Forty Thousand Kilometers Under Quantum Protection

Security

By Terra Quantum AG
terraquantum.swiss

2023

Forty Thousand Kilometers Under Quantum Protection

N. S. Kirsanov, V. A. Pastushenko, A. D. Kodukhov, M. V. Yarovikov, A. B. Sagingalieva, D. A. Kronberg, M. Pflitsch, and V. M. Vinokur

Terra Quantum AG

The quantum key distribution (QKD) is a revolutionary cryptography response to the rapidly growing cyberattacks threat posed by quantum computing. Yet, the roadblock limiting the vast expanse of secure quantum communication is the exponential decay of the transmitted quantum signal with the distance. Today's quantum cryptography is trying to solve this problem by focusing on quantum repeaters. However, efficient and secure quantum repetition at sufficient distances is still far beyond modern technology. Here, we shift the paradigm and build the long-distance security of the QKD upon the quantum foundations of the Second Law of Thermodynamics and end-to-end physical oversight over the transmitted optical quantum states. Our approach enables us to realize quantum states' repetition by optical amplifiers keeping states' wave properties and phase coherence. The unprecedented secure distance range attainable through our approach opens the door for the development of scalable quantum-resistant communication networks of the future.

The quantum threat to secure communications makes top headlines and Niagara Falls of reviews and research explaining how quantum computers using, for example, Shor's algorithm [1], devalue the existing cryptographic schemes. Remarkably, the same advances in quantum physics that have created this quantum threat enable solutions for quantum security. The core of the novel quantum technology protecting the data transmission is known as quantum key distribution (QKD) [2–6]. However, existing QKD protocols appear to be efficient only at relatively short distances [7,8]. A general restriction is the Pirandola-Laurenza-Ottaviani-Banch (PLOB) bound [9], according to which the secret key rate decreases exponentially with the channel length. The simplest approach to dealing with this issue is to use the trusted reproduction nodes along the transmission line [10–12], which is a compromise to the overall security. The alternative solution is the utilization of quantum repeaters [13–28] which eliminates the need for trust in the intermediate relay. However, since quantum repetition manipulates fragile entangled states, its implementation at a long scale remains beyond state-of-the-art technologies. Here, contemplating the physical nature of the quantum states' transmission, we lift the PLOB bound by using restrictions of quantum thermodynamics and the end-to-end physical control over losses in the optical quantum channel. We shift the quantum cryptography paradigm building on the same quantum considerations that provide the foundations of the Second Law of Thermodynamics. Our approach ensures signal repetition through optical amplification, presumes no trust at the intermediate channel points, and expands the secure transmission range to global distances.

General idea

Conventionally, the eavesdropper (Eve) is seen as capable of exploiting all the losses from the transmission channel, irrespective of their origin. This puts a strong restriction on the number of photons in the transmitted quantum states, which significantly complicates their repetition. However, upon close quantum mechanical examination, this presupposition appears unrealistic. In reality, the majority of losses in optical fibers occur due to the light scattering on the quenched disorder and are distributed homogeneously along the line (hereinafter, we will be referring to such losses as to natural losses). In a single mode silica fiber's 1530–1565 nm wavelength window, the standard for modern telecommunications, these losses amount to approximately 4×10^{-5} of the passing signal's intensity per meter.

We describe the information dynamics of the randomized signal transmitted over an optical channel. This consideration is carried out analogously to consideration of the Second Law of Thermodynamics, i.e., the dynamics of entropy, through the lens of the microscopic quantum mechanical laws [29–31]. Had the system been isolated, its entropy would not decrease, i.e., Eve would not be able to obtain any information. In the presence of natural losses, the system can no longer be regarded as isolated, and thus, the eavesdropper gets an opportunity to decrease the system's entropy in analogy with the quantum Maxwell demon. However, in order to glean information from the scattering losses of relatively weak signals that we employ for our approach, Eve has to use quantum detection devices spanning an unfeasible length of optical fiber, see Supplementary Note 1. That is why one concludes that in this weak signal regime, Eve is unable to effectively collect and exploit natural losses.

Losses other than natural ones can, in turn, be physically controlled. We propose a technique of physical line control (line tomography) implying that legitimate users detect local interventions by comparing the constantly updated tomogram of the line with the initial one, knowingly obtained in the absence of Eve. Line tomography involves sending the high-frequency test light pulses and analyzing their reflected (via the technique known as the time-domain reflectometry [32]) and the transmitted components. The coupling of photons to any eavesdropping system is impossible without modifying the fiber medium, which in turn inevitably changes the line tomogram. Unable to perform such radical interventions unnoticed, Eve is thus restricted to introducing small local leakages, which are precisely measured by the users. This implicates the possibility of employing the information-carrying light states containing the numbers of photons that are sufficient to repeat the states through optical amplification yet not enough to be easily eavesdropped on. Utilizing a cascade of accessible optical amplifiers to counteract the degradation of signals over extensive distances, as opposed to the employment of quantum repeaters [13–28], enables global transmission and high key distribution rates. It is important to note that these optical amplifiers should not be viewed as trusted nodes, as the integrity of the transmission scheme is maintained through end-to-end control by legitimate users, and there is no recourse to the form of classical data.

We showcase our approach via a prepare-and-measure QKD protocol utilizing non-orthogonal coherent photonic states $|\gamma_0\rangle$ and $|\gamma_1\rangle$ for encoding 0 and 1 bits. In the protocol's framework, our approach

means restricting the fraction of photons leaked to Eve, r_E, to ensure that the leaked states $|\sqrt{r_E}\gamma_0\rangle$ and $|\sqrt{r_E}\gamma_1\rangle$ sufficiently overlap, i.e., $\left\langle \sqrt{r_E}\gamma_0 \middle| \sqrt{r_E}\gamma_1 \right\rangle \sim 1$ (these states become mixed if the transmission channel includes amplifiers, but for now we ignore this fact for the sake of simplicity). Eve cannot by any means—except by completely blocking part of the signal pulses [33] but this is prevented by the line tomography—extract more information than the Holevo quantity χ_E [34] which tends to zero when $\left\langle \sqrt{r_E}\gamma_0 \middle| \sqrt{r_E}\gamma_1 \right\rangle \to 1$. The users monitor the value of r_E and adapt the parameters of $|\gamma_0\rangle$ and $|\gamma_1\rangle$ to ensure that the intercepted pulses are poorly distinguishable.

Thus, we overcome the PLOB bound by what can be called the "channel device-dependent" approach. This approach is no less physically justified as a traditional device-dependent scenario where the eavesdropper is assumed not to be able to substitute some of the equipment at the sender and receiver side. Hence, there are no compromises in security that allow us to increase the secret key distribution distance, only higher device dependence, with correct channel work ensured by tomography methods.

Protocol description

We put forth an exemplary protocol based on our physical control approach. Let the legitimate users, the sender, Alice, and the receiver, Bob, be connected via a classical authenticated communication channel and optical line serving as a quantum channel. The protocol is designed as follows:

0. *Initial preparation*—Alice and Bob carry out initial line tomography to determine the natural losses that Eve cannot exploit. At this and only this preliminary step, the legitimate users must be certain that Eve has no influence on the line. The users share the tomogram via the classical channel.

1. Alice and Bob perform the physical loss control over the line and, through comparison with the initial line tomogram, infer the fraction r_E of the signal possibly seized and exploited by Eve. The users also localize the points of Eve's intervention. To update the line tomogram, users exchange information via the classical channel. If the stolen fraction grows too large so that the evaluated legitimate users' information advantage over Eve disappears—the analytical estimate for this advantage is provided below—the transmission is terminated.

2. Using a random number generator, Alice produces a bit sequence of the length L. Alice ciphers her bit sequence into a series of L coherent light pulses, which she sends to Bob. The bits 0 and 1 are encoded into coherent states $|\gamma_0\rangle$ and $|\gamma_1\rangle$ respectively. Their parameters are optimized based on the known fraction of the signal seized by Eve r_E and Eve's position in the line. The optimal parameters correspond to the maximum key distribution rate at given losses in the channel, the analytical relation for which is presented below. The optimal parameters are considered to be known to Alice and Bob and also to Eve.

3. The signals are amplified by the cascade of optical amplifiers installed along the optical line, possibly equidistantly. Bob receives the signals and measures them.

4. Alice and Bob perform the postselection, i.e., they discard the positions corresponding to inconclusive measurement outcomes. The postselection criteria are defined by the set of parameters, which are optimally calculated by the users.

5. The users perform error correction. The procedure can be done with well-known classical methods, e.g., linear codes [35–37], or with methods designed specifically for the QKD, such as the Cascade protocol [38–40].

6. The users estimate Eve's information obtained at the previous stages and perform the privacy amplification procedure to produce a shorter key (e.g., using the universal hashing method [41]) on which Eve has none or negligibly small information.

Alice and Bob repeat steps from 1 to 6 until satisfied with the total shared key length. The particular way of encoding bits 0 and 1 into the parameters of coherent pulses $|\gamma_0\rangle$ and $|\gamma_1\rangle$ may vary. For illustrative purposes, we concentrate on the two simplest and straightforward schemes, viz. encoding bits into pulses with (a) different photon numbers, $|\gamma_0|^2 \neq |\gamma_1|^2$, and phase randomization [42–44], and (b) same photon numbers, $|\gamma_0|^2 = |\gamma_1|^2$, and phases different by π. In both encoding schemes, Alice varies $|\gamma_0|^2$ and $|\gamma_1|^2$.

More sophisticated encoding schemes, for instance, schemes leveraging the pulses' shapes, make exploiting the natural scattering losses even more unsolvable. To complicate the problem further, the cable design may include an encapsulating layer of metal of heavily doped silica, transforming the scattering radiation into heat under the control of the users; see Supplementary Note 2 for details.

Protocol security

Here, we delve into the security of the described protocol, by building upon the following:

1. Alice and Bob each generate random numbers that Eve cannot predict.

2. Other from the transmission channel—which is a fiber line with the embedded optical amplifiers—and the classical authenticated channel, users' equipment is isolated from Eve.

3. Eve cannot effectively collect and exploit natural losses from the transmission channel. To eavesdrop on the signal, Eve must introduce new artificial local leakages. Eve can also use the local leakages on the original fiber discontinuities, such as bends or connections.

4. The transmission line between Alice and Bob is characterized by the initial line tomogram. All losses constituting deviations from the initial tomogram are attributed to Eve.

5. Eve is bound to the beam-splitting attack: she may seize some fraction of the signal at any point of the optical line.

Attacks that deviate from the beam-splitting attack necessitate a significant alteration of the line tomogram, in which case the protocol should be terminated; as such, we will not delve into them here. We will refer to the point of Eve's intrusion into the line as the "beam splitter" and assume that any reflection back towards Alice from this point is insignificant. As our analysis will demonstrate, the protocol's efficiency is contingent on Eve's placement along the line. For the sake of simplicity, we will not examine scenarios in which Eve intercepts from multiple points along the line. However, with some overhead, this scenario can be reduced to a situation in which Eve is effectively positioned at the single worst spot (for the users) among all of the locations from which she intercepts the light.

To evaluate the protocol's security, we describe the evolution of Alice's, Bob's, and Eve's quantum systems and quantify the information available to different parties. We derive an analytical expression for the length of the final secure key L_f, which represents the users' informational advantage over Eve given the fixed value of r_E and the distance between Alice and Eve D_{AE}. This expression depends on the encoding and postselection parameters and should be maximized by the users to determine the parameters' optimal values. The condition $L_f/L > 0$ for the chosen parameters ensures successful secret key generation [45].

At the beginning of the protocol, Alice encodes the logical bits into the coherent states with the different complex amplitudes, $0 \to |\gamma_0\rangle$, $1 \to |\gamma_1\rangle$. In the photon number encoding scheme, the pulses are different

in the average numbers of photons $|\gamma_0|^2$ and $|\gamma_1|^2$, while the phase of each pulse is random. The photon number measurement at Bob's end is formalized in terms of the projective operators:

$$\hat{E}_0 = \sum_{k=\mu-\theta_3}^{\mu-\theta_1} |k\rangle\langle k|\,,\ \hat{E}_1 = \sum_{k=\mu+\theta_2}^{\mu+\theta_4} |k\rangle\langle k|\,,\ \hat{E}_{\text{fail}} = \hat{\mathbb{1}} - \hat{E}_0 - \hat{E}_1, \tag{1a}$$

where $\hat{E}_0$, $\hat{E}_1$ and $\hat{E}_{\text{fail}}$ correspond to 0, 1, and inconclusive—meaning that this result should be later discarded—outcomes respectively, $|k\rangle$ is the Fock state of k photons, $\hat{\mathbb{1}}$ is the identity operator, $\mu = \left(|\gamma_0|^2 + |\gamma_1|^2\right)/2$, and θ_{1-4} are the postselection parameters tuned by Bob depending on the proportion of the stolen signal. The photon numbers between $\mu - \theta_1$ and $\mu + \theta_2$ are difficult to relate to 0 or 1, while numbers below $\mu - \theta_3$ and above $\mu + \theta_4$ are associated with the information corruption: as we show in Supplementary Note 4, optical amplification imposes correlations between pulses received by Bob and Eve, and extreme photon numbers at Bob's end also constitute very distinguishable signals for Eve.

For the phase encoding (note that using this scheme requires that the optical fiber is phase-preserving), the pulses are characterized by the same average photon number, $|\gamma_0|^2 = |\gamma_1|^2$, but by different, although fixed, phases. For instance, the relative phase can be π, $\gamma_0 = -\gamma_1 = \gamma \in \mathbb{R}$, and then, to distinguish the pulses, Bob should perform homodyne measurement of the quadrature $\hat{q}$ corresponding to the real axis in the phase space:

$$\hat{E}_0 = \int_{\theta'_1}^{\theta'_2} dq\,|q\rangle\langle q|\,,\ \hat{E}_1 = \int_{-\theta'_2}^{-\theta'_1} dq\,|q\rangle\langle q|\,,\ \hat{E}_{\text{fail}} = \hat{\mathbb{1}} - \hat{E}_0 - \hat{E}_1, \tag{1b}$$

where $|q\rangle$ is the eigenstate of $\hat{q}$, and $\theta'_{1,2}$ play the same role as θ_{1-4} in the photon number encoding case. With this scheme, we deal only with two postselection parameters because probability distributions of measurement results for two pulses are symmetric with respect to $q = 0$.

