	2004	Turbo	-	-	-	-	-
Bloch et al. [110]	2006	LDPC	2×10^5	3	88.7%	-	-
		LDPC	2×10^5	15	92.2%	-	-
Lodewyck et al. [111]	2008	LDPC	2×10^5	-	88.7%	10^{-4}	-
Lu et al. [112]	2010	LDPC	2×10^5	-	89%	-	-
Jouguet et al. [113]	2014	LDPC	$2^{20} \approx 10^6$	1	94.2%	-	-
		LDPC	$2^{20} \approx 10^6$	3	94.1%	-	-
Qian et al. [114]	2016	Polar	-	3	90%	-	-
Pacher et al. [115]	2016	LDPC	10^5	3	95.2%	-	-
		LDPC	10^5	31	98.2%	-	-
Bai et al. [117]	2017	LDPC	10^6	1	95.02%	0.19	-
			10^6	3	95.26%	0.22	-
Yang et al. [118]	2020	LDPC	$349{,}952 \approx 3.5 \times 10^5$	1	93.02%	0.14	14.83
		LDPC	$262{,}144 \approx 2.6 \times 10^5$	3	93.06%	0.11	100.9
Mani et al. [119]	2021	LDPC	1.024×10^6	-15.46 db ≈ 0.284	98.8%	-	-
Wen et al. [120]	2021	Polar	$2^{24} \approx 1.6 \times 10^7$	3	94.85%	<10%	-
Wang et al. [122]	2022	Polar	10^9	1	95.12%	<20%	-
				3	95.16%		-
				10	95.82%		-

A series of error-correcting codes, including MET-LDPC (multi-edge-type low-density parity check) [124], Raptor codes [125], and Spain codes [126], have been effectively utilized in multidimensional reconciliation. MET-LDPC codes are known for their flexibility and efficiency in adapting to various channel conditions, which makes them ideal for handling the complexities of multidimensional data. Raptor codes, a class of fountain codes, are highly efficient and offer near-optimal performance with linear time encoding and decoding, making them suitable for rate-adaptive schemes in multidimensional reconciliation. The primary advantage of Spain codes is their robustness and adaptability in high QBER environments, enhancing reliable key distribution over noisy channels. Numerous other error-correcting codes are also suitable for multidimensional reconciliation; due to the limitation of space, they are not detailed here.

In 2008, Leverrier et al. proposed a multidimensional reconciliation protocol that transformed the error correction issue of Gaussian modulation CV-QKD into a channel-coding problem on a Gaussian additive white noise channel through the use of multidimensional spherical transformation. Since the spherical transformation operation itself does not cause quantization loss and can effectively avoid the problem of noise susceptibility in low signal-to-noise ratio scenarios, the transmission distance of CV-QKD systems was extended to 50–100 km. However, the spherical transformation operation in multidimensional reconciliation is essentially a one-to-one mapping, meaning that a continuous variable is mapped to a binary bit after spherical transformation. This limits the code rate of multidimensional reconciliation to no more than 1 bit, meaning that no more than 1 bit of reconciliation code can be extracted from a single raw data point. Therefore, the multidimensional reconciliation protocol is more suitable for low signal-to-noise ratio CV-QKD systems [127].

In 2011, Jouguet et al. used the multidimensional reconciliation protocol combined with multi-edge-type LDPC (MET-LDPC) codes with a code length of 1 Mb. They achieved a high reconciliation efficiency of 96.9% under a signal-to-noise ratio of 0.029, but the frame error rate was as high as 33.3%. Additionally, due to the extremely low code rate of the check matrix, only less than 10^{-3} bits of the secure key could be obtained per pulse in a CV-QKD system with a transmission distance of 120 km [128].

In 2014, Jouguet et al. first introduced polar codes into CV-QKD data reconciliation, achieving a reconciliation efficiency of 95.2% at a signal-to-noise ratio of 1.097 [97].

In 2015, D.Lin et al. designed and implemented a multidimensional reconciliation algorithm on a GPU with a reconciled key rate of 25 Mbps and a reconciliation efficiency of up to 96.5% [129].

In 2017, X. Wang et al. implemented adaptive reconciliation based on MET-LDPC codes combined with the multidimensional reconciliation protocol. This scheme achieved reconciliation efficiencies of around 93.5%, 95.4%, and 96.4% within the signal-to-noise ratio ranges of (0.143, 0.176), (0.069, 0.081), and (0.0277, 0.0314), respectively [130].

In 2018, X. Jiang et al. used spatially coupled LDPC (SC-LDPC) codes as error-correcting codes to achieve multidimensional reconciliation with a maximum reconciliation efficiency of 93.6% [131].

Furthermore, in 2018, X. Wang et al. employed similar methods to implement multi-dimensional reconciliation based on MET-LDPC codes on a GPU. They achieved average reconciled key rates of 30.39 Mbps, 21.23 Mbps, and 16.41 Mbps at signal-to-noise ratios of 0.160, 0.075, and 0.029, respectively, with reconciliation efficiencies of 93.40%, 95.84%, and 96.99% [132].

Furthermore, in 2018, Milicevic et al. proposed a quasi-cyclic construction technique for multi-edge-type LDPC (QC-MET-LDPC) codes and applied them to the multidimensional reconciliation protocol. Given the constraints on code length, their approach enabled CV-QKD systems to operate over distances up to 142 km, attaining a secure key rate of 6.64×10^{-8} pulse/s for key distribution [133].

In 2019, Y. Guo et al. applied QC-LDPC codes to multidimensional reconciliation protocols. When the signal-to-noise ratio (SNR) was 0.623, they achieved a reconciliation efficiency of 92.6% [134]. Furthermore, in 2019, X.Wen et al. simplified the decoding initialization formula by examining the necessary parameters for the process, which helped reduce the information transmission burden in the multidimensional reconciliation process. This was significant for advancing the practical application of CV-QKD [135]. Additionally, in 2019, C. Zhou et al. introduced Raptor codes into multidimensional reconciliation. By designing multiple different degree distributions, they achieved adaptive reconciliation with a maintained reconciliation efficiency of around 95% for SNRs ranging from 0.01 to 1 [136].

In 2020, Y. Li et al. implemented multidimensional reconciliation based on QC-MET-LDPC codes on a GPU. With SNRs of 0.161, 0.076, and 0.03 and using check matrices with code rates of 0.1, 0.05, and 0.02 for parallel processing, the average reconciled key rates reached 64.11 Mbps, 48.65 Mbps, and 39.51 Mbps, respectively. However, the reconciliation efficiencies were only 92.86%, 94.63%, and 93.80% [137]. Furthermore, in 2020, J. Shi et al. applied globally coupled LDPC (GC-LDPC) codes to multidimensional reconciliation, achieving a data reconciled key rate of 23.8 Mbps and a reconciliation efficiency of 95.42% at an SNR of 0.6 [138].

Furthermore, in 2020, X. Wen et al. applied spinal codes to the field of CV-QKD and proposed a novel adaptive information reconciliation protocol. Experimental results showed that the proposed protocol maintained a reconciliation efficiency of around 95% over a wide range of SNRs. Compared to previous adaptive reconciliation schemes, it exhibited better adaptive capabilities and reconciliation performance. Additionally, its simple structure made it easy to implement, providing a practical solution for achieving high-performance adaptive reconciliation and promoting the miniaturization of long-distance CV-QKD systems [139].

In 2020, K. Zhang et al. constructed QC-LDPC codes based on LDPC codes and applied them to multidimensional reconciliation. At an SNR of 0.6431, they achieved a reconciliation efficiency of 93.05% [140].

In 2021, Gumus et al. proposed a modification to the traditional reconciliation protocol used in four-state CV-QKD systems, known as the multiple decoding attempt (MDA) protocol, achieving an 8.5% improvement in SKR while reducing the frame error rate by 10% [141].

In 2021, M. Zhang et al. proposed an improved multidimensional information reconciliation protocol based on polar codes. Simulation results showed that the protocol achieved a reconciliation efficiency of around 97% within a wide range of signal-to-noise ratios (0, 0.18) with a very low frame error rate (Pe < 0.001) [142]. Furthermore, in 2021, M.

Zhang et al. introduced a polar code-based adaptive-rate multidimensional information reconciliation protocol, which effectively improved the secure key rate [143].

In the same year, C. Zhou et al. addressed the issue of varying signal-to-noise ratios in time-varying quantum channels. They achieved a reconciliation efficiency of up to 98% within a range of signal-to-noise ratios (0.0229, 0.0493) [144].

In 2022, X. Fan et al. proposed a reconciliation scheme based on RC-LDPC codes. This scheme could cover all potential SNRs (0.01–15) with a single check matrix, achieving a reconciliation efficiency of 91.80% [145]. Furthermore, in 2022, Jeong et al. introduced a reconciliation algorithm based on MET-LDPC codes, significantly increasing the secure key rate of CV-QKD systems by up to 2.10 times while effectively reducing complexity [146].

Furthermore, in 2022, C. Zhou et al. proposed an efficient decoding scheme. Experimental results showed that for LDPC codes with rates of 0.2 and 0.1, the proposed decoding scheme significantly reduced the bit error rate, achieving throughputs of 152.47 Mbps and 88.32 Mbps [147].

In 2023, Z. Cao et al. proposed a polar code-based adaptive rate reconciliation scheme, achieving a minimum frame error rate of less than 10^{-3} within a range of signal-to-noise ratios from -0.5 to -4.5 dB [148]. Furthermore, in 2023, Z. Cao et al. introduced an information reconciliation algorithm based on an intermediate channel LDPC code cascaded with polar codes (IC-LDPC polar code). Experimental results showed that the IC-LDPC polar code achieved a reconciliation efficiency of over 98% with a minimum frame error rate of 0.19 when the signal-to-noise ratio ranged from -13.2 dB to -20.8 dB [149].

In the same year, J. Liu et al. implemented an eight-dimensional data reconciliation algorithm on the OpenCL heterogeneous computing framework [150].

In 2023, X. Wang et al. proposed a non-Gaussian reconciliation scheme that utilizes the layered belief propagation decoding algorithm for MET LDPC codes to reduce decoding complexity and increase decoding speed [151]. Furthermore, in 2023, S. Yang et al. implemented a high-speed MET-LDPC decoding module based on FPGA. Simulation results demonstrated that when the signal-to-noise ratio is 0.16, the module's reconciliation efficiency is 93.4%, the frame error rate is 19%, and the throughput can reach 9.6 Mbps [152]. In the same year, K. Zhang et al. investigated the relationship between SVP and reconciliation frame error rate in iterative decoding, proposing an early termination scheme based on SVP. Simulation results showed that when the reconciliation efficiency reaches 97.09%, the information throughput of this scheme is improved by 617.1% compared to existing solutions [153].

In 2024, H. Yang et al. proposed a high-efficiency rate-adaptive information reconciliation scheme that integrates Raptor-like (RL) LDPC codes with the addition of trusted noises, aiming to optimize the secret key rate under fluctuating SNR conditions typical in realistic CV-QKD scenarios. By implementing hardware acceleration on GPUs, their approach achieved a decoding throughput of 65.5 Mbits/s, with reconciliation efficiencies maintained over 94.4% across a 15% SNR fluctuation range [154].

Similarly, in 2024, X. Jiang et al. introduced an adaptive reconciliation protocol that modifies Raptor codes to enhance reconciliation efficiency and reduce complexity, particularly at low signal-to-noise ratios (SNRs). This protocol achieved reconciliation efficiencies exceeding 98.1% at SNRs below -20 dB, facilitating higher secret key rates over longer transmission distances [155].

Research studies about multidimensional reconciliation in CV-QKD are listed in Table 5.

Table 5. Multidimensional reconciliation schemes in CV-QKD. Data extracted from graphs by tools are marked with an asterisk (*).

Reference	Year	Method	Code Length	SNR	β	FER	Throughput (Mbps)
Leverrier et al. [127]	2008	-	-	-	-	-	-
Jouguet et al. [128]	2011	LDPC	2^{20}	0.029	96.9%	0.33	-
Jouguet et al. [97]	2012	Polar	2^{24}	1.097	95.2%	0.10	8.0
		LDPC	2^{20}	1.097	95.9%	0.09	6.5
		LDPC	2^{20}	0.161	93.1%	0.04	7.1
Lin et al. [129]	2015	LDPC	10^4	-	96.5%	-	25
Wang et al. [130]	2017	LDPC	10^6	0.0306	96.59%	-	-
		LDPC	10^6	0.077	95.68%	-	-
		LDPC	10^6	0.163	93.64%	-	-
Jiang et al. [131]	2018	LDPC	6.28×10^5	0.642	93.1%	0.036	-
		LDPC	6.28×10^5	0.468	90.3%	3.2×10^{-3}	-
Wang et al. [132]	2018	LDPC	10^6	0.160	93.40%	0.055	30.39
		LDPC	10^6	0.075	95.84%	0.203	21.23
		LDPC	10^6	0.029	96.99%	0.375	16.41
Milicevic et al. [133]	2018	LDPC	10^6	0.0283	99%	0.883	1.807
		LDPC	2^{20}	0.161	-	0.0243	9.17
Guo et al. [134]	2019	LDPC	6.8×10^4	0.623	92.6%	0.5	-
Li et al. [135]	2019	LDPC	10^5	1.121 db	92.19%	0	-
Zhou et al. [136]	2019	Raptor	9900	-20 db	98%	-	-
		Raptor	9900	-0 db	95%	-	-
Li et al. [137]	2020	LDPC	10^6	0.161	92.86%	0.1797	64.11
		LDPC	10^6	0.076	94.63%	0.25	48.65
		LDPC	10^6	0.03	93.80%	0.328	39.51
Shi et al. [138]	2020	LDPC	32,096	0.6	95.42%	3.25×10^{-3}	23.8
Wen et al. [139]	2020	Spinal	2^{10}	(0, 0.5)	≈95%	≤0.056	-
Zhang et al. [140] *	2020	LDPC	6.48×10^6	0.2157	≥95%	≤0.001	-
		LDPC	6.48×10^5	0.635	≥94%	≤0.001	-
Zhang et al. [142]	2021	Polar	-	0.0277	99.54%	<0.001	-
	-	Polar		0.176	97.13%	<0.001	-
Zhang et al. [143] *	2021	Polar	-	(-3 db, -0.5 db)	≥97%	(0.00009, 0.04)	-
Zhou et al. [144]	2021	LDPC	1.25×10^6	-	98%	0.75	8.14
			657,480	-	95%	0.375	16.47
Fan et al. [145]	2022	LDPC	6.48×10^5	0.01–15	91.80%	-	-
Jeong et al. [146]	2022	LDPC	10^6	-15.25 db	-	-	-
Zhou et al. [147] *	2022	LDPC	8×10^4	(0.385, 0.390)	-	≤0.2	152.47
		LDPC	9.6×10^4	(0.171, 0.180)	-	≤0.1	88.32
Cao et al. [148] *	2023	Polar		(-4.5 db, -0.5 db)	>98%	$(0.15, 4 \times 10^{-4})$	-
Cao et al. [149]	2023	LDPC	8192	-20.13 db	98.06%	0.19	-
		LDPC	8192	-19.3 db	99.2%	0.5	-
Wang et al. [151] *	2023	LDPC	10^6	(0.0745, 0.0770)	(93.5%, 96.5%)	(≈0.8, 0)	-
		LDPC	10^6	(0.156, 0.161)	(93%, 96%)	(≈0.2, ≈0.04)	-
Yang et al. [152]	2023	LDPC	1.6×10^5	0.16	93.4%	0.19	9.6
Zhang et al. [153] *	2023	LDPC	10^6	-	(92%, 99%)	(≤0.1, ≈1)	-
Yang et al. [154] *	2024	LDPC	$\approx 10^6$	(0.147, 0.171)	>94.4%	≤0.093	>65.5
Jiang et al. [155] *	2024	Raptor	10^{12}	(-20 db, -8 db)	(98%, 95%)	-	-

For multidimensional reconciliation for CV-QKD, Tables 7 and 8 in [123] and Table IX in [20] provide comprehensive summaries of previous studies. When organizing our Table 5, we added earlier studies not cited in the tables of [20,123] and several newly published papers from 2023 to 2024.

