scientific reports

Check for updates

OPEN

Loss control-based QKD with noisy devices

Valeria Pastushenko[1,2], Aleksei Kodukhov[1,2], Artyom Shindin[1], Vladislav Zemlyanov[1], Markus Pflitsch[1] & Valerii Vinokur[1]✉

Quantum cryptography protocols aimed at providing communication security are based on the fundamental principle of quantum physics that non-orthogonal quantum states cannot be perfectly distinguished. The majority of practically applicable quantum cryptography realizations belong to the so-called device-dependent class of quantum key distribution (QKD) protocols. Security of the device-dependent protocols cannot be ensured without considering all the noises in the incorporated devices. Here, we analyze the influence of the preparation and detection noise on the loss control-based QKD that is built on continuous monitoring of the leakages in the fiber channel. By estimating the achievable secret key generation rates, we show the robustness of the loss control approach to trusted preparation and detection noises. Our findings demonstrate a positive impact of the trusted preparation noise on the QKD based on loss control for reverse and direct reconciliation scenarios.

A novel secret communication technique, quantum cryptography, is a breakthrough technology built on a fundamental principle of quantum physics establishing that non-orthogonal quantum states cannot be perfectly distinguished. This principle provides the fundamental base for secure communications and restores the communication safety that appeared to be under a strong threat because of the impressive progress and upcoming use of quantum computing promising very effective decoding techniques. The quantum principle stating that measurements disturb the measured state guarantees that any attempt to compromise the security of the communication network will be detected, thus making invisible network interceptions and eavesdropping impossible.

The most prominent representative of quantum cryptography is quantum key distribution (QKD)[1–4]. In addition to QKD, quantum cryptography includes, for example, the quantum secure direct communication method[5–9], which allows for the direct transmission of secret messages. Realizations of the QKD, the main focus of the current article, fall into three main categories of dependencies on the incorporated devices: Device-dependent (DD) QKD[10–12], measurement device-independent (MDI) QKD[13,14], and device-independent (DI) QKD[15,16] ones. To provide a successful security analysis of the DD-QKD protocols, one needs a comprehensive description of the utilized equipment since any incompleteness of mathematical models used for the QKD protocols can allow for quantum hacking attacks breaking the security[17–21].

An essential device utilized in most of the DD-QKD protocols is a modulator, a tool for encoding classical information into the parameters of quantum states at the sender's side. The most commonly used modulators necessary for realizing QKD protocols on optical coherent states are the Mach-Zehnder electro-optical (EO) modulators. The noise in the EO-modulators is primarily caused by the instability of the operating point, electrical noises of the modulating signal and temperature fluctuations[22–27], which makes the output quantum states rather mixed than pure. Another factor that stimulates the initial mixedness of quantum states is the non-ideal laser source. In many QKD protocols, it is assumed that an eavesdropper produces all noises in a cryptographic protocol. Yet, a wide range of studies considers the noise in preparation and detection equipment as trusted, i. e. uncontrollable by an adversary. This feature significantly modifies the security analysis. The most comprehensive research on the trusted preparation[28–34] and detection[33–36] noises is provided in the context of the continuous variable (CV) QKD[37,38]. CV-QKD is a class of quantum cryptographic protocols that use continuous properties of light and can be implemented with standard telecom components.

The recently developed integrity and loss control-based approach to secret key generation[39–42] is built on the continuous monitoring of a fiber line. In the preceding works dedicated to the loss control-based approach, it was shown that the assumptions about Eve's unrestricted ability to intercept and utilize all losses in the channel are practically unfeasible[39,40]. The reason is that losses in the optical fiber channels typically occur due to the Rayleigh scattering and, thus, are homogeneously spread along the communication line. To extract the information about the key, an adversary needs several hundreds-meter-long coherent detection devices capable of distinguishing between bit-encoding quantum states. Such detectors are a decade-long future development

[1]Terra Quantum AG, Kornhausstrasse 25, 9000 St. Gallen, Switzerland. [2]Valeria Pastushenko and Aleksei Kodukhov contributed equally to this work. ✉email: vv@terraquantum.swiss

rather than existing devices. Thus, at this moment, it is natural to assume that Eve can interact with the channel only locally.

In order to conduct a local attack, the eavesdropper has to disrupt the integrity of the optical fiber, since direct physical access to the optical quantum states is required for extracting information from these states. Any integrity violation of the fiber's cladding produces increased leakage of a propagating optical state and, thus, produces loss additional to Rayleigh scattering.

According to the experimental results of Refs.[41,43,44], legitimate users can detect local deformations of optical fiber structure by sending special test pulses and measuring the back-scattered radiation on the sender's side using optical time-domain reflectometry (OTDR). The OTDR procedure reflects the loss distribution along the whole quantum channel length and allows for determining the degree of local deformations, which, in turn, contains information about the fraction of the signal which the eavesdropper effectively interacted with.

We model an eavesdropper getting access to a part of the optical signal by a beam-splitter transformation. Therefore, we analyze the security of the protocol basing on the assumption that an eavesdropper conducts a beam-splitter attack, i.e., diverts a part of the signal propagating through the optical fiber in one or several points of the optical line. Notably, the model also takes into account the fact that a potential eavesdropper can exploit local losses that had already occurred in a channel, for instance, by attempting to extract information from losses at connectors, welding, and bends. The OTDR technique allows for evaluating all the losses irrespective of their origin.

Moreover, the loss control technique eliminates the possibility of any undetected intercept-resend attack, since for this type of attack Eve needs to unplug the channel or fully violate the integrity of the channel's cladding and core. Such an event can be detected on a line tomogram since the back-scattered radiation will stop propagating from the fiber section after the attack point. Alice will not obtain any signal when it is expected to arrive and will make a conclusion about Eve's interaction with the channel. In fact, for Alice, it is enough to send only one test pulse to observe unplugging of the fiber or the break of its integrity. For Eve to inject a false "back-scattering" signal and, thus, to hide the intrusion, they must predict the exact time when a test pulse will pass and make the time shift between the intrusion and the injection tending to zero. Otherwise, such an intrusion can be detected on the tomogram as a dip and gain of the signal. In addition, Alice can randomly modulate test pulses to make it impossible for Eve to produce a reliable false signal[45].

For the OTDR data to be informative, the line tomogram has to reflect the state of the line during the exchange of bit-encoding pulses. We naturally assume that the line itself preserves its properties. And since the operational speed of cutting-edge optical elements such as switches is significantly restricted, Eve with the best modern devices is not able to tune the leakage inferentially fast. Thus, for the purposes of this this article, we also assume that Eve acts the same way during line tomography and the exchange of bit-encoding pulses.

In this article, we build upon the results of our previous works[39–41] and examine the robustness of the QKD based on the loss control with respect to trusted preparation and detection noise for a relatively short, 10 km long fiber line. We then consider different error correction scenarios: the direct and reverse reconciliation. The work is organized as follows. In Sect. 2, we delve into the issue of the trusted preparation noise and present the experimental results obtained from our setup. Section 3 is devoted to our QKD protocol and the theoretical approach which we use to estimate the influence of trusted preparation and detection noise on its efficiency. The main numerical findings are presented in Sect. 4, and, finally, we discuss the results and their implication in Sect. 5.