For both encoding schemes, the operational values of $|\gamma_0|$, $|\gamma_1|$ and θ_{1-4} ($\theta'_{1,2}$) are determined via maximizing the analytical expression for the predicted length of the final secure key L_{f}, which, in turn, depends on the proportion of the stolen signal r_{E} and the distance between Alice and Eve D_{AE}. Correlations between the states at Eve's and Bob's disposal due to optical amplification drastically complicate the analytical description of states' evolution necessary for obtaining the expression for L_{f}. We provide such a description in Methods, while here we write the final state of the combined quantum system of Alice's random bit (A), the signal component seized by Eve (E), and Bob's memory device storing the measurement outcome (B) after the legitimate users discard invalid bits, i.e., conditional to the successful measurement outcome:

$$\hat{\rho}^{\text{f}}_{\text{ABE}} = \sum_{b=0,1}\sum_{a=0,1} \frac{1}{2p(\checkmark|a)} \int d^2\alpha\ P(\alpha, \sqrt{T_1}\gamma_a, G_1) \int d^2\beta\ \langle\beta|\,\hat{E}_b\,|\beta\rangle$$
$$\times\, P\left(\beta, \sqrt{(1-r_{\text{E}})T_2}\alpha, G_2\right) |a\rangle\langle a|_{\text{A}} \otimes |b\rangle\langle b|_{\text{B}} \otimes |\sqrt{r_{\text{E}}}\alpha\rangle\langle\sqrt{r_{\text{E}}}\alpha|_{\text{E}}\,, \tag{2}$$

where

$$P(\alpha, \gamma, G) = \frac{1}{\pi(G-1)} \exp\left(-\frac{|\alpha - \sqrt{G}\gamma|^2}{G-1}\right), \tag{3}$$

and integration operations are performed over the complex plane, i.e., $d^2\alpha \equiv d\text{Re}(\alpha)\, d\text{Im}(\alpha)$, $T_{1(2)}$ and $G_{1(2)}$ are, respectively, the transmission probability and amplification factor (the ratio of the output photon number to the input one of an amplification channel) of the effective loss and amplification channels equivalent to the cascade of amplifiers and losses before (after) Eve's beam splitter (these values depend on the distances between Alice and Eve, D_{AE}, between Alice and Bob, D_{AB}, and between neighboring amplifiers, d, see Eqs. (57–59) in Supplementary Note 3), $p(\checkmark|a)$ is the probability of conclusive result in the case that Alice sends bit $a = \{0, 1\}$ (the explicit form is given by Eqs. (12) and (13) in Methods).

In the case of photon number encoding, Alice randomizes the phase of each pulse. As a result, neither Bob nor Eve would know the phase φ of the incident pulse $|\gamma_a\rangle = \|\gamma_a|e^{i\varphi}\rangle$ which effectively means that the final state of the combined system is described by $\hat{\rho}^{\text{f}}_{\text{ABE}}$ from Eq. (2) averaged over φ (see Supplementary Note 4 for details):

$$\left\langle\hat{\rho}^{f}_{\text{ABE}}\right\rangle_{\varphi} = \sum_{b=0,1}\sum_{a=0,1} \frac{1}{2p(\checkmark|a)} \frac{1}{2\pi} \int_0^{2\pi} d\varphi \cdot \int d^2\alpha\ P(\alpha, \sqrt{T_1}|\gamma_a|e^{i\varphi}, G_1)$$
$$\times\, |a\rangle\langle a|_{\text{A}} \otimes |b\rangle\langle b|_{\text{B}} \otimes \left|\sqrt{r_{\text{E}}}\alpha\right\rangle\left\langle\sqrt{r_{\text{E}}}\alpha\right|_{\text{E}}$$
$$\times \int d^2\beta\ P\left(\beta, \sqrt{(1-r_{\text{E}})T_2}\alpha, G_2\right) \langle\beta|\hat{E}_b|\beta\rangle\,. \tag{4}$$

After the invalid bits are discarded, the information available to Eve about the bits kept by Alice (per bit) is given by

$$I(\text{A},\text{E}) = S(\text{A}) - S(\text{A}|\text{E}), \tag{5}$$

where $S(\text{X}) = -\text{tr}\left[\hat{\rho}_{\text{X}} \log_2 \hat{\rho}_{\text{X}}\right]$ is the quantum von Neumann entropy of system X (which is A, B, E, or their combinations, the corresponding density matrices are obtained from Eq. (2), or Eq. (4) if there is phase randomization, by taking partial traces), and $S(\text{Y}|\text{X}) = S(\text{XY}) - S(\text{X})$ is the conditional entropy. We calculate the upper bound of $I(\text{A},\text{E})$ differently in the cases of photon number and phase encoding. In the first case, we use the Holevo bound [34], see Supplementary Note 4. In the second case, we also rely on the concavity of relative entropy, see Supplementary Note 5.

By performing the error correction procedure, the legitimate users establish a shared bit sequence at the price of disclosing an additional error syndrome of the length $f \cdot S(\text{A}|\text{B})$, where $f \geq 1$ depends on the particular error correction code. As we do not intend to address any specific error correction method, we put $f = 1$ corresponding to Shannon's limit. After the procedure, Eve's information becomes $\tilde{I}(\text{A},\text{E}) = I(\text{A},\text{E}) + S(\text{A}|\text{B})$. To eradicate Eve's information about the shared bit sequence (raw key), Alice and Bob perform the privacy amplification procedure tailored precisely for the estimated information leakage due to the local line losses and error correction, see Methods. The length of the final key is

$$L_{\text{f}} = p_{\checkmark} L \cdot \left(S(\text{A}) - \tilde{I}(\text{A},\text{E})\right) = p_{\checkmark} L \cdot \left(S(\text{A}) - S(\text{A}|\text{B}) - I(\text{A},\text{E})\right), \tag{6}$$

where L is the number of originally generated random bits, and $p_{\checkmark} = \frac{1}{2}\sum_{a,b=0,1} p(b|a)$ is the proportion of bits that are not discarded at the postselection stage.

Taking L and L_{f} as the numbers of bits per unit of time, Eq. (6)—the explicit form of which can be obtained using Eqs. (1a or 1b), (2 or 4), and Eqs. (12, 13) from Methods—gives us the key distribution rate (or key rate for short) as a function of r_{E}, $|\gamma_0|$, $|\gamma_1|$ and θ_{1-4} (or $\theta'_{1,2}$). Implicitly, the equation also includes the distance between two neighboring amplifiers d and the distances between Alice and Bob, D_{AB}, and Alice and Eve, D_{AE}. As we specified above, the users obtain the optimal values of $|\gamma_0|$, $|\gamma_1|$ and θ_{1-4} (or $\theta'_{1,2}$) by maximizing this analytic formula for measured values of r_{E} and D_{AE}. To be able to distribute secret keys, the users have to possess an information advantage over Eve [45], which in our case is indicated by the positivity of the calculated L_{f}/L. If the evaluated L_{f}/L is not positive, the protocol should be terminated.

Numerical simulations

Figure 1 displays the results of our numerical simulations. We plot the optimum (over the signal and postselection parameters) of the normalized key rate L_{f}/L as a function of the proportion r_{E} for two different transmission distances: **a, b, c** $D_{\text{AB}} = 1000$ km, **d, e, f** $D_{\text{AB}} = 40,000$ km. The distance between the neighboring amplifiers $d = 50$ km. Plots **a, d** relate to the photon number encoding with different curves corresponding to different values of D_{AE}. Within the selected range of r_{E} we have $1 \gtrsim L_{\text{f}}/L \gtrsim 10^{-4}$; correspondingly, if the initial random number generation rate $L = 1$ Gbit/s, then 1 Gbit/s $\gtrsim L_{\text{f}} \gtrsim$ 100 Kbit/s. Notice that the

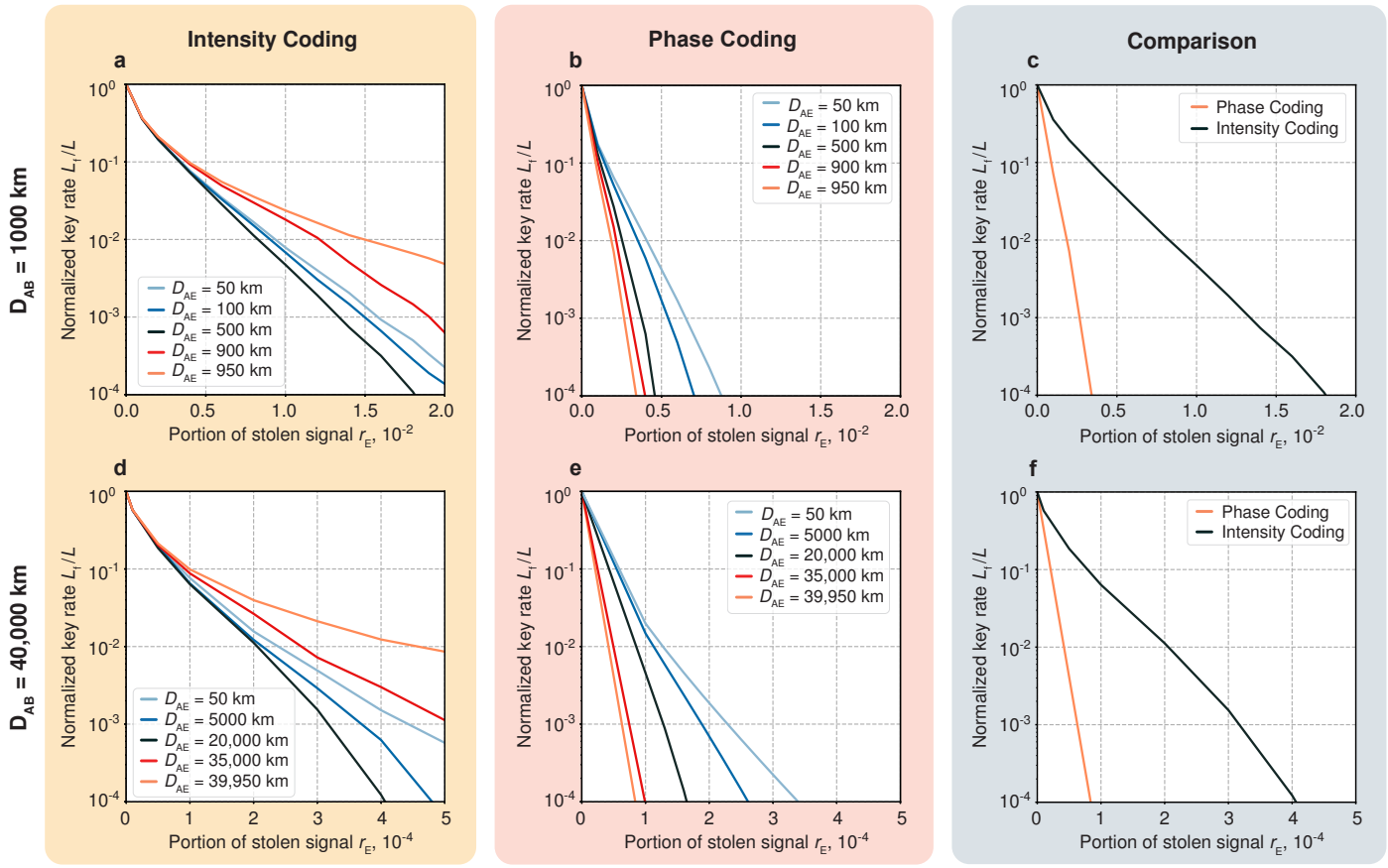

Figure 1 | **Numerical simulations of the protocol for different parameters and encoding schemes. a** The normalized key rate L_f/L as function of the proportion of stolen signal r_E for the photon number encoding and $D_{AB} = 1000\,\text{km}$. **b** The same for the phase encoding. **c** Comparison of the photon number and phase encoding schemes for $D_{AB} = 1000\,\text{km}$. **d** $L_f/L(r_E)$ for the photon number encoding and $D_{AB} = 40,000\,\text{km}$. **e** The same for the phase encoding. **f** Comparison for the distance $D_{AB} = 40,000\,\text{km}$. In all plots, the distance between neighboring amplifiers $d = 50\,\text{km}$. Different curves in each plot correspond to varying distances between Alice and Eve, D_{AE}. The dependence of L_f/L on D_{AE} is due to the fact that the amount of eavesdropped information is affected by correlations and noise imposed by optical amplifiers. The comparative plots **c, f** of two encoding schemes imply the respective worst conditions (with Eve positioned in her best way). In each point of every plot, the protocol's parameters—i.e., the photon numbers $|\gamma_{0,1}|^2$ and postselection parameters θ_{1-4} (or $\theta'_{1,2}$)—are numerically optimized for the fixed values of D_{AB}, D_{AE} and r_E with respect to L_f/L. Depending on r_E, the optimal photon numbers $|\gamma_0|^2$ and $|\gamma_1|^2$ vary from $0.8 \cdot 10^4$ to $3.0 \cdot 10^4$ photons in **a**, from $0.4 \cdot 10^3$ to $7.2 \cdot 10^3$ photons in **b**, from $2.0 \cdot 10^5$ to $3.0 \cdot 10^5$ photons in **d**, and from $0.4 \cdot 10^5$ to $3.0 \cdot 10^5$ photons in **e**.

key rate is the worst in the situation where Eve is close to the middle of the transmission line. This is explained by the side effects of signal amplification: the closer Eve is to Bob, the more Eve's part of the signal is correlated with Bob's, yet, the noisier it becomes (see Supplementary Note 4). Given such a trade-off, Eve gets the largest amount of information, standing somewhere in the vicinity of the line's midpoint. However, in the phase encoding case, reflected in **b, e**, the correlations outweigh noise even when Eve is close to Bob—hence, the lower key rate for larger D_{AB}.

Plots **c, f** show the protocol's performance under both encoding schemes in the respective worst-case scenarios: Eve's position is such that the key rate is the lowest. As we qualitatively estimate in Methods and further rigorously reaffirm in Supplementary Note 3, the minimal detectable leakage for a long line comprising a cascade of M equidistant amplifiers is $r_E^{\min} \sim \sqrt{MG/n}$, where G is the amplification factor of a single amplifier, and n is the number of photons in a test pulse. Taking the distance between the neighboring amplifiers $d = 50\,\text{km}$, $G = 10$, and $n = 10^{14}$, for the 1000 km-long ($M = 20$) and 40,000 km-long lines ($M = 800$) we get $r_E^{\min} \sim 10^{-6}$ and $r_E^{\min} \sim 10^{-5}$, respectively. Near to the loss control precision limit, both encoding schemes allow for high key rates: in the case of the photon number encoding maximum L_f/L is 0.99 for 1000 km and 0.57 for 40,000 km; for the phase encoding, the respective values are 0.98 and 0.27. Being better in terms of the key rates, the photon number encoding is also less demanding to the infrastructure as the phase preservation and phase reference are unnecessary.

Physical loss control and amplification

Let us outline possible implementations of the basic technological components of the protocol, the physical loss control and the signal repetition by optical amplifiers. The physical loss control methods are based on analyzing scattered components of the high-energy test pulses sent along the fiber. The optical time-domain reflectometry comprises the injection of test pulses into the fiber and the subsequent measurement of the temporal sequence of their back-scattered components. The response delay defines the distance to a particular scattering point, while its magnitude reflects the respective losses. Moreover, characteristic features of the response allow for determining the nature of the respective line's discontinuity; see the exemplary reflectogram in Supplementary Note 2. This is essential for identifying and mitigating local losses at the initial preparation stage and for localizing the potential eavesdropper later. An accurate reflectogram is obtained by averaging over multiple test runs (during which a test pulse travels to the end of the fiber and all its reflections return back); accumulating sufficient statistics may, in reality, take a few seconds. Then the high operational speed of the loss control is assured by its second element that we call transmittometry: Alice sends test pulses comprising a large number of photons to Bob, and they cross-

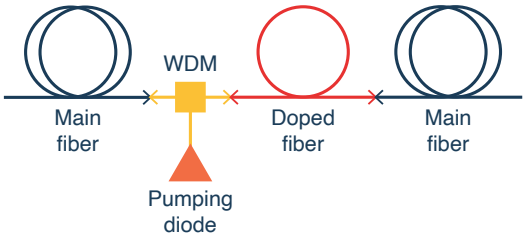

Figure 2 | Schematics of the proposed bidirectional optical amplifier. The doped fiber section is embedded into the main fiber line and linked to the pumping diode through the WDM.

check the sent and received photon numbers inferring the losses in the channel. Unlike reflectometry, transmittometry does not enable the users to localize and identify individual leakages but immediately updates their magnitude. Thus, the two control methods complement each other: the users are constantly aware of the magnitude of leakages and can localize them after accumulating sufficient reflectometry statistics.

