cryptography

MDPI

Article

Boosting Quantum Key Distribution via the End-to-End Loss Control

Aleksei D. Kodukhov †, Valeria A. Pastushenko †, Nikita S. Kirsanov, Dmitry A. Kronberg, Markus Pflitsch and Valerii M. Vinokur *

Terra Quantum AG, Kornhausstrasse 25, 9000 St. Gallen, Switzerland
* Correspondence: vv@terraquantum.swiss
† These authors contributed equally to this work.

Abstract: With the rise of quantum technologies, data security increasingly relies on quantum cryptography and its most notable application, quantum key distribution (QKD). Yet, current technological limitations, in particular, the unavailability of quantum repeaters, cause relatively low key distribution rates in practical QKD implementations. Here, we demonstrate a remarkable improvement in the QKD performance using end-to-end line tomography for the wide class of relevant protocols. Our approach is based on the real-time detection of interventions in the transmission channel, enabling an adaptive response that modifies the QKD setup and post-processing parameters, leading, thereby, to a substantial increase in the key distribution rates. Our findings provide everlastingly secure efficient quantum cryptography deployment potentially overcoming the repeaterless rate-distance limit.

Keywords: quantum key distribution; optical fiber; Rayleigh scattering; loss control; transmittometry; optical time-domain reflectometry; line tomography; privacy amplification

check for updates

Citation: Kodukhov, A.D.; Pastushenko, V.A.; Kirsanov, N.S.; Kronberg, D.A.; Pflitsch, M.; Vinokur, V.M. Boosting Quantum Key Distribution via the End-to-End Loss Control. *Cryptography* **2023**, *7*, 38. https://doi.org/10.3390/cryptography7030038

Academic Editor: Josef Pieprzyk

Received: 2 June 2023
Revised: 25 July 2023
Accepted: 31 July 2023
Published: 2 August 2023

1. Introduction

As we step towards the quantum computing era, quantum cryptography is emerging as the primary solution for ensuring data security. A cornerstone of quantum cryptography is quantum key distribution (QKD). This technique harnesses unique quantum properties, such as the no-cloning property of quantum states and quantum entanglement, to securely share encryption keys between two or more parties. Paired with the symmetric classical cryptography routines, the QKD becomes a silver bullet against the security threats posed by quantum computers. Yet, deploying the QKD in the real world meets strong challenges. While the QKD protocols, such as BB84, boast theoretical security, their practical implementations face a wide range of challenges. in particular, the practical realization of quantum transmission channels is marred by substantial signal losses, and it is assumed that an eavesdropper, Eve, can seize and manipulate these losses to her advantage. Here, we show how physical control over the channel losses can ward off the known attacks targeted at exploiting those losses against the existing prepare-and-measure QKD protocols, in particular, Decoy-State BB84 [1–5] and COW [6–8]. Furthermore, we find how this physical loss control can be used to overcome the fundamental PLOB (Pirandola-Laurenza-Ottaviani-Banchi) bound [9]. This boundary predicts an exponential decrease in key rates in correspondence with increasing communication distance, posing a significant limitation to long-distance secure quantum communications.

Our approach shifts the conventional quantum cryptography paradigm, which assumes that an eavesdropper, Eve, can capture and exploit all losses occurring in the transmission channel. We state that during the transmission along the optical fiber, most of the signal losses occur due to scattering on the fiber density fluctuations in the channel and that it is practically impossible to collect these scattered losses. Thus, by complementing quantum mechanical restriction imposed on a potential eavesdropper with realistic restrictions stemming from the development of technology, we narrow the class of attacks that

have to be considered down to attacks utilizing deliberate local interventions. Moreover, relying on the end-to-end loss control method proposed in [10], legitimate users can detect these local intrusions. Remarkably, we find that our approach enables legitimate users to employ higher signal intensities and radically improves key distribution rates.

We demonstrate the high quantum cryptography potential that can be realized utilizing the physical end-to-end control without making strong assumptions about the eavesdropper's capabilities. These assumptions will be explored in depth in Sections 2 and 3. Section 4 describes the scheme utilized in Sections 5 and 6 for analyzing the influence of the proposed method on BB84 and COW QKD protocols, respectively. Section 7 provides the comparison of the proposed loss control technique with the conventional decoy-state approach, Section 8 touches upon the limitations of our approach and, finally, Section 9 presents our conclusions.

2. Eavesdropping of Natural Losses

Most of the QKD realizations leverage telecom equipment and employ optical fiber as a transmission channel. The losses in the fiber channel stem predominantly from the Rayleigh scattering, caused by homogeneously distributed quenched disorder. Building on Quantum Thermodynamics considerations, see Ref. [10], we argue that these *natural* losses cannot be effectively harvested by Eve. We carry out an illustrative analysis, the results of which show that efficient eavesdropping of natural losses would require the length of the collection apparatus that is impossible to practically realize at the present level of technology.

In the most QKD protocols, the classical information is encoded via the parameters of the coherent states. We thus set that the bits 0 and 1 are encoded by the coherent states $|\gamma_0\rangle$ and $|\gamma_1\rangle$, respectively. Let us consider a fiber channel segment of the length l. In the absence of local leakages, the fraction of the signal scattered at this segment is given by

$$r_l = 1 - 10^{-\xi l}, \tag{1}$$

where $\xi = 0.02\,\mathrm{km}^{-1}$ is the attenuation constant typical for fiber. Then, in order to obtain information, Eve has to be able to distinguish between the equiprobable effective lost components $|\sqrt{r_l}\gamma_0\rangle$ and $|\sqrt{r_l}\gamma_1\rangle$. The maximum amount of information I_l that can be extracted from these states is upper-bounded by the fundamental Holevo quantity χ [11], which in this case can be written as

$$I_l \leq \chi = h_2\left(\frac{1 - |\langle\sqrt{r_l}\gamma_0|\sqrt{r_l}\gamma_1\rangle|}{2}\right), \tag{2}$$

where $h_2(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is binary entropy.

When considering protocols that utilize phase-randomized coherent states, such as practical realizations of BB84, where information is carried by polarization, we assume that Eve acquires a bit each time when a non-zero count of photons is retrieved from the scattered signal. Thus, the average information associated with the bit is defined by the Poisson statistics

$$I_l \leq 1 - e^{-r_l|\gamma|^2}, \tag{3}$$

where $|\gamma|^2$ is the average photon number in each signal pulse regardless of the encoded bit value.

Figure 1 depicts the information leakage, attributable to Rayleigh scattering, as a function of l. Three curves correspond to distinct types of protocols, differing by the physical parameters selected for information encoding, the intensity, phase, and polarization. We find that to gain a considerable informational advantage over the legitimate users, Eve would need to cover a line segment exceeding a hundred meters. This condition makes an undetectable attack utilizing the natural losses unfeasible.

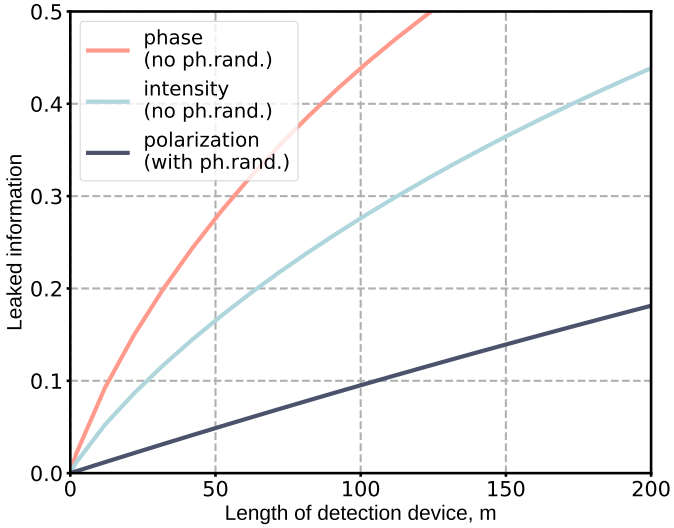

Figure 1. Information leaking from natural losses. The amount of information per pulse that Eve can obtain from natural losses as a function of the overall length of the detection device. The coral line depicts the information estimated according to Equation (2) for a protocol utilizing the following encoding scheme: "0"→ $|\gamma\rangle\,|\gamma\rangle$, "1"→ $|\gamma\rangle\,|-\gamma\rangle$, which resembles DPS protocol. The cyan line corresponds to the case of COW protocol: "0"→ $|0\rangle\,|\gamma\rangle$, "1"→ $|\gamma\rangle\,|0\rangle$ — the estimation was also conducted according to Equation (2). The dark blue line depicts the estimation Equation (3) built for the encoding into polarizations of phase-randomized coherent states of amplitude γ, i.e., for BB84 protocol. For all encoding methods, the average number of photons $|\gamma|^2 = 100$ that appeared to be optimal for bit-encoding states in the context of our approach (see Figures A1 and A2).