5.4. Error Verification

Suppose Alice and Bob each hold a bit string S_A and S_B. This verification process can be performed by exchanging shorter tags such as random sample bits, parity information [156], or hash values [21]. If Alice's and Bob's tags match, it can be assumed that Alice's and Bob's strings S_A and S_B are consistent.

Typically, the tag used for error verification will leak information about the key. To avoid this problem, the tag should be encrypted with an OTP. Therefore, error verification functions are similar to authentication [21]. Details of this procedure and its related

properties can be found in the section on authentication. Specifically, if a Toeplitz hash is used for error verification, the probability of failure is

$$\epsilon_{ev} = (K_{IR})2^{-t_{ev}+1} \tag{10}$$

Here, ϵ_{ev} represents the failure probability of error verification, K_{IR} represents the length of the key after information reconciliation, and t_{ev} represents the length of the error verification tag.

Another option is to perform verification after privacy amplification to reduce computation [157]. Suppose the privacy amplification often employs the Toeplitz hash functions. The probability of failure using this method is consistent with the approach that uses Toeplitz hash functions. Its disadvantage compared with the above approach is an unnecessary execution of the privacy amplification if errors are found [158].

6. Privacy Amplification

As the final step of QKD postprocessing, privacy amplification (PA) plays an important role in ensuring the security of the entire QKD system. During the process of information reconciliation, the information in the reconciled key may be partially exposed to an eavesdropper, Eve. Privacy amplification allows Alice and Bob to distill a consistent and highly secure key from a partially secure reconciled key through public discussion between the two parties. After privacy amplification, the mutual information between the final secure key and Eve is almost zero.

6.1. Preliminaries of Privacy Amplification

Privacy amplification algorithms are mainly implemented using universal hash functions.

Definition 1. *Let H be a class of hash functions from A to B. H is universal-2, if for any distinct elements* $x_1, x_2 \in X, x_1 \neq x_2, |g \in G, g(x_1) = g(x_2)| \leq \frac{|G|}{|B|}$.

The general process of privacy amplification is described in Figure 8: Alice and Bob obtain the reconciled key X. Through an authenticated public channel, Alice randomly selects a hash function g from the universal hash family G and sends it to Bob. Both Alice and Bob apply the hash function g to the reconciled key X, finally obtaining the secure key Y = g(X).

Both DV-QKD and CV-QKD require distilling the reconciled key to generate final secure keys. However, there are distinct differences in the PA schemes used by DV-QKD and CV-QKD. DV-QKD typically exhibits lower raw key rates compared to CV-QKD but achieves a larger proportion of secure keys. In contrast, although CV-QKD features higher initial key rates, the compression ratio is generally lower. This stems from the significant noise and uncertainty introduced during the quantization process, necessitating more aggressive steps in postprocessing to ensure the security of the final key. Thus, as shown in Figure 9, while both DV-QKD and CV-QKD require large input block sizes, DV-QKD necessitates high-performance PA algorithms that can operate at higher compression ratios. Conversely, CV-QKD demands PA algorithms with higher throughput capabilities to compensate for the extensive key rate reductions inherent in its process.

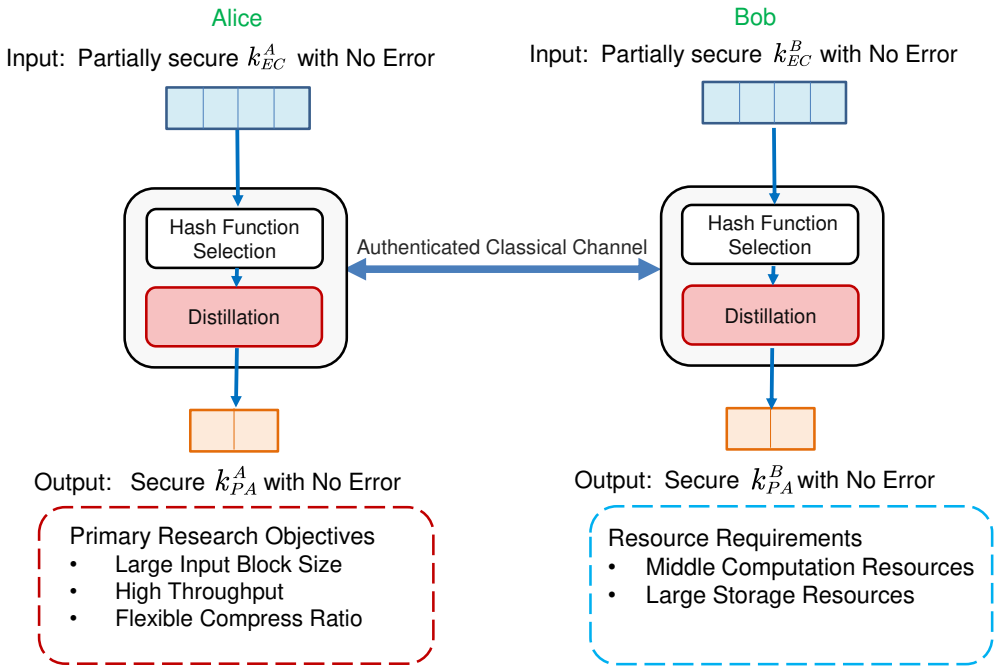

Figure 8. An overview of privacy amplification in the QKD postprocessing. k_{EC} denotes the reconciled key input to the information reconciliation module, and k_{PA} represents the final key output from the privacy amplification module.

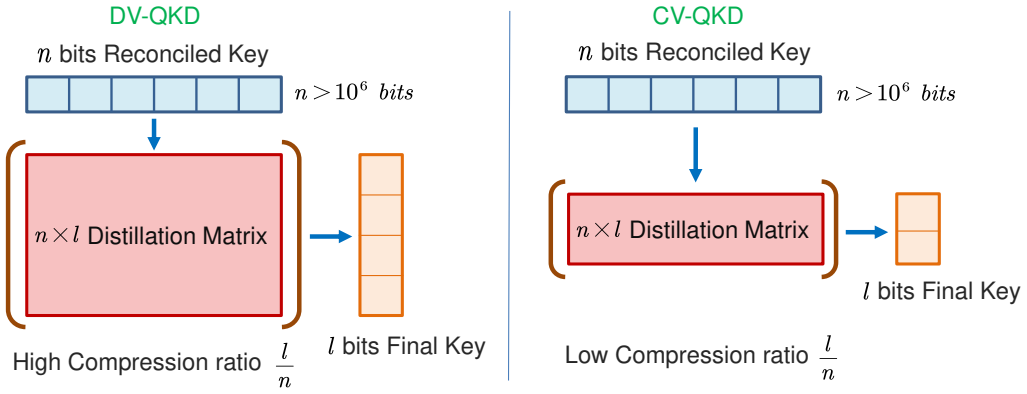

Figure 9. PA schemes suitable for CV-QKD and DV-QKD.

6.2. Security in Privacy Amplification

Since the concept of PA was introduced, research on the security of PA has never stopped. Researchers have conducted many theoretical proofs to ensure the security of the final key generated by PA.

The concept of PA was first proposed by Bennett and Brassard in 1988 [159]. In 1995, Bennett and Brassard further proved that Alice and Bob could distill highly secure keys from reconciled keys that are partially secret by universal-2 hash functions [160].

In 2005, Renner et al. introduced the concept of universal composable PA [161]. In this framework, the security of PA is measured by the distance between the key output by PA and the ideal key.

In this framework, PA is considered ϵ-secure if the distance between its output key and an ideal key is less than or equal to ϵ. Typically, this distance is measured using statistical distance, defined as follows: Let P and Q be two distributions on the same probability space X. The variation distance between them is

$$\delta(P, Q) = \frac{1}{2} \sum_{x \in X} |P(x) - Q(x)| \tag{11}$$

Based on this, P and Q are said to be ϵ-close if $\delta(P,Q) \leq \epsilon$.

Since PA employs a universal hash family for reconciled key extraction, it can be regarded as a randomness extractor [162]. A randomness extractor is defined as follows:

The min-entropy of a distribution X, denoted as $H_\infty(X)$, is defined as the maximum value of k for which $\Pr[X = x] \leq 2^{-k}$ holds true for all x in the support of X. We denote an n-bit distribution X with min-entropy k as an (n,k) distribution.

Definition 2. *Let $Ext : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^l$ be a function that takes as input a sample from an (n,k) distribution X and a d-bit random seed from U_d and outputs an l-bit string. Ext is a (k,ϵ)-extractor, if for all (n,k) distributions X, the output distribution of Ext is $\epsilon-$close to U_l.*

This distance in PA can be computed using the leftover hash lemma [163], presented as follows:

Lemma 1. *Let X be a random variable over $\mathcal{X}$ and let l be an integer greater than 0. Let $h\colon \mathcal{S} \times \mathcal{X} \to \{0,1\}^l$ be a 2-universal hash function. If $l \leq H_\infty(X) - 2\log\left(\frac{1}{\varepsilon}\right)$, then for random seed uniform over $\mathcal{S}$ and independent of X, we have*

$$\delta[(h(S,X),S),(U,S)] \leq \varepsilon \tag{12}$$

where U is uniform over $\{0,1\}^l$ and independent of S. The leftover hash lemma illustrates that we can extract a length asymptotic to $H_\infty(X)$ (the min-entropy of X) bits from a random variable X that is almost uniformly distributed.

In 2005, Renner et al. improved the security proof of PA from the perspective of composition security, fully considering the situation where eavesdroppers can acquire quantum information rather than only classical information, which led to a tighter security bound [164].

Assuming an eavesdropper possesses information E, a key achieves $\epsilon_{sec}-$ secrecy if the statistical distance between the actual key and an ideally uniform and independent key, with respect to E, is less than ϵ_{sec}. The statistical distance is defined as follows [165]:

Definition 3. *Let $\rho_{SE} \in S_\leq(\mathcal{H}_{SE})$, then we define the distance from the uniform of S conditioned on E as*

$$D_u(S|E)_\rho := \min_{\sigma_E} \frac{1}{2}\|\rho_{SE} - \omega_S \otimes \sigma_E\|_1, \tag{13}$$

where $\mathcal{H}$ is a finite-dimensional Hilbert space, $S_\leq(\mathcal{H}) := \{\rho \in \mathcal{P}(\mathcal{H}) : 0 < \mathrm{tr}\rho \leq 1\}$, $\mathcal{P}(\mathcal{H})$ denote positive semidefinite operators on $\mathcal{H}$, $\omega_S := \mathbf{1}_S / \dim \mathcal{H}_S$ is the fully mixed state on $\mathcal{H}_S$, and the minimum here means that all the $\sigma_E \in S_\leq(\mathcal{H}_E)$ satisfied $\mathrm{tr}\sigma_E = \mathrm{tr}\rho_E$ were taken into account.

In 2011, Tomamichel et al. proposed the quantum leftover hash lemma, demonstrating that even if side information is represented by the state of a quantum system, PA can still guarantee the security of the secure key [165].

Lemma 2. *Let F_U be a universal hashing family of functions from X to S, f_u is a hash function randomly selected from F_U, P_{F_U} satisfies uniform distribution, and $s = f_u(x)$. Let $\rho_{XE} = \sum_x |x\rangle\langle x|_X \otimes \rho_E^{[x]}$ and cq-states $\rho_{F_U SE} = \sum_{f_u}\sum_s P_{F_U}|f_u\rangle\langle f_u|_{F_U} \otimes |s\rangle\langle s|_S \otimes \rho_E^{[f_u,s]}$. Then for any $\epsilon \geq 0$, the distance*

$$D_u(S|F_u E)_\rho \leq \frac{1}{2} \times 2^{-\frac{1}{2}[H_{\min}^\varepsilon(\rho_{XE}|E)-l]} + \varepsilon, \tag{14}$$

where E is the side information of eavesdropper [165].

In 2011, Hayashi et al. proposed using the (1+s)th-order Renyi entropy instead of the second-order Renyi entropy for evaluating the uncertainty of a reconciled key [166]. In 2012, Fung et al. proposed the idea of delayed PA and proved its security. Delayed PA could be applied to secret key sharing between nodes of a QKD network [167]. In 2016, Hayashi et al. proposed using smooth Rényi entropy for a more accurate assessment [168]. In the same year, Hayashi et al. demonstrated that the uniformity of the random number seed has an impact on the security of the final key, showing that the impact of non-uniformity of the random numbers on the security of the final key is related to the minimum entropy of the random numbers [169]. In 2022, Y. Huang et al. proposed a stream PA scheme, which can be carried out ahead of information reconciliation, making the data postprocessing more flexible [170].

6.3. Implementation in Privacy Amplification

The development of QKD systems demands higher processing speed for PA. In practical QKD systems, considering the finite size effect, the input block size for PA must be sufficiently large. In addition, the miniaturization of devices requires less computation and storage resource consumption.