To discriminate between the intrinsic and artificial line losses, the legitimate users prerecord the initial undisturbed line tomogram, including the reflectogram and the total proportion of losses in the line, and use this tomogram as a reference. The fiber material, silica, has an amorphous nonreproducible structure, making its reflectogram a physically unclonable function. With that, the fiber core can be slightly doped, with, e.g., Al, P, N, or Ge, to tune its tomography results and achieve the optimal parameters such as dispersion. The most general eavesdropping attack implies a unitary transformation of the state of the combined system comprising the propagating signal and some ancillary eavesdropping system. However, coupling of photons to devices outside the line requires making significant alterations to the fiber medium, which would inevitably change the reflectogram and hence will be detected. Quantum cryptography also addresses attacks exercising the partial blocking of the signal and the subsequent unauthorized substitution of the blocked part. Any intervention like that would inevitably and permanently (even if Eve at some point decided to disconnect from the line) affect the tomogram of the transmission line and hence will be detected by the legitimate users.

The key distribution itself should go in parallel with accumulating the reflectometry statistics. If, at some point, the reflectogram shows an intrusion into the line, the users should respond with the appropriate post-processing of the bits distributed during the formation of the reflectogram. This may possibly come down to discarding the whole bit sequence. Ideally, the physical loss control should be conducted permanently and should not halt even during the pauses in the key distribution. Taking the transmittometry test pulses' duration of the order of 1 ns makes any real-time mechanical intrusion into the line immediately detectable.

The principal task of the physical loss control is to ensure that Eve does not get enough photons to obtain the informational advantage over Bob. With that, signal pulses and test pulses still carry large numbers of photons, making it possible to repeat them via optical amplification. The repeater can particularly be arranged as a doped fiber section embedded into the main line and pumped to produce amplification gain in the primary mode. In telecommunications, the most common dopant is erbium: pumped at the wavelength of 980 nm the erbium-doped fiber generates the gain at around 1550 nm which fits into the transmission window of the silica-based fiber. The magnitude of the resulting signal amplification depends on the concentration of the erbium ions, the length of the doped fiber section, and the power of the pumping radiation. The amplification principle is explained in Methods.

Usually, doped fiber amplifiers utilize optical isolators, which allow the light to pass only in one direction. This minimizes the risk of multiple reflections inside the doped fiber section. In our protocol, however, the optical isolators would block the reflected light hindering the end-to-end time-domain reflectometry. Besides, the amplifiers typically include tap couplers diverting about 1% of the radiation into the photodetectors to monitor the amplifiers' operation, and this fraction can possibly be seized by the eavesdropper. We hence opt out of both the optical isolators and tap couplers and utilize the design of the bidirectional optical amplifier. The amplifier's sketch is displayed in Fig. 2. The fiber core is connected to the wavelength-division multiplexing (WDM) system. The WDM system is a beam splitter-like device for guiding the radiation of the different wavelengths into a single optical fiber. In our case, it is intended to feed the doped fiber section with the pumping radiation necessary to excite the active fiber's dopant atoms. Correspondingly, the WDM is connected to the active fiber and the pumping diode. Finally, active fiber is connected to the main fiber line. Provided that the neighboring amplifiers are separated enough, they are not subject to significant cross-talk. Our preliminary experiments reveal how the 1000 km-long line with the standard telecom distance $d = 50$ km between amplifiers can be made stable with the very restricted signal noise in the line, even in the absence of optical isolators. We find that the signal wavelength of 1530 nm—corresponding to the peak of the amplification factor spectrum of the erbium-doped fiber amplifier—is more preferable than the standard 1550 nm wavelength. Fixing $G = 1/T$ for 1550 nm means greater amplification for the noise in the modes near 1530 nm, which, in turn, may disrupt the stability of the amplifiers' operation, possibly turning them into lasers. But this is not the case if 1530 nm is already the target wavelength itself.

A possible eavesdropping attack on the amplifier may consist of increasing the pumping power and stealing the surplus of the amplified radiation. Of course, hooking up to the line would change its tomogram and thus will be detected. Nevertheless, the following constructive feature of the amplifier will serve as an additional element of protection. The doped fiber section will contain the near minimum number of dopant ions necessary to amplify the signal with the target amplification factor. Let the operational pumping power P_p match the target amplification factor G. With the increase of the pumping power, the relative population inversion asymptotically approaches unity, which corresponds to the amplification factor $G + \delta G$. The fraction of signal that Eve can possibly steal by inflating the pumping power is limited by $\delta G/G$, which is small, if at P_p almost all of the ions are already excited. The number of ions and the value of P_p should be such that the maximum achievable Eve's makeweight, summed over all amplifiers installed into the line, is smaller than the minimum detectable leakage.

Discussion and conclusions

The standard assumption in quantum cryptography, known as channel device independence, posits that all leakages from the quantum channel can be fully exploited by an eavesdropper. This assumption limits key rates to the PLOB bound [9], where the maximum rate scales as $-\log_2(1-\eta)$ bits per channel with the transmittivity η, making the rates impractically small at long distances. By considering the physical quantum principles of the signals' transmission and introducing physical loss control, we change this paradigm. In our approach, legitimate users can check what fraction of losses is available to the eavesdropper and make sure that this fraction contains a deficient quantity of information. While Eve must face the thorny task of discriminating between weak quantum states, Bob receives signals containing relatively large numbers of photons and has a vast information advantage. By utilizing end-to-end line tomography and by capitalizing on the fact that the natural losses are virtually impossible to be exploited by an eavesdropper, our approach lifts the PLOB restriction, and significantly extends the distance over which practical QKD can be implemented without compromising security: particularly, without relying on trusted nodes. Unlike trusted nodes, optical amplifiers do not convert sent quantum information into the classical form, and are controlled directly by users with their end-to-end control.

The proposed approach maintains the fundamental advantage of the QKD, everlasting security [46–49], ensuring that distributed keys will re-

main secure even against future technologies or attacks that may be developed. In the forthcoming publication, we will address the experimental realization of the QKD based on our approach for the transmission distance over 1000 kilometers.

References

1. Shor, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev.* **41**, 303-332 (1999).
2. Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Proc. IEEE Int. Conf. Comput. Syst. Signal Process* , 175-179 (1984).
3. Ekert, A. K. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.* **67**, 661–663 (1991).
4. Bennet, C. H. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* **68**, 3121 (1992).
5. Bruss, D. Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.* **81**, 3018 (1998).
6. Pirandola, S. *et al.* Advances in quantum cryptography. *Adv. Opt. Photon.* **12**, 1012–1236 (2020).
7. Pittaluga, M. *et al.* 600-km repeater-like quantum communications with dual-band stabilization. *Nat Photon.* **15**, 530–535 (2021).
8. Wang, S. *et al.* Twin-field quantum key distribution over 830-km fibre. *Nat Photon.* **16**, 154–161 (2022).
9. Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **8**, 1–15 (2017).
10. Liao, Sheng-Kai *et al.* Satellite-relayed intercontinental quantum network. *Phys. Rev. Lett.* **120**, 030501 (2018).
11. Chen, Yu-Ao *et al.* An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature* **589**, 214–219 (2021).
12. Chen, Teng-Yun *et al.* Implementation of a 46-node quantum metropolitan area network. *npj Quantum Inf.* **7**, 1–6 (2021).
13. Kimble, H. J. The quantum internet. *Nature* **453**, 1023–1030 (2008).
14. Sangouard, N., Simon, C., de Riedmatten, H. & Gisin, N. Quantum repeaters based on atomic ensembles and linear optics. *Rev. Mod. Phys.* **83**, 33–80 (2011).
15. Simon, C. *et al.* Quantum repeaters with photon pair sources and multimode memories. *Phys. Rev. Lett.* **98**, 190503 (2007).
16. Duan, L.-M., Lukin, M. D., Cirac, J. I. & Zoller, P. Long-distance quantum communication with atomic ensembles and linear optics. *Nature* **414**, 413–418 (2001).
17. Briegel, H.-J., Dür, W., Cirac, J. I. & Zoller, P. Quantum repeaters: The role of imperfect local operations in quantum communication. *Phys. Rev. Lett.* **81**, 5932–5935 (1998).
18. Kok, P., Williams, C. P. & Dowling, J. P. Construction of a quantum repeater with linear optics. *Phys. Rev. A* **68**, 022301 (2003).
19. Childress, L., Taylor, J. M., Sørensen, A. S. & Lukin, M. D. Fault-tolerant quantum communication based on solid-state photon emitters. *Phys. Rev. Lett.* **96**, 070504 (2006).
20. van Loock, P. *et al.* Hybrid quantum repeater using bright coherent light. *Phys. Rev. Lett.* **96**, 240501 (2006).
21. Wang, T.-J., Song, S.-Y. & Long, G. L. Quantum repeater based on spatial entanglement of photons and quantum-dot spins in optical microcavities. *Phys. Rev. A* **85**, 062311 (2012).
22. Sangouard, N., Dubessy, R. & Simon, C. Quantum repeaters based on single trapped ions. *Phys. Rev. A* **79**, 042340 (2009).
23. Azuma, K., Takeda, H., Koashi, M. & Imoto, N. Quantum repeaters and computation by a single module: Remote nondestructive parity measurement. *Phys. Rev. A* **85**, 062309 (2012).
24. Zwerger, M., Dür, W. & Briegel, H. J. Measurement-based quantum repeaters. *Phys. Rev. A* **85**, 062326 (2012).
25. Munro, W. J., Harrison, K. A., Stephens, A. M., Devitt, S. J. & Nemoto, K. From quantum multiplexing to high-performance quantum networking. *Nat. Photon.* **4**, 792–796 (2010).
26. Jiang, L. *et al.* Quantum repeater with encoding. *Phys. Rev. A* **79**, 032325 (2009).
27. Munro, W. J., Stephens, A. M., Devitt, S. J., Harrison, K. A. & Nemoto, K. Quantum communication without the necessity of quantum memories. *Nat. Photon.* **6**, 777–781 (2012).
28. Grudka, A. *et al.* Free randomness amplification using bipartite chain correlations. *Phys. Rev. A* **90**, 032322 (2014).
29. Lesovik, G. B., Sadovskyy, I. A., Suslov, M. V., Lebedev, A. V. & Vinokur, V. M. Arrow of time and its reversal on the IBM quantum computer. *Sci. Rep.* **9**, 4396 (2019).
30. Kirsanov, N. S. *et al.* Entropy dynamics in the system of interacting qubits. *J.Russ. Laser Res.* **39**, 120–127 (2018).
31. Lesovik, G. B., Lebedev, A. V., Sadovskyy, I. A., Suslov, M. V. & Vinokur, V. M. H-theorem in quantum physics. *Sci. Rep.* **6**, 32815 (2016).
32. Tateda, M. & Horiguchi, T. Advances in optical time domain reflectometry. *J.Lightwave Technol.* **7**, 1217–1224 (1989).
33. Kenbaev, N. R. & Kronberg, D. A. Quantum postselective measurements: Sufficient condition for overcoming the Holevo bound and the role of max-relative entropy. *Phys. Rev. A* **105**, 012609(2022).
34. Holevo, A. Bounds for the quantity of information transmitted by a quantum communication channel. *Probl. Peredachi Inf.* **9**, 3–11 (1973).
35. MacKay, D., Kay, D. & Press, C. U. *Information Theory, Inference and Learning Algorithms* (Cambridge University Press, 2003).
36. Johnson, S. J. *Iterative Error Correction: Turbo, Low-Density Parity-Check and Repeat-Accumulate Codes* (Cambridge University Press, 2009).
37. Hamming, R. *Coding and Information Theory* (Prentice-Hall, Inc., 1980).
38. Brassard, G. & Salvail, L. Secret-key reconciliation by public discussion. *Adv. Cryptology, EUROCRYPT '93*, 410–423 (Springer, Berlin, Heidelberg, 1994).
39. Pedersen, T. B. & Toyran, M. High performance information reconciliation for qkd with cascade. *Quantum Inf. Comput.* **15**, 419–434 (2015).
40. Martinez-Mateo, J., Pacher, C., Peev, M., Ciurana, A. & Martin, V. Demystifying the information reconciliation protocol cascade. *Quantum Inf. Comput.* **15**, 453–477 (2015).
41. Carter, J. L. & Wegman, M. N. Universal classes of hash functions. *J. Comp. Syst. S.* **18**, 143–154 (1979).
42. Mølmer, K. Optical coherence: A convenient fiction. *Phys. Rev. A* **55**, 3195 (1997).
43. Lütkenhaus, N. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A* **61**, 052304 (2000).
44. Van Enk, S. & Fuchs, C. A. Quantum state of an ideal propagating laser field. *Phys. Rev. Lett.* **88**, 027902 (2001).
45. Devetak, I. & Winter, A. Distillation of secret key and entanglement from quantum states. *Proc. R. Soc. Lond. A* **461**, 207–235 (2005).
46. Unruh, D. Everlasting multi-party computation. *CRYPTO 2013*, 380–397 (2013).
47. Portmann, C.& Renner, R. Security in quantum cryptography. *Rev. Mod. Phys.* **94**, 025008 (2022).
48. Stebila, D., Mosca, M. & Lütkenhaus, N. The case for quantum key distribution. *Quantum Communication and Quantum Networking* **36**, 283–296 (2009).
49. Alléaume, R. *et al.* Quantum key distribution and cryptography: a survey. *Dagstuhl Seminar Proceedings* **3**,100–107 (2010).

Methods

Combined quantum state evolution under beam splitting attack
Here we provide the description of states' evolution in the case of the beam splitting attack. We will use that (a) an amplifier transforms pure coherent state into a mixture of the coherent states,

$$|\gamma\rangle \to \int d^2\alpha\, P(\alpha,\gamma,G)\,|\alpha\rangle\langle\alpha|\,, \tag{7}$$

where $P(\alpha,\gamma,G)$ is given by Eq. (3) and integration is performed over the complex plane with $d^2\alpha \equiv d\mathrm{Re}(\alpha)\,d\mathrm{Im}(\alpha)$; and that (b) formally, a sequence of losses and amplifications can be reduced to a single pair of the loss and amplification quantum channels—see Supplementary Note 3 for details.