Trusted preparation noise

The main part of the preparation stage of most QKD protocols is the encoding of classical information into a sequence of quantum states. In the QKD implementations based on the coherent states, the preparation stage is executed by using an EO-modulator that properly adjusts the phase and intensity of the sent signal. The result of the natural noises emerging in the laser and EO-modulator is that the signal produced by the sender, Alice, is a statistical mixture of coherent states rather than a pure state.

In a standard setting and arrangement of the device-dependent quantum cryptography, Eve cannot influence the functioning of the equipment in the laboratories of the legitimate users. It implies that preparation and detection-related noises can be naturally considered as trusted and thus can be preliminarily measured and calibrated by legitimate users. The effects of trusted noise have been widely studied in the context of the CV-QKD. The results show that trusted preparation[28–30,46] and detection[32–34,47–49] noises can have both positive and negative impacts on the QKD efficiency. To apply the trusted noise approach, legitimate users should verify that considered noises remain constant at least during one quantum communication session. Before starting quantum state transmission, Alice and Bob always must remeasure the noise in their devices and update the parameters of the mathematical model that is used for treatment.

The main factor that can make the trusted noise non-constant during a key distribution session is temperature fluctuations. Thus, Alice and Bob should carefully control the temperature conditions in their laboratories. In any practical implementation, users' equipment is located in data centers where high efforts are made to keep the temperature constant. Additionally, legitimate users can introduce thermal isolation for their devices to make them less dependent on the temperature fluctuations in data centers. To further proceed, we, thus, accept that in Alice and Bob's laboratories the temperature is constant.

In the context of the loss control approach[39–42], trusted preparation noise results in an additional uncertainty of measurement outcomes on the receiver's (Bob's) side and also generates correlations between Bob's and Eve's measurement results. These correlations lead to a dependence of Eve's density matrix on a particular postselection strategy of the receiver and, accordingly, make upper bounding of the information that Eve receives a challenging problem.

To address this problem, we consider the most general case of an arbitrary statistical mixture of coherent states coming out from the Alice's side. The analysis of the important specific cases will be carried out in Sec. 4. For a given bit $a = 0, 1$, let $\mathcal{M}_a(|\gamma|^2)$ be the intensity distribution induced by the laser and optical modulator on Alice's side. Here, $|\gamma|^2$ stands for the intensity of a particular output of the Alice's preparation equipment. The coherent state created by Alice is influenced by the laser's and modulator's noise and also by the phase randomization[50,51], which transforms a pure coherent state into the statistical mixture of Fock states. Phase randomization reduces the adversary's capabilities to attack the communication and is used in standard QKD protocols like the decoy state BB84, for example. As a result, the output density matrix can be written as

$$\hat{\rho}_a = \int_0^\infty d|\gamma|^2 \mathcal{M}_a(|\gamma|^2) \frac{1}{2\pi} \int_0^{2\pi} d\varphi ||\gamma|e^{i\varphi}\rangle\langle|\gamma|e^{i\varphi}|. \tag{1}$$

The second integral over the phase φ of a coherent state $||\gamma|e^{i\varphi}\rangle$ appears due to the phase randomization. In experimental realizations, the phase randomization can differ from the mathematical model. However, for the sake of simplicity, we assume phase randomization to be perfect, exactly according to Eq. (1). The shape of the distribution $\mathcal{M}_a(|\gamma|^2)$ depends on the particular equipment, and the Eq. (12) presents the specific shape we consider in the numerical part of the study. Figure 1a depicts exemplary intensity distributions on Alice's side (Fig. 1b–d show Bob's photon number distribution and Eve's photon number distribution before and after postselection), while Fig. 2 shows experimentally obtained data, which reflect the contribution of the modulator's noises to the density matrix sent by Alice. To stress the illustrative purposes of the plot, the laser is assumed to be ideal, yet, the approach proposed above incorporates the most general case.

Application to the loss control-based quantum cryptography

In this section, we study the influence of the trusted noise on the efficiency of the QKD based on the loss control. The loss control approach relies on the assumptions associated with the properties of the fiber quantum channel. Firstly, Eve is limited in collecting and extracting information from homogeneously distributed scattered losses. To get access to the propagating part of the photons' wave function, Eve must locally violate the fiber's integrity and introduce additional losses. Finally, we assume that an eavesdropper conducts the beam-splitting attack in an i.i.d. setting. The key generation process effectively splits into 4 stages described below. Detailed description of the evolution of bit-encoding density matrix can be found in the Supplementary Information (SI), Note 1.

I. At the first stage, Alice prepares mixed states, see Fig. 1a and Eq. (1), using the noisy laser source and modulator and transfers these states to Bob through the quantum channel. The exact noise profile utilized in the further numerical calculations can be found in Eq. (12). The quantum channel is an optical fiber line and is characterized by its transmittivity T. The transmittivity is connected with the length of the line D by the equation

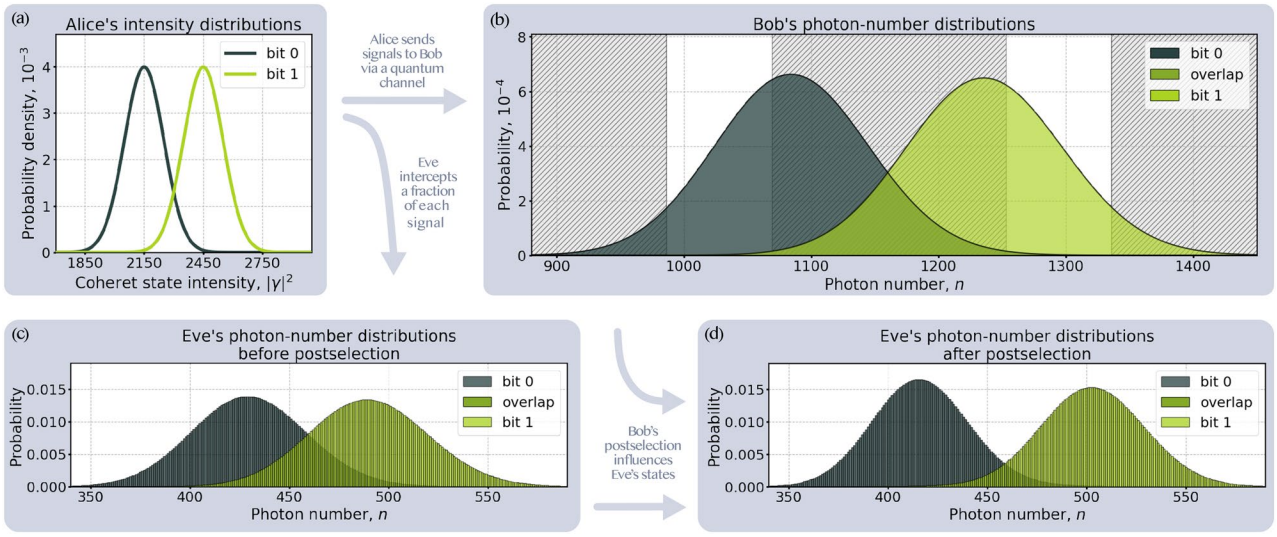

Fig. 1. Probability distributions describing quantum states of Alice, Bob and Eve. (**a**) The intensity distributions on Alice's side modulating the preparation noises, where the mean intensity of a signal encoding bit '0' is taken to be $\mu_0 = 2150$, the mean intensity of a signal encoding bit '1' is $\mu_1 = 2450$, the corresponding variances are $\sigma_0 = \sigma_1 = 100$. (**b**) The photon-number distributions on Bob's side. Bob obtains signals sent by Alice via a 10 km quantum channel. White regions correspond to the measurement results surviving the postselection, shaded areas correspond to measurement result discarded during postselection. (**c**) The photon-number distributions on Eve's side before the postselections stage. Eve intercepts a fraction of signal, $r_E = 20\%$, at the very beginning of the line. (**d**) The photon-number distributions on Eve's side after the postselections stage.

