entropy

IMPACT FACTOR 2.738

Indexed in: PubMed

CITESCORE 4.7

Article

Improving the Performance of Quantum Cryptography by Using the Encryption of the Error Correction Data

Valeria A. Pastushenko and Dmitry A. Kronberg

Special Issue

Quantum Information: From Fundamental Aspects to Practical Applications

Edited by

Dr. Aleksey Fedorov

MDPI

https://doi.org/10.3390/e25060956

entropy

MDPI

Article

Improving the Performance of Quantum Cryptography by Using the Encryption of the Error Correction Data

Valeria A. Pastushenko and Dmitry A. Kronberg *

Terra Quantum AG, Kronhausstrasse 25, 9000 St. Gallen, Switzerland; vp@terraquantum.swiss
* Correspondence: dk@terraquantum.swiss

Abstract: Security of quantum key distribution (QKD) protocols rely solely on quantum physics laws, namely, on the impossibility to distinguish between non-orthogonal quantum states with absolute certainty. Due to this, a potential eavesdropper cannot extract full information from the states stored in their quantum memory after an attack despite knowing all the information disclosed during classical post-processing stages of QKD. Here, we introduce the idea of encrypting classical communication related to error-correction in order to decrease the amount of information available to the eavesdropper and hence improve the performance of quantum key distribution protocols. We analyze the applicability of the method in the context of additional assumptions concerning the eavesdropper's quantum memory coherence time and discuss the similarity of our proposition and the quantum data locking (QDL) technique.

Keywords: quantum key distribution; quantum information; quantum superadditivity; quantum data locking

Citation: Pastushenko, V.A.; Kronberg, D.A. Improving the Performance of Quantum Cryptography by Using the Encryption of the Error Correction Data. *Entropy* **2023**, *25*, 956. https://doi.org/10.3390/e25060956

Academic Editor: Aleksey Fedorov

Received: 5 May 2023
Revised: 14 June 2023
Accepted: 15 June 2023
Published: 20 June 2023

1. Introduction

The main goal of quantum key distribution (QKD) [1–3] is to generate a secret key between two remote users (Alice and Bob), with the security of the key not based on computational assumptions on a potential eavesdropper (Eve). The first ever QKD protocol, BB84, was proposed by Bennett and Brassard [4]. In the protocol, the legitimate sender, Alice, encodes random bit string into polarization states of single photons and sends them to the legitimate receiver, Bob. For the encoding purposes, Alice randomly chooses one of two orthogonal polarization bases, while all the four states form a non-orthogonal set. Bob uses a random basis guess when conducting his measurement. The bit values corresponding to wrong guesses on Bob's side are discarded after a round of classical communication, which provides an advantage to the legitimate users.

The security of quantum key distribution is based on the indistiguishability of the states available to the eavesdropper. For QKD protocols, any eavesdropping attempt leads to a disturbance of the states at the receiver side, and the value of the disturbance in the observed parameters allows the legitimate users to estimate the quantum states of Eve and hence bound her information. When this information is below the information available to the legitimate users, they can use classical post-processing methods to distill a secret key.

Along with QKD, an adjacent technology of quantum data locking (QDL) is of interest. In the QDL scenario, a potential adversary does not have enough data to perform a correct measurement of the available quantum states, while the total extractable information may be relatively high. Hence, a relatively short amount of classical data can lock a large amount of information. The first QDL protocol was proposed in [5] and resembles BB84, as the same two bases are used. Now, there is a single pre-shared bit that specifies the basis choice for each bit of Alice's string and for Bob's measurement at every position. As was shown in [5], the eavesdropper who has intercepted N signals obtains no more than $N/2$ bits of information; hence, the single secret bit is sufficient for "locking" $N/2$ bits of classical information. Later, other QDL protocols based on different principles were introduced [6,7].

Here, we propose a method that can increase the secret key rate in QKD by simple additional actions of the legitimate users, namely the encryption of information that is disclosed during error correction. Encryption of the postprocessing data was also used in [8] to simplify the security proof, but here, we discuss its usage for a different purpose—for a QDL-like technique that does not allow an eavesdropper to perform the best possible measurement.

The paper is organized as follows. In Section 2, we recall the main stages of prepare-and-measure QKD protocols and discuss various types of eavesdropping attacks. Section 3 is devoted to the condition sufficient for quantum accessible information additivity and its application to QKD in a QDL scenario. Section 4 addresses the case of the most general eavesdropping attacks and the limitations of the method we propose. Finally, we discuss the results in Section 5.