To mitigate the impact of the finite size effect, the input block length for PA needs to be at least 10^6 bits. The large block size leads to great computation pressure, so reducing the computation of the hash function is important for the throughput of PA.

The two most typical families of universal hash functions used for PA implementations are binary matrix-based hash functions and multiplication-based hash functions.

A binary matrix-based universal hash function is frequently used in the implementation of PA algorithms. Let M be an $l \times n$ binary matrix, define a family of hash functions $h_M(x) = Mx$ from $\{0,1\}^n$ to $\{0,1\}^l$, then $h_M(x)$ is universal. However, the matrix M requires $n \times l$ bits to represent, which is not acceptable in a practical QKD system. Therefore, it is common to use a Toeplitz matrix instead of the random matrix M. A Toeplitz matrix is a matrix in which the elements on the main diagonal are equal. Let M be a Toeplitz matrix; it just requires $n + l - 1$ bits to represent, which greatly reduces the consumption of random numbers. In addition, the Toeplitz matrix multiplication can be accelerated by fast Fourier transform (FFT), reducing the computational complexity from $O(n^2)$ to $O(nlogn)$. A typical Toeplitz matrix can be represented as follows:

$$T_{l\times n} = \begin{bmatrix} t_{l-1} & t_l & t_{l+1} & \cdots & t_{n+l-4} & t_{n+l-3} & t_{n+l-2} \\ t_{l-2} & t_{l-1} & & & & t_{n+l-4} & t_{n+l-3} \\ \vdots & \vdots & \ddots & & \ddots & \vdots & \vdots \\ t_1 & t_2 & & & & t_{n-1} & t_n \\ t_0 & t_1 & t_2 & \cdots & t_{n-3} & t_{n-2} & t_{n-1} \end{bmatrix} \quad (15)$$

Another family of universal hash functions which is frequently used in the implementation of PA algorithms is a family of modular arithmetic-based hash functions, which can be represented as follows:

$$H_{n,l} = \{h_{c,d} : c, d \in Z_{2^n}, gcd(c,2) = 1\}, h_{c,d}(x) = \lfloor (cx + dmod2^n)/2^{n-l} \rfloor, x \in Z_{2^n} \quad (16)$$

The main operation of a modular arithmetic hash function is integer multiplication. Therefore, the optimization of a modular arithmetic hash function can be achieved through the utilization of fast large integer multiplication algorithms, e.g., Karatsuba, Toom–Cook, and Schönhage and Strassen algorithms. Compared to the Toeplitz matrix-based hash function, the modular arithmetic-based hash function has significantly higher computational complexity when the compression ratio is low. However, in a practical QKD system, the Toeplitz hash function utilizes FFT to reduce computational complexity, and high-precision floating-point numbers can significantly increase the consumption of storage resources. In contrast, the modular arithmetic hash function that performs calculations in the inte-

ger domain has a smaller demand for storage resources, making it more suitable for the miniaturization of devices and chip-based realization of the QKD system.

PA algorithms are predominantly implemented through three platforms: CPU, FPGA, and GPU. A comparison of these three platforms is listed in Table 6.

Table 6. Comparison of CPU, FPGA, and GPU.

	CPU	FPGA	GPU
Parallel capability	Medium	High	High
Computational resources	Medium	Medium	High
Memory resources	High	Low	Medium
Power consumption	Medium	Low	High
Cost	Medium	Medium	High
Programming flexibility	High	Low	Medium

A practical PA scheme is supposed to have a large input block size, high throughput, and low resource consumption. A lot of high-performance PA schemes have been designed for practical QKD systems, as enumerated in Table 7.

Numerous PA schemes have been implemented using central processing units (CPUs), which possess substantial internal storage capacity. This feature enables the efficient processing of large input block sizes. However, CPUs exhibit relatively limited parallel computing capabilities when confronted with high-density parallel computation tasks. In 2014, C. Zhang et al. designed and implemented a length-adaptive PA algorithm based on a modular arithmetic hash function on a CPU platform. With an input block size of 10^7 bits, it achieved a throughput of 10.88 Mbps [171]. In 2016, B. Liu et al. proposed a scheme to accelerate the Toeplitz matrix multiplication using the fast Fourier transform (FFT) on a central processing unit (CPU) platform, reducing the computational complexity from $O(n^2)$ to $O(nlogn)$. When the input block size reached 10^7 bits, the throughput could achieve 60 Mbps [172]. Using a CPU coprocessor, Takahashi et al. employed the number theoretical transform (NTT) to accelerate Toeplitz matrix multiplication. This scheme achieved a throughput of 108 Mbps with an input block size of 10^8 bits, resulting in a final secure code rate of 20 Mbps [173]. In 2018, D. Li et al. proposed an enhanced PA scheme based on an improved linear feedback shift register (LFSR). This scheme significantly reduced the consumption of storage resources; however, it had a lower throughput, achieving only 2 Mbps with an input block size of 10^6 bits [174]. In 2019, B. Tang et al. proposed a high-speed and large-scale PA scheme that utilized the fast Fourier transform (FFT) on commercial CPU platforms. The scheme divided the large input string into multiple blocks and executed them in parallel. When the maximum compression ratio was 0.125, the scheme could achieve an input block size of 10^{10} bits and throughput of 32 Mbps [175]. In 2020, B. Yan et al. proposed a high-speed PA scheme based on a modular arithmetic universal hash function on a CPU platform. The scheme utilized the GNU Multiple Precision Arithmetic Library (GMP) to optimize the large number multiplication operations. With an input block size of 10^8 bits, the throughput could reach 140 Mbps [176]. E. Bai et al. proposed a PA scheme based on linear Toeplitz matrices. This scheme constructed the Toeplitz matrix using a linear feedback shift register (LFSR), significantly saving storage space [177]. Building upon this scheme, Y. Lu et al. replaced the LFSR with the cellular automata, which could generate pseudo-random sequences more rapidly [178].

Field-programmable gate arrays (FPGAs) are increasingly favored in QKD systems due to their programmability, configurable parallelism, and lower energy requirements. As a result, many PA schemes have been successfully deployed through the utilization of FPGAs. In 2012, H. Zhang et al. implemented a PA scheme based on the Toeplitz matrix using an FPGA. With a maximum compression ratio of 0.3, it achieved an input block size of 256 Kb and a throughput of 70 Kbps, resulting in a secure key rate of 17 Kbps [179]. Tanaka et al. implemented a postprocessing engine using six FPGAs. This engine employed the Toeplitz matrix, with an input block size of up to 1 M bits. The secure key rate of this engine

could reach 200 Kbps [91]. In 2017, Constantin et al. proposed an optimized block-based parallel PA scheme utilizing the Toeplitz matrix. The scheme achieved an input block size of 10^6 bits and a throughput of 41 Mbps [92]. Based on this scheme, S. Yang et al. proposed a PA scheme based on the diamond-structure Toeplitz matrix. On the Xilinx Virtex-7 series FPGA platform, it achieved an input block size of 10^6 bits and a throughput of 65 Mbps. Additionally, this scheme could adapt to different input and output sizes and required fewer storage resources [180]. In 2019, Q. Li et al. proposed a scheme based on the Toeplitz matrix, which leveraged two-dimensional FFT acceleration to achieve an input block size of 10^6 bits and a processing rate of 116 Mbps. Moreover, the compression ratio of this scheme could be adjusted arbitrarily within the range of 0 to 1 [181]. In 2022, B. Yan et al. designed a novel hybrid PA scheme based on an FPGA platform. The scheme processed the input sequence in blocks based on the maximum compression ratio and utilized the number theoretic transform (NTT) to achieve high-speed large number multiplication, elevating the throughput to the Gbps level. With an input block size of 10^8 bits, the algorithm could achieve a throughput of 1.8 Gbps [182].

While graphics processing units (GPUs) provide superior computational and parallel processing capabilities, leading to enhanced performance, they also consume more power and demand higher costs. This has led to a limited amount of research on GPU-based PA schemes. X. Wang et al. implemented a high-speed PA scheme based on the Toeplitz matrix on a GPU platform. By improved FFT acceleration and block parallel computing algorithm, the scheme achieved a throughput exceeding 1 Gbps when the input block size was 128 Mb [183].

Implementations of the PA algorithm are listed in Table 7. In the table, we selected the data corresponding to the optimal input block size and throughput from the referenced PA schemes.

Table 7. Comparison of PA schemes.

Reference	Year	Platform	Scheme	Input Block Size	Throughput
Zhang et al. [171]	2014	CPU	Modular MULT	512 Kb	17.4 Mbps
				12 Mb	12.9 Mbps
Liu et al. [172]	2016	CPU	Toeplitz	1.6 Mb	78.1 Mbps
				12.8 Mb	60.4 Mbps
Takahashi et al. [173]	2016	CPU	Toeplitz	100 Mb	108.7 Mbps
Li et al. [174]	2018	CPU	Toeplitz	3.1 Mb	2.1 Mbps
Tang et al. [175]	2019	CPU	Toeplitz	1 Mb	118 Mbps
				128 Mb	71.1 Mbps
				128 Gb	0.44 Mbps
Yan et al. [176]	2020	CPU	Modular MULT	1 Mb	262.1 Mbps
			MULT	100 Mb	140.9 Mbps
Bai et al. [177]	2022	CPU	Toeplitz	1.28 Mb	19.5 Kbps
				3 Mb	22.7 Kbps
Lu et al. [178]	2022	CPU	Toeplitz	5.1 Mb	0.6 Mbps
Zhang et al. [179]	2012	FPGA	Toeplitz	256 Kb	70 Kbps
Tanaka et al. [91]	2012	FPGA	Toeplitz	1 Mb	-
Constantin et al. [92]	2017	FPGA	Toeplitz	1 Mb	20 Mbps
Yang et al. [180]	2017	FPGA	Toeplitz	1 Mb	65.4 Mbps
Li et al. [181]	2019	FPGA	Toeplitz	1 Mb	116 Mbps
Yang et al. [118]	2020	FPGA	Toeplitz	341.75 Kb	186.9 Mbps
Yan et al. [182]	2022	FPGA	MMH-MH	100 Mb	1.5 Gbps
Wang et al. [183]	2018	GPU	Toeplitz	64 Mb	1.38 Gbps
				128 Mb	1.35 Gbps

7. Channel Authentication

Authentication ensures the integrity and security of the communication between Alice and Bob. It plays a crucial role in QKD systems because authentication directly impacts the security of QKD keys [184] and consumes a portion of QKD keys. In QKD systems, information-theoretic security authentication serves two main functions: on the one hand, it protects information from being tampered with by attackers, i.e., it ensures message integrity; on the other hand, it resists man-in-the-middle attacks [185], ensuring that messages come from the correct nodes.

Since the authentication scheme can run in parallel with other postprocessing protocols, authentication is not a bottleneck for postprocessing throughput. Current research is more focused on considering the security of authentication and key consumption, hoping to minimize key consumption as much as possible while maintaining necessary security levels. In this section, we first introduce the preliminaries of authentication, followed by discussing the development directions of authentication-related research from three perspectives: authentication protocols interaction modes, hash functions construction in authentication, and non-ideal conditions in authentication.

7.1. Preliminaries of Authentication

In QKD system security proofs, it is assumed that classical channel authentication is implemented to prevent Eve from impersonating Alice or Bob. Thus, it becomes necessary to authenticate the classical channel during the postprocessing of QKD. However, the authentication process must cost a portion of the final secure key. Consequently, authentication plays a significant role in determining the correctness and final secure key rate of QKD. Let M denote the message to be authenticated, and let k_au denote the authentication key preshared between Alice and Bob. M and k_au are inputs to Alice's channel authentication module, and the message–tag pair (M, T) is the output of Alice's channel authentication module. The received message–tag pair (M', T') serves as the input to Bob's channel authentication module, which helps determine whether the received (M', T') is correct. The inputs and outputs of the channel authentication module for the message sender and receiver are illustrated in Figure 10.

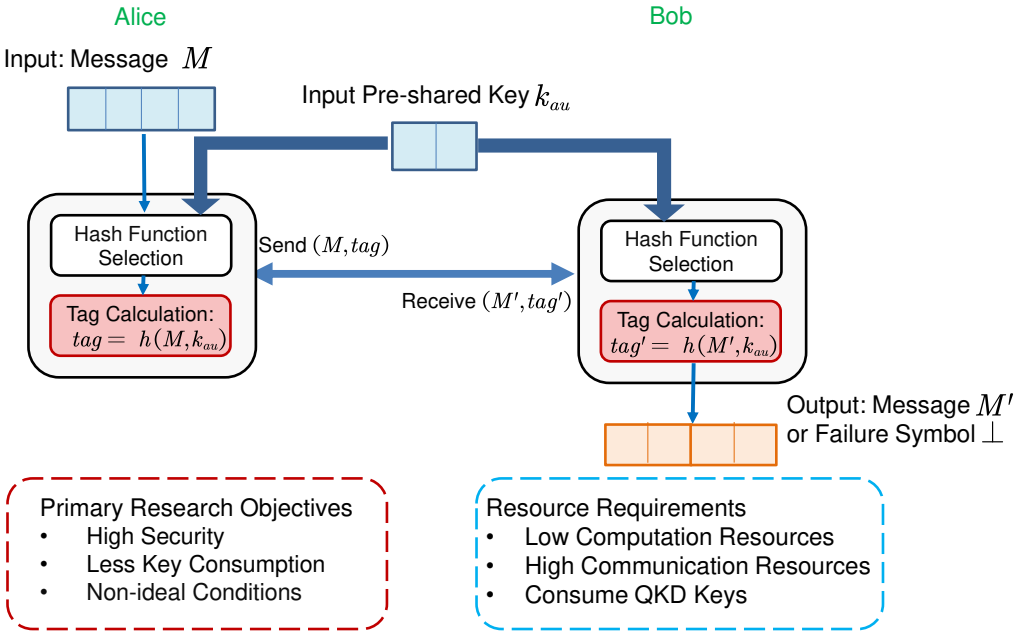

Figure 10. An overview of a channel authentication module in QKD postprocessing. If authentication succeeds, Bob outputs the message $M' = M$; otherwise, Bob outputs $\perp$, indicating authentication failure.

In the authentication protocol, we hope the probability of Eve deceiving Bob is less than a negligible value, which is the security parameter of the authentication ε_{auth}. The authentication scheme depicted is the most basic form of authentication; however, this scheme is merely an abstract description. In practical applications, we must consider many more factors in detail.