Notably, in the case of the bit-encoding states with equal energies, like polarization or phase encoding methods, the provided upper bounds are significantly higher than the amount of information that can be practically extracted. In principle, a potential eavesdropper may measure the losses from each scattering center individually. However, the resulting precision will be completely obscured by the quantum noise, and the obtained information will be much smaller than information estimations of Equations (2) and (3). Thus, a collective measurement unifying, for efficacy, all occurring losses into one narrow wave packet with the amplitude $\sqrt{r_l}\gamma_{0,1}$ is necessary for approaching the upper bounds. This problem is comparable, in its complexity, with reversing the evolution of a scattered wavefront [12–15].

3. Line Tomography

The line tomography as a constituent part of the key distribution process was originally proposed and thoroughly discussed in Ref. [10]. In this section, we briefly outline its basis and discuss its inalienable components. In our approach, losses other than natural are monitored through line tomography. By accurately quantifying the exploitable leakages, users precisely identify the amount of information potentially intercepted by Eve. This knowledge enables them to execute the most efficient privacy amplification procedure, thus, enhancing key distribution rates. Furthermore, it allows Alice and Bob to appropriately modify the parameters of the bit-encoding quantum states, making them less discernible to Eve, which, as we will show later, boosts the key rates even further.

Line tomography involves two distinct procedures: Optical Time-Domain Reflectometry (OTDR) and transmittometry, both of which contribute to a comprehensive knowledge of the losses in the line. Each component utilizes high-intensity test pulses which are dispatched at high frequencies, running concurrently with the bit-encoding states.

The OTDR is based on recording backscattered optical radiation from test pulses that travel through the fiber. The distance to a particular scattering point is calculated by measuring the time delay of its arrival, while the intensity of the backscattered signal

provides information about the magnitude of any detected leakage. Figure 2 sketches an exemplary reflectogram (upper trace) and the corresponding loss tomogram (lower trace). The tomogram is derived from the reflectogram by fitting it with a combination of a linear decline function, representing natural losses (keep in mind that the reflectogram is a semi-log plot), and weighted step-like functions. The tomogram maps the discrete derivative values of the step-like functions to the respective positions, thus pinpointing the local leakages. To achieve the loss detection accuracy of 0.5% and better test pulses must comprise about 10^{11} photons, while the time duration of a pulse is about 1 µs and wavelength λ is 1530 nm.

At the same time, transmittometry detects the transmitted components of the test pulses, enabling a cross-comparison of input and output intensities between the users. Although this method does not allow users to identify the exact locations of local leakages, it does provide the total leakage value r_{E}, calculated using the a priori known baseline of natural losses. Transmittometry can be further enhanced by modulating test pulses at high frequencies, similar to what is used in the lock-in technique. The test pulses' modulation is primarily needed to suppress the $1/f$ low-frequency noise of the laser emission. Analyzing the peaks of input and output spectral power corresponding to the modulation frequency ($\sim$MGz) allows users to calculate the lost proportion of the light. The $1/f$ noise is effectively suppressed, which enhances the accuracy of transmittometry. The fiber structure and hence line tomogram are physically unclonable functions [16]. Thus, global actions by Eve, such as substituting the line with a lossless channel or completely blocking certain signals, can be readily detected due to their significant impact on the line tomogram. We discuss this issue in detail in [10,16]. Consequently, these drastic Eve's actions would not provide an efficient method to interfere, since in case of these actions, the key generation will be immediately terminated by the legitimate users. Therefore, Eve's interventions are limited to creating minor local leakages which, however, are accurately measured by users and, correspondingly, are taken into account. Note that Eve is not able to selectively skip the high-intensity test pulses while being able to seize the low-intensity signal pulses, since physical detection of intensity requires her direct installation of splitters into the line. This would induce significant losses and significantly affect the reflectorgram of the line for a tangible period of time detectable by transmitometry. Moreover, measuring signal intensities causes time delays in the signal transmission from Alice to Bob which is also noticeable.

The primary constraint of the approach pertains to the accuracy of the loss control. Reflectometers are characterized by their resolution, which enables the localization of line discontinuities and the documentation of silica structure. If the resolution is not sufficient, the reflectogram, serving as an unclonable physical fingerprint of the line, would not enable registering some of the very localized anomalies in the line. Accumulating sufficient data to construct a meaningful reflectogram can also be time-intensive. Transmittometry provides an immediate update of the total effective loss magnitude, even before the reflectogram is fully constructed. Yet, its precision is restricted by line noises that need to be mitigated. Another limitation emerges when local line losses exceed a certain threshold at any point. In such cases, the transmission must be paused and the line inspected. This level of loss can indicate the potential installation of an interception equipment by Eve.

It is important to note that before starting the key generation process, Alice and Bob perform line tomography to determine the natural losses in the channel. Only at this preliminary step, the legitimate users must be certain that Eve does not introduce additional losses in the line. Eve may also exploit some of the predetermined leakages in the line, e.g., losses at connectors or fiber bends. For a particular line, such leakages have to be taken into account and added to the total leakage r_{E}.

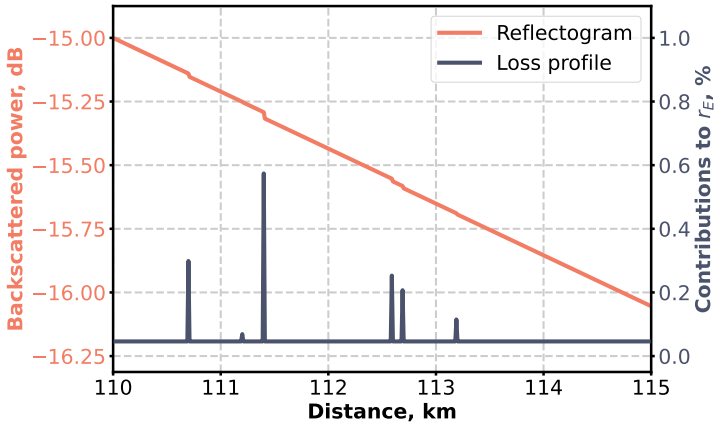

Figure 2. Exemplary reflectogram and line tomogram. The loss profile, which displays the magnitude of the *i*-th local leakage and its position, is derived from the reflectogram.

4. Analysis Scheme

Line tomography can be applied to a wide range of the QKD protocols and enable legitimate users to optimize the parameters of the bit-encoding states and post-processing and, thus, to significantly enhance the key rate, all while maintaining the same security threshold. Modified intensities of the bit-encoding pulses depend on the loss detection accuracy and may reach 10^2 photons per pulse (see Figures A1 and A2 for details). However, the specifics of each protocol do affect how the improved key rates are calculated. Depending on whether the protocol incorporates randomization of the bit-encoding states' phases [17–20] or not, the prepare-and-measure QKD protocols can be divided into two categories.

The first category includes protocols that employ quantum systems having a finite Hilbert space, specifically, qubits. In the ideal scenario, these protocols would use single photons for encoding. Despite the latest achievements in single photon sources for QKD, e.g., based on quantum dots [21], the weak phase-randomized coherent states are often utilized in the practical realization of these protocols, since they are more available and easier to exploit. The well-known examples of protocols of this group include the Decoy-State BB84 [1–5,22,23], Six-State [24], T-12 [25,26], and SARG04 [27]. One of the most powerful attacks on these protocols is the photon number splitting (PNS) attack [5,27–29] which allows Eve to collect surplus photons from the multiphoton pulses and forward the rest photons to Bob via a lossless channel. This attack provides an upper bound for the secret key rate, which, remarkably, together with the optimal single-photon attack, turns out to be the lower bound for the Decoy-state BB84 [5].

The second category includes protocols that encode information using pure coherent states and do not involve phase randomization. Protocols that fall under this category include Coherent One-Way protocols [6–8,30], early versions of the Differential Phase Shift protocols [31,32], Strong Reference B92 protocols [33–35] and Y-00 protocols [36,37]. The full security proof includes analysis of a general coherent attack, but to upper-bound the key generation rate in these protocols, we may consider the beam-splitting (BS) attack [38–40], in which Eve steals the portion of the signal expected to be lost in the line and then retransmits the remaining part to Bob through an ideal channel.

In the following analysis, we deal with the influence of the loss control approach on two distinct protocols: the Decoy-State BB84 and Coherent One-Way protocols, each exemplary of one of the two identified groups. The approach used in these protocols enables legitimate users to separate artificial losses from natural ones and, thus, precisely estimate the information available to Eve. This refined estimation results in a less destructive reduction of the key length during the privacy amplification stage (compared to the original versions of the protocols). We show that the improvement of privacy amplification in itself leads to a boost in the key generation rates for the considered protocols. Moreover, loss control allows legitimate users to utilize higher intensities of the signal states. We analyze

the influence of the intensities increase on the key generation rate and show that it leads to additional enhancement without sacrificing the everlasting security of the resulting key (see Section 8).