2. Background

The detailed description of the stages for the typical QKD protocol can be found in reviews, see, e.g., [1,2]. Here, we focus on the four stages that are the most significant for our study:

1. The quantum states are sent via a quantum channel from Alice to Bob, with Bob performing an appropriate measurement. Then, the legitimate users utilize a classical authenticated channel to perform key sifting and/or basis reconciliation. After this procedure, Alice and Bob have correlated but not yet coinciding classical bit sequences also correlated with Eve.
2. The legitimate users estimate the intervention of Eve and the information available to her based on the data observed at the receiver's side. The most significant parameter is quantum bit error rate (QBER), but other parameters including the visibility, attenuation, or gain of different classes of states can be utilized as well [9–11]. The aforementioned estimate can be performed by disclosing a part of the signals, which is then removed from the key as it is not secret any more.
3. The legitimate users perform error correction, which provides them with coinciding keys correlated with Eve. Classical error correction codes [12] or the Cascade method [13] may be used. The legitimate users take into account that some secret data are disclosed during error correction. The disclosed data actually specify the set of codewords used by Alice, e.g., for linear codes, the syndrome specifies that "a string of Alice is the one that produces the following syndrome", while the check matrix of the linear code may be fixed for many communication sessions. The Cascade method uses the interactive exchange of parity bits, which also specify the set of possible bit sequences used by Alice.
4. Finally, the privacy amplification stage follows. This results in a shorter key with very low correlation with the eavesdropper. The length of the final key depends on the data observed by the legitimate users and, correspondingly, their estimate of Eve's and their own information. In addition, the security proof, i.e., the proof of the statement that the key obtained with this formula is secure according to the security parameter (see, e.g., [14,15]), is the main theoretical element for the QKD protocol.

The classical or quantum data available to the participants after each of these stages can be described by a quantum states in the joint Hilbert space of Alice–Bob–Eve, with classical states of Alice and Bob being diagonal density matrices in some fixed basis. The total state depends on the attack performed by the eavesdropper.

All the eavesdropping attacks on QKD protocols can be categorized into three nesting groups. The most general type of attack entails conducting a joint unitary transformation with ancilla on an arbitrary number of signal quantum states and subsequent collective measurement of the ancillary system. This sequence of actions conducted by an eavesdropper is called a coherent attack. If the eavesdropper is limited to conducting an individual unitary transformation with an ancilla of every signal state followed by a collective measurement of all the ancillary systems, then their intervention can be attributed to a narrower class of col-

lective attacks. Finally, each attack including only individual unitary transformations and individual measurements of ancillary systems belongs to the subset of individual attacks.

Full security analysis of any QKD protocol, i.e., proving its unconditional security, requires considering Eve to be able to perform any action allowed by the laws of quantum physics, i.e., operating in the set of coherent attacks. However, on the basis of the quantum version of the de Finetti representation theorem [16,17], it was shown that coherent attacks are not more powerful than collective ones and, thus, the considered set can be narrowed: the only condition required for the statement to be true is that a given QKD protocol is permutation-invariant, i.e., invariant under arbitrary permutations of quantum channel uses [18]. The condition can be satisfied for the majority of standard QKD protocols including BB84 [4], six-state [19], and B92 [20] by introducing an additional step to their structure: legitimate users should publicly agree on a random permutation of raw key bits right after the first stage [18,21].

The secret key generation rate of a QKD protocol is defined as the maximum speed (per bit) at which a secret key can be distributed—here, secret means that the eavesdropper's knowledge about it is asymptotically small. In the case of classical key distribution protocols, the secret key rate can be calculated according to the Sciszar and Korner's equation [22]:

$$\text{rate} = I(\mathrm{X},\mathrm{Y}) - I(\mathrm{X},\mathrm{Z}), \tag{1}$$

where I is mutual information between two classical systems (X, Y, and Z stand for the random variable describing Alice's, Bob's, and Eve's systems, respectively): $I(\mathrm{X}_1,\mathrm{X}_2) = H(\mathrm{X}_1) + H(\mathrm{X}_2) - H(\mathrm{X}_1\mathrm{X}_2)$, with H being the Shannon entropy of a random variable. The legitimate users are to estimate the range of attacks that can be feasibly conducted by Eve (using the assumptions concerning her computational powers) and use the value of mutual information $I(\mathrm{X},\mathrm{Z})$ for the most effective one. The expression (1) should be implemented in the case of direct reconciliation—when Alice's bit string is considered to be correct and Bob has to amend his string. Although, the equation can be easily modified for the case of reverse reconciliation, which corresponds to Alice and Bob changing roles and thus leads to switching X and Y in the equation.