- Security: The level of security offered by an authentication protocol is crucial, as the property of compositional security dictates that the security of authentication ultimately affects the security of the keys [21]. Therefore, an information-theoretically secure authentication scheme is necessary for QKD systems. We need to pay attention to the security parameters ε_{auth} an authentication scheme can achieve.
- Key consumption: Implementing an information-theoretically secure authentication scheme requires the consumption of a certain amount of keys. These keys generally come from the information-theoretically secure keys distributed in the previous round of QKD. However, given that the current key rates of QKD are not sufficient to meet practical encryption needs, most research aims to reduce the consumption of authentication keys $|K_{au}|$.
- Non-ideal conditions: In practical protocol operations, it is typically challenging to guarantee that all conditions are optimal. For example, from the perspective of authentication, we usually assume that the keys shared between Alice and Bob are information-theoretically secure, meaning the attacker knows nothing about them. However, in practice, the security of the keys depends on the preshared scheme, and at this time, the security of authentication will be weaker than the ideal security parameters.

Generally, the most critical concern of protocols is the final security parameter of authentication. With the same security parameter, the goal is to minimize key consumption as much as possible. However, under general conditions, the use of different authentication interaction modes, universal hash families, and security conditions can lead to varying levels of key consumption. In this section, we discuss the current research content in three parts: 1. Research on authentication interaction modes. 2. Research on universal hash families for authentication. 3. Non-ideal security conditions.

7.2. Authentication Interaction Modes

When discussing the interaction modes between authentication protocols, it is important to first understand the basic interaction modes of the authentication process. For this subsection, we do not consider the differences in universal hash function families, as these can be addressed later in the analysis. Here, we provide an overview of three different authentication interaction modes.

First, we introduce the encode–decode authentication. This scheme is the most original information-theoretically secure authentication scheme, proposed by Gilbert et al. [186]. The authentication process, as illustrated in Figure 11, involves Alice being responsible for encoding the data and key, while Bob is responsible for decoding. This method requires the authentication key only to be used one time, leading to high key consumption during the authentication process. For example, when authenticating for N rounds, the key consumption would be $N|K_{au}|$.

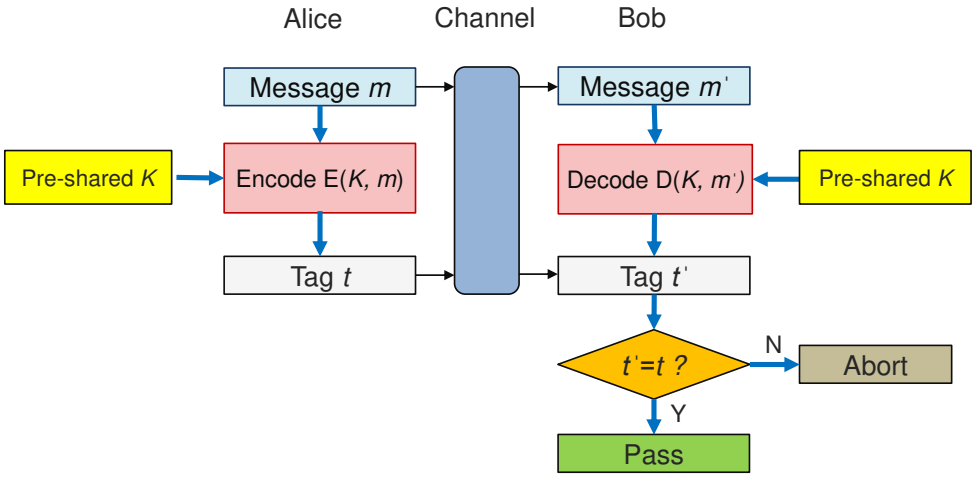

Figure 11. Interaction modes of encode–decode authentication.

Second, the key recycling (KR) authentication scheme was later proposed by Wegman-Carter [187]. Wegman-Carter pointed out that if the tag is encrypted with an OTP (one-time pad) for each authentication, the key K_{au} can be reused cyclically. The interaction mode of key recycling authentication is illustrated in Figure 12. Such schemes have a key consumption of $|K_{au}| + R|tag|$ for authenticating R rounds. The security of this key recycling scheme has been fully proven in [184].

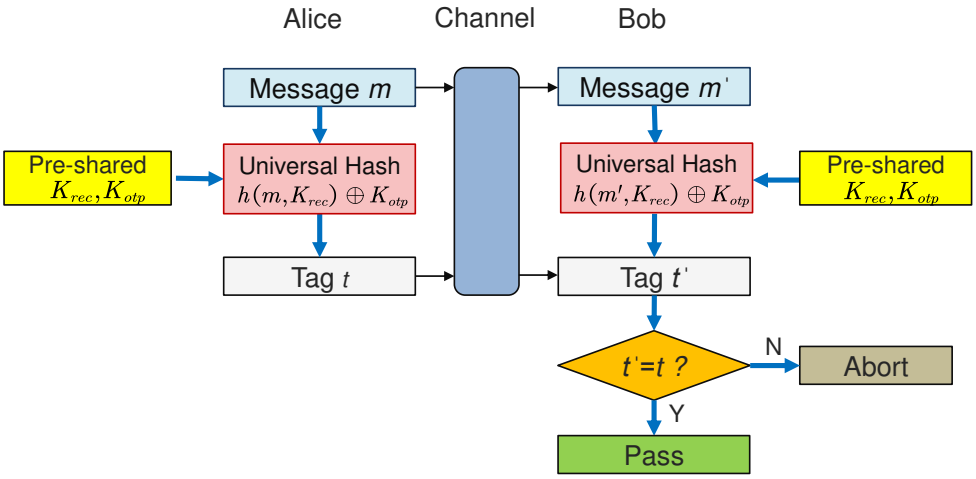

Figure 12. Interaction modes of key recycling authentication.

Third, ref. [188] proposed a ping-pong delayed authentication protocol. This protocol makes two improvements based on the key recycling protocol. First, it consolidates the information from each round of postprocessing for a single authentication, thereby reducing the number of authentications. Second, it changes the unidirectional authentication in the original scheme to a bidirectional authentication where Alice and Bob alternately initiate authentication. Only the QKD postprocessing that passes this bidirectional authentication is considered legitimate. The interaction mode of ping-pong delayed authentication is illustrated in Figure 13. Thus, the key consumption is defined by computing a single tag of all the classical messages used in one round of communication (bidirectional authentication can be referred to as two rounds). Such schemes' key consumption is also $|K_{au}| + R|tag|$ for authenticating R rounds of classical communication. However, ref. [188] provides a new method for constructing AXU_2 universal hash family using AU_2 and XU_2. This method minimizes the lengths of K_{au} and tag as much as possible, thereby enabling reduced consumption of authentication keys.

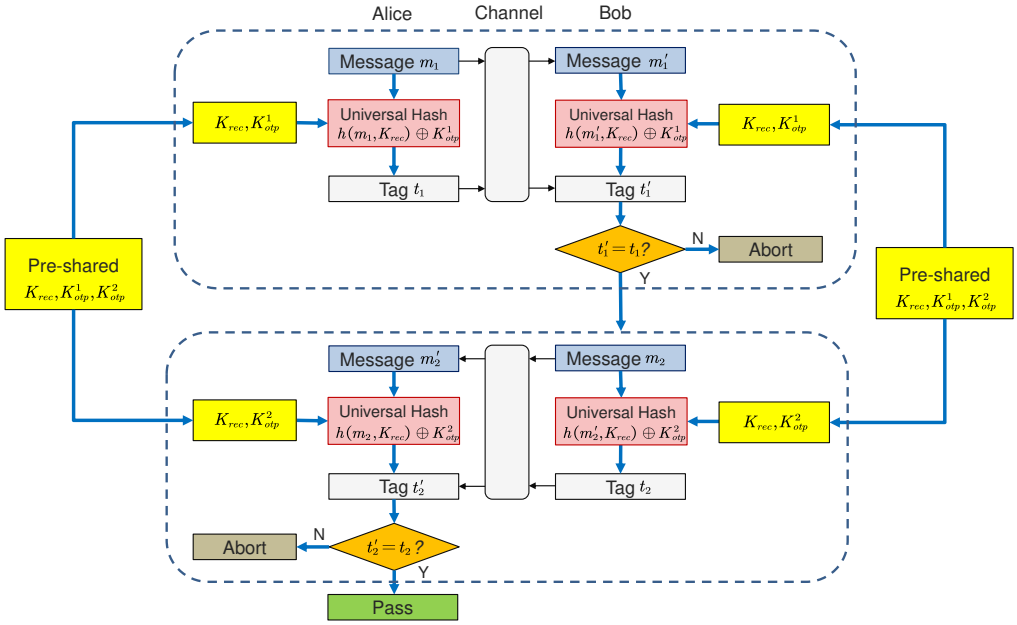

Figure 13. Interaction modes of ping-pong delayed authentication.

7.3. Hash Function Construction in Authentication

In authentication protocols, the computation of hash functions is a critical process. This process determines the probability that the tag or messages between the parties could be forged by Eve. Typically, it is desired that the probability of Eve successfully forging message–tag pairs (m, t) is less than the security parameter ε_{auth}, as shown in Equation (17).

$$P\left(h\left(m'\right) = t' | h(m) = t\right) \leq \varepsilon_{auth} \tag{17}$$

Usually, this requirement is achieved by constructing an almost strong universal (ASU) hash function family, as shown in Definition 4.

Definition 4 (ε-almost strong universal hash family)**.** *Let M and T be finite sets. The hash function $h \in H$ maps an element $m \in M$ into an element $t \in T$. The family of hash functions H is $\varepsilon - ASU_2$ if the following two conditions are satisfied:*

1. *For any $m \in M$ and $t \in T$:*
$$\{h | h(m) = t\} = |H|/|T|$$
2. *For any $m_0, m \in M (m_0 \neq m)$ and $t_0, t \in T$:*
$$\{h | h(m_0) = t_0, h(m) = t\} = \varepsilon |H|/|T|$$

Based on the properties of the $\varepsilon - ASU_2$ hash function family, the probability of an attacker successfully carrying out an attack can be deduced by Equation (18).

$$P\left(h\left(m'\right) = t' | h(m) = t\right) = \frac{P(h(m') = t', h(m) = t)}{P(h(m) = t)} \leq \varepsilon \tag{18}$$

Therefore, many authentication schemes utilize $\varepsilon - ASU_2$. In the research by [189–191], discussions were conducted on the construction of the upper and lower bounds of key lengths for $\varepsilon - ASU_2$ hash functions. Among these, ref. [191] provided new bounds that are tighter than the other bounds for key length. In addition to ASU hash function families, other universal hash function families have been used to construct authentication schemes, such as $\varepsilon - AU_2$ [192], $\varepsilon - AXU_2$ [193], and $\varepsilon - A\Delta U$ [194] (polynomial hash also falls into this category [195,196]). These definitions are as follows.

Definition 5 (ε-almost universal hash family)**.** *Let M and T be finite sets. The hash function $h \in H$ maps an element $m \in M$ into an element $t \in T$. The family of hash functions H is $\varepsilon - AU_2$ if the following two conditions are satisfied:*

For any $m_0, m \in M(m_0 \neq m)$ and $t_0, t \in T$:

$$\{h|h(m_0) = h(m)\} = \varepsilon|H|/|T|$$

Definition 6 (ε-almost XOR universal hash family)**.** *Let M and T be finite sets. The hash function $h \in H$ maps an element $m \in M$ into an element $t \in T$. $\oplus$ denotes the bitwise XOR operation. The family of hash functions H is $\varepsilon - AXU_2$ if the following two conditions are satisfied:*

For any $m_0, m \in M(m_0 \neq m)$ and $t \in T$:

$$\{h|h(m_0) \oplus h(m) = t\} = \varepsilon|H|/|T|$$

Definition 7 (ε-almost Δ universal hash family)**.** *Let M and T be finite sets. The hash function $h \in H$ maps an element $m \in M$ into an element $t \in T$ where T is the Abelian group. Δ denotes the group operation. The family of hash functions H is $\varepsilon - A\Delta U_2$ if the following two conditions are satisfied:*

For any $m_0, m \in M(m_0 \neq m)$ and $t \in T$:

$$\{h|h(m_0)\Delta h(m) = t\} = \varepsilon|H|/|T|$$

These categories of functions can be combined with each other to form universal hash function families with different properties. We provide common combinations in Theorem 2, and their security analysis can be referred to in [188,192,197].

Theorem 2. *For $i = 1, 2$, let $H_i : A_i \to B_i$ be above almost universal families. Here, define $\{H = h(m) = h_2(h_1(m))|h_1 \in H_1, h_2 \in H_2\}$. Then, H has the following properties:*

1. *If H_1 is $\varepsilon_1 - AU$ and H_2 is $\varepsilon_2 - AU$, then H is $(\varepsilon_1 + \varepsilon_2 - \varepsilon_1\varepsilon_2) - AU$.*
2. *If H_1 is $\varepsilon_1 - AU$ and H_2 is $\varepsilon_2 - A\delta U$, then H is $(\varepsilon_1 + \varepsilon_2 - \varepsilon_1\varepsilon_2) - A\delta U$.*
3. *If H_1 is $\varepsilon_1 - AU$ and H_2 is $\varepsilon_2 - ASU$, then H is $(\varepsilon_1 + \varepsilon_2 - \varepsilon_1\varepsilon_2 - ASU$.*

Additionally, it is noteworthy that the combination of $\varepsilon - AXU_2$ with an OTP determines the security of the key recycling (KR) scheme. The research in [198,199] suggests that the combination of $\varepsilon - AXU_2$ with an OTP can be equivalent to $\varepsilon - ASU_2$. This implies that in the KR scheme, an $\varepsilon - AXU_2$ hash family can be used to construct the authentication protocol.

Another important issue is the key consumption for constructing hash families. Because different hash family constructions require varying amounts of keys, the main concept in authentication schemes is to explore how to use fewer keys to achieve a scheme that meets the security parameter. Many studies have discussed this issue, such as [187–189,192,198,200,201], the key consumption and the security parameters of these schemes are summarized in a Table 8.

In Table 8, $|M|$ represents the length of the message, and $|tag|$ represents the length of the authentication tag. log is the logarithm with base 2. In [188], the message M is split into w-bit pieces, and λ is a minimal possible integer so that the condition $\lceil |M|/w \rceil^{\lambda} 2^{-\lambda w} \leq \varepsilon_{auth} - 2^{-|Tag|}$ is fulfilled.

Table 8. Security parameters and the key consumption of constructing hash families.