The initial density matrix of Alice's random bit (A) and the corresponding signal (S) is given by

$$\hat{\rho}^{\mathrm{i}}_{\mathrm{AS}} = \frac{1}{2}\,|0\rangle\langle 0|_{\mathrm{A}}\otimes|\gamma_0\rangle\langle\gamma_0|_{\mathrm{S}} + \frac{1}{2}\,|1\rangle\langle 1|_{\mathrm{A}}\otimes|\gamma_1\rangle\langle\gamma_1|_{\mathrm{S}}\,. \tag{8}$$

Just before the signal passes the beam splitter, the state of the AS system is

$$\hat{\rho}^{\to\square}_{\mathrm{AS}} = \frac{1}{2}\sum_{a=0,1}|a\rangle\langle a|_{\mathrm{A}}\otimes\int d^2\alpha\cdot P(\alpha,\,\sqrt{T_1}\gamma_a,G_1)\cdot|\alpha\rangle\langle\alpha|_{\mathrm{S}}\,, \tag{9}$$

where we use Eq. (7) to describe the state of sequentially attenuated and amplified signal, and T_1 and G_1 are, respectively, the transmission probability and amplification factor of the effective loss and amplification channels that are equivalent to the sequence of amplifications and losses prior to the beam splitter, see Supplementary Note 3, particularly Eq. (58). Just after the signal passes the beam splitter, the state of the joint system of Alice's random bit, the signal travelling to Bob and the signal component seized by Eve (E) is described by

$$\hat{\rho}^{\square\to}_{\mathrm{ASE}} = \frac{1}{2}\sum_{a=0,1}|a\rangle\langle a|_{\mathrm{A}}\otimes\int d^2\alpha\cdot P(\alpha,\,\sqrt{T_1}\gamma_a,G_1)$$
$$\times\,|\sqrt{1-r_{\mathrm{E}}}\alpha\rangle\langle\sqrt{1-r_{\mathrm{E}}}\alpha|_{\mathrm{S}}\otimes|\sqrt{r_{\mathrm{E}}}\alpha\rangle\langle\sqrt{r_{\mathrm{E}}}\alpha|_{\mathrm{E}}\,, \tag{10}$$

where r_{E} is the fraction of signal stolen by Eve. After the signal passes the second series of losses and amplifiers and right before it is measured by Bob, the state of the joint system is

$$\hat{\rho}^{\to\mathrm{Bob}}_{\mathrm{ASE}} = \frac{1}{2}\sum_{a=0,1}|a\rangle\langle a|_{\mathrm{A}}\otimes\int d^2\alpha\cdot P(\alpha,\,\sqrt{T_1}\gamma_a,G_1)$$
$$\times\left(\int d^2\beta\cdot P\left(\beta,\,\sqrt{(1-r_{\mathrm{E}})T_2}\alpha,G_2\right)\cdot|\beta\rangle\langle\beta|_{\mathrm{S}}\right)\otimes|\sqrt{r_{\mathrm{E}}}\alpha\rangle\langle\sqrt{r_{\mathrm{E}}}\alpha|_{\mathrm{E}}\,, \tag{11}$$

where we again utilize Eq. (7) to describe the evolved signal state, and T_2 and G_2 are the effective transmission probability and amplification factor of the region between the beam splitter and Bob, see Eq. (59) in Supplementary Note 3. Bob receives the signal state, measures it and, together with Alice, discards the outcome if it is inconclusive. The probability that Bob's measurement outcome is $b = \{0,\,1\}$ given that Alice's sent bit is $a = \{0,\,1\}$ can be written as

$$p(b|a) = \mathrm{tr}_{\mathrm{ASE}}\left[\left(2\cdot|a\rangle\langle a|_{\mathrm{A}}\otimes\hat{E}_b\otimes\hat{\mathbb{1}}_{\mathrm{E}}\right)\hat{\rho}^{\to\mathrm{Bob}}_{\mathrm{ASE}}\right], \tag{12}$$

where $\hat{E}_b$ is given by Eq. (1a) or (1b) depending on the encoding scheme, and $\mathrm{tr}_{\mathrm{ASE}}[\ldots]$ is the trace over the ASE system. The probability that Bob gets a conclusive outcome if Alice sends bit a is

$$p(\checkmark|a) = p(0|a) + p(1|a). \tag{13}$$

Equation (2) follows from Eq. (11) after applying measurement operators to the signal subsystem, discarding sum components associated with the inconclusive outcomes, and renormalizing.

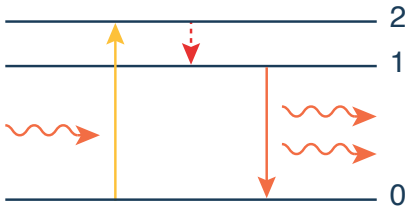

Figure 3 | Energy diagram of the light amplification in the erbium-doped fiber section. Pumping radiation excites erbium ions from the ground state 0 into the 2nd energy level. Shortly after, ions drop to the metastable level 1. The times of the relaxation from 2 to 1 and from 1 to 0 are around 20 μs and 10 ms respectively. The incident photons stimulate the transition $1 \to 0$ which results in the coherently synchronized radiation of additional photons at the same wavelength.

Privacy amplification
Privacy amplification can be realized through applying the universal hashing method [41], which requires the users to initially agree on the family $\mathcal{H}$ of hash functions. At the privacy amplification stage [38,50,51], they randomly select such a function $h : \{0,1\}^{p_{\checkmark}L} \to \{0,1\}^{L_{\mathrm{f}}} \in \mathcal{H}$ that maps the raw key of length $p_{\checkmark}L$ to the final key of length L_{f}. If Eve is estimated to know $p_{\checkmark}L\cdot\tilde{I}(\mathrm{A},\mathrm{E})$ bits of the raw key, the letter must be taken in accord with Eq. (6). Family $\mathcal{H}$ can, for example, span Toeplitz matrices [52]: a random binary Toeplitz matrix $\hat{T}$ with $p_{\checkmark}L$ rows and L_{f} columns translates the binary vector representation of the raw key $\mathbf{v}$ into the vector $\mathbf{k}$ representing the final key, $\mathbf{k} = \hat{T}\cdot\mathbf{v}$.

Optical amplification principle
The principle of optical amplification is illustrated in Fig. 3. Upon the absorption of the pumping radiation, erbium ions transit from the ground state 0 into the short-lived state 2, from which they non-radiatively relax to the metastable state 1. The relaxation times for the transitions $2 \to 1$ and $1 \to 0$ are around 20 μs and 10 ms, respectively. The passing light stimulates the transition from the state 1 to state 0 which leads to the coherently synchronized photon emission.

Physical loss control precision
Assume that Bob is equipped with an optical filter with a very narrow wavelength band which blocks noise from the secondary light modes (for details on this additional noise, see Supplementary Note 3). Assume also that all amplifiers are positioned equidistantly, each having amplification factor $G = 1/T$ with T being the transmission probability of the line section between two neighboring amplifiers.

Approaching an amplifier, the test pulse comprising n photons is attenuated down to Tn photons. The amplifier restores the number of photons back to n but adds noise. The photons in the pulse follow the Poisson statistics; thus, the photon noise just before the amplifier can be taken as a square root of the input signal $\sqrt{Tn}$. The noise is amplified by factor G as well, so after a single amplifier the noise is $G\sqrt{Tn}$. Coming through a sequence of M amplifiers which add fluctuations independently, the total noise raises by the factor $\sqrt{M}$. The noise at Bob's end is thus $\delta n_{\mathrm{B}} \simeq G\sqrt{MTn} = \sqrt{GMn}$. The minimum detectable leakage can be calculated as $r^{\min}_{\mathrm{E}} \sim \delta n_{\mathrm{B}}/n = \sqrt{MG/n}$. Our qualitative estimates match with the rigorous calculations in Supplementary Note 3.

References

50. Bennett, C. H., Brassard, G. & Robert, J.-M. Privacy amplification by public discussion. *SIAM J. Comput.* **17**, 210–229 (1988).
51. Bennett, C. H., Brassard, G., Crépeau, C. & Maurer, U. M. Generalized privacy amplification. *IEEE T. Inform. Theory* **41**, 1915–1923 (1995).
52. Krawczyk, H. LFSR-based hashing and authentication. In *Annual International Cryptology Conference*, 129–139 (Springer, 1994).

Acknowledgements We are delighted to thank Pavel Sekatski and Renato Renner for illuminating discussions.

Author contribution M.P. and V.M.V. conceived the work, N.S.K., V.A.P., A.D.K., D.A.K., and V.M.V. developed the theory behind the protocol, N.S.K., V.A.P., A.D.K., and A.B.S. carried out the calculations, V.A.P. and A.D.K. performed numerical simulations, N.S.K., V.M.V., V.A.P., A.D.K., and D.A.K wrote the manuscript, N.S.K., V.A.P., and A.D.K. wrote the supplementary information, M.V.Y. obtained experimental data with an optical time-domain reflectometer.

Competing interests The Authors declare that they have no competing interests.

Correspondence Correspondence and requests for materials should be addressed to V.M.V. (vv@terraquantum.swiss).

Supplementary Information

NOTE 1. Natural losses

In this note, we discuss the unfeasibility of eavesdropping on the natural losses occurring due to the scattering of photons in optical fiber. Here we explore quantum considerations analogous to those that serve to derive the Second Law of Thermodynamics [29–31]. In quantum cryptography, the thermodynamic considerations should focus on the collection of optical states traveling through a lossy fiber. In the standard telecommunication scenario, with the signal power of around 10 mW and a pulse duration of 1 ns, each light pulse contains about 10^8 photons, with staggering leaks of about 10^3 photons per meter that can be measured outside of the fiber. This scenario implies that the system is clearly not isolated, and, through the measurement of leaked photons, Eve can decrease the system's entropy—a process which, in accordance with Shannon's definition of entropy, is equivalent to extracting information.

On the other hand, in a relatively weak signal region of our choice with 10^4 to 10^5 photons or less (which is still enough for the optical amplification), the system can be considered quasi-isolated since only a small number of photons are lost from each pulse. Eve's attempt to measure the leaked parts of a signal's wave function and obtain information about the sent bit would decrease the entropy. However, extracting a substantial amount of information from leaked photons requires Eve to operate and observe multitudes of degrees of freedom, which, as we will demonstrate in the next section, is unfeasible.

1.1 Required length of the eavesdropping device

In assessing the feasibility of the potential eavesdropping on the natural losses, we consider a scheme in which logical bits are encoded into optical coherent states $|\gamma_0\rangle$ and $|\gamma_1\rangle$ with different photon numbers $\mu_0 = |\gamma_0|^2$ and $\mu_1 = |\gamma_1|^2$. Let the signal pulses have the duration of 1 ns (0.2 m long) and comprise 10^4 photons on average. The optimal values for μ_0 and μ_1 on a 1000 km line, as determined by our simulations (see the main text), are 9000 and 11,000, respectively. To eavesdrop on the homogeneously spread natural losses, an eavesdropper would be forced to undertake measurements along various segments of the fiber, possibly using single-photon detectors. However, as our calculations indicate, such a method would be impractical in terms of the sheer length required to successfully determine the value of any given bit.

The natural losses coefficient of a fiber section of length l can be calculated as

$$r_l = 1 - 10^{-\xi \cdot l}, \tag{14}$$

where ξ is the decay constant. The number of photons lost from a wave packet containing μ_a photons is given by:

$$\mu_{\mathrm{E}}^{(a)} = \mu_a \cdot r_l. \tag{15}$$

The lower index E denotes that the photons can be seized by an eavesdropper, the upper index a represents the corresponding random bit value.

The observable (positive operator-valued measure, or POVM) describing the single-photon detector includes two projective operators corresponding to two possible outcomes:

$$\mathcal{M}_{\text{single photon}} = \left\{ \hat{M}_0 = |0\rangle\langle 0|\,,\ \hat{M}_{\text{click}} = \sum_{n=1}^{+\infty} |n\rangle\langle n| \right\}. \tag{16}$$

The probability of the detector's "click" conditional to the bit value a is determined by the Poisson statistics of Eve's coherent state

$$\begin{aligned} q_a \equiv p\,(\text{click}\,|\,a) &= \mathrm{Tr}\left(\hat{M}_{\text{click}} \cdot |\sqrt{r_l}\gamma_a\rangle\langle\sqrt{r_l}\gamma_a|\right) \\ &= 1 - \mathrm{Tr}\left(\hat{M}_0 \cdot |\sqrt{r_l}\gamma_a\rangle\langle\sqrt{r_l}\gamma_a|\right) = 1 - \left|\langle 0|\sqrt{r_l}\gamma_a\rangle\right|^2 \\ &= 1 - e^{-|\sqrt{r_l}\gamma_a|^2} = 1 - e^{-\mu_{\mathrm{E}}^{(a)}}. \end{aligned} \tag{17}$$

According to the measurement outcomes, Eve makes bit decisions. Probability distribution of measurement results can be considered as Binomial which variance is $q_a(1-q_a)$. Carrying out N independent measurements of sequential parts of the line, the combined variance is a sum of variances of each individual measurement. Thus, the expression for the square root of the variance takes form

$$\delta n_a = \sqrt{N \cdot q_a(1-q_a)}. \tag{18}$$

Bits zero and one produce different distributions, the distance between the maximums of these distributions can be calculated as

$$\Delta n = N \cdot \left|\mu_{\mathrm{E}}^{(1)} - \mu_{\mathrm{E}}^{(0)}\right|. \tag{19}$$

In order to obtain significant amount of information Eve needs the distance between the maximums of the distributions to exceed the sum of their standard derivations, i.e. the notional critical condition can be written as

$$\begin{aligned} &\Delta n = \delta n_0 + \delta n_1 \quad \Rightarrow \\ &N \cdot \left|\mu_{\mathrm{E}}^{(1)} - \mu_{\mathrm{E}}^{(0)}\right| = \sqrt{N} \cdot \left(\sqrt{q_0(1-q_0)} + \sqrt{q_1(1-q_1)}\right). \end{aligned} \tag{20}$$

Then, supposing that each of the detectors covers a piece of fiber of the length equal to the length of the considered pulses, i.e. $l = 0.2$ m, and taking $\xi = 0.02\,\mathrm{km}^{-1}$, which is a common value for the single-mode optical fiber, the required number of detectors

$$N = \frac{\left(\sqrt{q_0(1-q_0)} + \sqrt{q_1(1-q_1)}\right)^2}{\left|\mu_{\mathrm{E}}^{(1)} - \mu_{\mathrm{E}}^{(0)}\right|^2} \simeq 10^3. \tag{21}$$

Combining all measured pieces, we obtain the total length of the whole detection device $N \cdot l \simeq 10^3 \cdot 0.2\,\mathrm{m} = 200\,\mathrm{m}$.

Moreover, not all the leakages can be measured in reality: some of the scattered photons transform to different modes propagating along the fiber and do not radiate outwards. Along with that, to measure a leaked part of the signal with the single photon detector, it is necessary to isolate the measured part of the line from the external radiation and concentrate the leaked photons to the cryogenic setup. The effects combined reduce the number of photons available to Eve approximately by an order of magnitude. These physically motivated assumptions lead to enormous lengths of detection devices even in the case of higher intensities (for instance, $\mu_{0,1} \sim 10^5$, which turned out to be optimal for the 40 000 km line – see Numerical Simulations). It is important to acknowledge that while the aforementioned attacks utilizing scattering losses are hardly realistic, one can employ methods of protection that can counteract them as well. These include utilizing specialized cable design enabling the controlled dissipation of scattering losses (described in Note 2), utilizing lower numbers of photons in pulses, and implementing advanced encoding schemes that utilize the phase or shape of the pulses.

1.2 Precise estimation of Eve's information

To estimate the precise amount of information that Eve can get from the N individual measurements of natural losses with single photon detectors, we calculate the mutual information between Alice's sent bit $a \in \{0, 1\}$ and Eve's measurement results. The conditional probabilities of obtaining n "clicks" can be written as

$$p(n|a) = C_N^n \cdot q_a^n \cdot (1-q_a)^{N-n}, \tag{22}$$

where $C_N^n = \frac{N!}{n!(N-n)!}$ is a binomial coefficient and q_a is the click probability in the individual measurement in the case where the sent bit value is a. The expression for the mutual information is determined by the joint

probability distribution $p(n,a) = p(n|a) \cdot p(a)$:

$$I\left(\mathrm{A} : \mathrm{E}_{\mathrm{ind}}^{(N)}\right) = \sum_{n=0}^{N}\sum_{a=0}^{1} p(n,a) \cdot \log_2\left(\frac{p(n,a)}{p(n)\cdot p(a)}\right)$$
$$= \sum_{n=0}^{N}\sum_{a=0}^{1} \frac{1}{2} p(n|a) \cdot \log_2\left(\frac{p(n|a)}{p(n|0)+p(n|1)}\right)$$
$$= 1 - \frac{1}{2}\sum_{n=0}^{N}\left(p(n|0)+p(n|1)\right)\cdot h_2\left(\frac{p(n|0)}{p(n|0)+p(n|1)}\right). \quad (23)$$

The dependence of the Eq. (23) on the total length of the detection device is depicted in Fig. 4. Was the device's length equal to 200 m, the mutual information $I\left(\mathrm{A} : \mathrm{E}_{\mathrm{ind}}^{(N)}\right)$ would almost reach 0.5, meaning that Eve would know half of the raw shared key—these results are in a good agreement with the preliminary estimations from the previous section. While in the case of more feasible lengths (a couple of meters, for example), the information Eve can obtain is of the order of 10^{-2} bit. One can note that the Eq. (23) does not depend on whether phase randomization is applied or not, since the probabilities are determined only by photon numbers (for details see Note 4).