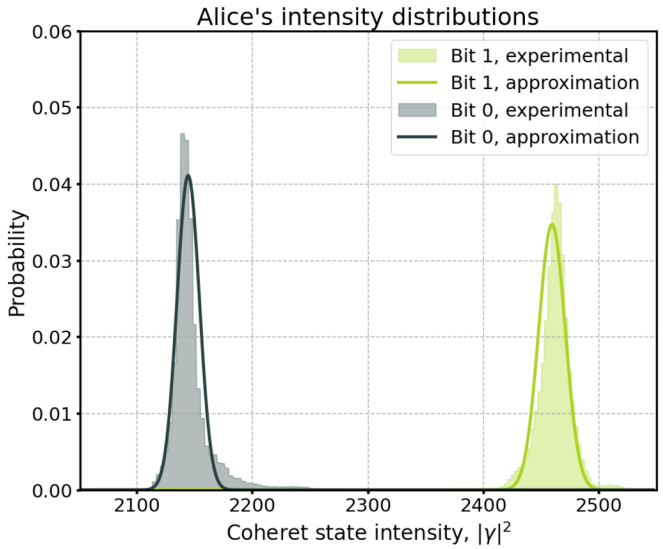

Fig. 2. Probability distribution of intensity on Alice's side. Experimentally obtained data from the installed modulator shows the distributions of signal's intensity for both logical bits (gray and green histograms). Gaussian approximations for both experimental distributions are shown in black and green lines: $\mu_0 = 2145$, $\mu_1 = 2460$, $\sigma_0 = 11$, $\sigma_1 = 11$.

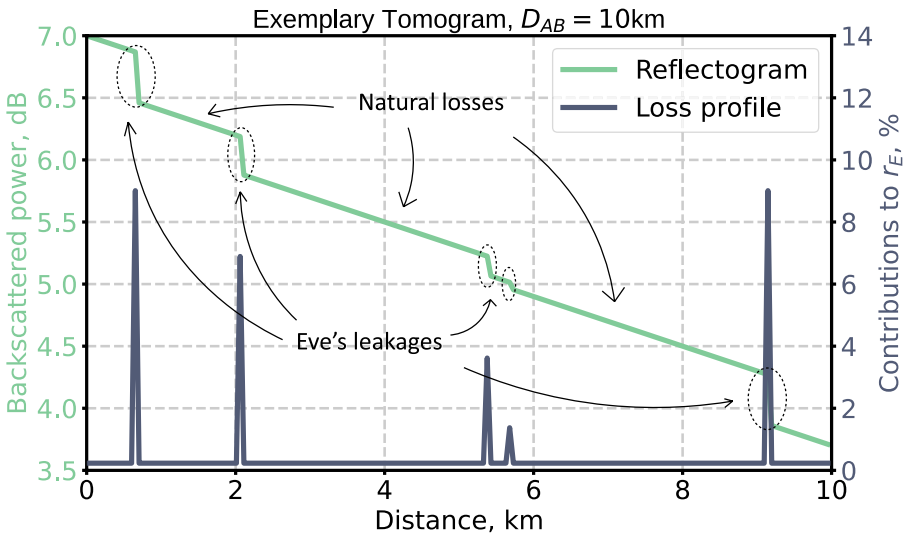

Fig. 3. Exemplary reflectogram and line tomogram. The loss profile, which displays the magnitude of each local leakage and its position, is derived from the reflectogram.

$T = 10^{-\xi D}$, where for standard optical fibers $\xi = 0.02\,\mathrm{km}^{-1}$. Optical fiber is a purely lossy channel and does not introduce additional noise to the propagating quantum states.

II. At the second stage, Eve intercepts the part r_{E} of the propagating intensity by introducing a local leakage, see Fig. 1c. We describe this leakage by introducing a non-symmetrical beam-splitter. In fact, the eavesdropper does not have to introduce additional leakage but can exploit local leakages that had already occurred, for example, losses on connectors or at welding points. Another approach to attack locally is to hide the presence of an artificial leakage by replacing a section of the original channel with a lower-loss fiber cable, see Note 2 of SI for details. This action leads to additional local losses in the points where fibers of different types are spliced[52–54]. Legitimate users can detect local leakages with the line tomography procedure, i. e., by measuring transmitted and back-scattered parts of the optical test signals. Alice and Bob compare the obtained tomogram, see Fig. 3, with the initial (reference) one. An important assumption that must always be verified in a practical realization is that an adversary does not attack the quantum channel before Alice and Bob compose the initial channel tomogram. Further details on the line tomography can be found in Refs.[39–43].

III. When the bit-encoding states reach the end of the line, Bob conducts noisy photon-number measurement, see Fig. 1b, Eq. (2) and Eq. (13) for a detection noise profile considered in numerical calculations.

IV. After the measurement stage, the legitimate users conduct classical post-processing procedures. Namely, postselection, error correction and privacy amplification.

Bob's measurement can be described by a positive operator-valued measure (POVM), which is a set of positive semi-definite Hermitian operators with the sum equal to the identity operator. In our case, Bob's POVM consists of three elements see details in SI Note 3,

$$\hat{E}_0 = \sum_{n=0}^{+\infty} \left(\sum_{k=\theta_3}^{\theta_1} \mathcal{D}_n(k) \right) |n\rangle\langle n|, \quad \hat{E}_1 = \sum_{n=0}^{+\infty} \left(\sum_{k=\theta_2}^{\theta_4} \mathcal{D}_n(k) \right) |n\rangle\langle n|, \quad \hat{E}_{\text{fail}} = \hat{\mathbb{1}} - \hat{E}_0 - \hat{E}_1, \tag{2}$$

where operators $\hat{E}_0$ and $\hat{E}_1$ correspond to the measurement results which Bob interprets as a bit value '0' or '1', while the operator $\hat{E}_{\text{fail}}$ stands for the measurement results discarded during the postselection stage. The probability distribution $\mathcal{D}_n$ describes the noise of the detector. To be concrete, $\mathcal{D}_n(k)$ defines the probability of obtaining an outcome k in the case of measuring the Fock quantum state $|n\rangle\langle n|$ by a given detector. The specific form of the distribution $\mathcal{D}_n$ which we use for the numerical analysis is presented in Eq. (13), yet, the framework allows for an arbitrary distribution. Real-valued parameters θ_i determine the choice of a postselection algorithm. Inner values, θ_1 and θ_2 represent the discarding of the overlapped parts of the measurement results' distributions, see Fig. 1b, and decrease bit error rate (BER) in the raw key. Outer values, θ_3 and θ_4 discard the tails of the Bob's distributions. By discarding the tails, we expect an increase of the BER on Bob's side, but at the same time a decrease of an average information that Eve obtains from the intercepted parts of the states. The shaded areas in Fig. 1b correspond to the measurement results on Bob's side discarded during postselection.