Transitioning into the quantum cryptography framework implies that legitimate users no longer use any assumptions related to the eavesdropper's computational powers; they rely only on the laws of quantum mechanics in order to determine the range of attacks that could have been conducted. They have to determine the set Γ of all quantum states ρ_{AB} that can be shared between them according to the set of observed data. For each state ρ_{AB} describing the system shared between Alice and Bob, ρ_{ABE} is defined as its arbitrary purification and includes Eve. Then, after the measurements conducted on Bob's and Alice's ends combined with the reconciliation procedure, the final state ρ_{XYE} describes the system shared between Alice, Bob, and Eve right after stage 1 (conditioned on the conclusive result, i.e., when the position survived key sifting):

$$\rho_{\mathrm{XYE}} = \sum_{x,y} p_{xy} \left|x\right\rangle \left\langle x\right|_{\mathrm{A}} \otimes \left|y\right\rangle \left\langle y\right|_{\mathrm{B}} \otimes \rho_{\mathrm{E}}^{xy}.$$

where p_{xy} is the joint probability of Alice sending classical value x and Bob obtaining the result y; $\left|x\right\rangle_{\mathrm{A}}$ and $\left|y\right\rangle_{\mathrm{B}}$ denote the classical states of the legitimate user's systems corresponding to the values. Then, Eve's ensemble $\mathcal{E}_{\mathrm{E}} = \{(p_x, \rho_x)\}_x$ of quantum states ρ_x corresponding to different bit values on Alice's side reads

$$\mathcal{E}_{\mathrm{E}} = \left\{ \left(p_x \equiv \sum_y p_{xy},\ \rho_x \equiv \sum_y p_{xy} \cdot \rho_{\mathrm{E}}^{xy} \right) \right\}_x.$$

This knowledge is sufficient to upper bound the information available to Eve. The Holevo bound [23] can be used for the purpose, as the Holevo quantity $\chi(\mathcal{E}_{\mathrm{E}}) = S(\sum_x p_x \rho_x) -$

$\sum_x p_x S(\rho_x)$, where $S(\rho) = \mathrm{Tr}\rho \log_2 \rho$ is the von Neumann entropy, upper bounds the accessible information

$$I_{\mathrm{acc}}(\mathcal{E}_{\mathrm{E}}) = \sup_{\mathcal{M}_{\mathrm{Z}\leftarrow\mathrm{E}}} I(\mathrm{X},\mathrm{Z}),$$

which can be extracted from the ensemble $\mathcal{E}_{\mathrm{E}}$ by performing the most optimal of all the quantum measurements $\mathcal{M}_{\mathrm{Z}\leftarrow\mathrm{E}}$ on the system E. The estimation allows transitioning from the classical Equation (1) to the equation lower-bounding the secret key rate in QKD:

$$\text{rate} \geq \inf_{\rho_{\mathrm{AB}}\in\Gamma} \Big(I(\mathrm{X}:\mathrm{Y}) - \chi(\mathcal{E}_{\mathrm{E}}) \Big), \tag{2}$$

which is the content for the seminal Devetak–Winter result [24]. Here, we described the intuition behind this result based on Sciszar and Korner classical equation, while a complete proof of (2) is much more complex.

3. The Method Description

We use Theorem 2 in [25], bounding the accessible information in new conditions, which we want to achieve in quantum cryptography by simple actions of the legitimate users.

Let us briefly describe this result of [25]. The above-mentioned theorem provides a sufficient condition for the additivity of accessible information, which is the independent use of all the states' combinations. To put it in formal terms: if a multipartite ensemble of quantum states $\mathcal{E}^N = \{\xi_i^N, \rho_i^N\}_i$ has a product form, i.e., if $\xi_i^N = \xi_{i_i}^{(1)} \cdot \ldots \cdot \xi_{i_N}^{(N)}$ and $\rho_i^N = \rho_{i_1}^{(1)} \otimes \ldots \otimes \rho_{i_N}^{(N)}$, the quantum accessible information of the ensemble is additive:

$$I_{\mathrm{acc}}\Big(\mathcal{E}^N\Big) = I_{\mathrm{acc}}\Big(\mathcal{E}^{(1)}\Big) + \ldots + I_{\mathrm{acc}}\Big(\mathcal{E}^{(N)}\Big), \tag{3}$$

where $\mathcal{E}^{(n)} = \big\{\big(\xi_{i_n}^{(n)}, \rho_{i_n}^{(n)}\big)\big\}_{i_n}$ is the nth partial ensemble describing the nth system. Thus, for such product-form ensembles, collective measurements do not provide any advantage over a sequence of independent individual measurements in terms of extracted information.