1.3 Ideal photon number measurement

Next, we consider collective photon number measurement over the whole N pieces of the fiber which can be conducted after gathering all the scattered photons at one ideal detector. The corresponding observable in terms of the POVM effects can be expressed as projectors on the Fock-states

$$\mathcal{M}_{\text{photon number}} = \left\{\hat{M}_n = |n\rangle\langle n|\right\}_{n=0}^{+\infty}. \quad (24)$$

The probability of obtaining k photons is determined by the average number of all scattered photons in a signal corresponding to sent bit a

$$p(k|a) = e^{-N\cdot\mu_{\mathrm{E}}^{(a)}} \cdot \frac{\left(N\mu_{\mathrm{E}}^{(a)}\right)^k}{k!} \quad (25)$$

Almost analogously to the previous paragraph, one can calculate the mutual information as

$$I\left(\mathrm{A} : \mathrm{E}_{\mathrm{col}}^{(N)}\right) = 1 - \frac{1}{2}\sum_{k=0}^{+\infty}\left(p(k|0)+p(k|1)\right)\cdot h_2\left(\frac{p(k|0)}{p(k|0)+p(k|1)}\right). \quad (26)$$

The only difference from the Eq. (23) is that upper limit of the summation is now infinity. As depicted in the Fig. 4, the informational advantage of Eq. (26) over single-photon measurements is insignificant.

1.4 The Holevo bound

To build an upper-bound on the information that Eve may extract from the scattered photons, we calculate the Holevo quantity, which for an ensemble of quantum states $\mathcal{E} = \left\{\left(1/2, \hat{\rho}^{(0)}\right), \left(1/2, \hat{\rho}^{(1)}\right)\right\}$ is defined as

$$\chi(\mathcal{E}) = S\left(\frac{1}{2}\hat{\rho}^{(0)} + \frac{1}{2}\hat{\rho}^{(1)}\right) - \frac{1}{2}S\left(\hat{\rho}^{(0)}\right) - \frac{1}{2}S\left(\hat{\rho}^{(1)}\right), \quad (27)$$

where $S(\hat{\rho}) = -\mathrm{Tr}\left(\hat{\rho}\cdot\log_2\hat{\rho}\right)$ is von Neuman entropy. Without phase randomization, Eve has to distinguish between pure coherent states of the form

$$\hat{\rho}^{(a)} = |\sqrt{r_l N}\gamma_a\rangle\langle\sqrt{r_l N}\gamma_a|. \quad (28)$$

Since entropy of a pure state is zero, the Holevo quantity is just the entropy of the average ensemble's state

$$\chi(\mathcal{E}) = S\left(\frac{1}{2}\hat{\rho}^{(0)} + \frac{1}{2}\hat{\rho}^{(1)}\right) = h_2\left(\frac{1}{2} - \frac{1}{2}\left|\langle\sqrt{r_l N}\gamma_0|\ \sqrt{r_l N}\gamma_1\rangle\right|\right)$$
$$= h_2\left(\frac{1}{2} - \frac{1}{2}\exp\left[-\frac{1}{2}\cdot r_l N\left(\gamma_1-\gamma_0\right)^2\right]\right), \quad (29)$$

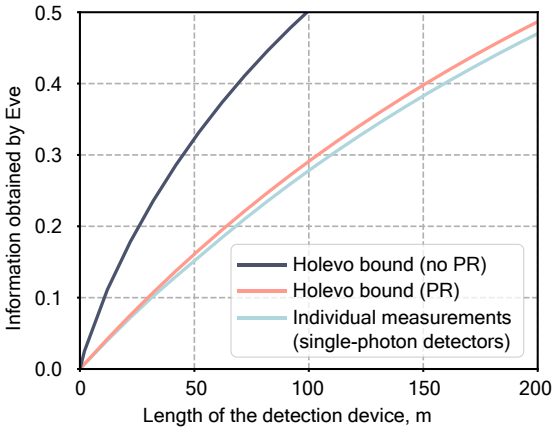

Figure 4 | The information Eve can obtain from natural losses as a function of the overall length of the detection device. The cyan line corresponds to individual measurements (by single-photon detectors) as determined by Eq. (23). The orange line depicts Holevo bound with phase randomization (PR) according to Eq. (31). The black line is for the Holevo bound (no PR) in the absence of PR Eq. (29).

where $h_2(x) = x\cdot\log_2(x) - (1-x)\cdot\log_2(1-x)$ is binary entropy. Applying phase randomization transforms the ensemble of pure coherent states into the mixtures of Fock states

$$\mathcal{E}_{\mathrm{PR}} = \left\{\left(\frac{1}{2}, \hat{\rho}_{\mathrm{PR}}^{(0)}\right), \left(\frac{1}{2}, \hat{\rho}_{\mathrm{PR}}^{(1)}\right)\right\},$$
$$\hat{\rho}_{\mathrm{PR}}^{(a)} = \frac{1}{2\pi}\int_0^{2\pi} d\varphi\, |\sqrt{r_l N}\gamma_a\cdot e^{i\varphi}\rangle\langle\sqrt{r_l N}\gamma_a\cdot e^{i\varphi}| = \sum_{k=0}^{+\infty} p(k|a)\cdot|k\rangle\langle k|, \quad (30)$$

where $p(k|a)$ is defined in Eq. (25). Now ensemble's states are diagonal, thus, quantum entropy is replaced with classical Shannon entropy

$$\chi(\mathcal{E}_{\mathrm{PR}}) = S\left(\frac{1}{2}\hat{\rho}_{\mathrm{PR}}^{(0)} + \frac{1}{2}\hat{\rho}_{\mathrm{PR}}^{(1)}\right) - \frac{1}{2}S\left(\hat{\rho}_{\mathrm{PR}}^{(0)}\right) - \frac{1}{2}S\left(\hat{\rho}_{\mathrm{PR}}^{(1)}\right)$$
$$= H\left(\left\{\frac{p(k|0)+p(k|1)}{2}\right\}_{k=0}^{+\infty}\right) - \frac{1}{2}\left[H\left(\left\{p(k|0)\right\}_{k=0}^{+\infty}\right) + H\left(\left\{p(k|1)\right\}_{k=0}^{+\infty}\right)\right]. \quad (31)$$

Carrying out trivial mathematical transformations, one may conclude that the Holevo quantity for the phase randomization case Eq. (31) coincides with the information obtained in ideal photon number measurement Eq. (26). Figure 4 also shows that the Holevo quantity for pure coherent states Eq. (29) appeared to be much higher than considered photon number measurements, meaning that Eve may potentially utilize information about the phase to conduct more effective measurement. It prompts legitimate users to implement phase randomization in their QKD scheme.

NOTE 2. Controlled dissipation of natural losses and advanced line tomography

In this note, we turn our attention to a particular cable design and advanced line tomography that transforms scattered photons into heat in a controlled manner. This method effectively precludes Eve from exploiting the natural losses.

The cable design transforming scattering losses into heat is sketched in Fig. 5. The inner fiber core carrying the information light pulses is surrounded by a cladding with a smaller refractive index and then by the dissipative cladding made out of metal or metal-doped silica. The dissipative cladding screens the scattering losses escaping the fiber core since the scattered wave undergoes the inelastic secondary scattering and transforms into heat. The resulting dissipative thermal losses cannot be deciphered even in principle. The dissipative cladding is, in turn, coated

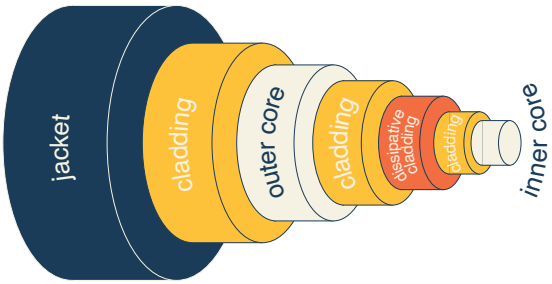

Figure 5 | Cable design. The cable namely includes (i) the inner core for information transmission and physical loss control, (ii) dissipative cladding converting scattering losses from the inner core into heat and completely destructing their information contents, and (iii) outer core for monitoring line integrity.

by the second standard refractive cladding layer, surrounded by an outer hollow fiber core and the outside refractive cladding. The outer core enables legitimate users to perform constant reflectometry and transmittometry, thus exercising control over the dissipation of the scattering losses. To remove the dissipative cladding for collecting the scattering losses or to create an artificial leakage from the inner core, Eve first needs to get through the outer core. The action, however, will not go unnoticed because of the permanent Alice and Bob's updating of the outer core's loss profile. Finally, the structure is surrounded by an outer jacket which may include a strengthening layer. To mitigate local losses on fiber connections, they should be made spliced.

Physical loss control allows for a quantitative estimate and localization of any damage inflicted upon the outer or inner cores, see an experimentally obtained example of a reflectogram in Fig. 6, presenting the dependence of the backscattered power upon the distance to the scattering point: the linear regions represent homogeneous scattering along the line, while the sharp peaks or drops correspond to the local losses at fiber contacts and bends. As opposed to the regular optical fiber, this specific line design eliminates the possibility of an undetected collection of scattering losses. Any local intrusion brings Eve a negligible number of scattered photons; then, to collect a sufficient amount of the scattering losses, she needs to breach a large section of the controlled outer core, and before it is done, the legitimate users terminate the protocol. Yet, our approach—particularly, the protocol outlined in the main text—resists a significant signal leakage fraction without the necessity of terminating transmission at first sight of the channel breach. Instead, the legitimate users adapt the encoding and post-processing parameters based on the evaluation of the fraction of the signal possibly leaked to Eve, the outer and inner cores being monitored separately. Importantly, although the inner core of the line is controlled only at step 1 of the protocol, legitimate users must control the outer core at all steps of the protocol. The users can count scattering losses that leaked from the breached outer core region as stolen by Eve and then act accordingly, i.e., adapt or terminate the protocol. In other words, the scattering losses escaping the breached outer core region can be equated to the artificial leakages directly from the inner core. If the outer core is breached at the same spot where the inner core has an irredeemable local leakage, such as a bend, the users must take that this leakage is seized by Eve.

NOTE 3. Signal amplification

In this note, we address optical amplification using the formalism of quantum channels. We develop a mathematical representation of a sequence of optical amplifiers, which we later use for modeling a general beam splitter attack on the transmission. Using this representation, we calculate the amplification-induced noise.

3.1 Amplification in doped fibers and losses

In Er/Yt doped fiber, the photonic mode propagates through the inverted atomic medium. To keep the medium inverted, a seed laser of a different frequency co-propagates with the signal photonic mode in the fiber and is then filtered out at the output by means of wavelength-division multiplexing (WDM). The interaction between the inverted atom at the position z and propagating light field mode $\hat{a}$ is given by the Hamiltonian in the rotating wave approximation

$$\hat{H}_{\text{int}} = i\kappa \sum_{n=1}^{N} \left(\hat{a}^\dagger \hat{\sigma}_-^{(n)} - \hat{a}\hat{\sigma}_+^{(n)} \right) = i\kappa \left(\hat{a}^\dagger \hat{S}_- - \hat{a}\hat{S}_+ \right), \tag{32}$$

$$\hat{\sigma}_-^{(n)} = |g\rangle\langle e|_n, \quad \hat{\sigma}_+^{(n)} = |e\rangle\langle g|_n, \quad \hat{S}_\pm = \sum_{n=1}^{N} \hat{\sigma}_\pm^{(n)}, \tag{33}$$

where we enumerate the atoms by index n, with N being the overall number of atoms in the medium at the position z ($N \gg 1$), κ is the interaction constant. Here, each medium's atom is assumed to be a two-level system with its basis states $|g\rangle$ and $|e\rangle$ denoting the ground and excited states, respectively; $\hat{\sigma}_\pm^{(n)}$ is the n-th atom raising/lowering operator, while $\hat{S}_\pm$ is the collective raising/lowering operator, that shifts the number of excited atoms in the medium by one. To simplify further calculations, we utilize the Holstein-Primakoff [53] transformation which provides mapping between the collective $(\hat{S}_+, \hat{S}_-)$ and boson $(\hat{b}, \hat{b}^\dagger)$ operators

$$\hat{S}_+ \approx \sqrt{N}\hat{b}, \quad \hat{S}_- \approx \sqrt{N}\hat{b}^\dagger, \quad \left[\hat{b}, \hat{b}^\dagger\right] = 1. \tag{34}$$

The initial state of fully inverted atomic medium is $|e\rangle_1 \otimes |e\rangle_2 \ldots \otimes |e\rangle_N$ (all N atoms are in the excited state). The Holstein-Primakoff transformation maps it to the vacuum $|0\rangle_b$ (i.e. no excitations in the boson mode b). The amplifier's medium with m atoms in the ground state is now described by the state with m excitations $|m\rangle_b$ that obeys the standard annihilation and creation operations

$$\begin{aligned} \hat{b}\,|m\rangle_b &= \sqrt{m}\,|m-1\rangle_b\,, \\ \hat{b}^\dagger\,|m\rangle_b &= \sqrt{m+1}\,|m+1\rangle_b\,. \end{aligned} \tag{35}$$

With that we have

$$\hat{H}_{\text{int}} \approx i\kappa\sqrt{N}\left(\hat{a}^\dagger\hat{b}^\dagger - \hat{a}\hat{b}\right). \tag{36}$$

The evolution operator of a propagating photon is given by

$$\hat{U}_g = e^{-i\hat{H}_{\text{int}}t/\hbar} = e^{g(\hat{a}^\dagger\hat{b}^\dagger - \hat{a}\hat{b})}, \tag{37}$$

where $g = \kappa\sqrt{N}t/\hbar$ and t is effective time of interaction between the photonic mode and atomic medium. Besides considering the channel acting on the propagating state, we also have to consider a conjugate channel acting on the creation operator $\hat{a}$ (it will be needed in the following cryptanalysis)

$$\text{Amp}_G^*[\hat{a}] = \hat{U}_g^\dagger\,\hat{a}\,\hat{U}_g = \cosh(g)\hat{a} + \sinh(g)\hat{b}^\dagger. \tag{38}$$

In practice, the performance of erbium-doped fiber amplifiers (EDFAs) suffers from technical limitations, which arise in addition to the amplification limits on added quantum noise. These limitations are mainly caused by two factors: (i) the atomic population may be not completely inverted throughout the media, (ii) there may be coupling imperfection between the optical mode and the doped fiber section or main part of the fiber. We will imply that these factors are accounted for in the loss channel prior to the amplification channel, as shown in Ref. [54].