For the modified versions of the protocols, we primarily focus on the most feasible type of attack, the local leakage modeled by the beam-splitter. Given that photons are chargeless, the only practicable method for an eavesdropper to interact with the transmitted signal is the altering the fiber medium. Consequently, any attack strategies that deviate from local leakage attacks would necessitate significant changes to the line tomogram. Such alterations would trigger the protocols to cease operations, assuming that the resolution of the line tomography is sufficient to enable users to detect and pinpoint any modifications to the fiber medium.

5. The BB84 Protocol

We begin our analysis with the Decoy-State BB84, an exemplary QKD protocol using phase randomization. Our objective is to determine the achievable key rates, first in the presence, and then in the absence of the line tomography. In this protocol, Alice encodes random bits utilizing four distinctive quantum states. These states constitute two sets of mutually unbiased orthonormal basises, namely the eigenbasis of the Pauli matrices, σ_x and σ_z. The first set, X, consists of the $|0\rangle_x$ and $|1\rangle_x$ states; the second set, Z, contains $|0\rangle_z = (|0\rangle_x + |1\rangle_x)/\sqrt{2}$ and $|1\rangle_z = (|0\rangle_x - |1\rangle_x)/\sqrt{2}$ states. Bob receives each state, guesses the basis with the 50% success rate, and measures the states accordingly. Once all measurements are completed, Alice discloses the correct basises, leading the users to discard any bit positions where the guessed and actual basises do not align. The remaining bit sequence undergoes post-processing to correct errors and eliminate the leaked information. A visual layout of the protocol is depicted in Figure 3a.

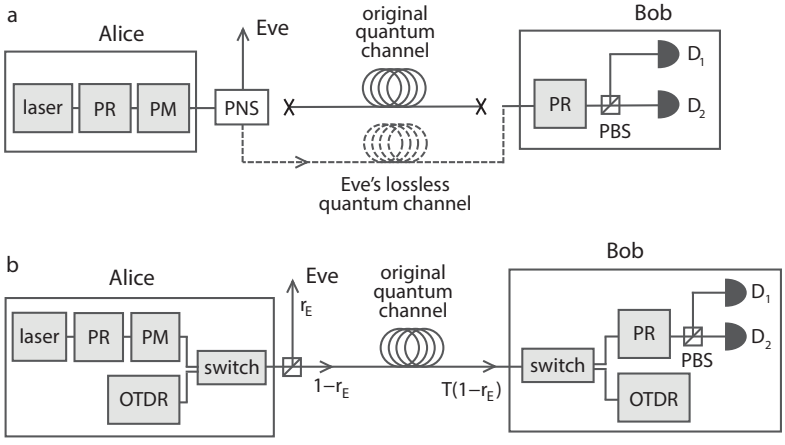

Figure 3. The BB84 protocol scheme. (**a**), An original BB84 protocol. Alice prepares a signal or a decoy state by utilizing the amplitude modulator (AM) and uses the polarization rotator (PR) to encode the information into the signal states. Phase modulator (PM) randomizes the output states. Bob chooses the basis by the PR and measures the arriving states by using the polarizing beam-splitter (PBS) and single-photon detectors D_1, D_2. Eve performs the PNS (photon number-splitting) attack. (**b**), The enhanced BB84. Alice and Bob exploit the optical time-domain reflectometer (OTDR) to monitor losses in the line. The switch element defines the working regime: generating a key or monitoring the line. Eve introduces local intervention and intercepts the portion r_E of the signal.

Initially, the BB84 protocol was designed to be implemented via single-photon states [1]. The security of such a realization was strictly proven [41–43], yet, practical implementation of a single-photon generator is the highly demanding engineering task and, in practice, phase randomized weak coherent states are utilized as information carriers instead of single-photon pulses [44–46]. Due to phase randomization, a mixed state $\hat{\rho}$, a statistical

mixture of the Fock photon-number states, is sent each time instead of the pure coherent state $|\gamma\rangle$,

$$\hat{\rho} = \frac{1}{2\pi}\int_0^{2\pi} d\varphi\, |\gamma e^{i\varphi}\rangle\langle\gamma e^{i\varphi}| = \sum_{n=0}^{\infty} P_\gamma(n)\,|n\rangle\langle n|\,, \tag{4}$$

where $|n\rangle$ is the n-photon Fock state and $P_\gamma(n) = e^{-|\gamma|^2}|\gamma|^{2n}/n!$ is the Poisson distribution [29].

Thus, with the probability $P_\gamma(0)$, Alice sends a vacuum state to the optical line. With the probability $P_\gamma(1)$, she sends a single-photon state and with the probability $1 - P_\gamma(0) - P_\gamma(1)$, she sends a multi-photon state. The presence of the multi-photon pulses allows Eve to perform the photon-number splitting (PNS) attack which involves replacing the original quantum channel with an ideal, lossless one and performing the non-demolition photon-number measurement [18,28,29]. Eve collects one photon from each of the multi-photon pulses and stores the obtained photons in quantum memory until the basis reconciliation stage. In order to compensate for the additional losses created during the PNS attack, Eve is to send the remaining photons to Bob via an ideal channel. The condition $\langle 0_x|1_x\rangle = \langle 0_z|1_z\rangle = 0$ enables Eve to distinguish between the logical bits '0' and '1' without a mistake by carrying out the measurement over kept photon in an appropriate basis. Hence, only single-photon pulses emitted by Alice's laser guarantee secure key distribution. In order to estimate the contribution to the raw key provided by the single-photon pulses, legitimate users have to implement the decoy-state method [3–5] which involves sending the additional pulses differing in intensities from the signal ones and analyzing their parameters at the receiver's side.

5.1. Secret Key Rate in Modified BB84

Adopting the proposed method based on the losses monitoring in the BB84 protocol, we build up the efficiency of the protocol, since Eve's attacks get restricted to inflicting local artificial losses that are not disruptive enough to be noticed by the line tomography. An eavesdropper may store intercepted photons until basis reconciliation and apply optimal measurement to obtain full information about a bit. Thus, whenever at least one photon is intercepted, Eve knows the bit value of the raw key:

$$I(\mathrm{A,E}) = \sum_{n=1}^{+\infty} P_{\sqrt{r_\mathrm{E}}\gamma}(n) = 1 - P_{\sqrt{r_\mathrm{E}}\gamma}(0) = 1 - e^{-r_\mathrm{E}|\gamma|^2}, \tag{5}$$

where r_E is the portion of the signal that Eve may seize imperceptibly. In case of obtaining the conclusive result, receiving a non-zero number of photons, and correctly guessing Alice's basis choice, Bob obtains full information about the bit value as well. If D_AB is the distance between Alice and Bob, the transmittance of the whole optical line is determined as $T = 10^{-\xi D_\mathrm{AB}}$, $\xi = 0.02\,\mathrm{km}^{-1}$. Thus, the probability of the conclusive result is

$$p_\checkmark = \frac{1}{2}\left(1 - P_{\sqrt{T(1-r_\mathrm{E})}\gamma}(0)\right) = \frac{1}{2}\left(1 - e^{-T(1-r_\mathrm{E})|\gamma|^2}\right). \tag{6}$$

In such a case, Bob's information about Alice's raw key, i.e., about the bit string Alice obtains after the post-selection stage, is $I(\mathrm{A,B}) = 1 - (h_2(p^x_\mathrm{err}) - h_2(p^z_\mathrm{err}))/2$, where p^x_err and p^z_err is error probabilities in the bases x and z respectively. The analysis of errors' influence is provided in Appendix C. Applying the Devetak-Winter equation [47], we explicitly calculate the final key generation rate L_f for the modified version of the protocol

$$\begin{aligned} L_f &\geq Lp_\checkmark \cdot \Big(I(\mathrm{A,B}) - I(\mathrm{A,E})\Big) \\ &= \frac{L}{2}\cdot\left(1 - \frac{1}{2}h_2(p^x_\mathrm{err}) - \frac{1}{2}h_2(p^z_\mathrm{err}) - e^{-T(1-r_\mathrm{E})|\gamma|^2}\right)\cdot e^{-r_\mathrm{E}|\gamma|^2}, \end{aligned} \tag{7}$$

where L is the rate at which Alice's random number generator produces bits. This key generation rate estimation can be optimized over signal intensity $|\gamma|^2$. Optimal intensity for Equation (7) is depicted in Figure A1 of Appendix A.