If a given QKD protocol is permutation-invariant, the set of considered eavesdropping attacks can be narrowed to collective ones. Thus, after N channel uses, Eve's ensemble $\mathcal{E}_E^N$ satisfies the conditions of this theorem: the states of the ensemble have product form, as well as the states' probabilities, which are distributed according to the initial probability distribution on the Alice side, as Alice sends the states independently in each position. Hence, if Eve performs the measurement at this time, the mutual information between the result of Eve's measurement (contained in a classical system E) and the classical value sent by Alice (system X) is bounded by additive accessible information:

$$I^N(\mathrm{X},\mathrm{E}) \leq I_{\mathrm{acc}}\Big(\mathcal{E}_{\mathrm{E}}^N\Big) = N I_{\mathrm{acc}}(\mathcal{E}_{\mathrm{E}}). \tag{4}$$

Now, observe that when Alice and Bob perform the error correction step, they change the probability distribution, as they disclose the set of possible codewords, and the new probabilities do not have the product form. Hence, the estimate (4) do not hold any longer, and Eve's information may overcome $N I_{\mathrm{acc}}(\mathcal{E}_{\mathrm{E}})$. This is the subject of the quantum coding theorem [26,27]: if the sender and the receiver have fixed the set of the codewords, then the receiver may perform a collective measurement which allows the Holevo capacity to be achieved. The result of [25] therefore states that without coding (i.e., without a non-trivial subset of all the possible bit strings to be the codewords), the users cannot achieve any superadditive information, let alone the Holevo capacity. Within our framework, this means that Eve, who plays the role of the receiver now, does not get the amount of information characterized by the Holevo quantity and is limited by a more strict bound. Hence, using the Holevo capacity as the estimate for Eve's information becomes too pessimistic.

Disclosing additional information may be regarded as implementing the QDL protocol between Alice and Eve, who are now in the conditions of quantum coding theorem. Here, as it happens in QDL, Eve cannot perform the proper measurement without additional information but can do so after obtaining it, namely, after knowing the set of codewords to perform a collective measurement (see Section 4 in [6]).

Our idea is that the legitimate users should not change the probabilities of the states available to the eavesdropper. They can avoid doing this by encrypting the information disclosed during error correction. When Eve gets no additional information, she is restricted by (3), and her information obtained with the best possible measurement is still below $NI_{\mathrm{acc}}(\mathcal{E}_{\mathrm{E}})$.

A potential problem may appear due to the information disclosure taking place during privacy amplification procedure, since it makes Eve's states statistically dependent, and thus her ensemble $\mathcal{E}_{\mathrm{E}}^{N}$ loses product form—see Section 4 for detail. However, in the case when Eve is forced to measure the obtained quantum states before the legitimate users begin privacy amplification routine, the method works well. Instead of disclosing the $H(\mathrm{X}|\mathrm{Y})$ bits during the error correction stage, the legitimate users would consume a part of the pre-distributed key in order to encrypt the classical communication using the one-time pad. Here, $H(\mathrm{X}|\mathrm{Y}) = H(\mathrm{XY}) - H(\mathrm{Y})$ is the conditional entropy, which characterizes the lack of knowledge about X when the full information about Y is provided [28]. At the same time, after Eve's measurement, when all the participants operate with classical data, the legitimate users are able to substitute the value $\chi(\mathcal{E}_{\mathrm{E}})$ in the Devetak–Winter equation with $I_{\mathrm{acc}}(\mathcal{E}_{\mathrm{E}})$, thus obtaining a higher key generation rate without compromising the security of the whole scheme:

$$\text{rate} \geq \inf_{\rho_{\mathrm{AB}} \in \Gamma} \Big(I(\mathrm{X}:\mathrm{Y}) - I_{\mathrm{acc}}(\mathcal{E}_{\mathrm{E}}) \Big). \tag{5}$$

Recall that the set Γ includes all the bipartite states that can be shared between the legitimate users based on the statistics of their measurement results. Let us emphasize that no hardware modification is required for this secret key rate boost.