Right after the postselection stage, bits 0 and 1 in the Alice's string can be not equiprobable due to the potential asymmetry in preparation noise and in postselection procedure itself. The asymptotic fraction of the bit value a in the Alice's string is

$$q_a = \frac{p(\checkmark|a)}{2p_\checkmark}, \tag{3}$$

where we used the notation $p_\checkmark$ for the total probability of a conclusive measurement result (that will survive postselection) and $p(\checkmark|a)$ for the probability of a conclusive measurement result for a sent bit a. On Bob's side, after discarding "fail" results, the asymptotic fraction of a bit value $b \in \{0, 1\}$ in the raw key is

$$w_b = \frac{p(b|a=0) + p(b|a=1)}{2p_\checkmark}, \tag{4}$$

where $p(b|a)$ stands for the conditional probability of obtaining measurement result b, when the sent bit is a.

Next, we execute an analysis of the information available to the adversary. Eve's information strongly depends on the error correction strategy. In the direct reconciliation (DR) scenario, Alice's bit string is considered to be a reference, and Bob adjusts the raw key with respect to a syndrome of a chosen error correction code. In this case, Eve is attempting to make a guess about the sent bits, thus, we are to estimate the information, $I(\mathrm{A};\mathrm{E})$, which Eve obtains about Alice's subsystem. Conversely, in the reverse reconciliation (RR) case, Bob's bit string is a reference and the sender has to modify their bit string. Here, the adversary's aim is to get the knowledge about Bob's string.

We focus, first, on the direct reconciliation case. Eve's density matrix after the postselection procedure conditioned on the Alice's bit a, see Fig. 1d and SI, Note 1**a** for details, is

$$\hat{\rho}_{\mathrm{E}}^{(a)} = \frac{1}{p(\checkmark|a)} \int_0^\infty d|\gamma|^2 \mathcal{M}_a(|\gamma|^2) f_\checkmark(|\gamma|) \cdot e^{-r_{\mathrm{E}}|\gamma|^2} \sum_{n=0}^{\infty} \frac{\left(r_{\mathrm{E}}|\gamma|^2\right)^n}{n!} |n\rangle\langle n|_{\mathrm{E}}, \tag{5}$$

where

$$f_\checkmark(|\gamma|) = \langle \sqrt{T(1-r_{\mathrm{E}})}\gamma| \left(\hat{E}_0 + \hat{E}_1\right) |\sqrt{T(1-r_{\mathrm{E}})}\gamma\rangle. \tag{6}$$

This factor shows the contribution to the probability of a conclusive measurement result on Bob's side from a pure coherent state $|\gamma\rangle$, which is a component of the statistical mixture. Notably, the function $f_\checkmark(|\gamma|)$ does not depend on the phase of γ and, thus, it is not affected by the phase randomization. The denominator $p(\checkmark|a)$ is a normalization factor that can be determined by the condition $\mathrm{Tr}\ \hat{\rho}_{\mathrm{E}}^{(a)} = 1$. We find that receiver's postselection modifies the initial preparation distribution $\mathcal{M}_a(|\gamma|^2)$ by discarding inappropriate measurement results and, thus, alters Eve's density matrix as depicted on Fig. 1c and d. The density matrix of the form (5) fundamentally differs from the form it assumes in the case in which Eve obtains a part of the pure coherent state. In the latter case, Eve-Bob state is a product state and, thus, Bob's postselection cannot affect Eve's measurement results.

The information that Eve can extract from the intercepted part of the signals in the DR case is limited by the Holevo quantity[55] of the ensemble $\mathcal{E}_{\mathrm{DR}} = \left\{ q_a, \rho_{\mathrm{E}}^{(a)} \right\}_a$:

$$I(\mathrm{A};\mathrm{E}) \leq \chi\left(\mathcal{E}_{\mathrm{DR}}\right) = S\left(q_0\rho_{\mathrm{E}}^{(0)} + q_1\rho_{\mathrm{E}}^{(1)}\right) - q_0 S\left(\rho_{\mathrm{E}}^{(0)}\right) - q_1 S\left(\rho_{\mathrm{E}}^{(1)}\right), \tag{7}$$

where $S(\rho) = -\mathrm{Tr}\,(\rho \log_2 \rho)$ is the von Neumann entropy and $q_{0(1)}$ is defined in Eq. (3). According to Eq. (5), Eve's density matrix is diagonal due to the phase randomization. Thus, von Neumann entropy can be replaced by the classical Shannon entropy.

In the RR case, an adversary has to distinguish between intercepted states conditioned on Bob's measurement results $b \in \{0, 1\}$. Eve's density matrix for a given Bob's bit value b, see Note 1**b** in SI for details, is

$$\hat{\eta}_{\mathrm{E}}^{(b)} = \int_0^{+\infty} d|\gamma|^2 \, \frac{\mathcal{M}_0(|\gamma|^2) + \mathcal{M}_1(|\gamma|^2)}{p(b|0) + p(b|1)} \, f_b\left(|\gamma|\right) \cdot e^{-r_{\mathrm{E}}|\gamma|^2} \sum_{n=0}^{\infty} \frac{\left(r_{\mathrm{E}}|\gamma|^2\right)^n}{n!} |n\rangle\langle n|_{\mathrm{E}}, \tag{8}$$

where $f_b(|\gamma|) = \langle\sqrt{T(1-r_{\mathrm{E}})}\gamma|\hat{E}_b|\sqrt{T(1-r_{\mathrm{E}})}\gamma\rangle$ represents the contribution to the probability of obtaining the measurement result b from a given component of Alice's statistical mixture. This factor also depends only on the absolute value of an amplitude γ. The ensemble from which Eve has to extract information consists of density matrices of Eq. (8) with the corresponding probability distribution w_b defined in Eq. (4).

To put an upper bound on the adversary's information about Bob's subsystem, we use the Holevo quantity of the described ensemble $\mathcal{E}_{\mathrm{RR}} = \left\{w_b, \hat{\eta}_{\mathrm{E}}^{(b)}\right\}_{b=0,1}$:

$$I(\mathrm{B};\mathrm{E}) \leq \chi\left(\mathcal{E}_{\mathrm{RR}}\right) = S\left(w_0\eta_{\mathrm{E}}^{(0)} + w_1\eta_{\mathrm{E}}^{(1)}\right) - w_0 S\left(\eta_{\mathrm{E}}^{(0)}\right) - w_1 S\left(\eta_{\mathrm{E}}^{(1)}\right). \tag{9}$$

Since we assume that the beam-splitting attack is the same for each of the signal pulses in a communication round, we work in the i.i.d. assumption, and the asymptotic secret key generation rate can be calculated according to the Devetak-Winter equation[56] for both error correction strategies

$$K_f^{(\mathrm{DR})} = \max_{\theta_1,\ldots,\theta_4} K p_{\checkmark}\left(I(\mathrm{A};\mathrm{B}) - I(\mathrm{A};\mathrm{E})\right), \quad K_f^{(\mathrm{RR})} = \max_{\theta_1,\ldots,\theta_4} K p_{\checkmark}\left(I(\mathrm{A};\mathrm{B}) - I(\mathrm{B};\mathrm{E})\right), \tag{10}$$

where K is the initial rate of the random bits generation and transmitting bit-encoding quantum states and maximum is taken over all post-selection parameters, while $I(\mathrm{A};\mathrm{B})$ is the mutual information shared between Alice and Bob. Information of the legitimate users is not defined by the error correction strategy and depends on the discrepancy between Alice's and Bob's bit strings and on a particular choice of an error correction code.