Reference	Security Parameter ε_{auth}	Key Consumption
Wegman et al. [187]	$2^{-\lvert Tag\rvert+1}$	$4(\lvert Tag\rvert + \log\log\lvert M\rvert)\log\lvert M\rvert$
Stinson et al. [189]	$(\log\lvert M\rvert - \log\lvert Tag\rvert + 1)/2^{\lvert Tag\rvert}$	$(\log\lvert M\rvert - \log\lvert Tag\rvert + 2)\lvert Tag\rvert$
Den Boer et al. [200]	$(\lvert M\rvert/\lvert Tag\rvert)/2^{\lvert Tag\rvert}$	$2\lvert Tag\rvert$
Bierbrauer et al. [201]	$2^{-\lvert Tag\rvert+1}$	$3\lvert Tag\rvert + 2\log\lvert M\rvert$
Krawczyk [198]	$(1 + 2\lvert M\rvert)/2^{\lvert Tag\rvert}$	$3\lvert Tag\rvert + 1$
Abidin et al. [202]	$2^{-\lvert Tag\rvert+1}$	$4\lvert Tag\rvert + 3\log\lvert M\rvert + 4$
Kiktenko et al. [188]	$2^{-\lvert Tag\rvert} + \lceil \lvert M\rvert/w\rceil^{\lambda}2^{-\lambda w}$	$2\lambda w + \lambda + 2\lvert tag\rvert - 1$

7.4. Non-Ideal Security Conditions in Authentication

In most QKD authentication research, only key consumption and security parameters are considered, while implicit conditions are overlooked. These conditions can affect the final security of authentication. In this section, we discuss three non-ideal conditions in the authentication process that need to be considered:

- Non-ideal condition of the initial authentication key: During the initial authentication, the security of the preshared key might be non-ideal. We denote its security parameter as ε_{pre}. This reflects the possibility that the initial setup or the process of establishing the shared key does not fully adhere to the ideal security assumptions, potentially due to practical constraints or vulnerabilities in the key distribution process.
- Non-ideal condition in subsequent authentications: During subsequent authentications, a portion of the key may need to be reused, which could have exposed some information during the previous authentication round. Attackers could infer limited information about the key from the message–tag pairs of earlier rounds, thus diminishing its security. This degradation is related to the recycling authentication process's security parameter ε_{re}.
- Non-ideal conditions of QKD-generated keys: The keys used for authentication changes are sourced from the QKD key pool, whose security is determined by the security parameter of QKD, ε_{QKD}. We discuss the first authentication and subsequent authentications separately. Typically, the key used for the first authentication is not a QKD-generated key because the key distribution process has not yet started at this point, so its security may be weaker than that of QKD-generated keys. Subsequent authentications use keys generated after the first authentication using QKD, and the security of these keys is determined by the QKD's security parameter ε_{QKD}.

Here, we provide a review of the three non-ideal conditions mentioned above. First, the non-ideal condition of the initial authentication key is a challenging problem to solve. In practical protocol implementations, we usually assume that the keys shared between Alice and Bob are information-theoretically secure, meaning the attacker knows nothing about them. However, in practice, the security of the keys depends on the preshared scheme, and at this time, the security of authentication will be weaker than the ideal security parameters. Therefore, some articles [188,203,204] consider QKD merely as a key-growing scheme. Currently, there is no information-theoretically secure method to solve this problem, but recent works [185,205] have proposed a postquantum cryptography solution that aims to address this issue.

Second, the key recycling may affect the final security of authentication. In the research by [206], it is believed that the first hash function is randomly chosen from the family of hash functions, so the first tag does not need to be encrypted with the OTP. Ref. [207] suggests that every tag should be encrypted by the OTP for information-theoretically secure authentication. This is because the information of the reused hash function may be leaked to Eve if the first tag is not encrypted; therefore, the security of subsequent authentication may be compromised in QKD. The research by [184] addresses the aforementioned issues and comprehensively discusses the specific security of the key recycling (KR) scheme, providing a method for calculating the security parameters for multiple rounds of the KR scheme.

Third, the imperfection of QKD keys was first discussed in the literature by [202], which addressed the information-theoretic security of authentication with a partially known key. Ref. [208] further discussed this issue, providing a way to calculate the security of authentication when Eve has obtained some information about the QKD key.

Finally, in the research by [188], a comprehensive consideration of the above three non-ideal factors was taken into account, offering a universal compositional security framework and providing a method for calculating security parameters within the ping-pong authentication scheme. Following this, the study by [209] discussed the security parameters in a general KR scheme, considering the integration of the three non-ideal factors mentioned above. Here, we provide Table 9, which summarizes the analysis of authentication security under various non-ideal conditions.

Table 9. Summary of authentication security analysis under various non-ideal conditions. ε_{pre} represents a non-ideal condition of the initial key authentications, ε_{re} represents a non-ideal condition in subsequent authentications, and ε_{QKD} represents non-ideal conditions of QKD-generated keys. The ✓symbol indicates that a specific non-ideal condition has been discussed in the corresponding literature.

Reference	Years	ε_{pre}	ε_{re}	ε_{QKD}
Aticia et al. [206]	1996		✓	
Abidin et al. [207]	2012		✓	
Abidin et al. [202]	2013		✓	✓
Portmann [184]	2014		✓	✓
Li et al. [208]	2016		✓	✓
Kiktenko et al. [188]	2020	✓	✓	✓
Molotkov [209]	2022	✓	✓	✓

8. Conclusions

In this review, we explored the optimization and development of practical QKD post-processing. Our analysis emphasizes the importance of refining postprocessing strategies to bridge the theoretical and practical applications of QKD. We highlight challenges in implementing these subprotocols in real-world scenarios, like limited resources and non-ideal factors. Additionally, we show how improvements in each subprotocol affect key rate and security, offering valuable insights for future QKD advancements. Furthermore, we advocate for a more balanced approach that not only aims at maximizing the secure key rate or throughput but also ensures the robustness of security parameters of postprocessing.

Toward the end of this review, we present future research prospects for QKD postprocessing across five main aspects: parameter estimation, sifting, information reconciliation, privacy amplification, and authentication:

- Parameter estimation: Firstly, one research direction involves developing parameter estimation methods that are tighter, more accurate, and more efficient. Secondly, the other research direction is to provide more detailed parameter estimation methods to specific QKD protocols such as CV-QKD or MDI-QKD. Additionally, these methods may take into account specific channel conditions, attacker's assumptions, and imperfections of the practice device.

- Sifting: Although sifting is based on relatively simple principles and has seen limited research, future studies should focus on enhancing sifting efficiency and balancing the precision of parameter estimation. Additionally, minimizing interactive data exchange during sifting is a valuable research direction, as it can improve throughput while reducing the length of authenticated data.
- Information reconciliation: Further research is needed to enhance information reconciliation for improved efficiency and reduced FER. Optimizing the implementation of information reconciliation protocols for practical QKD systems is vital for future advancements. The practicality of QKD systems necessitates miniaturization and chip-scale implementation of information reconciliation. Addressing how to ensure the efficiency and processing speed of the information reconciliation component under constraints in computational, storage, and communication resources will be an important focus of future research.
- Privacy amplification: In the future, it is important to integrate the non-ideal conditions of QKD systems into security theory analysis, updating models to better reflect real-world operational threats, such as considering the uniformity of random seeds. Furthermore, it is important to further optimize PA algorithms to meet the demands of high-performance QKD systems and improve input block size and throughput.
- Channel authentication: Balancing security and key consumption through optimal constructions of universal hash functions is essential. Additionally, developing a robust QKD network authentication scheme based on universal hash [210] or postquantum cryptography [205] is also important. QKD network authentication that additionally secures node identities and prevents attacks without relying on asymmetric cryptography poses a significant challenge for future research.

In conclusion, this review highlights the intricate dynamics of QKD postprocessing, proposing pathways to enhance the security and efficiency of QKD systems. Through a detailed examination of the intersection between postprocessing improvements and QKD security, we contribute to the ongoing dialogue on advancing quantum secure communications to meet the demands of the real world.

Author Contributions: Writing—original draft, Y.L. and X.C.; writing—review and editing, Y.L., X.C., Q.L. and H.-K.M.; funding acquisition, Q.L. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by National Natural Science Foundation of China (Grant number: 62071151) and Innovation Program for Quantum Science and Technology (Grant No. 2021ZD0300701).

Institutional Review Board Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

QKD	Quantum key distribution
OTP	One-time pad
ITS	Information-theoretic security
PA	Privacy amplification
EC	Error correction
DV	Discrete variable
CV	Continuous variable

QBER	Quantum bit error rate
FEC	Forward error correction
LDPC	Low-density parity check
SCL	Successive cancellation list
FER	Frame error rate
FPGA	Field-programmable gate array
GPU	Graphics processing unit
SNR	Signal-to-noise ratio
LFSR	Linear feedback shift register
FFT	Fast Fourier transform
NTT	Number theoretic transform
MULT	Multiplication
MMH	Multilinear modular hashing
MH	Modular arithmetic hashing
KR	Key recycling
ASU	Almost strong universal
AU	Almost universal

References

1. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [CrossRef]
2. Wootters, W.K.; Wootters, W.K.; Zurek, W.H. A single quantum cannot be cloned. *Nature* **1982**, *299*, 802–803. [CrossRef]
3. Dieks, D. Communication by EPR devices. *Phys. Lett.* **1982**, *92*, 271–272. [CrossRef]
4. Xu, F.; Ma, X.; Zhang, Q.; Lo, H.K.; Pan, J.W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **2020**, *92*, 025002. [CrossRef]
5. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **2014**, *560*, 7–11. [CrossRef]
6. Ekert, A. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **1991**, *67*, 661–663. [CrossRef] [PubMed]
7. Bennett, C.H.; Brassard, G.; Mermin, N.D. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.* **1992**, *68*, 557–559. [CrossRef] [PubMed]
8. Grosshans, F.; Grangier, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **2001**, *88*, 057902. [CrossRef]
9. Inoue, K.; Waks, E.; Yamamoto, Y. Differential-phase-shift quantum key distribution using coherent light. *Phys. Rev.* **2003**, *68*, 022317. [CrossRef]
10. Lo, H.K.; Ma, X.; Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **2004**, *94*, 230504. [CrossRef]
11. Lo, H.K.; Curty, M.; Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **2011**, *108*, 130503. [CrossRef] [PubMed]
12. Lucamarini, M.; Yuan, Z.L.; Dynes, J.F.; Shields, A.J. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature* **2018**, *557*, 400–403. [CrossRef] [PubMed]
13. Ma, X.; Zeng, P.; Zhou, H. Phase-Matching Quantum Key Distribution. *Phys. Rev. X* **2018**, *8*, 031043. [CrossRef]
14. Zeng, P.; Zhou, H.; Wu, W.; Ma, X. Mode-pairing quantum key distribution. *Nat. Commun.* **2022**, *13*, 3903. [CrossRef] [PubMed]
15. Pirandola, S.; Andersen, U.L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; et al. Advances in quantum cryptography. *Adv. Opt. Photon.* **2020**, *12*, 1012–1236. [CrossRef]
16. Lo, H.K.; Curty, M.; Tamaki, K. Secure quantum key distribution. *Nat. Photonics* **2014**, *8*, 595–604. [CrossRef]
17. Diamanti, E.; Lo, H.K.; Qi, B.; Yuan, Z. Practical challenges in quantum key distribution. *NPJ Quantum Inf.* **2016**, *2*, 16025. [CrossRef]
18. Zhang, Q.; Xu, F.; Chen, Y.A.; Peng, C.Z.; Pan, J.W. Large scale quantum key distribution: Challenges and solutions [Invited]. *Opt. Express* **2018**, *26*, 24260–24273. [CrossRef] [PubMed]
19. Zhang, C.X.; Wu, D.; Cui, P.W.; Ma, J.C.; Wang, Y.; An, J.M. Research progress in quantum key distribution. *Chin. Phys. B* **2023**, *32*, 124207. [CrossRef]
20. Zhang, Y.; Bian, Y.; Li, Z.; Yu, S.; Guo, H. Continuous-variable quantum key distribution system: Past, present, and future. *Appl. Phys. Rev.* **2024**, *11*, 011318. [CrossRef]
21. Fung, C.H.F.; Ma, X.; Chau, H.F. Practical issues in quantum-key-distribution postprocessing. *Phys. Rev. A* **2010**, *81*, *012318*. [CrossRef]
22. Holevo, A.S. Bounds for the quantity of information transmitted by a quantum communication channel. *Probl. Peredachi Inf.* **1973**, *9*, 3–11.
23. Portmann, C.; Renner, R. Security in quantum cryptography. *Rev. Mod. Phys.* **2022**, *94*, 025008. [CrossRef]
24. Maurer, U.M., The Strong Secret Key Rate of Discrete Random Triples. In *Communications and Cryptography*; Springer: New York, NY, USA, 1994; Volume NaN , pp. 271–285.
25. Renner, R. Security of Quantum Key Distribution. *Int. J. Quantum Inf.* **2008**, *6*, 1–127. [CrossRef]