5.2. Comparison with Standard Decoy-State BB84

For the unmodified version of the Decoy-State BB84 protocol, we provide the upper bound on the secret key generation rate, see Appendix B for details,

$$L_f^{\text{orig}} \leq L \cdot \frac{1}{2}\left[T|\gamma|^2 e^{-|\gamma|^2} - \left(1 - e^{-T|\gamma|^2}\right)\frac{1}{2}\left(h_2(p_{\text{err}}^x) + h_2(p_{\text{err}}^z)\right)\right]. \tag{8}$$

Figure 4 shows the dependence of the key rate on the distance between legitimate users D_{AB} for original and modified versions of the BB84. Precise estimation of Eve's information, which our method provides, enables legitimate users to exploit signal pulses with dozens of photons (see Figure A1). At a distance of 200 km with today's reflectometers one may reach the detection accuracy of 0.5% and enhance the performance of the protocol by about 100 times. Even in the pessimistic case of the detection accuracy, $r_{\text{E}} = 0.10$, one can boost the key generation rate several times. Also, Alice and Bob may monitor the losses and not tune the average photon number in the signal pulses. In this case, legitimate users, modifying only privacy amplification (dashed lines at Figure 4), increase the key generation rate more than 2 times. In comparison, the asymptotic behavior of the key rate provided by the PLOB at a 200 km distance is limited to values around 10^{-4}, which is the order of magnitude lower than the rates achievable with the appropriate level of leakage detection accuracy. To conclude, a significant boost can be achieved without modifying the QKD equipment, one only needs to monitor the losses in the line and carry out more rational privacy amplification. It makes the QKD protocols available for a wide range of users at the present time.

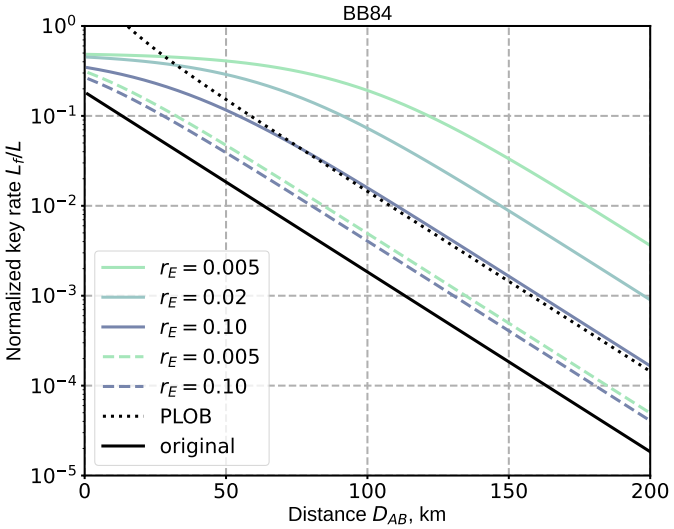

Figure 4. The BB84, secret key rate. The key generation rate as a function of the transmission distance D_{AB} for enhanced Equation (7) and original Equation (8) versions of the BB84 protocol. Different values of the leakage detection accuracy r_{E} are considered: 0.005, 0.01, 0.10. Solid lines stand for key rates of the enhanced version of the protocol for which the intensity maximizes Equation (7). Optimal signal intensity $|\gamma|^2$ varies from 4 to 200 photons per pulse for the enhanced protocol (see Figure A1). Dashed lines stand for the key rates in the case when the loss control approach is applied, but the intensity is not optimized and is taken the same as in the original version of the protocol. The dotted line corresponds to the PLOB bound. Here, the errors in both bases are taken to be zero: $p_{\text{err}}^x = p_{\text{err}}^z = 0$.

6. Coherent One-Way Protocol

In the COW protocol, see Figure 5a, Alice utilizes an attenuated laser and prepares coherent states with the intensity $|\gamma|^2$ to encode a random bit string into two-pulse sequences composed of the non-empty and empty pulses, $0 \to |0\rangle\,|\gamma\rangle$, $1 \to |\gamma\rangle\,|0\rangle$. Through the optical fiber, prepared states are sent to Bob, who measures them by single photon detector D_B. The detector monitors the pulses' arrival time, according to which Bob makes bit decisions. Since the coherent and vacuum states are non-orthogonal, the detector D_B sometimes does not click on the non-empty pulses. Bob considers such measurement results as inconclusive and discards them at the post-selection stage.

Bob's scheme also includes the interferometer, the long arm of which has the length assuring that the two non-empty neighboring pulses interfere at the last beam-splitter (see Figure 5a). Thus, the detector D_{M2} does not react to the arriving pulse sequence of the form $|\gamma\rangle\,|\gamma\rangle$, contained in the sequence corresponding to logical bits "01" ($|0\rangle\,|\gamma\rangle\,|\gamma\rangle\,|0\rangle$). If an eavesdropper blocks a part of such a sequence, the visibility between detectors D_{M2} and D_{M1} will inevitably change. As a result, the attacks that include blocking a part of transmitted pulses in the original scenario of the COW can be potentially detected by sending the control states $|\gamma\rangle\,|\gamma\rangle$.

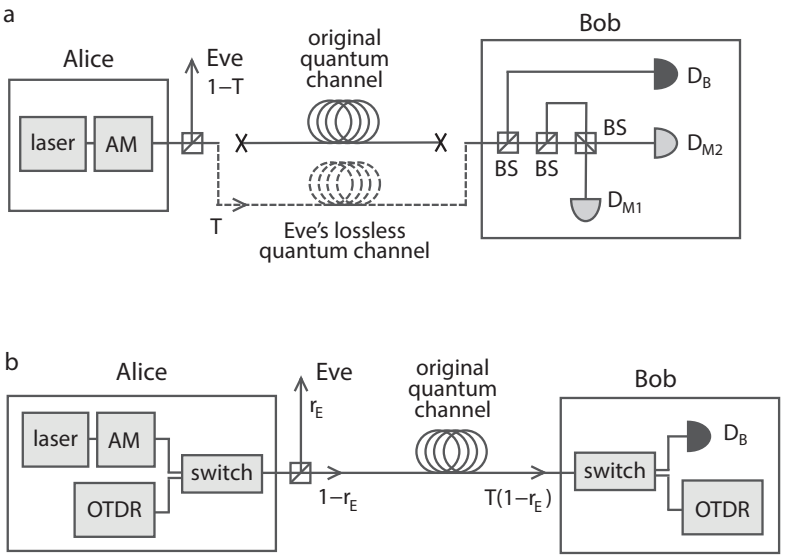

Figure 5. COW protocol scheme. (**a**) Original COW. Alice prepares coherent states using the laser and adjusts the signal's amplitude with the amplitude modulator (AM). BS stands for a beam-splitter. The detector D_B monitors the arrival time of the signals. Detectors D_{M2} and D_{M1} check weather the arriving sequence has the from $|\gamma\rangle\,|\gamma\rangle$. Eve performs the BS attack. (**b**) Enhanced COW. Alice and Bob exploit OTDR (optical time-domain reflectometer) to monitor losses in the line. The switch element defines the working regime: generating a key or monitoring the line. Eve introduces local intervention and intercepts the portion r_E of the signal.

6.1. Secret Key Rate in Modified COW

Next, we delve into the analysis of the COW in the context of the loss control approach that restricts the eavesdropper's actions to local interventions in the line (see Figure 5b). If r_E is the minimal detectable artificial leakage, an eavesdropper has to measure the states from the ensemble $|\sqrt{r_E}\gamma\rangle|0\rangle$, $|0\rangle|\sqrt{r_E}\gamma\rangle$, the Holevo quantity [11] χ of which upper-bounds the mutual information between Alice and Eve

$$I(\mathrm{A},\mathrm{E}) \leq \chi = h_2\left(\frac{1-|\,\langle 0|\sqrt{r_E}\gamma\rangle\,|^2}{2}\right). \tag{9}$$

In this context, Eve does not introduce any errors in the raw key. Hence, when Bob obtains a conclusive measurement result, the mutual information between Alice and Bob is one bit: $I(\mathrm{A},\mathrm{B}) = 1$, here we neglect the dark counts in detectors and other equipment's imperfections. The probability that measures a single bit-carrying signal through which Bob gets a conclusive outcome is determined by the Poisson statistics of the coherent state $|\sqrt{T(1-r_{\mathrm{E}})}\gamma\rangle$

$$p_{\checkmark} = 1 - \left|\langle 0|\sqrt{T(1-r_{\mathrm{E}})}\gamma\rangle\right|^2 = 1 - e^{-T(1-r_{\mathrm{E}})|\gamma|^2}. \tag{10}$$