Practically, legitimate users should be able to switch between direct and reverse reconciliation regimes. For particular observed parameters, namely, additional losses in the fiber line, preparation noise and detection noise, one of the strategies will be optimal, i. e., proving highest key generation rate. Thus, the the final key generation rate K_f is maximum among the resulting key rates produced by reverse and direct reconciliation

$$K_f = \max\left(K_f^{(\mathrm{DR})}, K_f^{(\mathrm{RR})}\right). \tag{11}$$

Numerical estimations

Preparation noise influence

To demonstrate the performance of the QKD based on the loss control in the presence of the trusted preparation noise, we make numerical estimations of the key generation rate given by Eq. (11). For illustrative purposes, we consider a particular form of the trusted preparation noise, namely, a Gaussian distribution over the intensities on the Alice's side.

A Gaussian distribution implies a non-zero probability for negative values of a random variable. Intensity, by its definition, is always non-negative. To avoid the effect of the contribution from the non-existing negative values of the intensity, we consider a truncated normal distribution. For positive values of the intensity, it has the standard form of a normal distribution, while for negative values, it should be set equal to zero. For the bit value a, it can be written as

$$\mathcal{M}_a\left(|\gamma|^2\right) = \frac{1}{\sqrt{2\pi\sigma_a^2}} \exp\left(-\frac{\left(|\gamma|^2 - \mu_a\right)^2}{2\sigma_a^2}\right) \cdot \frac{2}{1 - \mathrm{erf}\left(-\mu_a/(\sigma_a\sqrt{2})\right)}, \tag{12}$$

where μ_a is the average intensity for the bit a, σ_a is the variance parameter and $\mathrm{erf}(\cdot)$ is the error function.

Figure 2 represents the experimentally obtained histogram from the already installed lithium niobate modulator and its Gaussian approximation. The experimental distribution agrees well with the chosen approximation except for the fact that the tails of experimental distributions seem to demonstrate a polynomial rather than exponential behavior. Such heavy tails can be induced by the instability of the operating point in the modulator and the electrical noise in the modulating signal. Yet, the truncated normal distribution is an appropriate starting point for further illustrations. In a particular QKD based on the loss control realization, one has to consider all specifics of the observed intensity distribution.

The following calculations are conducted for fixed parameters of the optical line's length and mean values of signals' intensities for both logical bits. Namely, we consider $\mu_0 = 2150$ and $\mu_1 = 2450$ for the mean values and a quiet short transmission line of the length $D_{\mathrm{AB}} = 10$ km. The final normalized key generation rate K_f/K is

maximized over all post selection parameters $\theta_{1,2,3,4}$. For the reminder of the subsection, we elaborate only on trusted preparation noise, while we consider Bob's detector as an ideal device.

Figure 4 shows the results of numerical optimization of the key rate for different values of the artificial leakage, $r_{\mathrm{E}} = 10\%, 20\%$, and 30%. The data is presented in the form of counter plot accounting for two variances characterizing preparation noise levels for each of the logical bits. Each curve corresponds to a fixed value of the final key generation rate. The choice of optimal error correction strategy is related to the noise's variances. Grey areas show those values of the noise level where direct reconciliation is optimal, while reverse reconciliation provides higher key rate in the white areas. In the SI Note 4, one can find additional graphs presenting our numerical results for DR and RR individually. As Fig. 4 demonstrates, the reverse reconciliation strategy is optimal until the preparation noise reaches a relatively high level. The result can be explained by the fact that we consider a noiseless optical channel which only introduces losses and, thus, the optimal eavesdropping position (in both reconciliation scenarios) is located right after Alice. Thus, the eavesdropper's information about Alice's string should be expected to be higher than the information about Bob's one. Nevertheless, direct reconciliation becomes more beneficial for the legitimate users when the preparation noise becomes significantly high. Moreover, it is important to note that reverse reconciliation advantage should not be treated as a general rule – for instance, in the case of DI QKD direct reconciliation tends to provide better results[57,58].

A general trend which can be observed in each of the plots provided in Fig. 4 is the significant key rate reduction which takes place when we transit from the case of noiseless states ($\sigma_0, \sigma_1 = 0$) to the case of significantly noisy states ($\sigma_0, \sigma_1 \gtrapprox 50$). Our experimental data with $\sigma_0, \sigma_1 = 11$ lies in the area of low noises shown in the left bottom corner of each plot. The increase of the noise's variance from 11 to 100 ($\sigma_0, \sigma_1 \approx 100$) reduces the key generation rate by more than over half. Nevertheless, for the high leakage $r_{\mathrm{E}} = 30\%$, at the area of low noises we observe a positive impact of the preparation noise on the key rate. Hatching area highlights the region of the maximum key generation rate. Notably, on the Fig. 4c one can see that the area containing the maximum key generation rate is not convex. This takes place due to the fact that the depicted function has two point of local maximums, and each of them is located on one of the coordinate axis: $\{\sigma_0 = 0, \sigma_1 = 52\}$ and $\{\sigma_0 = 50, \sigma_1 = 0\}$. More details and additional visuals supporting the statement can be found in the SI Note 4.

The reasons for the observed key rate growth with the increase of the preparation noise is the choice of the mean intensities' values. Considered mean values, 2150 and 2450, correspond to a high level of distinguishability in the case of pure states. Only in case of low values of r_{E}, the overlap between states intercepted by Eve is significant. And preparation noise makes the initial coherent states less distinguishable and, thus, reduces the information available to the adversary. For the high eavesdropping leakage of 30%, we observe a beneficial trade-off between reduction of Eve's information and information of legitimate users with the increase of the preparation noise. While the work is devoted to the study of the trusted noises, i.e., noises occurring naturally from the system's hardware, the fact that for hight enough values of r_{E} a slight increase in σ_0, σ_1 leads to the increase in the secret key generation rate, shows that noisy preprocessing[57–59]—deliberate noise introduction—can be beneficial for the system.

Detection noise influence

While the trusted preparation noise changes the properties of quantum states sent by Alice and, thus, affect both Eve's and Bob's data, the trusted noise in detection equipment influences only Bob's subsystem. Trusted detection noise increases the discrepancy between Alice's and Bob's bit strings and at the same time decreases the correlations between Bob's and Eve's measurement results. Thus, the presence of the detection noise reduces