26. Li, W.; Zhang, L.; Tan, H.; Lu, Y.; Liao, S.K.; Huang, J.; Li, H.; Wang, Z.; Mao, H.K.; Yan, B.; et al. High-rate quantum key distribution exceeding 110 Mb s^{-1}. *Nat. Photonics* **2023**, *17*, 416–421. [CrossRef]
27. Scarani, V.; Renner, R. Quantum Cryptography with Finite Resources: Unconditional Security Bound for Discrete-Variable Protocols with One-Way Postprocessing. *Phys. Rev. Lett.* **2008**, *100*, 200501. [CrossRef] [PubMed]
28. Ostrev, D. QKD parameter estimation by two-universal hashing. *Quantum* **2023**, *7*, 894. [CrossRef]
29. George, I.; Lin, J.; Lütkenhaus, N. Numerical calculations of the finite key rate for general quantum key distribution protocols. *Phys. Rev. Res.* **2021**, *3*, 013274. [CrossRef]
30. Tomamichel, M.; Lim, C.C.W.; Gisin, N.; Renner, R. Tight finite-key analysis for quantum cryptography. *Nat. Commun.* **2012**, *3*, 634. [CrossRef]
31. Sun, S.; Huang, A. A Review of Security Evaluation of Practical Quantum Key Distribution System. *Entropy* **2022**, *24*, 260. [CrossRef]
32. Liang, K.; Chai, G.; Cao, Z.; Yuan, Y.; Chen, X.; Lu, Y.; Peng, J. Bayesian Parameter Estimation for Continuous-Variable Quantum Key Distribution. *Phys. Rev. Appl.* **2022**, *18*, 054077. [CrossRef]
33. Jing, F.; Liu, X.; Wang, X.; Lu, Y.; Wu, T.; Li, K.; Dong, C. Compressive sensing based parameter estimation for free-space continuous-variable quantum key distribution. *Opt. Express* **2022**, *30*, 8075–8091. [CrossRef]
34. Luo, H.; Wang, Y.J.; Ye, W.; Zhong, H.; Mao, Y.Y.; Guo, Y. Parameter estimation of continuous variable quantum key distribution system via artificial neural networks. *Chin. Phys. B* **2022**, *31*, 020306. [CrossRef]
35. Lupo, C.; Ottaviani, C.; Papanastasiou, P.; Pirandola, S. Parameter estimation with almost no public communication for continuous-variable quantum key distribution. *Phys. Rev. Lett.* **2018**, *120*, 220505. [CrossRef] [PubMed]
36. Guo, Y.; Xie, C.; Huang, P.; Li, J.; Zhang, L.; Huang, D.; Zeng, G. Channel-parameter estimation for satellite-to-submarine continuous-variable quantum key distribution. *Phys. Rev. A* **2018**, *97*, 052326. [CrossRef]
37. Chen, Z.; Zhang, Y.; Wang, X.; Yu, S.; Guo, H. Improving parameter estimation of entropic uncertainty relation in continuous-variable quantum key distribution. *Entropy* **2019**, *21*, 652. [CrossRef]
38. Chai, G.; Cao, Z.; Liu, W.; Wang, S.; Huang, P.; Zeng, G. Parameter estimation of atmospheric continuous-variable quantum key distribution. *Phys. Rev. A* **2019**, *99*, 032326. [CrossRef]
39. Wang, X.; Zhang, Y.; Yu, S.; Guo, H. High efficiency postprocessing for continuous-variable quantum key distribution: Using all raw keys for parameter estimation and key extraction. *Quantum Inf. Process.* **2019**, *18*, 264. [CrossRef]
40. Zhong, H.; Ye, W.; Zuo, Z.; Huang, D.; Guo, Y. Kalman filter-enabled parameter estimation for simultaneous quantum key distribution and classical communication scheme over a satellite-mediated link. *Opt. Express* **2022**, *30*, 5981–6002. [CrossRef]
41. 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]
42. Lucamarini, M.; Patel, K.A.; Dynes, J.F.; Fröhlich, B.; Sharpe, A.W.; Dixon, A.R.; Yuan, Z.L.; Penty, R.V.; Shields, A.J. Efficient decoy-state quantum key distribution with quantified security. *Opt. Express* **2013**, *21*, 24550–24565. [CrossRef]
43. Pfister, C.; Lütkenhaus, N.; Wehner, S.; Coles, P.J. Sifting attacks in finite-size quantum key distribution. *New J. Phys.* **2016**, *18*, 053001. [CrossRef]
44. Lo, H.K.; Chau, H.; Ardehali, M. Efficient Quantum Key Distribution Scheme and a Proof of Its Unconditional Security. *J. Cryptol.* **2004**, *18*, 133–165. [CrossRef]
45. Li, Q.; Le, D.; Wu, X.; Niu, X.; Guo, H. Efficient Bit Sifting Scheme of Post-Processing in Quantum Key Distribution. *Quantum Inf. Process.* **2015**, *14*, 3785–3811. [CrossRef]
46. Qiong, L.; Dan, L.; Haokun, M.; Xiamu, N.; Tian, L.; Hong, G. Study on error reconciliation in quantum key distribution. *Quantum Info. Comput.* **2014**, *14*, 1117–1135.
47. Martinez-Mateo, J.; Pacher, C.; Peev, M.; Ciurana, A.; Martin, V. Demystifying the information reconciliation protocol cascade. *Quantum Inf. Comput.* **2015**, *15*, 453–477. [CrossRef]
48. Calver, T.; Grimaila, M.; Humphries, J. An empirical analysis of the cascade error reconciliation protocol for quantum key distribution. In Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research, Oak Ridge, TN, USA, 12–14 October 2011; 1p.
49. Li, M.; Patcharapong, T.; Zhang, C.M.; Yin, Z.Q.; Chen, W.; Han, Z.F. Efficient error estimation in quantum key distribution. *Chin. Phys. B* **2015**, *24*, 010302. [CrossRef]
50. Lu, Z.; Shi, J.H.; Li, F.G. Error rate estimation in quantum key distribution with finite resources. *Commun. Theor. Phys.* **2017**, *67*, 360. [CrossRef]
51. 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; IEEE: Piscataway, NJ, USA, 2014; pp. 351–355.
52. 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]
53. 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]

54. Bennett, C.H.; Bessette, F.; Brassard, G.; Salvail, L.; Smolin, J. Experimental quantum cryptography. *J. Cryptol.* **1992**, *5*, 3–28. [CrossRef]
55. Brassard, G.; Salvail, L. Secret-key reconciliation by public discussion. In Proceedings of the Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, 23–27 May 1993; Springer: Berlin/Heidelberg, Germany, 1993; pp. 410–423.
56. Lo, H.K. Method for decoupling error correction from privacy amplification. *New J. Phys.* **2003**, *5*, 36. [CrossRef]
57. Van Dijk, M.; Koppelaar, A. High rate reconciliation. In Proceedings of the IEEE International Symposium on Information Theory, Ulm, Germany, 29 June–4 July 1997; IEEE: Piscataway, NJ, USA, 1997; p. 92.
58. Sugimoto, T.; Yamazaki, K. A study on secret key reconciliation protocol. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **2000**, *83*, 1987–1991.
59. Liu, S.; Van Tilborg, H.C.; Van Dijk, M. A practical protocol for advantage distillation and information reconciliation. *Des. Codes Cryptogr.* **2003**, *30*, 39–62. [CrossRef]
60. Nakassis, A.; Bienfang, J.C.; Williams, C.J. Expeditious reconciliation for practical quantum key distribution. In Proceedings of the Quantum Information and Computation II. SPIE, Orlando, FL, USA, 12–16 April 2004; Volume 5436, pp. 28–35.
61. Yan, H.; Ren, T.; Peng, X.; Lin, X.; Jiang, W.; Liu, T.; Guo, H. Information reconciliation protocol in quantum key distribution system. In Proceedings of the 2008 Fourth International Conference on Natural Computation, Jinan, China, 18–20 October 2008; IEEE: Piscataway, NJ, USA, 2008; Volume 3, pp. 637–641.
62. Ma, W.; Zeng, G. An improvement on 'Cascade'protocol in quantum key distribution. *Acta Sin. Quantum Opt.* **2010**, *16*, 271–275.
63. Ii-Yung, R.N. A Probabilistic Analysis of Binary and Cascade. 2013. Available online: https://math.uchicago.edu/~may/REU2013/REUPapers/Ng.pdf (accessed on 2 April 2024).
64. Pacher, C.; Grabenweger, P.; Martinez-Mateo, J.; Martin, V. An information reconciliation protocol for secret-key agreement with small leakage. In Proceedings of the 2015 IEEE International Symposium on Information Theory (ISIT), Hong Kong, China, 14–19 June 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 730–734.
65. Pedersen, T.B.; Toyran, M. High performance information reconciliation for QKD with cascade. *Quantum Inf. Comput.* **2015**, *15*, 419–434. [CrossRef]
66. Hu, L.; Liu, H.; Lin, Y. Parameter optimization of cascade in quantum key distribution. *Optik* **2019**, *181*, 156–162. [CrossRef]
67. Mao, H.K.; Li, Q.; Hao, P.L.; Abd-El-Atty, B.; Iliyasu, A.M. High performance reconciliation for practical quantum key distribution systems. *Opt. Quantum Electron.* **2022**, *54*, 163. [CrossRef]
68. Buttler, W.T.; Lamoreaux, S.K.; Torgerson, J.R.; Nickel, G.; Donahue, C.; Peterson, C.G. Fast, efficient error reconciliation for quantum cryptography. *Phys. Rev. A* **2003**, *67*, 052303. [CrossRef]
69. Zhao, F.; Fu, M.; Wang, F.; Lu, Y.; Liao, C.; Liu, S. Error reconciliation for practical quantum cryptography. *Optik* **2007**, *118*, 502–506. [CrossRef]
70. Yan, H.; Peng, X.; Lin, X.; Jiang, W.; Liu, T.; Guo, H. Efficiency of winnow protocol in secret key reconciliation. In Proceedings of the 2009 WRI World Congress on Computer Science and Information Engineering, Los Angeles, CA, USA, 31 March–2 April 2009; IEEE: Piscataway, NJ, USA, 2009; Volume 3, pp. 238–242.
71. Cui, K.; Wang, J.; Zhang, H.F.; Luo, C.L.; Jin, G.; Chen, T.Y. A real-time design based on FPGA for expeditious error reconciliation in QKD system. *IEEE Trans. Inf. Forensics Secur.* **2012**, *8*, 184–190. [CrossRef]
72. Li, Q.; Wang, S.; Mao, H.; Han, Q.; Niu, X. An Adaptive Improved Winnow Algorithm. In Proceedings of the 2015 IEEE 39th Annual Computer Software and Applications Conference, Taichung, Taiwan, 1–5 July 2015; IEEE: Piscataway, NJ, USA, 2015; Volume 3, pp. 303–306.
73. Li, Q.; Yang, Z.; Mao, H.; Wang, X. Study on scrambling algorithms of error reconciliation in QKD. In Proceedings of the 2018 Eighth International Conference on Instrumentation & Measurement, Computer, Communication and Control (IMCCC), Harbin, China, 19–21 July 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1363–1367.
74. Cassagne, A.; Hartmann, O.; Leonardon, M.; He, K.; Leroux, C.; Tajan, R.; Aumage, O.; Barthou, D.; Tonnellier, T.; Pignoly, V.; et al. Aff3ct: A fast forward error correction toolbox! *SoftwareX* **2019**, *10*, 100345. [CrossRef]
75. Gallager, R. Low-density parity-check codes. *IRE Trans. Inf. Theory* **1962**, *8*, 21–28. [CrossRef]
76. MacKay, D.J. Good error-correcting codes based on very sparse matrices. *IEEE Trans. Inf. Theory* **1999**, *45*, 399–431. [CrossRef]
77. Ryan, W.; Lin, S. *Channel Codes: Classical and Modern*; Cambridge University Press: Cambridge, UK, 2009.
78. Pearson, D. High-speed QKD reconciliation using forward error correction. In Proceedings of the AIP Conference Proceedings, Glasgow, UK, 25–29 July 2004; American Institute of Physics: College Park, MD, USA, 2004; Volume 734, pp. 299–302.
79. Elkouss, D.; Leverrier, A.; Alléaume, R.; Boutros, J.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; IEEE: Piscataway, NJ, USA, 2009; pp. 1879–1883.
80. Elkouss, D.; Martinez-Mateo, J.; Martin, V. Information Reconciliation for Quantum Key Distribution. *Quantum Inf. Comput.* **2011**, *11*, 0226–0238.
81. Elkouss, D.; Martinez-Mateo, J.; Martin, V. Analysis of a rate-adaptive reconciliation protocol and the effect of leakage on the secret key rate. *Phys. Rev. A* **2013**, *87*, 042334. [CrossRef]
82. Elkouss, D.; Martinez-Mateo, J.; Martin, V. Untainted puncturing for irregular low-density parity-check codes. *IEEE Wirel. Commun. Lett.* **2012**, *1*, 585–588. [CrossRef]