After post-selection and privacy amplification procedures, the length of the final key L_f is also calculated according to the Devetak-Winter approach

$$L_f = p_{\checkmark} L \cdot (I(\mathrm{A},\mathrm{B}) - I(\mathrm{A},\mathrm{E})) \geq p_{\checkmark} L \cdot \left(1 - h_2(p_{\mathrm{err}}) - h_2\left(\frac{1 - e^{-r_{\mathrm{E}}|\gamma|^2}}{2}\right)\right). \tag{11}$$

6.2. Comparison with Original COW

To find an upper bound of the key rate in the original protocol, it is sufficient to consider any of the possible eavesdropping attacks. We consider the beam-splitting (BS) attack which is not the most optimal eavesdropping on the COW but which is a suitable reference since in our approach such an attack appears to be a basic one. As an example of a more powerful attack, we mention the one based on the soft filtering operation [40]. We analyze the BS attack, in which Eve replaces the optical line with the ideal one and intercepts the signal's part expected to be lost. Thus, Eve, simulating the natural losses in the channel with a proportion of $1 - T$, has to distinguish between states $|\sqrt{1-T}\gamma\rangle\,|0\rangle$, $|0\rangle\,|\sqrt{1-T}\gamma\rangle$. The maximum information that Eve can obtain, on average, about Alice's bit is bounded by the Holevo quantity, which for pure equiprobable states has the form

$$I(\mathrm{A},\mathrm{E}) \leq \chi = h_2\left(\frac{1 - |\,\langle 0|\sqrt{1-T}\gamma\rangle\,|^2}{2}\right). \tag{12}$$

Similarly to the previous consideration of the local leakage r_{E}, errors will not occur for the conclusive results at Bob's side ($I(\mathrm{A},\mathrm{B}) = 1$). The probability of a conclusive outcome is determined by the Poisson statistics of the coherent state $|\sqrt{T}\gamma\rangle$

$$p_{\checkmark} = 1 - \left|\langle 0|\sqrt{T}\gamma\rangle\right|^2 = 1 - e^{-T|\gamma|^2}. \tag{13}$$

Thus, the resulting key generation rate for the BS-attack can be estimated as follows

$$L_f^{\mathrm{orig}} \leq p_{\checkmark} L \cdot (I(\mathrm{A},\mathrm{B}) - I(\mathrm{A},\mathrm{E})) = p_{\checkmark} L \cdot \left(1 - h_2(p_{\mathrm{err}}) - h_2\left(\frac{1 - e^{-(1-T)|\gamma|^2}}{2}\right)\right). \tag{14}$$

Figure 6 displays the result of numerical simulations for the COW with the loss control approach and the original version of the protocol. The normalized key rate L_f/L is depicted as a function of the transmission distance D_{AB} for different values r_{E}: 0.005, 0.01, 0.10. For each portion of the stolen signal, r_{E}, and distance D_{AB}, the optimal intensity $|\gamma|^2$ is found to maximize the key rate determined by Equation (11). Applying the loss control approach allows for an increase in the intensity of signal pulses up to dozens of photons, see Figure A2 of Appendix A, and significantly boosts the key rate compared to the original version of the COW. The modified protocol produces a higher key rate even in the pessimistic case where Eve gets stolen about 10% of the signal. At a distance of 200 km and leakage detection precision $r_{\mathrm{E}} = 0.005$, the COW performance can be improved about 100 times in terms of key rates. Without modifying the signal average photon number, legitimate users can double the achievable key generation rate, see dashed lines at Figure 6. Again, if we are able to ensure the loss control of the level $r_{\mathrm{E}} < 0.1$, we can overcome the PLOB bound.

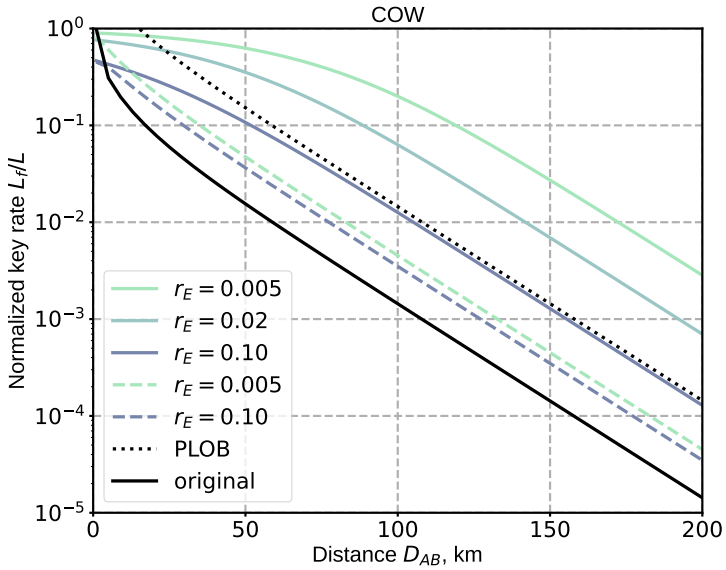

Figure 6. COW, secret key rate. The key generation rate as a function of the transmission distance D_{AB} for enhanced Equation (11) and original Equation (14) versions of the COW protocol. Different values of the leakage detection accuracy r_{E} are considered: 0.005, 0.01, 0.10. Solid lines stand for key rates of the enhanced version of the protocol for which the intensity maximizes Equation (11). Optimal signal intensity $|\gamma|^2$ varies from 2 to 100 photons per pulse for the enhanced protocol (see Figure A2). Dashed lines stand for the key rates in the case when the loss control approach is applied, but the intensity is not optimized and is taken the same as in the original version of the protocol. The dotted line corresponds to the PLOB bound. Here, we consider zero-error case $p_{\mathrm{err}} = 0$.

7. Loss Control Compared to the Decoy-State Method

The decoy-state method, utilized in the BB84, allows for legitimate users to detect, by estimating the number of non-blocked single-photon pulses, Eve's attacks using the complete blocking of some transmitted states. This method, employing decoy pulses with intensities different from ones in the bit-encoding states, is mostly aimed to cope with the PNS attack that appears to be highly relevant in the context of the experimental QKD realizations. Our approach also exploits special test pulses in addition to the signal ones but allows us to detect a wider spectrum of eavesdropping attacks. Based on the natural losses analysis and on the infeasibility of their exploitation, we step beyond the conventional decoy-state method and acquire the ability to determine the portion of the signal available to Eve. Precise estimate of the eavesdropper's information in the proposed approach leads to the less destructive compression of the key during the privacy amplification stage and allows for the utilization of bit-encoding states with hundreds of photons.

8. Beyond the Prepare-and-Measure QKD

In our work, we concentrate on the enhancement of the prepare-and-measure QKD protocols. Notably, protocols belonging to other classes can be modified as well. One can consider the Twin-Field (TF) QKD protocol [48] as an example. The working principle of the TF-QKD lies in sending the quantum state from Alice and Bob to the intermediate measurement point. The setting is equivalent to using one quantum repeater that results in overcoming the PLOB bound. Applying our approach to the TF-QKD protocol, legitimate users may monitor the losses from both ends of the line and, thus, they can produce secret keys with rates significantly exceeding the ones achieved in the state-of-the-art realizations [49–56].

It is important to clarify that our approach is formulated in the framework of the device-dependent QKD (according to the definition by R. Renner [57]), protocols that rely "on the exact specification of the deployed devices for their security proof". Examples of such protocols are all the prepare-and-measure and the entanglement-based QKD. Our method is more device-dependent than conventional QKD protocols since we also rely on the OTDR and transmittometry devices (see Table 1). Thus, protocols that belong to the device independent QKD [58–62] including the MDI variant of the Twin-Field QKD [63] are beyond the framework of our work. Nevertheless, the key generated using our approach is everlastingly secure, meaning that the key remains secret in time even against the non-existing technologies or attacks [64–67].

Table 1. Cryptography approaches comparison. Post-quantum cryptography, Point-to-point QKD, MDI QKD and Point-to-Point with loss control have different properties with regard to key rate, everlasting security and device dependency. In the table, "✓" means that key generated by a particular method is secure in time and resistant to both software and hardware future developments, while "✗" means that the key does not posses the everlasting security property.

	Secret Key Rate	**Everlasting Security**	**Device Dependency**
Post-quantum cryptography	high	✗	—
Point-to-point QKD	relatively low	✓	relatively high
MDI QKD	low	✓	medium
Point-to-point QKD with loss control	relatively high	✓	high

9. Discussion

The fundamental PLOB bound [9] of the key rate arises from the fact that all losses occurring in a quantum channel can be effectively measured by an eavesdropper. In this paradigm, protocols that do not exploit quantum repeaters provide relatively small key rates at hundreds of kilometers. Aimed at deflecting known attacks associated with channel losses, our approach acknowledges that it is unfeasible to gain information from natural losses. At the same time, we assert that any intrusive actions by a global eavesdropper, like substituting a channel with an ideal one, can be detected via line tomography. As a result, Alice and Bob separate the natural losses from local artificial leakages and determine the part of the signal available to an eavesdropper. Legitimate users, thus, may carry out privacy amplification with a less destructive reduction of the key length. This complements the results of [68] devoted to secret key rate increase observed under another kind of technological constraints imposed on a potential eavesdropper. While, in this paper, we do not consider the efficiency of the methods combination, we see it as a promising area for future research.