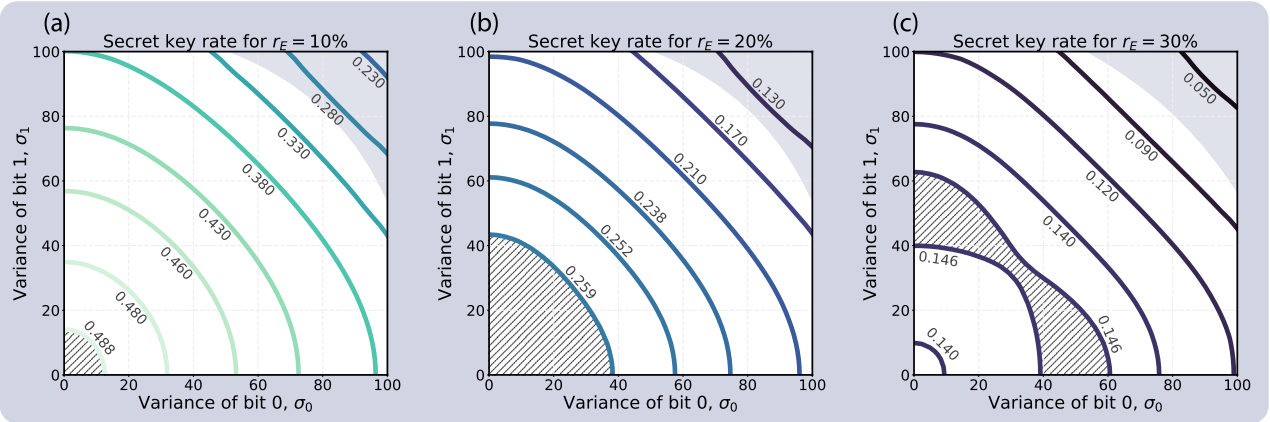

Fig. 4. Counter plot for the key rate in the presence of the trusted preparation noise in the absence of the detection noise. Key generation rate as a function of the preparation distribution variances of bits "0" and "1". Key rate is normalized to the initial bit rate K. Different values of the leakage r_{E} are considered: 10%, 20%, 30%. The length of the transmission line D_{AB} is 10 km. Values of average intensities μ_0 and μ_1 are 2150 and 2450, respectively. The gray areas of the plots comprises the values of σ_0 and σ_1 for which DR is optimal, the white areas correspond to the RR optimality. Hatching indicates the maximum key rate area.

the impact of Bob's postselection on the Eve's density matrix. All the effects associated with the detection noise are accounted for by the functions $f_{\checkmark}$ and f_b defined above.

As a framework for the noise detection, we use a simple Gaussian model as an approximation of all noises in detection devices. For the coefficients $\mathcal{D}_n(k)$ introduced in the Eq. (2), we consider truncated discrete Gaussian distribution, see details in SI Note 3,

$$\mathcal{D}_n(k) = \frac{1}{Z_n} \cdot \exp\left(-\frac{(n-k)^2}{2\Delta^2}\right), \tag{13}$$

where Δ is the real-valued parameter characterizing the noise level of the detector, and Z_n is the normalization factor defined by the condition $\sum_{k=0}^{+\infty} \mathcal{D}_n(k) = 1$. Here, the term 'truncated' is used, since all possible measurements result at the Bob's side are non-negative. For other properties and applications of the discrete Gaussian distributions see, for example, Ref.[60].

The motivation for the Gaussian model consideration lies in the electrical noises of Bob's detection device. Bob observes an electric signal converted from an incoming optical pulse through the interaction with the detector's medium. Electrical circuits always contain thermal noise. For a standard detector's electrical bandwidth $f = 500$ MHz and room temperature $T = 300$ K, we get that the bandwidth is much lower than the temperature $hf \ll kT$, where h and k are the Plank and Boltzmann constants, respectively. In these conditions, the thermal noise follows the Gaussian behavior. Consequently, the electrical signal from the optical pulse goes together with the Gaussian component, which blurs the final probability distribution of measurement results. In other conditions, the noise can follow different behavior types, and thus, the model should be adjusted accordingly.

Figure 5 presents the results of numerical optimization of the normalized key rate in the presence of the trusted detection and preparation noise. The optimization was conducted over four postselection parameters θ_{1-4}, while the intensities of the signals $\mu_0 = 2150$ and $\mu_1 = 2450$ were fixed. Different subplots correspond to different error correction strategies: DR and RR. The final key rate appears to be strictly monotonous with respect to the detection noise parameter Δ. The case of $\Delta = 0$ stands for the ideal photon number measurement on Bob's side. When the detection noise is equal to the 2% of the average signal's intensity, the key generation rate drops by three times comparing to the ideal measurement. These numerical results indicate that additional detection noise only reduces the setup performance for the QKD based on the loss control. Also, we observe that the detection noise reduces the positive impact of the preparation noise on key generation rate. In the loss control quantum cryptography implementation, the optimal error correction strategy (direct or reverse reconciliation) will depend on a particular setup of the line and the available precision of the leakage detection.

Figure 6 shows the dependence of the asymptotic key generation rate in the loss control-based QKD on the communication distance. The key generation rate decreases to the order of magnitude with the considered increase of the distance. Figure 6 also depicts the upper-bounds on the key generation rate in BB84 and exemplary CV-QKD. The upper-bound for BB84 is obtained according to Ref. [40]. For details on the key rate upper-bound in CV-QKD, see SI Note 5. As a result, the loss control-based QKD mostly outperforms BB84 and CV-QKD for the considered set of parameters. For the preparation noise less than $\sigma \leq 11$, the loss control-based QKD provides a more than 5 times higher key generation rate than upper-bound on CV-QKD.

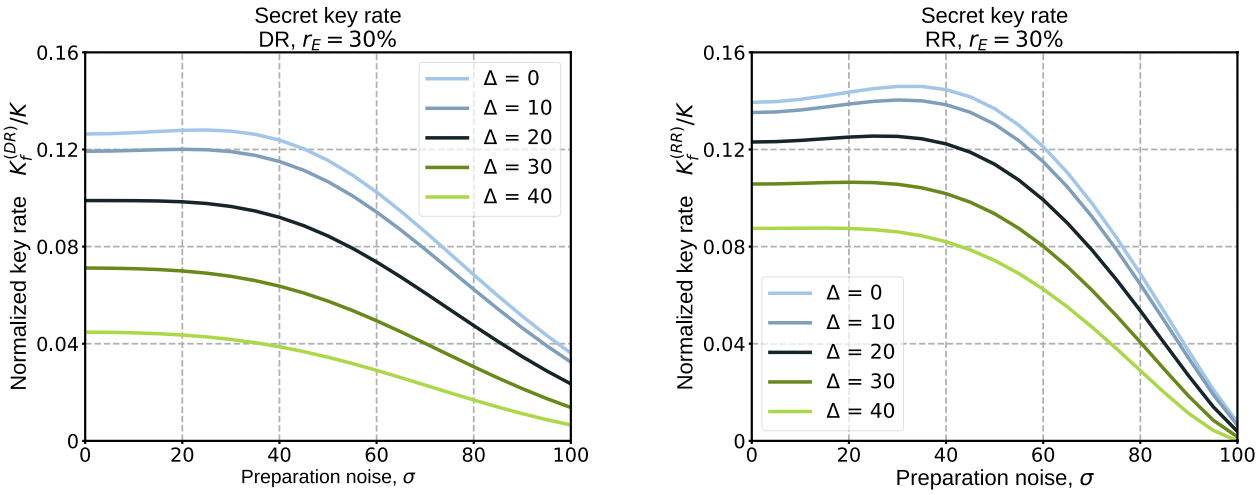

Fig. 5. Secret key rate as a function of the preparation noise's variance σ for different values of the detection noise parameter Δ. Preparation noise parameters are taken equal $\sigma_0 = \sigma_1 \equiv \sigma$. Average values of intensities are $\mu_0 = 2150$, $\mu_1 = 2450$. Leakage is $r_{\mathrm{E}} = 30\%$. Length of the fiber line $D_{\mathrm{AB}} = 10$ km.