83. Martinez-Mateo, J.; Elkouss, D.; Martin, V. Blind reconciliation. *Quantum Inf. Comput.* **2012**, *12*, 791–812. [CrossRef]
84. Kiktenko, E.O.; Trushechkin, A.S.; Lim, C.C.W.; Kurochkin, Y.V.; Fedorov, A.K. Symmetric blind information reconciliation for quantum key distribution. *Phys. Rev. Appl.* **2017**, *8*, 044017. [CrossRef]
85. Liu, Z.; Wu, Z.; Huang, A. Blind information reconciliation with variable step sizes for quantum key distribution. *Sci. Rep.* **2020**, *10*, 171. [CrossRef]
86. Mao, H.K.; Qiao, Y.C.; Li, Q. High-Efficient Syndrome-Based LDPC Reconciliation for Quantum Key Distribution. *Entropy* **2021**, *23*, 1440. [CrossRef] [PubMed]
87. Borisov, N.; Petrov, I.; Tayduganov, A. Asymmetric adaptive LDPC-based information reconciliation for industrial quantum key distribution. *Entropy* **2022**, *25*, 31. [CrossRef] [PubMed]
88. Dixon, A.; Sato, H. High speed and adaptable error correction for megabit/s rate quantum key distribution. *Sci. Rep.* **2014**, *4*, 7275. [CrossRef] [PubMed]
89. Mao, H.; Li, Q.; Han, Q.; Guo, H. High-throughput and low-cost LDPC reconciliation for quantum key distribution. *Quantum Inf. Process.* **2019**, *18*, 232. [CrossRef]
90. Guo, Y.; Gao, C.; Jiang, D.; Chen, L. 100 Mbps Reconciliation for Quantum Key Distribution Using a Single Graphics Processing Unit. *SN Comput. Sci.* **2021**, *2*, 125. [CrossRef]
91. Tanaka, A.; Fujiwara, M.; Yoshino, K.i.; Takahashi, S.; Nambu, Y.; Tomita, A.; Miki, S.; Yamashita, T.; Wang, Z.; Sasaki, M.; et al. High-speed quantum key distribution system for 1-Mbps real-time key generation. *IEEE J. Quantum Electron.* **2012**, *48*, 542–550. [CrossRef]
92. Constantin, J.; Houlmann, R.; Preyss, N.; Walenta, N.; Zbinden, H.; Junod, P.; Burg, A. An FPGA-Based 4 Mbps Secret Key Distillation Engine for Quantum Key Distribution Systems. *J. Signal Process. Syst.* **2017**, *86*, 1–15. [CrossRef]
93. Walenta, N.; Burg, A.; Caselunghe, D.; Constantin, J.; Gisin, N.; Guinnard, O.; Houlmann, R.; Junod, P.; Korzh, B.; Kulesza, N.; et al. A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing. *New J. Phys.* **2014**, *16*, 013047. [CrossRef]
94. Elkouss, D.; Martinez, J.; Lancho, D.; Martin, V. Rate compatible protocol for information reconciliation: An application to QKD. In Proceedings of the 2010 IEEE Information Theory Workshop on Information Theory (ITW 2010, Cairo), Cairo, Egypt, 6–8 January 2010; IEEE: Piscataway, NJ, USA, 2010; pp. 1–5.
95. Tarable, A.; Paganelli, R.P.; Ferrari, M. Rateless Protograph LDPC codes for Quantum Key Distribution. *IEEE Trans. Quantum Eng.* **2024**, *5*, 4100311. [CrossRef]
96. Arikan, E. Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels. *IEEE Trans. Inf. Theory* **2009**, *55*, 3051–3073. [CrossRef]
97. Jouguet, P.; Kunz-Jacques, S. High performance error correction for quantum key distribution using polar codes. *Quantum Inf. Comput.* **2014**, *14*, 329–338. [CrossRef]
98. Nakassis, A.; Mink, A. Polar codes in a QKD environment. In Proceedings of the Quantum Information and Computation XII. SPIE, Baltimore, MD, USA, 11–12 September 2014; Volume 9123, pp. 32–42.
99. Yan, S.; Wang, J.; Fang, J.; Jiang, L.; Wang, X. An Improved Polar Codes-Based Key Reconciliation for Practical Quantum Key Distribution. *Chin. J. Electron.* **2018**, *27*, 250–255. [CrossRef]
100. Lee, S.; Heo, J. Efficient reconciliation protocol with polar codes for quantum key distribution. In Proceedings of the 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN), Prague, Czech Republic, 3–6 July 2018; IEEE: Piscataway, NJ, USA, 2018, pp. 40–43.
101. Kiktenko, E.O.; Malyshev, A.O.; Fedorov, A.K. Blind information reconciliation with polar codes for quantum key distribution. *IEEE Commun. Lett.* **2020**, *25*, 79–83. [CrossRef]
102. Tang, B.Y.; Liu, B.; Yu, W.R.; Wu, C.Q. Shannon-limit approached information reconciliation for quantum key distribution. *Quantum Inf. Process.* **2021**, *20*, 113. [CrossRef]
103. Fang, J.; Yi, Z.; Li, J.; Liang, Z.; Wu, Y.; Lei, W.; Jiang, Z.L.; Wang, X. Improved polar-code-based efficient post-processing algorithm for quantum key distribution. *Sci. Rep.* **2022**, *12*, 10155. [CrossRef] [PubMed]
104. Zhou, H.; Tang, B.Y.; Li, S.C.; Yu, W.R.; Chen, H.; Yu, H.C.; Liu, B. Appending information reconciliation for quantum key distribution. *Phys. Rev. Appl.* **2022**, *18*, 044022. [CrossRef]
105. Tang, B.Y.; Wu, C.Q.; Peng, W.; Liu, B.; Yu, W.R. Polar-code-based information reconciliation scheme with the frozen-bit erasure strategy for quantum key distribution. *Phys. Rev. A* **2023**, *107*, 012612. [CrossRef]
106. Guo, J.; Tang, B.; Lai, T.; Liang, X.; Zhang, S.; Tian, Z.; Huang, J.; Yuan, X.; Yu, W.; Liu, B.; et al. The implementation of Shannon-limited polar codes-based information reconciliation for quantum key distribution. *Quantum Sci. Technol.* **2023**, *8*, 035011. [CrossRef]
107. Silberhorn, C.; Ralph, T.C.; Lütkenhaus, N.; Leuchs, G. Continuous variable quantum cryptography: Beating the 3 dB loss limit. *Phys. Rev. Lett.* **2002**, *89*, 167901. [CrossRef]
108. Grosshans, F.; Grangier, P. Reverse reconciliation protocols for quantum cryptography with continuous variables. *arXiv* **2002**, arXiv:quant-ph/0204127.
109. Van Assche, G.; Cardinal, J.; Cerf, N.J. Reconciliation of a quantum-distributed Gaussian key. *IEEE Trans. Inf. Theory* **2004**, *50*, 394–400. [CrossRef]

110. Bloch, M.; Thangaraj, A.; McLaughlin, S.W.; Merolla, J.M. LDPC-based Gaussian key reconciliation. In Proceedings of the 2006 IEEE Information Theory Workshop-ITW'06 Punta del Este, Punta del Este, Uruguay, 13–17 March 2006; IEEE: Piscataway, NJ, USA, 2006; pp. 116–120.
111. Lodewyck, J.; Bloch, M.; García-Patrón, R.; Fossier, S.; Karpov, E.; Diamanti, E.; Debuisschert, T.; Cerf, N.J.; Tualle-Brouri, R.; McLaughlin, S.W. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Phys. Rev. A* **2007**, *76*, 042305. [CrossRef]
112. Lu, Z.; Yu, L.; Li, K.; Liu, B.; Lin, J.; Jiao, R.; Yang, B. Reverse reconciliation for continuous variable quantum key distribution. *Sci. Chin. Phys. Mech. Astron.* **2010**, *53*, 100–105. [CrossRef]
113. Jouguet, P.; Elkouss, D.; Kunz-Jacques, S. High-bit-rate continuous-variable quantum key distribution. *Phys. Rev. A* **2014**, *90*, 042329. [CrossRef]
114. Qian, C.C.; Zhao, S.M.; Mao, Q.p. Reconciliation of continuous variable QKD using Gaussian post-selection and systematic polar code. In Proceedings of the 2016 8th International Conference on Wireless Communications & Signal Processing (WCSP), Yangzhou, China, 13–15 October 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1–4.
115. Pacher, C.; Martinez-Mateo, J.; Duhme, J.; Gehring, T.; Furrer, F. Information Reconciliation for Continuous-Variable Quantum Key Distribution using Non-Binary Low-Density Parity-Check Codes. *arXiv* **2016**, arXiv:1602.09140.
116. Bai, Z.; Wang, X.; Yang, S.; Li, Y. High-efficiency Gaussian key reconciliation in continuous variable quantum key distribution. *Sci. Chin. Phys. Mech. Astron.* **2016**, *59*, 614201. [CrossRef]
117. Bai, Z.; Yang, S.; Li, Y. High-efficiency reconciliation for continuous variable quantum key distribution. *Jpn. J. Appl. Phys.* **2017**, *56*, 044401. [CrossRef]
118. Yang, S.S.; Lu, Z.G.; Li, Y.M. High-Speed Post-Processing in Continuous-Variable Quantum Key Distribution Based on FPGA Implementation. *J. Light. Technol.* **2020**, *38*, 3935–3941. [CrossRef]
119. Mani, H.; Gehring, T.; Grabenweger, P.; Ömer, B.; Pacher, C.; Andersen, U.L. Multiedge-type low-density parity-check codes for continuous-variable quantum key distribution. *Phys. Rev. A* **2021**, *103*, 062419. [CrossRef]
120. Wen, X.; Li, Q.; Mao, H.; Wen, X.; Chen, N. An Improved Slice Reconciliation Protocol for Continuous-Variable Quantum Key Distribution. *Entropy* **2021**, *23*, 1317. [CrossRef]
121. Ai, X.; Malaney, R. Optimised Multithreaded CV-QKD Reconciliation for Global Quantum Networks. *IEEE Trans. Commun.* **2022**, *70*, 6122–6132. [CrossRef]
122. Wang, X.; Wang, H.; Zhou, C.; Chen, Z.; Yu, S.; Guo, H. Continuous-variable quantum key distribution with low-complexity information reconciliation. *Opt. Express* **2022**, *30*, 30455–30465. [CrossRef]
123. Yang, S.; Yan, Z.; Yang, H.; Lu, Q.; Lu, Z.; Cheng, L.; Miao, X.; Li, Y. Information reconciliation of continuous-variables quantum key distribution: Principles, implementations and applications. *EPJ Quantum Technol.* **2023**, *10*, 40. [CrossRef]
124. Richardson, T.; Urbanke, R. Multi-edge type LDPC codes. In Proceedings of the Workshop Honoring Proceeding Bob McEliece on His 60th Birthday, California Institute of Technology, Pasadena, CA, USA, 20 April 2004; pp. 24–25.
125. Shokrollahi, A. Raptor codes. *IEEE Trans. Inf. Theory* **2006**, *52*, 2551–2567. [CrossRef]
126. Perry, J.; Iannucci, P.A.; Fleming, K.E.; Balakrishnan, H.; Shah, D. Spinal codes. *ACM Sigcomm Comput. Commun. Rev.* **2012**, *42*, 49–60. [CrossRef]
127. Leverrier, A.; Alléaume, R.; Boutros, J.; Zémor, G.; Grangier, P. Multidimensional reconciliation for a continuous-variable quantum key distribution. *Phys. Rev. A* **2008**, *77*, 042325. [CrossRef]
128. Jouguet, P.; Kunz-Jacques, S.; Leverrier, A. Long-distance continuous-variable quantum key distribution with a Gaussian modulation. *Phys. Rev. A* **2011**, *84*, 062317. [CrossRef]
129. Lin, D.; Huang, D.; Huang, P.; Peng, J.; Zeng, G. High performance reconciliation for continuous-variable quantum key distribution with LDPC code. *Int. J. Quantum Inf.* **2015**, *13*, 1550010. [CrossRef]
130. Wang, X.; Zhang, Y.; Yu, S.; Xu, B.; Li, Z.; Guo, H. Efficient rate-adaptive reconciliation for continuous-variable quantum key distribution. *Quantum Inf. Comput.* **2017**, *17*, 1123–1134.
131. Jiang, X.Q.; Yang, S.; Huang, P.; Zeng, G. High-speed reconciliation for CVQKD based on spatially coupled LDPC codes. *IEEE Photonics J.* **2018**, *10*, 7600410. [CrossRef]
132. Wang, X.; Zhang, Y.; Yu, S.; Guo, H. High speed error correction for continuous-variable quantum key distribution with multi-edge type LDPC code. *Sci. Rep.* **2018**, *8*, 10543. [CrossRef]
133. Milicevic, M.; Feng, C.; Zhang, L.M.; Gulak, P.G. Quasi-cyclic multi-edge LDPC codes for long-distance quantum cryptography. *NPJ Quantum Inf.* **2018**, *4*, 21. [CrossRef]
134. Guo, Y.; Wang, K.; Huang, D.; Jiang, X. High efficiency continuous-variable quantum key distribution based on QC-LDPC codes. *Chin. Opt. Lett.* **2019**, *17*, 112701. [CrossRef]
135. Li, Q.; Wen, X.; Mao, H.; Wen, X. An improved multidimensional reconciliation algorithm for continuous-variable quantum key distribution. *Quantum Inf. Process.* **2019**, *18*, 25. [CrossRef]
136. Zhou, C.; Wang, X.; Zhang, Y.C.; Zhang, Z.; Yu, S.; Guo, H. Continuous-Variable Quantum Key Distribution with Rateless Reconciliation Protocol. *Phys. Rev. Appl.* **2019**, *12*, 054013. [CrossRef]
137. Li, Y.; Zhang, X.; Li, Y.; Xu, B.; Ma, L.; Yang, J.; Huang, W. High-throughput GPU layered decoder of quasi-cyclic multi-edge type low density parity check codes in continuous-variable quantum key distribution systems. *Sci. Rep.* **2020**, *10*. [CrossRef]