In order to force Eve to measure her states at an early stage and use the bound (4), legitimate users can employ some additional assumptions concerning Eve's technical abilities. The assumption about the upper-bound on the eavesdropper's quantum memory decoherence time is a natural one typically utilized in a quantum data locking scenario as well as in a QKD scenario with a restricted Eve. This allows us to benefit from postponing the privacy amplification for an amount of time sufficient for the eavesdropper's quantum memory to lose coherence or from encrypting all the classical communication necessary for the stage with an asymmetrical cipher such as AES. In the latter case, the legitimate users are to assume that Eve cannot break a chosen encryption during her quantum memory coherence time. The tactic allows legitimate users to assume that an eavesdropper is to conduct the measurement without any additional knowledge associated with the information from privacy amplification.

In this scenario, the size of Eve's quantum memory is not limited, and her ability to conduct collective measurements is not restricted as well—this significantly distinguishes the approach we propose from the bounded quantum storage model (BQSM), which is built on the assumption concerning the maximal number of quantum states that an eavesdropper can keep in their quantum memory [2,29,30]. Nevertheless, our approach makes collective attacks no more efficient than individual ones and thus eliminates the necessity to consider any eavesdropping relying on quantum memory capable of storing more than one quantum state at a time. Moreover, Eve may know all the information concerning bit reconciliation and post-selection procedures, as the availability of the data does not destroy the statistical independence of separate signal states.

Thus, we propose a modification of the initial scheme presented in Section 2: the first two stages may remain unchanged, while the subsequent stages are modified in the following way:

3′. Alice and Bob perform error correction in a standard manner, with the only difference that now they utilize a private channel for the purpose, i.e., all the communication conducted at this stage is encoded by one-time pad cipher using the pre-distributed key. Thus, they deprive Eve of any information concerning codewords choice.

4′. The legitimate users perform privacy amplification with some delay sufficient for Eve's quantum memory to lose coherence or encrypt all the communication necessary for the privacy amplification stage (in contrast to the previous step, an asymmetrical cipher such as AES is to be utilized). The compression ratio depends on the legitimate users' assumptions concerning Eve. If the decoherence time of her quantum memory is considered to be limited by some finite value, then privacy amplification goes according to Equation (5) up to a minor value of the extra key needed for symmetric encryption.

Notably, the method relies on using a pre-distributed secret key for encoding a part of classical communication. However, this does not change the common QKD paradigm, as any quantum key distribution protocols begin with an authenticating classical channel using a relatively short initial key (for this reason, key distribution protocols have an alternative name: "key expansion protocols"). Our approach leads to the necessity of a longer initial key for the very first round of key distribution, while no data on the raw key are disclosed during the error correction stage, in contrast with the conventional scenario. The key for encoding classical communication in each subsequent round is to be taken from the secret string distributed in the preceding one.

The scheme works well in an asymptotic case, when the size of the distributed key is large enough and post-processing procedures are asymptotically efficient. However, in practice, the difficulties related to the finiteness of the key length lead us to the paradigm of ε-secure data exchange [14,31]. Additional difficulties appear when a part of the generated secret key is utilized in the following round of communication, resulting in the overall security slightly degrading with the number of rounds. It worth noting that within our framework, the security level decreases more quickly than in conventional QKD schemes, since we propose using larger amounts of the previously distributed key for the next round. Thus, an accurate analysis of our method beyond the asymptotic case is a perspective and important area for future research.

In summary, the modified scheme involves encrypting classical communication (during error correction and privacy amplification stages) and leaving a part of generated key for the next round. Combined with the assumption concerning the upper bound on the decoherence time of Eve's quantum memory, this allows the legitimate users to come to classical signals analysis and the equation analogous to the result of Sciszar and Korner (1), where Eve's information is bounded according to (5) operating with restricted accessible information (4).

4. Beyond Memory-Restricted Scenario

If Eve is not forced to conduct her measurements right after the error-correction stage, it is more beneficial for her to measure the states later—when she will be able to take into account the information disclosed during the privacy amplification procedure. In this case, an observable that was optimal when measuring the original states can become non-optimal for measuring the states after information processing. In [32], an explicit example was provided, which shows that the strategy yields gain for Eve, i.e., that classical processing of states of a quantum ensemble changes the set of observables providing accessible information.