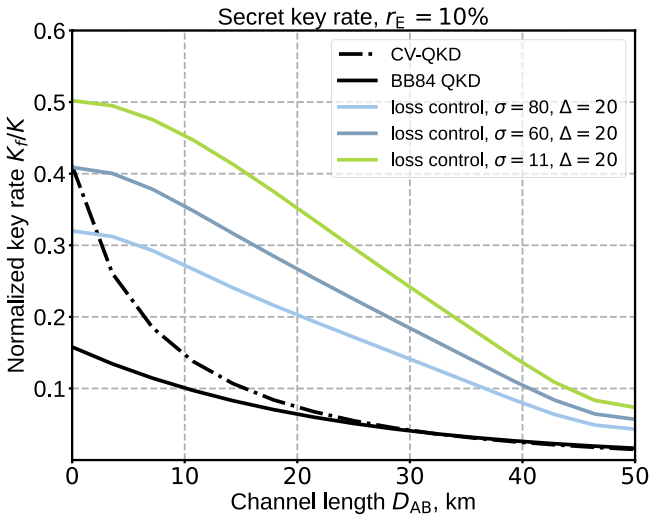

Fig. 6. Secret key generation rate as a function of distance for different QKD protocols. The value of the leakage artificially created by an eavesdropper is fixed $r_E = 10\%$ for all the considered protocols to compare their performance for the same type of quantum channel. The dashed black line represents the results obtained for CV-QKD, the solid black line corresponds to BB84 QKD and the three coloured lines correspond to the loss control-based QKD with different noise levels.

Discussion

For the security analysis of device-dependent cryptography, it is required to thoroughly characterize incorporated devices, noise sources, and possible information leakages. On the sender's side, the laser and electro-optical modulator introduce significant noise into the prepared bit-encoding quantum states. Thus, the output states are mixed. In our work, we considered the noise as trusted for the framework of the loss control QKD approach. We studied the influence of the trusted preparation noise on the key generation process in the case of the short 10 km fiber line. Firstly, trusted preparation noise induces correlations between Eve's and Bob's subsystems: Bob's postselection modifies Eve's density matrix. Secondly, trusted preparation noise can potentially introduce a positive impact on the key generation rate for both direct and reverse reconciliation scenarios. For the small values of preparation noise level and high eavesdropping leakage, the resulting key rate appeared to be higher than in the case of noiseless states. It is important to note that we do not claim to provide full security proof for the considered protocol, but rather consider a set of powerful eavesdropping attacks on it. We assume Eve does not perform coherent attacks.

Furthermore, we considered the effects of trusted detection noise in both error correction scenarios. As a model of the detection noise, we took the discrete Gaussian distribution. Detection noise demonstrates only a negative impact on the key rate despite the reduction of Eve-Bob correlations. Detection noise also blurs the effect of the key rate increase caused by the preparation noise.

In practical device-dependent QKD implementations, legitimate users should base the security analysis on particular observed statistics from the modulator. It means that before starting the key distribution procedure, Alice and Bob should pre-measure noises in the incorporated modulator and detector as shown in Fig. 2. To validate the applicability of the trusted noise approach, legitimate users must remeasure and recalibrate the noise parameters before each quantum communication session.

Notably, the loss control approach does not rely on the computational assumptions opposing classical or post-quantum cryptography. Our set of assumptions builds on the physical principles of incorporated devices, especially of the fiber channel. Eve's capabilities on extracting information from the scattered losses can increase in future and, thus, can potentially violate the set of assumptions utilized in the loss control-based QKD. In this case, the analysis conducted in loss control should be modified properly[40]. Yet, an eavesdropper with future-developed technologies, who will manage to violate the current set of assumptions, will not be able to compromise the secrecy of already distributed keys since these technologies will occur after the protocol's execution. As a result, the loss control approach possesses the desired everlasting security quality—the crucial advantage of quantum protocols over classical and post-quantum ones[61].

Data availibility

All data generated or analysed during this study are included in this published article (and its Supplementary Information files).

Received: 9 February 2025; Accepted: 26 August 2025
Published online: 02 October 2025