138. Shi, J.J.; Li, B.P.; Huang, D. Reconciliation for CV-QKD using globally-coupled LDPC codes. *Chin. Phys. B* **2020**, *29*. [CrossRef]
139. Wen, X.; Li, Q.; Mao, H.; Luo, Y.; Yan, B.; Huang, F. Novel reconciliation protocol based on spinal code for continuous-variable quantum key distribution. *Quantum Inf. Process.* **2020**, *19*, 350. [CrossRef]
140. Zhang, K.; Jiang, X.Q.; Feng, Y.; Qiu, R.; Bai, E. High efficiency continuous-variable quantum key distribution based on ATSC 3.0 LDPC codes. *Entropy* **2020**, *22*, 1087. [CrossRef] [PubMed]
141. Gumus, K.; Eriksson, T.A.; Takeoka, M.; Fujiwara, M.; Sasaki, M.; Schmalen, L.; Alvarado, A. A novel error correction protocol for continuous variable quantum key distribution. *Sci. Rep.* **2021**, *11*, 10465. [CrossRef]
142. Zhang, M.; Dou, Y.; Huang, Y.; Jiang, X.Q.; Feng, Y. Improved information reconciliation with systematic polar codes for continuous variable quantum key distribution. *Quantum Inf. Process.* **2021**, *20*, 327. [CrossRef]
143. Zhang, M.; Hai, H.; Feng, Y.; Jiang, X.Q. Rate-adaptive reconciliation with polar coding for continuous-variable quantum key distribution. *Quantum Inf. Process.* **2021**, *20*, 318. [CrossRef]
144. Zhou, C.; Wang, X.; Zhang, Z.; Yu, S.; Chen, Z.; Guo, H. Rate compatible reconciliation for continuous-variable quantum key distribution using Raptor-like LDPC codes. *Sci.-Chin.-Phys. Mech. Astron.* **2021**, *64*, 260311. [CrossRef]
145. Fan, X.; Niu, Q.; Zhao, T.; Guo, B. Rate-Compatible LDPC Codes for Continuous-Variable Quantum Key Distribution in Wide Range of SNRs Regime. *Entropy* **2022**, *24*, 1463. [CrossRef] [PubMed]
146. Jeong, S.; Jung, H.; Ha, J. Rate-compatible multi-edge type low-density parity-check code ensembles for continuous-variable quantum key distribution systems. *NPJ Quantum Inf.* **2022**, *8*, 6. [CrossRef]
147. Zhou, C.; Li, Y.; Ma, L.; Luo, Y.; Huang, W.; Yang, J.; Hu, J.; Zhang, L.; Zhang, S.; Xu, B. An efficient and high-speed two-stage decoding scheme for continuous-variable quantum key distribution system. In Proceedings of the Conference on Quantum and Nonlinear Optics IX, Online, 5–11 December 2022; Volume 12323. [CrossRef]
148. Cao, Z.; Chen, X.; Chai, G.; Liang, K.; Yuan, Y. Rate-Adaptive Polar-Coding-Based Reconciliation for Continuous-Variable Quantum Key Distribution at Low Signal-to-Noise Ratio. *Phys. Rev. Appl.* **2023**, *19*, 044023. [CrossRef]
149. Cao, Z.; Chen, X.; Chai, G.; Peng, J. IC-LDPC Polar codes-based reconciliation for continuous-variable quantum key distribution at low signal-to-noise ratio. *Laser Phys. Lett.* **2023**, *20*, 045201. [CrossRef]
150. Liu, J.; Guo, D.; Guo, T.; Li, X.; Wang, Y.; Meng, Y. Design of Data Reconciliation System Based on FPGA Heterogeneous Computing. *Acta Opt. Sin.* **2023**, *43*, 0227001. [CrossRef]
151. Wang, X.; Xu, M.; Zhao, Y.; Chen, Z.; Yu, S.; Guo, H. Non-Gaussian Reconciliation for Continuous-Variable Quantum Key Distribution. *Phys. Rev. Appl.* **2023**, *19*, 054084. [CrossRef]
152. Yang, S.; Yan, Z.; Lu, Q.; Yang, H.; Lu, Z.; Miao, X.; Li, Y. Hardware design and implementation of high-speed multidimensional reconciliation sender module in continuous-variable quantum key distribution. *Quantum Inf. Process.* **2023**, *22*, 362. [CrossRef]
153. Zhang, K.; Hou, J.; Jiang, X.Q.; Bai, E.; Huang, P.; Zeng, G. High-speed information reconciliation with syndrome-based early termination for continuous-variable quantum key distribution. *Opt. Express* **2023**, *31*, 34000–34010. [CrossRef] [PubMed]
154. Yang, H.; Liu, S.; Yang, S.; Lu, Z.; Li, Y.; Li, Y. High-efficiency rate-adaptive reconciliation in continuous-variable quantum key distribution. *Phys. Rev. A* **2024**, *109*, 012604. [CrossRef]
155. Jiang, X.Q.; Xue, S.; Tang, J.; Huang, P.; Zeng, G. Low-complexity adaptive reconciliation protocol for continuous-variable quantum key distribution. *Quantum Sci. Technol.* **2024**, *9*, 025008. [CrossRef]
156. Lütkenhaus, N. Estimates for practical quantum cryptography. *Phys. Rev. A* **1999**, *59*, 3301–3319. [CrossRef]
157. Hughes, R.J.; Nordholt, J.E.; Derkacs, D.; Peterson, C.G. Practical free-space quantum key distribution over 10 km in daylight and at night. *New J. Phys.* **2002**, *4*, 43. [CrossRef]
158. Marøy, ø.; Lydersen, L.; Gudmundsen, M.; Skaar, J. Error estimation, error correction and verification in quantum key distribution. *IET Inf. Secur.* **2014**, *8*, 277–282. [CrossRef]
159. Bennett, C.H.; Brassard, G.; Robert, J.M. Privacy amplification by public discussion. *SIAM J. Comput.* **1988**, *17*, 210–229. [CrossRef]
160. Bennett, C.H.; Brassard, G.; Crepeau, C.; Maurer, U.M. Generalized privacy amplification. *IEEE Int. Symp. Inf. Theory Proc.* **1994**, *41*, 350. [CrossRef]
161. Renner, R.; König, R. Universally composable privacy amplification against quantum adversaries. In Proceedings of the Theory of Cryptography Conference, Cambridge, MA, USA, 10–12 February 2005; Springer: Berlin/Heidelberg, Germany, 2005; pp. 407–425.
162. Nisan, N.; Zuckerman, D. More deterministic simulation in logspace. In Proceedings of the Twenty-Fifth Annual ACM Symposium on Theory of Computing, San Diego, CA, USA, 16–18 May 1993; pp. 235–244.
163. Impagliazzo, R.; Levin, L.A.; Luby, M. Pseudo-random generation from one-way functions. In Proceedings of the Twenty-First Annual ACM Symposium on Theory of Computing, Seattle, WA, USA, 14–17 May 1989; pp. 12–24.
164. Renner, R.; König, R. Universally composable privacy amplification against quantum adversaries. *Lect. Notes Comput. Sci.* **2005**, *3378*, 407–425. [CrossRef]
165. Tomamichel, M.; Schaffner, C.; Smith, A.; Renner, R. Leftover hashing against quantum side information. *IEEE Trans. Inf. Theory* **2011**, *57*, 5524–5535. [CrossRef]
166. Hayashi, M. Exponential decreasing rate of leaked information in universal random privacy amplification. *IEEE Trans. Inf. Theory* **2011**, *57*, 3989–4001. [CrossRef]

167. Fung, C.H.F.; Ma, X.; Chau, H.F.; Cai, Q.Y. Quantum key distribution with delayed privacy amplification and its application to the security proof of a two-way deterministic protocol. *Phys. Rev. At. Mol. Opt. Phys.* **2012**, *85*, 032308. [CrossRef]
168. Hayashi, M. Security Analysis of Almost Dual Universal-2 Hash Functions- Smoothing of Min Entropy versus Smoothing of Rényi Entropy of Order 2. *IEEE Trans. Inf. Theory* **2016**, *62*, 3451–3476. [CrossRef]
169. Hayashi, M.; Tsurumaru, T. More Efficient Privacy Amplification with Less Random Seeds via Dual Universal Hash Function. *IEEE Trans. Inf. Theory* **2016**, *62*, 2213–2232. [CrossRef]
170. Huang, Y.; Zhang, X.; Ma, X. Stream Privacy Amplification for Quantum Cryptography. *PRX Quantum* **2022**, *3*, 020353. [CrossRef]
171. Zhang, C.M.; Li, M.; Huang, J.Z.; Li, H.W.; Li, F.Y.; Wang, C.; Yin, Z.Q.; Chen, W.; Han, Z.F.; Treeviriyanupab, P.; et al. Fast implementation of length-adaptive privacy amplification in quantum key distribution. *Chin. Phys. B* **2014**, *23*, 090310. [CrossRef]
172. Liu, B.; Zhao, B.; Yu, W.; Wu, C. FiT-PA: Fixed scale FFT based privacy amplification algorithm for quantum key distribution. *J. Internet Technol.* **2016**, *17*, 309–320. [CrossRef]
173. Takahashi, R.; Tanizawa, Y.; Dixon, A.R. High-speed implementation of privacy amplification in quantum key distribution. In Proceedings of the 6th International Conference on Quantum Cryptography, Washington, DC, USA, 12–16 September 2016.
174. Li, D.; Huang, P.; Zhou, Y.; Li, Y.; Zeng, G. Memory-Saving Implementation of High-Speed Privacy Amplification Algorithm for Continuous-Variable Quantum Key Distribution. *IEEE Photonics J.* **2018**, *10*, 7600712. [CrossRef]
175. Tang, B.y.; Liu, B.; Zhai, Y.p.; Wu, C.q.; Yu, W.r. High-speed and Large-scale Privacy Amplification Scheme for Quantum Key Distribution. *Sci. Rep.* **2019**, *9*, 15733. [CrossRef]
176. Yan, B.; Li, Q.; Mao, H.; Xue, X. High-Speed Privacy Amplification Scheme Using GMP in Quantum Key Distribution. *IEEE Photonics J.* **2020**, *12*, 7600213. [CrossRef]
177. Bai, E.; Jiang, X.q.; Wu, Y. Memory-saving and high-speed privacy amplification algorithm using lfsr-based hash function for key generation. *Electronics* **2022**, *11*, 377. [CrossRef]
178. Lu, Y.; Bai, E.; Jiang, X.q.; Wu, Y. High-Speed Privacy Amplification Algorithm Using Cellular Automate in Quantum Key Distribution. *Electronics* **2022**, *11*, 2426. [CrossRef]
179. Zhang, H.f.; Wang, J.; Cui, K.; Luo, C.l.; Lin, S.z.; Zhou, L.; Liang, H.; Chen, T.Y.; Chen, K.; Pan, J.w. A Real-Time QKD System Based on FPGA. *J. Light. Technol.* **2012**, *30*, 3226–3234. [CrossRef]
180. Yang, S.s.; Bai, Z.l.; Wang, X.y.; Li, Y.M. FPGA-Based Implementation of Size-Adaptive Privacy Amplification in Quantum Key Distribution. *IEEE Photonics J.* **2017**, *9*, 7600308. [CrossRef]
181. Li, Q.; Yan, B.Z.; Mao, H.K.; Xue, X.F.; Han, Q.; Guo, H. High-Speed and Adaptive FPGA-Based Privacy Amplification in Quantum Key Distribution. *IEEE Access* **2019**, *7*, 21482–21490. [CrossRef]
182. Yan, B.; Li, Q.; Mao, H.; Chen, N. An efficient hybrid hash based privacy amplification algorithm for quantum key distribution. *Quantum Inf. Process.* **2022**, *21*, 130. [CrossRef]
183. Wang, X.; Zhang, Y.; Yu, S.; Guo, H. High-Speed Implementation of Length-Compatible Privacy Amplification in Continuous-Variable Quantum Key Distribution. *IEEE Photonics J.* **2018**, *10*, 7600309. [CrossRef]
184. Portmann, C. Key Recycling in Authentication. *IEEE Trans. Inf. Theory* **2014**, *60*, 4383–4396. [CrossRef]
185. Yang, Y.H.; Li, P.Y.; Ma, S.Z.; Qian, X.C.; Zhang, K.Y.; Wang, L.J.; Zhang, W.L.; Zhou, F.; Tang, S.B.; Wang, J.Y.; et al. All optical metropolitan quantum key distribution network with post-quantum cryptography authentication. *Opt. Express* **2021**, *29*, 25859. [CrossRef]
186. Gilbert, E.N.; Macwilliams, F.J.; Sloane, N.J.A. Codes which detect deception. *Bell Syst. Tech. J.* **1974**, *53*, 405–424. [CrossRef]
187. Wegman, M.N.; Carter, J. New hash functions and their use in authentication and set equality. *J. Comput. Syst. Sci.* **1981**, *22*, 265–279. [CrossRef]
188. Kiktenko, E.O.; Malyshev, A.O.; Gavreev, M.A.; Bozhedarov, A.A.; Pozhar, N.O.; Anufriev, M.N.; Fedorov, A.K. Lightweight Authentication for Quantum Key Distribution. *IEEE Trans. Inf. Theory* **2020**, *66*, 6354–6368. [CrossRef]
189. Stinson, D.R. Universal hashing and authentication codes. *Des. Codes Cryptogr.* **1991**, *4*, 369–380. [CrossRef]
190. Kabatiansky, G.A.; Smeets, B.J.M.; Johansson, T. On the cardinality of systematic authentication codes via error-correcting codes. *IEEE Trans. Inf. Theory* **1996**, *42*, 566–578. [CrossRef]
191. Nguyen, L.; Roscoe, A. *A New Bound for T-Wise almost Universal Hash Functions*; Technical Report RR-10-24; OUCL: London, UK, 2010.
192. Abidin, A.; Larsson, J.Å. New Universal Hash Functions. In *Research in Cryptology*; Springer: Berlin/Heidelberg, Germany, 2012; Volume NaN, pp. 99–108.
193. Rogaway, P. *Bucket Hashing and Its Application to Fast Message Authentication*; Springer: Berlin/Heidelberg, Germany, 1995; Volume 12. [CrossRef]
194. Stinson, D.R. On the Connections Between Universal Hashing, Combinatorial Designs and Error-Correcting Codes. *Electron. Colloquium Comput. Complex.* **1995**, *TR95*, 7–28.
195. Bibak, K.; Kapron, B.M.; Srinivasan, V. Authentication of variable length messages in quantum key distribution. *EPJ Quantum Technol.* **2022**, *9*, 8. [CrossRef] [PubMed]
196. Bibak, K. Quantum key distribution using universal hash functions over finite fields. *Quantum Inf. Process.* **2022**, *21*, 121. [CrossRef]

197. Bibak, K.; Ritchie, R. Quantum key distribution with PRF(Hash, Nonce) achieves everlasting security. *Quantum Inf. Process.* **2021**, *20*, 228. [CrossRef]
198. Krawczyk, H. LFSR-based Hashing and Authentication. In *Advances in Cryptology—CRYPTO '94*; Springer: Berlin/Heidelberg, Germany, 1994; Volume NaN, pp. 129–139.
199. Krawczyk, H. New Hash Functions For Message Authentication. In Proceedings of the EUROCRYPT, Saint-Malo, France, 21–25 May 1995.
200. den Boer, B. A Simple and Key-Economical Unconditional Authentication Scheme. *J. Comput. Secur.* **1993**, *2*, 65–72.
201. Bierbrauer, J.; Johansson, T.; Kabatianskii, G.; Smeets, B.J.M. On Families of Hash Functions via Geometric Codes and Concatenation. In Proceedings of the Advances in Cryptology—CRYPTO '93, 13th Annual International Cryptology Conference, Santa Barbara, CA, USA, 22–26 August 1993; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 1993; Volume 773, pp. 331–342. [CrossRef]
202. Abidin, A.; Larsson, J.Å. Direct proof of security of Wegman–Carter authentication with partially known key. *Quantum Inf. Process.* **2013**, *13*, 2155–2170. [CrossRef]
203. Cederlof, J.; Larsson, J.Å. Security Aspects of the Authentication Used in Quantum Cryptography. *IEEE Trans. Inf. Theory* **2008**, *54*, 1735–1741. [CrossRef]
204. Mehic, M.; Fazio, P.; Rass, S.; Maurhart, O.; Peev, M.; Poppe, A.; Rozhon, J.; Niemiec, M.; Voznak, M. A Novel Approach to Quality-of-Service Provisioning in Trusted Relay Quantum Key Distribution Networks. *IEEE/ACM Trans. Netw.* **2020**, *28*, 168–181. [CrossRef]
205. Wang, L.J.; Zhang, K.Y.; Wang, J.Y.; Cheng, J.; Yang, Y.H.; Tang, S.B.; Yan, D.; Tang, Y.L.; Liu, Z.; Yu, Y.; et al. Experimental authentication of quantum key distribution with post-quantum cryptography. *NPJ Quantum Inf.* **2021**, *7*, 67. [CrossRef]
206. Atici, M.; Stinson, D.R. Universal Hashing and Multiple Authentication. In Proceedings of the CRYPTO, Santa Barbara, CA, USA, 18–22 August 1996.
207. Abidin, A. On Security of Universal Hash Function Based Multiple Authentication. In *Information and Communications Security*; Springer: Berlin/Heidelberg, Germany, 2012; Volume NaN, pp. 303–310.
208. Li, Q.; Zhao, Q.; Le, D.; Niu, X. Study on the security of the authentication scheme with key recycling in QKD. *Quantum Inf. Process.* **2016**, *15*, 3815–3831. [CrossRef]
209. Molotkov, S.N. On the robustness of information-theoretic authentication in quantum cryptography. *Laser Phys. Lett.* **2022**, *19*, 075203. [CrossRef]
210. Luo, Y.; Mao, H.K.; Li, Q.; Chen, N. An Information-Theoretic Secure Group Authentication Scheme for Quantum Key Distribution Networks. *IEEE Trans. Commun.* **2023**, *71*, 5420–5431. [CrossRef]