The example is based on considering a quantum ensemble $\mathcal{E}_{\text{init}}$ obtained as the result of a simple two-letter classical-quantum channel utilized twice (the lower index "init" indicated that the ensemble is obtained before the classical information processing).

$$\mathcal{E}_{\text{init}} = \left\{ \left(\frac{1}{4}, \sigma_0 \otimes \sigma_0 \right), \left(\frac{1}{4}, \sigma_0 \otimes \sigma_1 \right), \left(\frac{1}{4}, \sigma_1 \otimes \sigma_0 \right), \left(\frac{1}{4}, \sigma_1 \otimes \sigma_1 \right) \right\},$$

where the equiprobable letter states (described by density operators on two-dimensional Hilbert space $\mathcal{H}$) σ_0 and σ_1 are pure and can be represented as real vectors in some orthonormal basis $\{|0\rangle, |1\rangle\} \subset \mathcal{H}$:

$$\forall x \in \{0,1\}: \ \sigma_x = |\psi_x\rangle \langle\psi_x|, \quad |\psi_x\rangle = \cos\alpha|0\rangle + (-1)^x \sin\alpha|1\rangle.$$

According to [25], an optimal strategy for extracting the maximal amount of information from the quantum ensemble $\mathcal{E}_{\text{init}}$ consists in conducting two independent local measurements (measurements in the Hadamard basis). Then, a simple classical data processing corresponding to an XOR operation can be considered. It merges some states and transforms $\mathcal{E}_{\text{init}}$ into an ensemble

$$\mathcal{E} = \left\{ \left(\frac{1}{2}, \frac{1}{2}\sigma_0 \otimes \sigma_0 + \frac{1}{2}\sigma_1 \otimes \sigma_1 \right), \left(\frac{1}{2}, \frac{1}{2}\sigma_0 \otimes \sigma_1 + \frac{1}{2}\sigma_1 \otimes \sigma_0 \right) \right\}.$$

It was shown in [32] that there exists such a range of α values for which it is true that any observable providing $I_{\text{acc}}(\mathcal{E})$ has to include entangled operators. Moreover, the measurement in the Bell basis is always the optimal measurement strategy for $\mathcal{E}$. Thus, classical information processing can significantly change the structure of the optimal observable. However, the question of the existence of classical data processing operations preserving an optimal observable remains, to our knowledge, open.

Privacy amplification in QKD is an important special case of classical data processing. In particular, the considered XOR operation can be an element of some universal hash functions family used for privacy amplification. This explains the significance of the example in the context of our study: it proves that there exist privacy amplification procedures turning the disclosure of privacy amplification-related information into QDL-type communication between legitimate users and an eavesdropper.

Notably, if the opposite statement was true and any observable that was optimal before classical data processing remained optimal after the operation, then it would not have been important whether an eavesdropper conducted their measurement before or after obtaining privacy amplification-related information (this would not influence the efficiency of their attack). In this *imaginary* situation, we could have constructed a statement about our method's applicability while leaving privacy amplification data exchange completely unencrypted.

To our knowledge, the problem of determining an exact upper bound on the information available to Eve conducting her measurement after the privacy amplification stage remains open due to the difficulty of calculating the accessible information for an ensemble of states of a high-dimensional space [33]. At the moment, this fact limits the applicability of the proposed method in the case of no assumptions made about the eavesdropper's quantum memory storage time. Nevertheless, future research may discover ways of calculating the value that are sufficiently easy to be practically implemented. Currently, it is known that the above-mentioned value is upper bounded by the Holevo quantity and lower bounded by additive accessible information (which is much easier to calculate than the exact value of information available to Eve due to a significantly lower dimensionality of the problem)—in both cases, we are to take the influence of the privacy amplification into account, i.e., to subtract the corresponding number of bits as if we worked with classical data.

Note that in contrast to the case of error-correction data encryption, using the one-time pad for encrypting communication related to the privacy amplification procedure would not necessarily guarantee a gain in the secret key generation rate, as it consumes a relatively large additional amount of the pre-distributed key because of the large number of hash functions in the family, e.g., a large bit string is needed to specify the Toeplitz matrix [34].

5. Discussion

In this paper, we proposed a method of increasing secret key distribution rates in the existing QKD protocols by encrypting classical communication or delaying it in the case of restrictions imposed on the eavesdropper's quantum memory coherence time. Notably, it is universal (its applicability does depend on the specific protocol; despite the fact that in this work we consider only prepare-and-measure protocols, the method can be applied to entanglement-based QKD as well) and can be implemented just by modifying existing post-processing routines without introducing any changes to the hardware part of QKD realization.