References

1. Diamanti, E., Lo, H.-K., Qi, B. & Yan, Z. Practical challenges in quantum key distribution. *NPJ Quantum Inf.* **2**, 1–12 (2016).
2. Pirandola, S. et al. Advances in quantum cryptography. *J. Opt. Soc. Am.* **12**, 1012–1236 (2020).
3. Portman, C. & Renner, R. Security in quantum cryptography. *Rev. Mod. Phys.* **94**, 025008 (2022).
4. Renner, R. & Wolf, R. Quantum advantage in cryptography. *AIAA J.* **61**, 1895–1910 (2023).
5. Zhou, L. & Sheng, Y.-B. One-step device-independent quantum secure direct communication. *Sci. China: Phys. Mech. Astron.* **65**, 250311 (2022).
6. Ying, J.-W., Zhou, L., Zhong, W. & Sheng, Y.-B. Measurement-device-independent one-step quantum secure direct communication. *Chin. Phys. B* **31**, 120303 (2022).
7. Sheng, Y.-B., Zhou, L. & Long, G.-L. One-step quantum secure direct communication. *Sci. Bull.* **67**, 367–374 (2022).
8. Zhou, L., Xu, B.-W., Zhong, W. & Sheng, Y.-B. Device-independent quantum secure direct communication with single-photon sources. *Phys. Rev. Appl.* **19**, 014036 (2023).
9. Yang, Y. et al. A 300-km fully-connected quantum secure direct communication network. *Sci. Bull.* **70**, 1445–1451 (2025).
10. Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **560**, 7–11 (2014).
11. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, 661–663 (1991).
12. Stucki, D., Brunner, N., Gisin, N., Scarani, V. & Zbinden, H. Fast and simple one-way quantum key distribution. *Appl. Phys. Lett.* **87**, 194108 (2005).
13. Braunstein, S. L. & Pirandola, S. Side-channel-free quantum key distribution. *Phys. Rev. Lett.* **108**, 130502 (2012).
14. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).
15. Pironio, S. et al. Device-independent quantum key distribution secure against collective attacks. *New J. Phys.* **11**, 045021 (2009).
16. Vazirani, U. & Vidick, T. Fully device independent quantum key distribution. *Commun. ACM* **62**, 133 (2019).
17. Félix, S., Gisin, N., Stefanov, A. & Zbinden, H. Faint laser quantum key distribution: Eavesdropping exploiting multiphoton pulses. *J. Mod. Opt.* **48**, 2009–2021 (2001).
18. Scarani, V. & Kurtsiefer, C. The black paper of quantum cryptography: Real implementation problems. *Theor. Comput. Sci.* **560**, 27–32 (2014).
19. Makarov, V., Anisimov, A. & Skaar, J. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Phys. Rev. A* **74**, 022313 (2006).
20. Lydersen, L. et al. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photonics* **4**, 686–689 (2010).
21. Babukhin, D. V. & Sych, D. V. Joint eavesdropping on the BB84 decoy state protocol with an arbitrary passive light-source side channel. *Lobachevskii J. Math.* **45**, 2454–2465 (2024).
22. Nagata, H. & Ichikawa, J. Progress and problems in reliability of ti: $LiNbO_3$ optical intensity modulators. *Opt. Eng.* **34**, 3284–3293 (1995).
23. Petrov, A., Tronev, A., Agruzov, P., Shamrai, A. & Sorotsky, V. System for stabilizing an operating point of a remote electro-optical modulator powered by optical fiber. *Electronics* **9**, 1861 (2020).
24. Yang, H. et al. Operating point control method for the Mach-Zehnder modulator in a phase-shift laser range finder. *Opt. Express* **32**, 19881–19894 (2024).
25. Salvestrini, J. P., Guilbert, L., Fontana, M., Abarkan, M. & Gille, S. Analysis and control of the DC drift in $LiNbO_3$-based Mach-Zehnder modulators. *J. Light. Technol.* **29**, 1522–1534 (2011).
26. Sosunov, A., Ponomarev, R., Zhuravlev, A., Mushinsky, S. & Kuneva, M. Reduction in DC-drift in $LiNbO_3$-based electro-optical modulator. *Photonics* **8**, 571 (2021).
27. Wang, M. et al. Thin-film lithium-niobate modulator with a combined passive bias and thermo-optic bias. *Opt. Express* **30**, 39706–39715 (2022).
28. Weedbrook, C., Pirandola, S., Lloyd, S. & Ralph, T. C. Quantum cryptography approaching the classical limit. *Phys. Rev. Lett.* **105**, 110501 (2010).
29. Weedbrook, C., Pirandola, S. & Ralph, T. C. Continuous-variable quantum key distribution using thermal states. *Phys. Rev. A* **86**, 022318 (2012).
30. Weedbrook, C., Ottaviani, C. & Pirandola, S. Two-way quantum cryptography at different wavelengths. *Phys. Rev. A* **89**, 012309 (2014).
31. Yamano, S., Matsuura, T., Kuramochi, Y., Sasaki, T. & Koashi, M. Experimental demonstration of scalable quantum key distribution over a thousand kilometers. arXiv:https://arxiv.org/abs/2305.17684 (2023).
32. Filip, R. Continuous-variable quantum key distribution with noisy coherent states. *Phys. Rev. A* **77**, 022310 (2008).
33. Usenko, V. C. & Filip, R. Feasibility of continuous-variable quantum key distribution with noisy coherent states. *Phys. Rev. A* **81**, 022318 (2010).
34. Usenko, V. C. & Filip, R. Trusted noise in continuous-variable quantum key distribution: A threat and a defense. *Entropy* **18**, 20 (2016).
35. Lodewyck, J. et al. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Phys. Rev. A* **76**, 042305 (2007).
36. Lin, J. & Lütkenhaus, N. Trusted detector noise analysis for discrete modulation schemes of continuous-variable quantum key distribution. *Phys. Rev. Appl.* **14**, 064030 (2020).
37. Weedbrook, C. et al. Gaussian quantum information. *Phys. Mod. Phys.* **84**, 621–669 (2012).
38. Laudenbach, F. et al. Continuous-variable quantum key distribution with Gaussian modulation—The theory of practical implementations. *Adv. Quantum Technol.* **1**, 1800011 (2018).
39. Kirsanov, N. et al. Forty thousand kilometers under quantum protection. *Sci. Rep.* **13**, 8756 (2023).
40. Kodukhov, A. D. et al. Boosting quantum key distribution via the end-to-end loss control. *Cryptography* **7**, 38 (2023).
41. Kirsanov, N. et al. Loss control-based key distribution under quantum protection. *Entropy* **26**, 437 (2024).
42. Aliev, A. *et al.* Experimental demonstration of scalable quantum key distribution over a thousand kilometers. arXiv:https://arxiv.org/abs/2306.04599 (2023).
43. 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* **23**, 6390 (2023).
44. Yarovikov, M., Smirnov, A., Aliev, A. & Strizhak, D. Highly sensitive optical time-domain reflectometry: Detecting 0.01 dB leakage over 1000 km for classical and quantum communication. *Sensors* **25**, 1407 (2025).
45. Statiev, V. et al. In-field quantum-protected control-based key distribution with a lossy urban fiber link. *Quantum Rep.* **7**, 16 (2025).
46. Derkach, I., Usenko, V. C. & Filip, R. Continuous-variable quantum key distribution with a leakage from state preparation. *Phys. Rev. A* **96**, 062309 (2017).
47. Renner, R., Gisin, N. & Kraus, B. Information-theoretic security proof for quantum-key-distribution protocols. *Phys. Rev. A* **72**, 012332 (2005).
48. García-Patrón, R. & Cerf, N. J. Continuous-variable quantum key distribution protocols over noisy channels. *Phys. Rev. Lett.* **102**, 130501 (2009).
49. Laudenbach, F. & Pacher, C. Analysis of the trusted device scenario in continuous-variable quantum key distribution. *Adv. Quantum Technol.* **2**, 1900055 (2019).

50. Lütkenhaus, N. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A* **61**, 052304 (2000).
51. Acin, A., Gisin, N. & Scarani, V. Coherent pulse implementations of quantum cryptography protocols resistant to photon number splitting attacks. *Phys. Rev. A* **69**, 012309 (2004).
52. Eguchi, M. & Tsuji, Y. Influence of reflected radiation waves caused by large mode field and large refractive index mismatches on splice loss evaluation between elliptical-hole lattice core holey fibers and conventional fibers. *J. Opt. Soc. Am. B* **30**, 410–420 (2013).
53. Thapa, R. et al. Low-loss, robust fusion splicing of silica to chalcogenide fiber for integrated mid-infrared laser technology development. *Opt. Lett.* **40**, 5074–5077 (2015).
54. Hu, L. & Yuan, C. Analysis of splice loss of single-mode optical fiber in the high altitude environment. *Coatings* **11**, 876 (2021).
55. Holevo, A. S. Bounds for the quantity of information transmitted by a quantum communication channel. *Probl. Peredachi Inf.* **9**, 3–11 (1973).
56. Devetak, I. & Winter, A. Distillation of secret key and entanglement from quantum states. *Proc. R. Soc. A: Math. Phys. Eng. Sci.* **461**, 207–235 (2005).
57. Ho, Melvyn et al. Noisy preprocessing facilitates a photonic realization of device-independent quantum key distribution. *Phys. Rev. Lett.* **124**, 230502 (2020).
58. Zhang, Qi. et al. Device-independent quantum secret sharing with noise preprocessing and postselection. *Phys. Rev. A* **110**, 042403 (2024).
59. Zhang, Qi. et al. Device-independent quantum secret sharing with advanced random key generation basis. *Phys. Rev. A* **111**, 012603 (2025).
60. Canonne, C. L., Kamath, G. & Steinke, T. The discrete Gaussian for differential privacy. *Adv. Neural Inf. Process. Syst.* **33**, 15676–15688 (2020).
61. Unruh, D. Everlasting multi-party computation. *CRYPTO* **2013**, 380–397 (2013).

Acknowledgements

The work was supported by Terra Quantum AG. The authors are delighted to thank Vladimir Semenov, Dmitriy Kozluk and Vladlen Statiev for the illuminating discussions.

Author contributions

V.P., A.K., M.P. and V.V. conceptualized the work; V.V. supervised the work; V.P., A.K., A.S., V.V. carried out calculations, and V.Z. carried out measurements; all authors discussed the results; V.P., A.K. and V.V. wrote the manuscript and all authors discussed it.

Declarations

Conflict of interest

The authors declare that they have no conflict of interest.

Additional information

Supplementary Information The online version contains supplementary material available at https://doi.org/10.1038/s41598-025-17662-2.

Correspondence and requests for materials should be addressed to V.V.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.