3.2 P-function and its evolution under amplification

Consider a single photonic mode with bosonic operators $\hat{a}$ and $\hat{a}^\dagger$ acting in the Fock space. To understand the effect of the amplification on the bosonic mode state, we will use the P-function formalism allowing to express any density operator as a quasi-mixture of coherent states:

$$\hat{\rho} = \int d^2\alpha\, \text{P}(\alpha)\,|\alpha\rangle\langle\alpha|\,, \tag{39}$$

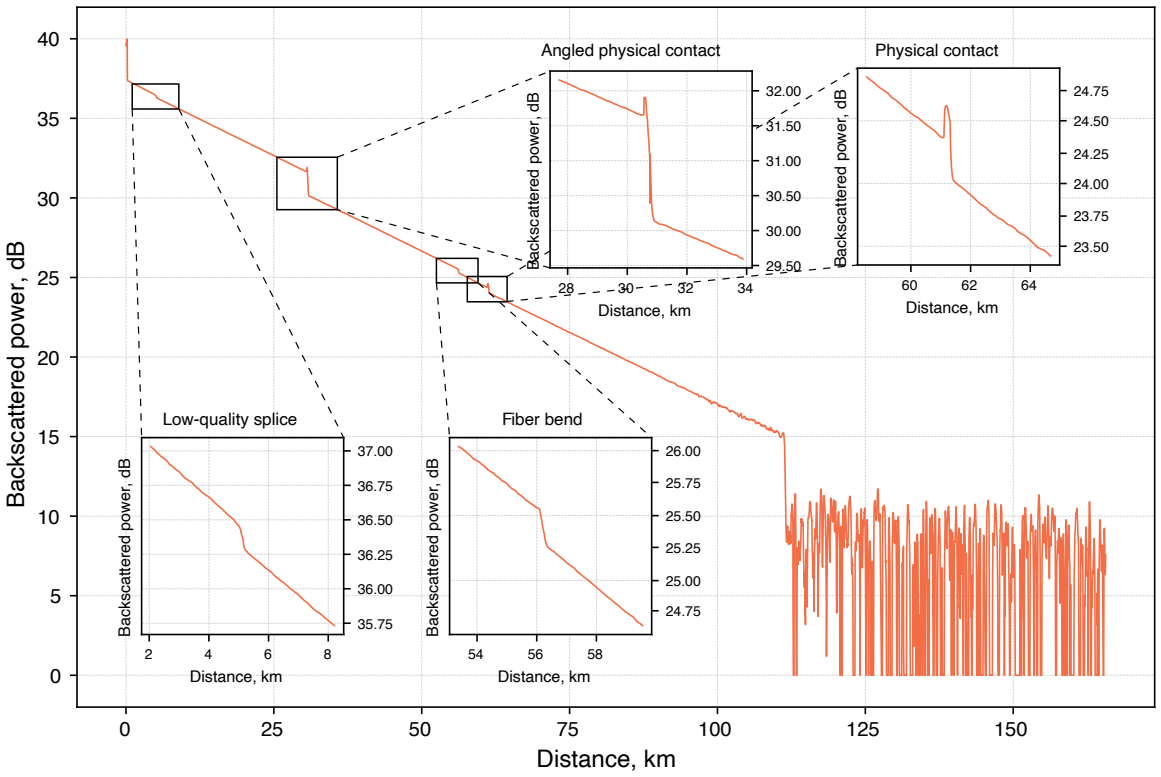

Figure 6 | **An exemplary plot obtained with the optical time-domain reflectometer.** The device sends the high-intensity test pulses into the fiber and registers its reflections providing the dependence of the backscattered power on the distance to the scattering point defined by the time of the signal's return. Every particular type of fiber discontinuity, whether it is physical contact, bending, or splice, can be identified by its own unique reflectographic pattern, as demonstrated in the inset plots. The appearance of peaks signifies the excessive scattering which happens, for instance, at the physical connectors where the signal undergoes the Fresnel reflection. The right noisy tail of the main plot corresponds to the end of the backscattered signal. The measurements are carried out with a $2\,\mu$s 1550 nm pulse laser with a power up to 40 mW. The experimental data is averaged over $16,000$ measurements.

where $d^2\alpha \equiv d\mathrm{Re}(\alpha)\, d\mathrm{Im}(\alpha)$ and the quasi-probability distribution $\mathrm{P}(\alpha)$ is not necessarily positive. For a given state with the density matrix $\hat{\rho}$ the P-function can be written as

$$\mathrm{P}(\alpha) = \mathrm{tr} : \delta(\hat{a} - \alpha) : \hat{\rho}, \tag{40}$$

where

$$: \delta(\hat{a} - \alpha) := \frac{1}{\pi^2} \int d^2\beta\, e^{\alpha\beta^* - \alpha^*\beta} e^{\beta\hat{a}^\dagger} e^{-\beta^*\hat{a}}, \tag{41}$$

see Ref. [55] for details. Phase-amplification is described by a quantum channel given by

$$\mathrm{Amp}_{G=\cosh^2(g)} : \hat{\rho} \mapsto \mathrm{Amp}_G[\hat{\rho}] = \mathrm{tr}_b \left[\hat{U}_g\, \hat{\rho} \otimes |0\rangle\langle 0|_b\ \hat{U}_g^\dagger \right], \tag{42}$$

where $\hat{U}_g$ is defined by Eq. (37), g is the interaction parameter characterizing the amplifier, $G = \cosh^2(g)$ is the factor by which the intensity of the input signal is amplified, and annihilation operator $\hat{b}$ corresponds to the auxiliary mode starting in the vacuum states. see e.g. [56].

To see how the P-function of a state transforms under the optical amplification, consider a simple situation where the input signal is in the pure coherent state $|\gamma\rangle\langle\gamma|$ with the corresponding initial P-function $\mathrm{P}_i(\alpha) = \delta(\alpha - \gamma)$ (delta-function acting on the complex plane). After the amplification the P-function becomes

$$P(\alpha, \gamma, g) = \mathrm{tr} : \delta(\hat{a} - \alpha) : \mathrm{Amp}_G\left[|\gamma\rangle\langle\gamma|\right]. \tag{43}$$

Bearing in mind the canonical transformation of the amplifier channel from Eq. (38), we get Eqs. (3) and (7) from the main text: given a pure coherent input state (with complex amplitude γ), the output state is a mixture of normally distributed coherent states; the mean complex amplitude is $\sqrt{G}\gamma$ and the standard deviation is $(G-1)/\sqrt{2}$:

$$P(\alpha, \gamma, g) = \frac{1}{\pi(G-1)} \exp\left(-\frac{|\alpha - \sqrt{G}\gamma|^2}{G-1} \right). \tag{44}$$

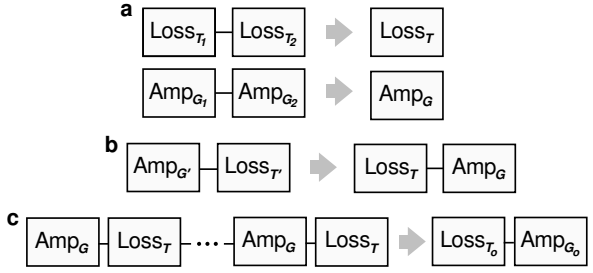

Figure 7 | **Compositions of loss and amplification channels and their equivalent representations. a** Two loss or amplification channels can be reduced to one. **b** Loss and amplification channels can be effectively rearranged. **c** A series of losses and amplifiers can be reduced to one pair of loss and amplification.

3.3 Composition of amplifiers and losses

In our quantum key distribution (QKD) protocol, the amplification is used to compensate the fiber losses. Long-distance transmission requires a cascade of amplifiers, in which case the signal's evolution is determined by a sequence of multiple loss and amplification channels. In this section we prove that any such sequence can be mathematically reduced to

a composition of one loss and one amplification channels. The canonical transformation of the loss channel is

$$\begin{aligned} \mathrm{Loss}^*_T[\hat{a}] = \hat{U}^\dagger_T \hat{a} \hat{U}_T = \sqrt{T}\hat{a} + \sqrt{1-T}\hat{c}, \\ T = \cos^2\lambda, \end{aligned} \tag{45}$$

where λ is the interaction parameter, T is the proportion of the transmitted signal, the annihilation operator $\hat{c}$ corresponds to the initially empty mode which the lost photons go to, and $\hat{U}_\lambda = e^{\lambda\hat{a}^\dagger\hat{c} - \lambda\hat{a}\hat{c}^\dagger}$.

Statement 1. *Two loss or amplification channels can be effectively reduced to one.*

First, we show that a pair of loss or amplification channels can be effectively reduced to the one channel (Fig.7**a**). To that end, let us consider two consequent loss channels:

$$\begin{aligned} \left(\mathrm{Loss}_{T_2} \circ \mathrm{Loss}_{T_1}\right)^* [\hat{a}] &= \sqrt{T_1 T_2}\hat{a} + \sqrt{T_1(1-T_1)}\hat{c}_1 + \sqrt{1-T_2}\hat{c}_2 \\ &= \sqrt{T_1 T_2}\hat{a} + \sqrt{1-T_1 T_2}\hat{c}, \end{aligned} \tag{46}$$

where we defined operator $\hat{c}$

$$\hat{c} = \frac{\sqrt{T_2(1-T_1)}\hat{c}_1 + \sqrt{1-T_2}\hat{c}_2}{\sqrt{1-T_1T_2}}, \tag{47}$$

acting on the vacuum state and satisfying the canonical commutation relation $[\hat{c}, \hat{c}^\dagger] = 1$. The last expression of Eq. (46) represents the action of one loss channel with the effective parameter $T = T_1 T_2$

$$\mathrm{Loss}_{T_2} \circ \mathrm{Loss}_{T_1} = \mathrm{Loss}_{(T=T_1T_2)}. \tag{48}$$

The same reasoning applies to amplifiers

$$\mathrm{Amp}_{G_2} \circ \mathrm{Amp}_{G_1} = \mathrm{Amp}_{G=G_1G_2}. \tag{49}$$

Statement 2. *Loss and amplification can always be represented as a composition where loss is followed by amplification.*

Let us show that the composition of an amplification channel followed by a loss channel can be mathematically replaced with the pair of certain loss and amplification channels acting in the opposite order (Fig.7**b**). Firstly, let us consider the transformation corresponding to the amplification followed by the loss

$$\begin{aligned} \left(\mathrm{Loss}_{T'} \circ \mathrm{Amp}_{G'}\right)^* [\hat{a}] &= \hat{U}^\dagger_{g'} \hat{U}^\dagger_{\lambda'} \hat{a}\, \hat{U}_\lambda \hat{U}_g \\ &= \sqrt{T'G'}\hat{a} + \sqrt{1-T'}\hat{c} + \sqrt{T'(1-G')}\hat{b}^\dagger. \end{aligned} \tag{50}$$

In the case of the opposite order we obtain

$$\begin{aligned} (\mathrm{Amp}_G \circ \mathrm{Loss}_T)^*[\hat{a}] = \hat{U}^\dagger_\lambda \hat{U}^\dagger_g \hat{a}\, \hat{U}_g \hat{U}_\lambda = \\ = \sqrt{TG}\hat{a} + \sqrt{G(1-T)}\hat{c} + \sqrt{G-1}\hat{b}^\dagger. \end{aligned} \tag{51}$$

Considered transformations become identical when the parameters are related as

$$\begin{aligned} \mathrm{Loss}_{T'} \circ \mathrm{Amp}_{G'} = \mathrm{Amp}_G \circ \mathrm{Loss}_T, \\ T = \frac{G'T'}{(G'-1)T'+1}, \\ G = (G'-1)T' + 1. \end{aligned} \tag{52}$$

In other words, the two types of channels "commute" provided that the parameters are modified in accord with these relations. In particular, the parameters in the equation above are always physically meaningful $G \geq 1$, $0 \leq T \leq 1$, meaning that we can always represent loss and amplification in form of a composition where loss is followed by amplification (the converse is not true).

Statement 3. *A series of losses and amplifiers can be effectively reduced to one pair of loss and amplification.*

Let us finally show that the sequence of loss and amplification channels can be mathematically represented as one pair of loss and amplification (Fig.7**c**). Consider the transformation

$$\Phi_M = (\mathrm{Amp}_G \circ \mathrm{Loss}_T)^{\circ M}, \tag{53}$$

corresponding to the series of M identical loss and amplification channels, for which we want to find a simple representation. According to Statement 2, we can effectively move all losses to the right end of the composition, i.e., permute the channels in such a way that all the losses act before amplification. Every time the loss channel with the transmission probability $T_{(i)}$ is moved before an amplifier with the amplification factor $G_{(i)}$, the parameters are transformed in accord with Eq. (52):

$$\begin{aligned} T_{(i)} \mapsto T_{(i+1)} = \frac{G_{(i)}T_{(i)}}{(G_{(i)}-1)T_{(i)}+1}, \\ G_{(i)} \mapsto G_{(i+1)} = (G_{(i)}-1)T_{(i)} + 1. \end{aligned} \tag{54}$$

In our sequence we can pairwise transpose all neighboring losses with amplifier (starting with the first amplifier and the second loss). After repeating this operation $M-1$ times, bearing in mind the Statement 1, we find that

$$\begin{aligned} \Phi_M = \mathrm{Amp}_{G_{(0)}} \circ \mathrm{Amp}_{G_{(1)}} \circ \cdots \circ \mathrm{Amp}_{G_{(M-1)}} \\ \circ \mathrm{Loss}_{T_{(M-1)}} \circ \mathrm{Loss}_{T_{(M-2)}} \circ \cdots \circ \mathrm{Loss}_{T_{(0)}} = \mathrm{Amp}_{G_\circ} \circ \mathrm{Loss}_{T_\circ}, \end{aligned} \tag{55}$$

where

$$T_\circ = \prod_{i=0}^{M-1} T_{(i)}, \quad G_\circ = \prod_{i=0}^{M-1} G_{(i)}, \tag{56}$$

i.e., the series of losses and amplifiers is equivalent to the loss channel of transmission $T_\circ$ followed by the amplifier with amplification factor $G_\circ$. Note now that the value $\eta \equiv G_{(i)}T_{(i)} = GT$ cannot be changed by permutations. Let us define

$$F_{(i)} = (G_{(i)}-1)T_{(i)} + 1, \tag{57}$$

and bear in mind that

$$F_{(i+1)} = (G_{(i+1)}-1)T_{(i+1)} + 1 = \frac{(F_{(i)}-1)}{F_{(i)}}TG + 1 = \eta\left(\frac{F_{(i)}-1}{F_{(i)}}\right) + 1. \tag{58}$$

We can write

$$T_{(i+1)} = \frac{TG}{F_{(i)}}, \quad G_{(i+1)} = F_{(i)}, \tag{59}$$

and

$$G_\circ = G\prod_{i=0}^{M-2} F_{(i)}, \quad T_\circ = \frac{T(TG)^{M-1}}{\prod_{i=0}^{M-2} F_{(i)}} = \frac{(TG)^M}{G_\circ}. \tag{60}$$

Let us find the explicit form of $G_\circ$ and $T_\circ$ by solving the recurrence relation. Define A_n and B_n through the relation

$$F_{(n-1)} = \frac{A_n}{B_n}. \tag{61}$$

Then

$$F_{(n+1)} = \frac{(\eta+1)F_{(n)} - \eta}{F_{(n)}} = \frac{(\eta+1)A_{n+1} - \eta B_{n+1}}{A_{n+1}}. \tag{62}$$