Intriguingly, it turns out that our approach also allows the users to increase the average photon number in bit-encoding states. This method, as we illustrate in the context of the COW and BB84 protocols, leads to a substantial enhancement in the key generation rate. At a distance of 200 km our method provides a 100 times higher key rate than the original versions of the protocols. Based on the proposed approach, with the appropriate level of leakage detection, we can potentially overcome the PLOB bound without exploiting quantum repeaters or devices acting as repeaters, for example, amplifiers. To overcome PLOB, we do not introduce mathematical modifications in existing analysis but change the model of the key generation process by relying on physically motivated assumptions.

Notably, while our method is applied to the existing QKD recipes and is based on the physics-motivated assumptions about the eavesdropper's opportunities, we leave an information-theoretical security proof for the increased photon number method, as well as a more formal security treatment, taking into account non-asymptotic effects, for our forthcoming work.

Author Contributions: N.S.K., M.P. and V.M.V. conceived the work and provided conceptualization; D.A.K. developed the methodology; A.D.K. and V.A.P. performed the formal analysis; A.D.K. and V.A.P. provided the original draft preparation; A.D.K., V.A.P., N.S.K., D.A.K. and V.M.V. wrote the manuscript; all authors reviewed and edited the manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data presented in this study are available in the article.

Acknowledgments: This work was supported by Terra Quantum AG.

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

Abbreviations

The following abbreviations are used in this manuscript:

AM	Amplitude Modulator
B92	Bennett 1992
BB84	Bennett-Brassard 1984
BS	Beam Splitter
COW	Coherent One-Way
DPS	Dfferential Phase-Shift
OTDR	Optical Time-Domain Reflectometer (Reflectometry)
PBS	Polarization Beam Splitter
PLOB	Pirandola-Laurenza-Ottaviani-Banchi
PM	Phase Modulator
PNS	Photon Number-Splitting
PR	Polarization Rotator
SARG04	Scarani-Acin-Ribordy-Gisin 2004
T-12	Toshiba 2012
TF-QKD	Twin-Field Quantum Key Distribution
QKD	Quantum Key Distribution
Y-00	Yuen 2000

Appendix A. Optimal Intensities for Modified Versions of BB84 and COW

Each QKD setup parameter should maximize the resulting key generation rate. In the original versions of the protocols, the optimal average photon number $|\gamma|^2$ is about 1 photon, which dramatically suffers from channel decay at hundreds of kilometers. Taking our approach, precise estimation of Eve's information allows legitimate users to utilize bit-encoding quantum states with much higher average photon numbers. Figure A1 shows $|\gamma|^2$ that maximizes key rate Equation (7) for the enhanced version of BB84. It, of course, depends on the leakage r_{E} and varies from several photons to more than 100 photons per pulse. The optimal intensity for COW is represented in Figure A2.

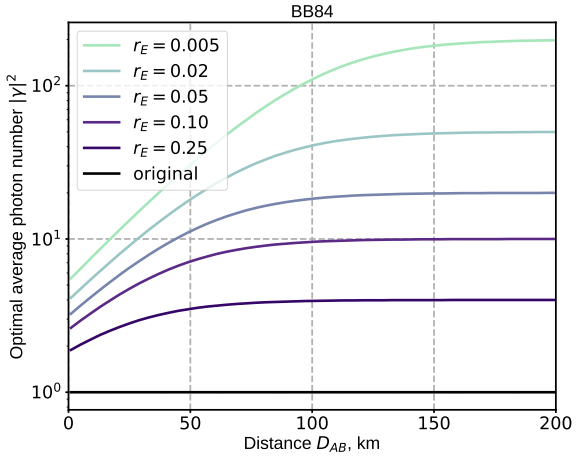

Figure A1. Optimal photon number BB84. The average photon number $|\gamma|^2$ which maximizes the key generation rate for both, original and enhanced, versions of the BB84 is a function of the transmission distance D_{AB}. For the enhanced version, $|\gamma|^2$ maximizes Equation (7) for different values of leakage r_{E}: 0.005, 0.01, 0.10 (color lines). For the original version, $|\gamma|^2$ that maximizes Equation (8) is equal to 1 (black line).

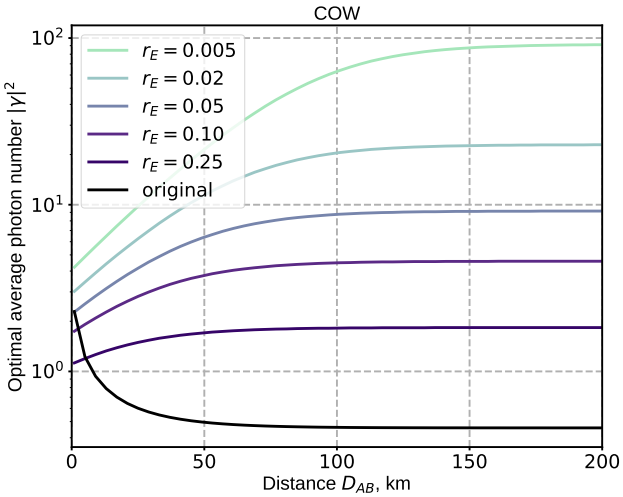

Figure A2. Optimal photon number COW. The average photon number $|\gamma|^2$ which maximizes the key generation rate for original and enhanced versions of COW is a function of the transmission distance D_{AB}. For the enhanced version $|\gamma|^2$ maximizes Equation (11) for different values of leakage r_{E}: 0.005, 0.01, 0.10 (color lines). For the original version $|\gamma|^2$ maximizes Equation (14) (black line).

Appendix B. Upper Bound on Key Rate in Decoy-State BB84

Due to the threat of the PNS attack, multi-photon pulses are insecure since Eve may keep one photon in quantum memory and re-send the rest to Bob through an ideal channel. Secure key generation is guaranteed only by one-photon pulses, the portion of which Eve can block. To detect such eavesdropping actions and estimate the number of one-photon pulses that reached Bob, Hwang introduced the decoy-state method [2]. In the decoy-state paradigm, Alice sends special pulses with different intensities compared to signal ones. The analytical expression [3,4] for the maximum length of the secret key that can be achieved is

$$L_f^{\mathrm{orig}} = L \cdot \frac{1}{2}[Q_1(1 - h_2(e_1)) - Q \cdot f(p_{\mathrm{err}}) \cdot h_2(p_{\mathrm{err}})], \tag{A1}$$

where Q is the gain of signal states (the probability that a signal state will be detected by Bob) and p_{err} is the quantum bit error rate (QBER); $f(p_{\mathrm{err}}) \geq 1$ is the efficiency of an

error-correction procedure with the Shannon limit $f(p_{\text{err}}) = 1$. The quantity Q_1 is the gain of single-photon states (a joint probability that a single-photon pulse was emitted by Alice and detected by Bob), and e_1 is the error rate on single-photon pulses. The quantities Q and p_{err} can be measured in the experiment, while Q_1 and e_1 cannot be observed directly due to the fact that Bob is not able to distinguish between photons that originated from the single-photon and multi-photon pulses. The values Q_1 and e_1 can be estimated by analyzing the parameters of decoy pulses on Bob's side [3,4].

We consider a situation when Eve is basically absent and does not conduct any attack at all, but the legitimate users do not know that and have to estimate the key generation rate fairly to be on the safe side. This approach enables us to estimate the upper bound on the key rate ensuring its independence of the experimentally observed parameters. To find an upper bound on Equation (A1), one can use non-negativity of binary entropy h_2: $h_2(e_1) \geq 0$ and $h_2(p_{\text{err}}) \geq 0$, and get that $L_f^{\text{orig}} \leq LQ_1/2$. Eve's activity causes the decrease of the gain of single-photon states Q_1, thus, it is maximum in Eve's absence: $Q_1 \leq T \cdot |\gamma|^2 e^{-|\gamma|^2}$. Consequently, the upper bound for the length of a shared secret is

$$L_f^{\text{orig}} \leq L \cdot \frac{1}{2} T \cdot |\gamma|^2 e^{-|\gamma|^2}. \tag{A2}$$

The analysis of this expression shows that its maximum is attained when $|\gamma| = 1$. When we are interested in the key rate dependence on the observed error, we should not discard the second term in Equation (8). The gain of signal states is determined by the average photon number in bit-encoding states $|\gamma|^2$ and transmittance T and equals to $Q = 1 - e^{-T|\gamma|^2}$. For the upper bound we consider $e_1 = 0$. Then, key rate as a function of the error probability takes the form Equation (8).