Under the assumption of limited coherence time of the eavesdropper's quantum memory, the method allows us to show that collective attacks become no more effective than individual ones. If for a given QKD protocol coherent eavesdropping strategies have no advantage over collective, then individual attacks are the only ones to consider, and the key rate formula can be modified to operate with additive quantum accessible information.

Without any assumptions concerning the technical abilities of a potential eavesdropper, the key rate formula can be modified as well. However, in such a case, the new bound for superadditive accessible information is still, to our knowledge, an open question. Thus, we emphasize that the paper does not claim to provide a full security proof for QKD protocols in case of the method being implemented.

Note that the method inherits the disadvantages of quantum data locking: the disclosure of one bit of classical information that is meant to be secret (in this case, it is data related to error correction and privacy amplification procedures) may lead to an eavesdropper obtaining more than one bit of additional information. This leads to increased demands on the safekeeping of the classical data. Thus, the method does not provide composable security [31] against an eavesdropper who has access to unbounded quantum resources. Nevertheless, the method provides everlasting security [35] in a narrow sense: if an eavesdropper does not have access to quantum memory with storage time being sufficiently long at the moment of performing an attack (if the legitimate users have strong arguments in favor of this assumption), then no future advances in quantum memory can make an already distributed key less secure.

Author Contributions: Conceptualization, V.A.P. and D.A.K.; Investigation, V.A.P. and D.A.K.; Writing—original draft, V.A.P.; Writing—review & editing, V.A.P. and D.A.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

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.

Acknowledgments: D.A.K. is grateful to E.O. Kiktenko, A.S. Trushechkin, and A.S. Holevo for useful discussions.

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

Abbreviations

The following abbreviations are used in this manuscript:

AES	Advanced encryption standard
BQSM	Bounded quantum storage model
QBER	Quantum bit error rate
QDL	Quantum data locking
QKD	Quantum key distribution