It follows from Eqs. (61) and (62) that $B_{n+1} = A_n$ and

$$A_{n+1} = (\eta+1)A_n - \eta B_n = (\eta+1)A_n - \eta A_{n-1}. \tag{63}$$

We see that the solution of this equation has a form

$$A_n = c_1 + c_2\eta^n, \tag{64}$$

where c_1 and c_2 are the constants, which are determined by $F_0 = (G-1)T+1$: we take $A_1 = (G-1)T+1$ and $A_0 = 1$, and obtain

$$c_1 = \frac{T-1}{GT-1}, \quad c_2 = \frac{(G-1)T}{GT-1}. \tag{65}$$

Notably, the product $\Pi_{n=0}^{M-2} F_{(n)}$ appearing in the final expression becomes relatively simple

$$\prod_{n=0}^{M-2} F_{(n)} = \frac{(G-1)(GT)^M + G(T-1)}{G(GT-1)}, \tag{66}$$

and we have

$$\begin{aligned} \Phi_M &= (\mathrm{Amp}_G \circ \mathrm{Loss}_T)^{\circ M} = \mathrm{Amp}_{G_\circ} \circ \mathrm{Loss}_{T_\circ}, \\ G_\circ &= \frac{(G-1)(GT)^M + G(T-1)}{GT-1}, \\ T_\circ &= \frac{(TG)^M}{G_\circ}. \end{aligned} \tag{67}$$

The case of $TG = 1$ is particularly interesting as the average photon number of the transmitted signal remains preserved (which is different from the total output photon number as it has the noise contribution). In the limit $G \to 1/T$ we have

$$\begin{aligned} G_\circ &= G(M(1-T)+T), \\ T_\circ &= \frac{T}{M(1-T)+T}. \end{aligned} \tag{68}$$

3.4 Effective model of the line

We consider how Eve performs the beam splitter attack seizing the part of the signal somewhere along the optical line as shown in Fig.8**a**. If the signal intensity incident to the beam splitter is 1, then intensity r_E goes to Eve, and $1 - r_\mathrm{E}$ goes to Bob's direction. The proportion of the transmitted signal on the distance d between two neighbouring amplifiers is determined by

$$T = 10^{-\xi \cdot d}, \quad G = \frac{1}{T}, \tag{69}$$

where $\xi = 0.02\,\mathrm{km}^{-1}$ is the parameter of losses typical for the optical fibers and G is amplification factor of each amplifier. Let $D_{\mathrm{AB(AE)}}$ be the distance between Alice and Bob (Alice and Eve), then the numbers of amplifiers before and after the beam splitter M_1 and M_2 are given by

$$\begin{aligned} M_1 &= D_{\mathrm{AE}}/d, \\ M_2 &= (D_{\mathrm{AB}} - D_{\mathrm{AE}})/d. \end{aligned} \tag{70}$$

According to Statement 3, the scheme can be simplified by reducing the losses and amplifications before and after the beam splitter to two loss and amplification pairs with the parameters $\{T_1, G_1\}$ and $\{T_2, G_2\}$ respectively (Fig. 8**b**)

$$G_1 = G\,(M_1(1-T)+T) = \left(10^{\xi \cdot d} - 1\right) \cdot \frac{D_{\mathrm{AE}}}{d} + 1, \; T_1 = \frac{1}{G_1}, \tag{71}$$

$$G_2 = G\,(M_2(1-T)+T) = \left(10^{\xi \cdot d} - 1\right) \cdot \frac{D_{\mathrm{AB}} - D_{\mathrm{AE}}}{d} + 1, \; T_2 = \frac{1}{G_2}. \tag{72}$$

3.5 Fluctuations

Let us calculate the fluctuation of the number of photons in a pulse after it passes through a sequence of M loss regions and amplifiers. Let $|\gamma|^2$ be the input average photon number; as follows from Eqs. (39) and (44), the average number of photons n in the output signal is

$$n = \langle \hat{a}^\dagger \hat{a} \rangle = |\gamma|^2 + G_\circ - 1, \tag{73}$$

where $G_\circ$ is given by Eq. (68). The variance of the output photon number is

$$\begin{aligned} \delta n &= \sqrt{\langle (\hat{a}^\dagger \hat{a})^2 \rangle - (\langle \hat{a}^\dagger \hat{a} \rangle)^2} \\ &= \left(M(G-1)(M(G-1)+1) + |\gamma|^2 (2M(G-1)+1) \right)^{1/2} \end{aligned} \tag{74}$$

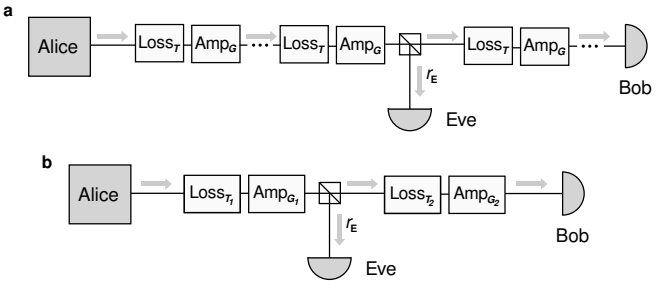

Figure 8 | Schematic representation of a beam splitter attack. a Alice and Bob are connected by a quantum channel comprised of the composition of amplifiers and losses. Eve conducts a beam splitter attack seizing a part of the signal somewhere along the optical line. Thus, she divides the line into two parts. **b** An equivalent scheme: the losses and amplifiers before and after the point of Eve's intervention are represented by two pairs of loss and amplification channels defined by the parameters $\{T_1, G_1\}$ and $\{T_2, G_2\}$ respectively.

Note that even if $|\gamma|^2 = 0$, n and δn are still non-zero. This particularly means that on top of the mode of interest, amplification also generates noise in other modes. Assume that Bob has an optical filter with bandwidth $\Delta\nu$ on which the amplification factor is constant, and the detection time is $\tau \gg 1/\Delta\nu$. Then, the average number of photons due to noise from the secondary modes is

$$n_{\mathrm{noise}} \simeq 2[G(M(1-T)+T) - 1]\tau\Delta\nu, \tag{75}$$

where factor 2 is due to two possible polarizations. We will thoroughly address the issue of noise at different optical filtration regimes in our forthcoming experimental publication.

In the limit $|\gamma|^2 \gg GM \gg 1$ for the ideal optical filter transmitting only the signal mode we get

$$\delta n \simeq \sqrt{nGM}. \tag{76}$$

Provided that there are no other sources of noise, this quantity determines the precision of the physical loss control: if the test pulse carries n photons, the minimum detectable leakage is

$$r_{\mathrm{E}}^{\min} \sim \sqrt{MGn}/n = \sqrt{MG/n} \tag{77}$$

The result coincides with the estimate given in Methods.

NOTE 4. Photon number encoding

This note is devoted to the detailed description of the photon number encoding scheme in the context of the beam splitter attack. We derive the respective amounts of information that the users and Eve know about the transmitted signal. We also address correlations due to the optical amplification between Eve's and Bob's quantum states.

4.1 Phase randomization

In the photon number encoding, we assume the phase of each signal pulse being completely random [57], and unknown both to the eavesdropper and the users. The phase alteration between consecutive signal pulses may be achieved through rebooting the light source after each pulse, or with an additional randomly acting phase modulator. We take that Bob's performs solely the energy measurement of the incoming states without measuring the phases, so Alice does not send the phase reference. In this case, Eve cannot measure the phases either, and the combined system of Alice's random bit (A), the signal incident to Bob (S) and Eve's seized state (E) can be expressed as a mixture of states averaged over all

possible phases,

$$\left\langle \hat{\rho}_{\mathrm{ASE}}^{\rightarrow\mathrm{Bob}} \right\rangle_{\varphi} = \frac{1}{2\pi} \int_0^{2\pi} d\varphi \left[\frac{1}{2} \sum_{a=0,1} |a\rangle\langle a|_{\mathrm{A}} \otimes \int d^2\alpha \; P(\alpha, \sqrt{T_1} e^{i\varphi}\gamma_a, G_1) \right.$$
$$\left. \times \left(\int d^2\beta \; P\left(\beta, \sqrt{(1-r_{\mathrm{E}})T_2}\alpha, G_2\right) \cdot |\beta\rangle\langle\beta|_{\mathrm{S}} \right) \otimes |\sqrt{r_{\mathrm{E}}}\alpha\rangle\langle\sqrt{r_{\mathrm{E}}}\alpha|_{\mathrm{E}} \right]. \quad (78)$$

It follows from Eq. (44) that for any $\varphi \in \mathbb{R}$ we have $P\left(x, ye^{i\varphi}, z\right) = P\left(xe^{-i\varphi}, y, z\right)$. We thus can write

$$\left\langle \hat{\rho}_{\mathrm{ASE}}^{\rightarrow\mathrm{Bob}} \right\rangle_{\varphi} = \frac{1}{2} \sum_{a=0,1} |a\rangle\langle a|_{\mathrm{A}} \otimes \int d^2\alpha \; P(\alpha, \sqrt{T_1}\gamma_a, G_1)$$
$$\times \int d^2\beta \; P\left(\beta, \sqrt{(1-r_{\mathrm{E}})T_2}\alpha, G_2\right)$$
$$\times \frac{1}{2\pi} \int_0^{2\pi} d\varphi \; |e^{i\varphi}\beta\rangle\langle e^{i\varphi}\beta|_{\mathrm{S}} \otimes |\sqrt{r_{\mathrm{E}}}e^{i\varphi}\alpha\rangle\langle\sqrt{r_{\mathrm{E}}}e^{i\varphi}\alpha|_{\mathrm{E}}. \quad (79)$$

4.2 Bob's information

We first estimate the mutual information between Alice and Bob, which is $S(\mathrm{A}) - S(\mathrm{A|B})$ in Eq. (6) of the main text. For that purpose, we trace out Eve's subsystem and consider a bipartite quantum state shared between legitimate users right before Bob's measurement is conducted $\left\langle \hat{\rho}_{\mathrm{AS}}^{\rightarrow\mathrm{Bob}} \right\rangle_{\varphi} = \mathrm{tr}_{\mathrm{E}} \left\langle \hat{\rho}_{\mathrm{ASE}}^{\rightarrow\mathrm{Bob}} \right\rangle_{\varphi}$

$$\left\langle \hat{\rho}_{\mathrm{AS}}^{\rightarrow\mathrm{Bob}} \right\rangle_{\varphi} = \frac{1}{2} \sum_{a=0,1} |a\rangle\langle a|_{\mathrm{A}} \otimes \int d^2\alpha \; P(\alpha, \sqrt{T_1}\gamma_a, G_1)$$
$$\times \left(\int d^2\beta \; P\left(\beta, \sqrt{(1-r_{\mathrm{E}})T_2}\alpha, G_2\right) \cdot \frac{1}{2\pi} \int_0^{2\pi} d\varphi \; |\beta e^{i\varphi}\rangle\langle\beta e^{i\varphi}|_{\mathrm{S}} \right). \quad (80)$$

Given that Alice sent bit $a \in \{0, 1\}$, the probability that Bob's measurement outcome is $b \in \{0, 1, \mathrm{fail}\}$ can be written as

$$p(b|a) = \int \frac{d^2\alpha}{\pi(G_1 - 1)} \cdot \exp\left(-\frac{\left|\alpha - \sqrt{G_1 T_1}\gamma_a\right|^2}{G_1 - 1} \right) \int \frac{d^2\beta}{\pi(G_2 - 1)}$$
$$\times \exp\left(-\frac{\left|\beta - \sqrt{(1-r_{\mathrm{E}})G_2 T_2}\alpha\right|^2}{G_2 - 1} \right) \cdot \frac{1}{2\pi} \int_0^{2\pi} d\varphi \, \langle\beta e^{i\varphi}| \hat{E}_b |\beta e^{i\varphi}\rangle. \quad (81)$$

The probability of finding k photons in the coherent state $|\beta e^{i\varphi}\rangle$ is defined by the Poisson distribution and depends only on $|\beta|$

$$\left|\langle k|\beta e^{i\varphi}\rangle\right|^2 = \frac{|\beta|^{2k} e^{-|\beta|^2}}{k!} = |\langle k|\beta\rangle|^2, \quad (82)$$

which particularly means that for any b $\langle\beta e^{i\varphi}| \hat{E}_b |\beta e^{i\varphi}\rangle = \langle\beta| \hat{E}_b |\beta\rangle$. As it follows from our numerical simulations, for the transmission distances of the order of 1000 km and more, the information pulses $|\gamma_a\rangle$ should comprise hundreds or thousands of photons. This enables us to replace the Poisson distributions with the normal distribution, $\mathcal{N}\left(|\beta|^2, |\beta|^2\right)$:

$$\langle\beta e^{i\varphi}| \hat{E}_1 |\beta e^{i\varphi}\rangle = \langle\beta| \hat{E}_1 |\beta\rangle =$$
$$= \sum_{k=\mu+\theta_2}^{\mu+\theta_4} \frac{|\beta|^{2k} e^{-|\beta|^2}}{k!} \approx \int_{\mu+\theta_2}^{\mu+\theta_4} \frac{dk}{\sqrt{2\pi|\beta|^2}} \cdot \exp\left(-\frac{\left(k - |\beta|^2\right)^2}{2|\beta|^2} \right)$$
$$= \frac{1}{2}\mathrm{erf}\left(\frac{|\beta|^2 - (\mu + \theta_2)}{\sqrt{2}|\beta|} \right) - \frac{1}{2}\mathrm{erf}\left(\frac{|\beta|^2 - (\mu + \theta_4)}{\sqrt{2}|\beta|} \right); \quad (83)$$

$$\langle\beta| \hat{E}_0 |\beta\rangle \approx \frac{1}{2}\mathrm{erf}\left(\frac{|\beta|^2 - (\mu - \theta_3)}{\sqrt{2}|\beta|} \right) - \frac{1}{2}\mathrm{erf}\left(\frac{|\beta|^2 - (\mu - \theta_1)}{\sqrt{2}|\beta|} \right). \quad (84)$$

Turning again to Eq. (81), we can change the integration order using Fubini's theorem. The analytical integration over $d^2\alpha$ gives us

$$p(b|a) = \frac{e^{-\frac{\gamma_a^2(1-r_{\mathrm{E}})}{G_1+G_2-2-r_{\mathrm{E}}(G_1-1)}}}{\pi(G_1 + G_2 - 2 - r_{\mathrm{E}}(G_1 - 1))} \cdot \int_0^{+\infty} d|\beta| \; |\beta| \cdot e^{-\frac{|\beta|^2}{G_1+G_2-2-r_{\mathrm{E}}(G_1-1)}}$$
$$\times \langle\beta| \hat{E}_b |\beta\rangle \int_0^{2\pi} d\varphi_\beta \; \exp\left(\frac{2\sqrt{1-r_{\mathrm{E}}}\gamma_a|\beta|\cos\varphi_\beta}{G_1 + G_2 - 2 - r_{\mathrm{E}}(G_1 - 1)} \right), \quad (85)$$

where $\varphi_\beta = \arg(\beta)$. The rightmost integral can be reduced to the modified Bessel function of the first kind:

$$\int_0^{2\pi} d\varphi_\beta \; \exp\left(\frac{2\sqrt{1-r_{\mathrm{E}}}\gamma_a|\beta|\cos\varphi_\beta}{G_1 + G_2 - 2 - r_{\mathrm{E}}(G_1 - 1)} \right)$$
$$= 2\pi \cdot I_0\left(\frac{2\sqrt{1-r_{\mathrm{E}}}\gamma_a|\beta|}{G_1 + G_2 - 2 - r_{\mathrm{E}}(G_1 - 1)} \right). \quad (86)$$