Appendix C. Error Analysis in BB84

In the modified version of BB84, errors may appear due to the imperfections of the line and other quantum devices rather than Eve's actions. The dependence of the key generation rate on the errors for both versions of the protocol is represented at Figure A3. For the accuracy of leakage detection $r_{\text{E}} = 0.005$ and error probability of 10% the modified version of the protocol provides 200 times higher key generation rate as in the analysis without errors.

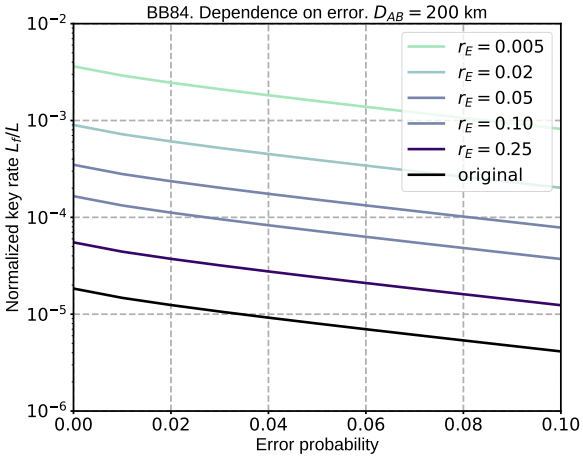

Figure A3. Dependence on error probability. The key generation rate as a function of error probability for both, original and enhanced, versions of BB84. The transmission distance is $D_{\text{AB}} = 200$ km. For the enhanced version, considered values of leakage r_{E}: 0.005, 0.01, 0.02, 0.10, 0.25 (color lines). For the original version, key rate is calculated according to Equation (8) (black line). Error probability is expected to be the same in both bases.

References

1. Bennett, C.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **1984**, *560*, 175–179. [CrossRef]
2. Hwang, W.Y. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.* **2003**, *91*, 057901. [CrossRef] [PubMed]
3. Lo, H.K.; Ma, X.; Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **2005**, *94*, 230504. [CrossRef]
4. Ma, X.; Qi, B.; Zhao, Y.; Lo, H.K. Practical decoy state for quantum key distribution. *Phys. Rev. A* **2005**, *72*, 012326. [CrossRef]
5. Trushechkin, A.S.; Kiktenko, E.O.; Kronberg, D.A.; Fedorov, A.K. Sectionrity of the decoy state method for quantum key distribution. *Physics-Uspekhi* **2021**, *64*, 88. [CrossRef]
6. 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]
7. Stucki, D.; Walenta, N.; Vannel, F.; Thew, R.T.; Gisin, N.; Zbinden, H.; Gray, S.; Towery, C.; Ten, S. High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres. *New J. Phys.* **2009**, *11*, 075003. [CrossRef]
8. Korzh, B.; Lim, C.C.W.; Houlmann, R.; Gisin, N.; Li, M.J.; Nolan, D.; Sanguinetti, B.; Thew, R.; Zbinden, H. Provably secure and practical quantum key distribution over 307 km of optical fibre. *Nat. Photon.* **2015**, *9*, 163–168. [CrossRef]
9. Pirandola, S.; Laurenza, R.; Ottaviani, C.; Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **2017**, *8*, 15043. [CrossRef]
10. Kirsanov, N.; Pastushenko, V.; Kodukhov, A.; Yarovikov, M.; Sagingalieva, A.; Kronberg, D.; Pflitsch, M.; Vinokur, V. Forty Thousand Kilometers Under Quantum Protection. *Sci. Rep.* **2023**, *13*, 8756. [CrossRef]
11. Holevo, A. Bounds for the Quantity of Information Transmitted by a Quantum Communication Channel. *Probl. Peredachi Informatsii* **1973**, *9*, 3–11.
12. Lesovik, G.B.; Lebedev, A.V.; Sadovskyy, I.A.; Suslov, M.; Vinokur, V.M. H-theorem in quantum physics. *Sci. Rep.* **2016**, *6*, 32815. [CrossRef] [PubMed]
13. Lesovik, G.B.; Sadovskyy, I.A.; Suslov, M.; Lebedev, A.V.; Vinokur, V.M. Arrow of time and its reversal on the IBM quantum computer. *Sci. Rep.* **2019**, *9*, 4396. [CrossRef] [PubMed]
14. Kirsanov, N.S.; Lebedev, A.V.; Suslov, M.; Vinokur, V.; Blatter, G.; Lesovik, G.B. Entropy dynamics in the system of interacting qubits. *J. Rus. Laser Res.* **2018**, *39*, 120–127. [CrossRef]
15. Kirsanov, N.; Lebedev, A.V.; Sadovskyy, I.; Suslov, M.; Vinokur, V.; Blatter, G.; Lesovik, G. H-theorem and Maxwell demon in quantum physics. *AIP Conf. Proc.* **2018**, *1936*, 020026.
16. Smirnov, A.; Yarovikov, M.; Zhdanova, E.; Gutor, A.; Vyatkin, M. An Optical-Fiber-Based Key for Remote Authentication of Users and Optical Fiber Lines. *Sensors* **2023**, *23*, 6390. [CrossRef]
17. Mølmer, K. Optical coherence: A convenient fiction. *Phys. Rev. A* **1997**, *55*, 3195. [CrossRef]
18. Lütkenhaus, N. Sectionrity against individual attacks for realistic quantum key distribution. *Phys. Rev. A* **2000**, *61*, 052304. [CrossRef]
19. Van Enk, S.; Fuchs, C.A. Quantum state of an ideal propagating laser field. *Phys. Rev. Lett.* **2001**, *88*, 027902. [CrossRef]
20. Zhao, Y.; Qi, B.; Lo, H.K. Experimental quantum key distribution with active phase randomization. *Appl. Phys. Lett.* **2007**, *90*, 044106. [CrossRef]
21. Chaiwongkhot, P.; Hosseini, S.; Ahmadi, A.; Higgins, B.L.; Dalacu, D.; Poole, P.J.; Williams, R.L.; Reimer, M.E.; Jennewein, T. Enhancing secure key rates of satellite QKD using a quantum dot single-photon source. *arXiv* **2020**, arXiv:2009.11818
22. Biswas, A.; Banerji, A.; Chandravanshi, P.; Kumar, R.; Singh, R.P. Experimental side channel analysis of BB84 QKD source. *IEEE J. Quantum Electron.* **2021**, *57*, 1–7. [CrossRef]
23. Pereira, M.; Currás-Lorenzo, G.; Navarrete, Á.; Mizutani, A.; Kato, G.; Curty, M.; Tamaki, K. Modified BB84 quantum key distribution protocol robust to source imperfections. *Phys. Rev. Res.* **2023**, *5*, 023065. [CrossRef]
24. 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]
25. Lucamarini, M.; Patel, K.; Dynes, J.; Fröhlich, B.; Sharpe, A.; Dixon, A.; Yuan, Z.; Penty, R.; Shields, A. Efficient decoy-state quantum key distribution with quantified security. *Opt. Express* **2013**, *21*, 24550–24565. [CrossRef]
26. 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]
27. Scarani, V.; Acin, A.; Ribordy, G.; Gisin, N. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.* **2004**, *92*, 057901. [CrossRef]
28. Brassard, G.; Lütkenhaus, N.; Mor, T.; Sanders, B.C. Limitations on Practical Quantum Cryptography. *Phys. Rev. Lett.* **2000**, *85*, 1330–1333. [CrossRef] [PubMed]
29. Acín, A.; Gisin, N.; Scarani, V. Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks. *Phys. Rev. A* **2004**, *69*, 012309. [CrossRef]
30. Duan, X.; Pearse, J.; Wonfor, A.; White, C.; Bahrami, A.; Straw, A.; Edwards, T.; Penty, R.; Lord, A.; Kumar, R.; et al. Performance analysis on co-existence of COW-QKD and classical DWDM channels transmission in UK national quantum networks. *J. Light. Technol.* **2023**, *41*, 4901–4906. [CrossRef]