References

1. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145–195. [CrossRef]
2. 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. Photonics* **2020**, *12*, 1012–1236. [CrossRef]
3. Liu, R.; Rozenman, G.G.; Kundu, N.K.; Chandra, D.; De, D. Towards the industrialisation of quantum key distribution in communication networks: A short survey. *IET Quantum Commun.* **2022**, *3*, 151–163. [CrossRef]
4. Bennett, C.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **1984**, *560*, 175–179. [CrossRef]
5. DiVincenzo, D.P.; Horodecki, M.; Leung, D.W.; Smolin, J.A.; Terhal, B.M. Locking classical correlations in quantum states. *Phys. Rev. Lett.* **2004**, *92*, 067902. [CrossRef]
6. Boixo, S.; Aolita, L.; Cavalcanti, D.; Modi, K.; Winter, A. Quantum locking of classical correlations and quantum discord of classical-quantum states. *Int. J. Quantum Inf.* **2011**, *9*, 1643–1651. [CrossRef]
7. Lupo, C.; Wilde, M.M.; Lloyd, S. Robust quantum data locking from phase modulation. *Phys. Rev. A* **2014**, *90*, 022326. [CrossRef]
8. Koashi, M.; Preskill, J. Secure quantum key distribution with an uncharacterized source. *Phys. Rev. Lett.* **2003**, *90*, 057902. [CrossRef]
9. Lo, H.K.; Ma, X.; Chen, K. Decoy State Quantum Key Distribution. *Phys. Rev. Lett.* **2005**, *94*, 230504. [CrossRef]
10. Ma, X.; Qi, B.; Zhao, Y.; Lo, H.K. Practical decoy state for quantum key distribution. *Phys. Rev. A* **2005**, *72*, 012326. [CrossRef]
11. Stucki, D.; Brunner, N.; Gisin, N.; Scarani, V.; Zbinden, H. Fast and simple one-way quantum key distribution. *Appl. Phys. Lett.* **2005**, *87*, 194108. [CrossRef]
12. 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. A* **2017**, *8*, 044017. [CrossRef]
13. Brassard, G.; Salvail, L. Secret-key reconciliation by public discussion. In Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques, Wollongong, NSW, Australia, 28 November–1 December 1994.
14. Trushechkin, A.S. On the operational meaning and practical aspects of using the security parameter in quantum key distribution. *Quantum Electron.* **2020**, *50*, 426–439. [CrossRef]
15. Sun, S.; Huang, A. A review of security evaluation of practical quantum key distribution system. *Entropy* **2022**, *24*, 260. [CrossRef]
16. Hudson, R.L.; Moody, G.R. Locally normal symmetric states and an analogue of de Finetti's theorem. *Z. Wahrscheinlichkeitstheorie Verwandte Geb.* **1976**, *33*, 343–351. [CrossRef]
17. Caves, C.M.; Fuchs, C.A.; Schack, R. Unknown quantum states: The quantum de Finetti representation. *J. Math. Phys.* **2002**, *43*, 4537–4559. [CrossRef]
18. Renner, R. Security of Quantum Key Distribution. Ph.D. Thesis, ETH Zurich, Zurich, Switzerland , 2005. Available online: http://arxiv.org/abs/quant-ph/0512258 (accessed on 8 April 2023).
19. Bechmann-Pasquinucci, H.; Gisin, N. Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography. *Phys. Rev. A* **1999**, *59*, 4238–4248. [CrossRef]
20. Bennett, C.H. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* **1992**, *68*, 3121–3124. [CrossRef]
21. Renner, R.; Gisin, N.; Kraus, B. Information-theoretic security proof for quantum-key-distribution protocols. *Phys. Rev. A* **2005**, *72*, 012332. [CrossRef]
22. Csiszár, I.; Körner, J. *Information Theory: Coding Theorems for Discrete Memoryless Systems*; Cambridge University Press: Cambridge, UK, 2011.
23. Holevo, A.S. Bounds for the quantity of information transmitted by a quantum communication channel. *Probl. Peredachi Inf.* **1973**, *9*, 3–11.
24. Devetak, I.; Winter, A. Distillation of secret key and entanglement from quantum states. *Proc. R. Soc. A* **2005**, *461*, 207–235. [CrossRef]
25. Sasaki, M.; Kato, K.; Izutsu, M.; Hirota, O. Quantum channels showing superadditivity in classical capacity. *Phys. Rev. A* **1998**, *58*, 146–158. [CrossRef]
26. Holevo, A.S. The capacity of the quantum channel with general signal states. *IEEE Trans. Inf. Theory* **1998**, *44*, 269–273. [CrossRef]
27. Schumacher, B.; Westmoreland, M.D. Sending classical information via noisy quantum channels. *Phys. Rev. A* **1997**, *56*, 131–138. [CrossRef]
28. Cover, T.M.; Thomas, J.A. Wiley Series in Telecommunications and Signal Processing. In *Elements of Information Theory*; Wiley-Interscience: Hoboken, NJ, USA, 2006.
29. Pironio, S.; Masanes, L.; Leverrier, A.; Acín, A. Security of device-independent quantum key distribution in the bounded-quantum-storage model. *Phys. Rev. X* **2013**, *3*, 031007. [CrossRef]
30. Damgård, I.; Fehr, S.; Salvail, L.; Schaffner, C. Cryptography in the bounded quantum-storage model. *SIAM J. Comput.* **2008**, *37*, 1865–1890. [CrossRef]
31. Portmann, C.; Renner, R. Security in quantum cryptography. *Rev. Mod. Phys.* **2022**, *94*, 025008. [CrossRef]
32. Pastushenko, V.A.; Kronberg, D.A. On classical data processing which affects additivity of quantum accessible information. *Lobachevskii J. Math.* **2023**, *44*, 2157–2165.
33. Suzuki, J.; Assad, S.M.; Englert, B.G. Accessible information about quantum states: An open optimization problem. In *Mathematics of Quantum Computation and Quantum Technology*; Chapman and Hall/CRC: Boca Raton, FL, USA, 2007; pp. 327–366.

34. Kiktenko, E.; Trushechkin, A.; Kurochkin, Y.; Fedorov, A. Post-processing procedure for industrial quantum key distribution systems. In *Journal of Physics: Conference Series, Proceedings of the 3rd International School and Conference on Optoelectronics, Photonics, Engineering and Nanostructures (Saint Petersburg OPEN 2016), St. Petersburg, Russia, 28–30 March 2016* ; IOP Publishing: Bristol, UK, 2016; Volume 741, p. 012081.
35. Renner, R.; Wolf, R. Quantum advantage in cryptography. *AIAA J.* **2023**, *61*, 1895–1910. [CrossRef]