31. Inoue, K.; Waks, E.; Yamamoto, Y. Differential-phase-shift quantum key distribution using coherent light. *Phys. Rev. A* **2003**, *68*, 022317. [CrossRef]
32. Takesue, H.; Nam, S.W.; Zhang, Q.; Hadfield, R.H.; Honjo, T.; Tamaki, K.; Yamamoto, Y. Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors. *Nat. Photon.* **2007**, *1*, 343–348. [CrossRef]
33. Tamaki, K. Unconditionally secure quantum key distribution with relatively strong signal pulse. *Phys. Rev. A* **2008**, *77*, 032341. [CrossRef]
34. Tamaki, K.; Lütkenhaus, N.; Koashi, M.; Batuwantudawe, J. Unconditional security of the Bennett 1992 quantum-key-distribution scheme with a strong reference pulse. *Phys. Rev. A* **2009**, *80*, 032302. [CrossRef]
35. Miroshnichenko, G.; Kozubov, A.; Gaidash, A.; Gleim, A.; Horoshko, D. Sectionrity of subcarrier wave quantum key distribution against the collective beam-splitting attack. *Opt. Express* **2018**, *26*, 11292–11308. [CrossRef]
36. Hirota, O.; Kato, K.; Shoma, M.; Usuda, T.S. Quantum key distribution with unconditional security for all optical fiber network. In *Quantum Communications and Quantum Imaging, Proceedings of the Optical Science and Technology, SPIE's 48th Annual Meeting, San Diego, CA, USA, 3–8 August 2003*; SPIE: Bellingham, WA, USA, 2004; Volume 5161, pp. 320–331.
37. Barbosa, G.A. Information theory for key distribution systems secured by mesoscopic coherent states. *Phys. Rev. A* **2005**, *71*, 062333. [CrossRef]
38. Branciard, C.; Gisin, N.; Lütkenhaus, N.; Scarani, V. Zero-error attacks and detection statistics in the coherent one-way protocol for quantum cryptography. *Quantum Inf. Comput.* **2007**, *7*, 639–664. [CrossRef]
39. Kronberg, D.A.; Kiktenko, E.O.; Fedorov, A.K.; Kurochkin, Y.V. Analysis of coherent quantum cryptography protocol vulnerability to an active beam-splitting attack. *Quantum Electron.* **2017**, *47*, 163. [CrossRef]
40. Kronberg, D.; Nikolaeva, A.; Kurochkin, Y.V.; Fedorov, A. Quantum soft filtering for the improved security analysis of the coherent one-way quantum-key-distribution protocol. *Phys. Rev. A* **2020**, *101*, 032334. [CrossRef]
41. Shor, P.W.; Preskill, J. Simple Proof of Sectionrity of the BB84 Quantum Key Distribution Protocol. *Phys. Rev. Lett.* **2000**, *85*, 441–444. [CrossRef]
42. Renner, R. Sectionrity of quantum key distribution. *Int. J. Quantum Inf.* **2008**, *6*, 1–127. [CrossRef]
43. Renner, R.; Gisin, N.; Kraus, B. Information-theoretic security proof for quantum-key-distribution protocols. *Phys. Rev. A* **2005**, *72*, 012332. [CrossRef]
44. Schmitt-Manderbach, T.; Weier, H.; Fürst, M.; Ursin, R.; Tiefenbacher, F.; Scheidl, T.; Perdigues, J.; Sodnik, Z.; Kurtsiefer, C.; Rarity, J.G.; et al. Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km. *Phys. Rev. Lett.* **2007**, *98*, 010504. [CrossRef] [PubMed]
45. Kobayashi, T.; Tomita, A.; Okamoto, A. Evaluation of the phase randomness of a light source in quantum-key-distribution systems with an attenuated laser. *Phys. Rev. A* **2014**, *90*, 032320. [CrossRef]
46. Boaron, A.; Boso, G.; Rusca, D.; Vulliez, C.; Autebert, C.; Caloz, M.; Perrenoud, M.; Gras, G.; Bussières, F.; Li, M.J.; et al. Sectionre quantum key distribution over 421 km of optical fiber. *Phys. Rev. Lett.* **2018**, *121*, 190502. [CrossRef]
47. Devetak, I.; Winter, A. Distillation of secret key and entanglement from quantum states. *Proc. R. Soc. Lond. A* **2005**, *461*, 207–235. [CrossRef]
48. 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]
49. Pittaluga, M.; Minder, M.; Lucamarini, M.; Sanzaro, M.; Woodward, R.I.; Li, M.J.; Yuan, Z.; Shields, A.J. 600-km repeater-like quantum communications with dual-band stabilization. *Nat. Photon.* **2021**, *15*, 530–535. [CrossRef]
50. Wang, S.; Yin, Z.Q.; He, D.Y.; Chen, W.; Wang, R.Q.; Ye, P.; Zhou, Y.; Fan-Yuan, G.J.; Wang, F.X.; Chen, W.; et al. Twin-field quantum key distribution over 830-km fibre. *Nat. Photon.* **2022**, *16*, 154–161. [CrossRef]
51. Xie, Y.M.; Weng, C.X.; Lu, Y.S.; Fu, Y.; Wang, Y.; Yin, H.L.; Chen, Z.B. Scalable high-rate twin-field quantum key distribution networks without constraint of probability and intensity. *Phys. Rev. A* **2023**, *107*, 042603. [CrossRef]
52. Ma, X.; Zeng, P.; Zhou, H. Phase-matching quantum key distribution. *Phys. Rev. X* **2018**, *8*, 031043. [CrossRef]
53. Lin, J.; Lütkenhaus, N. Simple security analysis of phase-matching measurement-device-independent quantum key distribution. *Phys. Rev. A* **2018**, *98*, 042332. [CrossRef]
54. Lu, F.Y.; Yin, Z.Q.; Cui, C.H.; Fan-Yuan, G.J.; Wang, R.; Wang, S.; Chen, W.; He, D.Y.; Huang, W.; Xu, B.J.; et al. Improving the performance of twin-field quantum key distribution. *Phys. Rev. A* **2019**, *100*, 022306. [CrossRef]
55. Curty, M.; Azuma, K.; Lo, H.K. Simple security proof of twin-field type quantum key distribution protocol. *Npj Quantum Inf.* **2019**, *5*, 64. [CrossRef]
56. Gu, J.; Cao, X.Y.; Fu, Y.; He, Z.W.; Yin, Z.J.; Yin, H.L.; Chen, Z.B. Experimental measurement-device-independent type quantum key distribution with flawed and correlated sources. *Sci. Bull.* **2022**, *67*, 2167–2175. [CrossRef]
57. Renner, R.; Wolf, R. Quantum advantage in cryptography. *AIAA J.* **2023**, *61*, 1895–1910. [CrossRef]
58. Lo, H.K.; Curty, M.; Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503. [CrossRef]
59. Braunstein, S.L.; Pirandola, S. Side-channel-free quantum key distribution. *Phys. Rev. Lett.* **2012**, *108*, 130502. [CrossRef]
60. Xie, Y.M.; Lu, Y.S.; Weng, C.X.; Cao, X.Y.; Jia, Z.Y.; Bao, Y.; Wang, Y.; Fu, Y.; Yin, H.L.; Chen, Z.B. Breaking the rate-loss bound of quantum key distribution with asynchronous two-photon interference. *PRX Quantum* **2022**, *3*, 020315. [CrossRef]
61. Zeng, P.; Zhou, H.; Wu, W.; Ma, X. Mode-pairing quantum key distribution. *Nat. Commun.* **2022**, *13*, 3903. [CrossRef]

62. Xie, Y.M.; Bai, J.L.; Lu, Y.S.; Weng, C.X.; Yin, H.L.; Chen, Z.B. Advantages of Asynchronous Measurement-Device-Independent Quantum Key Distribution in Intercity Networks. *Phys. Rev. Appl.* **2023**, *19*, 054070. [CrossRef]
63. Yin, H.L.; Fu, Y. Measurement-device-independent twin-field quantum key distribution. *Sci. Rep.* **2019**, *9*, 3045. [CrossRef] [PubMed]
64. Portmann, C.; Renner, R. Sectionrity in quantum cryptography. *Rev. Mod. Phys.* **2022**, *94*, 025008. [CrossRef]
65. Unruh, D. Everlasting multi-party computation. In Proceedings of the Advances in Cryptology—CRYPTO 2013: 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, 18–22 August 2013; Proceedings, Part II; Springer: Berlin/Heidelberg, Germany, 2013; pp. 380–397.
66. Stebila, D.; Mosca, M.; Lütkenhaus, N. The case for quantum key distribution. In Proceedings of the Quantum Communication and Quantum Networking: First International Conference, QuantumComm 2009, Naples, Italy, 26–30 October 2009; Revised Selected Papers 1; Springer: Berlin/Heidelberg, Germany, 2010; pp. 283–296.
67. Alléaume, R.; Lütkenhaus, N.; Renner, R.; Grangier, P.; Debuisschert, T.; Ribordy, G.; Gisin, N.; Painchault, P.; Pornin, T.; Slavail, L.; et al. Quantum key distribution and cryptography: A survey. In *Dagstuhl Seminar Proceedings*; Schloss Dagstuhl-Leibniz-Zentrum für Informatik: Wadern, Germany, 2010.
68. 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. [CrossRef] [PubMed]