Thus, we have

$$p(b|a) = \frac{2e^{-\frac{\gamma_a^2(1-r_{\mathrm{E}})}{G_1+G_2-2-r_{\mathrm{E}}(G_1-1)}}}{G_1 + G_2 - 2 - r_{\mathrm{E}}(G_1 - 1)} \int_0^{+\infty} d|\beta| \; |\beta| \cdot \langle\beta| \hat{E}_b |\beta\rangle$$
$$\times I_0\left(\frac{2\sqrt{1-r_{\mathrm{E}}}\gamma_a|\beta|}{G_1 + G_2 - 2 - r_{\mathrm{E}}(G_1 - 1)} \right) \cdot e^{-\frac{|\beta|^2}{G_1+G_2-2-r_{\mathrm{E}}(G_1-1)}}. \quad (87)$$

The mutual information between Alice and Bob after the post-selection can be calculated as

$$I(\mathrm{A,B}) \equiv S(\mathrm{A}) - S(\mathrm{A|B}) = S(\mathrm{A}) + S(\mathrm{B}) - S(\mathrm{AB})$$
$$= h_2\left(\sum_{b=0,1} \frac{p(b|0)}{2p_{\checkmark}} \right) + h_2\left(\sum_{a=0,1} \frac{p(0|a)}{2p_{\checkmark}} \right) + \sum_{a=0,1} \sum_{b=0,1} \frac{p(b|a)}{2p_{\checkmark}} \log_2\left(\frac{p(b|a)}{2p_{\checkmark}} \right), \quad (88)$$

where $h_2(p) = -p \cdot \log_2 p - (1-p) \cdot \log_2(1-p)$ is the binary entropy and the probability of the conclusive measurement outcome is

$$p_{\checkmark} = \frac{1}{2} \sum_{a=0,1} \sum_{b=0,1} p(b|a). \quad (89)$$

4.3 Eve's information

To estimate Eve's information ($I(\mathrm{A:E})$ in the Eq. (6) of the main text), we find the explicit form of the quantum state owned by Eve after the users perform post-selection. The density matrix of the joint ABE system is

$$\left\langle \hat{\rho}_{\mathrm{ABE}}^{f} \right\rangle_{\varphi} = \sum_{b=0,1} \sum_{a=0,1} \frac{1}{2p(\checkmark|a)} \int d^2\alpha \; P(\alpha, \sqrt{T_1}\gamma_a, G_1)$$
$$\times |a\rangle\langle a|_{\mathrm{A}} \otimes |b\rangle\langle b|_{\mathrm{B}} \otimes \frac{1}{2\pi} \int_0^{2\pi} d\varphi \; \left|e^{i\varphi}\sqrt{r_{\mathrm{E}}}|\alpha|\right\rangle \left\langle e^{i\varphi}\sqrt{r_{\mathrm{E}}}|\alpha|\right|_{\mathrm{E}}$$
$$\times \int d^2\beta \; P\left(\beta, \sqrt{(1-r_{\mathrm{E}})T_2}\alpha, G_2\right) \langle\beta|\hat{E}_b|\beta\rangle. \quad (90)$$

For the further calculations it is useful to introduce "conditional" Eve's density matrix, i.e., Eve's density matrix in the case that Alice sent bit a and Bob got a conclusive measurement outcome:

$$\hat{\rho}_{\mathrm{E}}^{(a)} \equiv \mathrm{tr}_{\mathrm{AB}}\left[\left(2|a\rangle\langle a|_{\mathrm{A}} \otimes \hat{\mathbb{1}} \otimes \hat{\mathbb{1}} \right) \cdot \left\langle \hat{\rho}_{\mathrm{ABE}}^{f} \right\rangle_{\varphi} \right]. \quad (91)$$

The explicit form of this matrix is

$$\hat{\rho}_{\mathrm{E}}^{(a)} = \frac{1}{p(\checkmark|a)} \int d^2\alpha \; P\left(\alpha;\, \sqrt{T_1}\gamma_a, G_1\right) \times \int d^2\beta \; P\left(\beta;\, \sqrt{(1-r_{\mathrm{E}})T_2}\alpha, G_2\right) \langle\beta|\hat{E}_{\checkmark}|\beta\rangle \times \left[\frac{1}{2\pi}\int_0^{2\pi} d\varphi \;\; \left|e^{i\varphi}\sqrt{r_{\mathrm{E}}}|\alpha|\right\rangle\left\langle e^{i\varphi}\sqrt{r_{\mathrm{E}}}|\alpha|\right|_{\mathrm{E}}\right], \quad (92)$$

where $\hat{E}_{\checkmark} \equiv \hat{E}_0 + \hat{E}_1$. To simplify the expression, one can convert integration into Polar coordinates ($\alpha = |\alpha|e^{i\varphi_\alpha}$, $d^2\alpha = |\alpha|\, d|\alpha|\, d\varphi_\alpha$), apply Fubini's theorem, and carry out integration over φ_α analytically

$$\int_0^{2\pi} d\varphi_\alpha \; P\left(|\alpha|e^{i\varphi_\alpha};\, \sqrt{T_1}\gamma_a, G_1\right) = \frac{2\exp\left(-\frac{|\alpha|^2+|\gamma_a|^2}{G_1-1}\right)}{G_1-1} \cdot I_0\left(\frac{2|\alpha|\gamma_a}{G_1-1}\right), \quad (93)$$

where $I_0(z)$ is the modified Bessel function of the first kind. The same procedure can be carried out for integration over β: bearing in mind that $\langle\beta|\hat{E}_{\checkmark}|\beta\rangle$ does not depend on φ_β, we have

$$\int_0^{2\pi} d\varphi_\beta \; P\left(|\beta|e^{i\varphi_\beta};\, \sqrt{(1-r_{\mathrm{E}})T_2}\alpha, G_2\right) = \frac{2\exp\left(-\frac{|\beta|^2+(1-r_{\mathrm{E}})|\alpha|^2}{G_2-1}\right)}{G_2-1} \cdot I_0\left(\frac{2|\beta|\sqrt{1-r_{\mathrm{E}}}|\alpha|}{G_2-1}\right). \quad (94)$$

The rightmost integral in Eq. (92) also can be calculated in the analytical way and expressed in terms of the Fock states $\{|n\rangle\}_{n=0}^{+\infty}$:

$$\frac{1}{2\pi}\int_0^{2\pi} d\varphi \;\; \left|e^{i\varphi}\sqrt{r_{\mathrm{E}}}|\alpha|\right\rangle\left\langle e^{i\varphi}\sqrt{r_{\mathrm{E}}}|\alpha|\right| = e^{-r_{\mathrm{E}}|\alpha|^2} \sum_{n=0}^{+\infty} \frac{\left(r_{\mathrm{E}}|\alpha|^2\right)^n}{n!} |n\rangle\langle n|. \quad (95)$$

Substituting the results from Eqs. (93–95) into Eq. (92), we get

$$\hat{\rho}_{\mathrm{E}}^{(a)} = \frac{4/p(\checkmark|a)}{(G_1-1)(G_2-1)} \int_0^{+\infty} d|\alpha| \;\; |\alpha| \exp\left(-\frac{|\alpha|^2+|\gamma_a|^2}{G_1-1}\right) I_0\left(\frac{2|\alpha|\gamma_a}{G_1-1}\right) \times \int_0^{+\infty} d|\beta| \;\; |\beta| \exp\left(-\frac{|\beta|^2+(1-r_{\mathrm{E}})|\alpha|^2}{G_2-1}\right) I_0\left(\frac{2|\beta|\sqrt{1-r_{\mathrm{E}}}|\alpha|}{G_2-1}\right) \cdot \langle\beta|\hat{E}_{\checkmark}|\beta\rangle \times \sum_{n=0}^{+\infty} \exp\left(-r_{\mathrm{E}}|\alpha|^2\right) \frac{\left(r_{\mathrm{E}}|\alpha|^2\right)^n}{n!} |n\rangle\langle n|. \quad (96)$$

Note that the resulting density matrix is diagonal in the Fock basis—which is natural given the phase randomization. The diagonal elements of the matrix can be expressed as

$$\langle n|\hat{\rho}_{\mathrm{E}}^{(a)}|n\rangle = \frac{4r_{\mathrm{E}}^n \exp\left(-\frac{\gamma_a^2}{G_1-1}\right)}{n!(G_1-1)(G_2-1)p(\checkmark|a)} \int_0^{+\infty} d|\beta| \;\; |\beta| \cdot f(|\beta|) \exp\left(-\frac{|\beta|^2}{G_2-1}\right) \times \int_0^{+\infty} d|\alpha| \;\; |\alpha|^{2n+1} \exp\left(-|\alpha|^2 \cdot \left[\frac{1}{G_1-1} + \frac{1-r_{\mathrm{E}}}{G_2-1} + r_{\mathrm{E}}\right]\right) \times I_0\left(\frac{2|\alpha|\gamma_a}{G_1-1}\right) \cdot I_0\left(\frac{2|\beta|\sqrt{1-r_{\mathrm{E}}}|\alpha|}{G_2-1}\right). \quad (97)$$

In order to take integral over $|\alpha|$ analytically, we utilize the fact that the main contribution to the integral comes from $|\alpha| \gg 1$ which enables us to use the asymptotic expansion [58]:

$$I_0(z) = \frac{e^z}{\sqrt{2\pi z}}\left(1 + \frac{1}{8z} + O\left(\frac{1}{|z|^2}\right)\right), \; z \in \mathbb{R}. \quad (98)$$

Thus, we have

$$I_0\left(\frac{2|\alpha|\gamma_a}{G_1-1}\right) \cdot I_0\left(\frac{2|\beta|\sqrt{1-r_{\mathrm{E}}}|\alpha|}{G_2-1}\right) = \frac{1}{4\pi|\alpha|}\sqrt{\frac{(G_1-1)(G_2-1)}{\gamma_a|\beta|\sqrt{1-r_{\mathrm{E}}}}} \exp\left(2|\alpha| \cdot \left(\frac{\gamma_a}{G_1-1} + \frac{|\beta|\sqrt{1-r_{\mathrm{E}}}}{G_2-1}\right)\right) \times \left(1 + \frac{1}{16|\alpha|}\left[\frac{G_1-1}{\gamma_a} + \frac{G_2-1}{|\beta|\sqrt{1-r_{\mathrm{E}}}}\right] + O\left(\frac{1}{|\alpha|^2}\right)\right). \quad (99)$$

Utilizing this form, we get

$$\langle n|\hat{\rho}_{\mathrm{E}}^{(a)}|n\rangle \approx \frac{r_{\mathrm{E}}^n \exp\left(-\frac{\gamma_a^2}{G_1-1}\right)/p(\checkmark|a)}{\pi\sqrt{\gamma_a|\beta|\sqrt{1-r_{\mathrm{E}}}}(G_1-1)(G_2-1)} \int_0^{+\infty} d|\beta| \;\; |\beta| \cdot f(|\beta|) \times \left(\varkappa_n(|\beta|) + \frac{1}{16}\left[\frac{G_1-1}{\gamma_a} + \frac{G_2-1}{|\beta|\sqrt{1-r_{\mathrm{E}}}}\right]\tilde{\varkappa}_n(|\beta|)\right) \cdot e^{-\frac{|\beta|^2}{G_2-1}}, \quad (100)$$

where we introduced two subsidiary functions $\varkappa_n(|\beta|)$ and $\tilde{\varkappa}_n(|\beta|)$, $n \in \mathbb{N}$: we define

$$\varkappa_n(|\beta|) = \int_0^{+\infty} d|\alpha| \;\; \frac{|\alpha|^{2n}}{n!} \cdot e^{-A|\alpha|^2+B|\alpha|} = \frac{1}{A^{n+1/2}} \cdot \left[\sqrt{\frac{B^2}{4A}} \cdot {}_1F_1\left(n+1, \frac{3}{2}, \frac{B^2}{4A}\right) + \frac{\Gamma\left(n+\frac{1}{2}\right)}{2\cdot n!} \cdot {}_1F_1\left(n+\frac{1}{2}, \frac{1}{2}, \frac{B^2}{4A}\right)\right], \quad (101)$$

where ${}_1F_1(x,y,z)$ is the Kummer confluent hypergeometric function (for large values of the third argument we utilize the approximation from Ref. [58]), and

$$A = \frac{1}{G_1-1} + \frac{1-r_{\mathrm{E}}}{G_2-1} + r_{\mathrm{E}}, \quad (102)$$

$$B \equiv B(|\beta|) = \frac{2\gamma_a}{G_1-1} + \frac{2|\beta|\sqrt{1-r_{\mathrm{E}}}}{G_2-1}. \quad (103)$$

Function $\tilde{\varkappa}_n(|\beta|)$ is defined similarly:

$$\tilde{\varkappa}_n(|\beta|) = \int_0^{+\infty} d|\alpha| \;\; \frac{|\alpha|^{2n-1}}{n!} \cdot e^{-A|\alpha|^2+B|\alpha|} = \frac{1}{A^{n-1/2}} \cdot \left[\sqrt{\frac{B^2}{4A}} \cdot \frac{\Gamma\left(n+\frac{1}{2}\right)}{n!} \cdot {}_1F_1\left(n+\frac{1}{2}, \frac{3}{2}, \frac{B^2}{4A}\right) + \frac{1}{2n} \cdot {}_1F_1\left(n, \frac{1}{2}, \frac{B^2}{4A}\right)\right]. \quad (104)$$

For $n = 0$ the integral from Eq. (104) does not converge—let us address this case individually. Instead considering two terms of the series in Eq. (98), we take into account only the first one, which makes the primary contribution to the sum for large $|\alpha|$; thus, we get

$$\varkappa_0(|\beta|) = \int_0^{+\infty} d|\alpha| \; e^{-A|\alpha|+B|\alpha|} = \frac{\sqrt{\pi}e^{B^2/4A}}{2\sqrt{A}}\operatorname{erfc}\left(\frac{B}{2\sqrt{A}}\right), \quad \tilde{\varkappa}_0(|\beta|) = 0. \quad (105)$$

With the beam splitter attack, Eve gets one of two non-equiprobable quantum states: $\hat{\rho}_{\mathrm{E}}^{(0)}$ with probability $q_0 = \frac{p(\checkmark|0)}{2p_{\checkmark}}$ and $\hat{\rho}_{\mathrm{E}}^{(1)}$ with $q_1 = \frac{p(\checkmark|1)}{2p_{\checkmark}}$. The explicit forms of diagonal $\hat{\rho}_{\mathrm{E}}^{(0)}$ and $\hat{\rho}_{\mathrm{E}}^{(1)}$ can be obtained by substituting the results from Eqs. (101–105) into Eq. (100). Eve's ensemble $\mathcal{E}$ can be shortly defined as

$$\mathcal{E} = \left\{\left(q_0, \hat{\rho}_{\mathrm{E}}^{(0)}\right), \left(q_1, \hat{\rho}_{\mathrm{E}}^{(1)}\right)\right\}. \quad (106)$$

The maximum information that Eve can obtain about Alice's bit on average is bounded by the Holevo quantity $\chi(\mathcal{E})$:

$$I(\mathrm{A},\mathrm{E}) \le \chi(\mathcal{E}) = S\left(q_0\hat{\rho}_{\mathrm{E}}^{(0)} + q_1\hat{\rho}_{\mathrm{E}}^{(1)}\right) - q_0 S\left(\hat{\rho}_{\mathrm{E}}^{(0)}\right) - q_1 S\left(\hat{\rho}_{\mathrm{E}}^{(1)}\right). \quad (107)$$

Since $\hat{\rho}_{\mathrm{E}}^{(0)}$ and $\hat{\rho}_{\mathrm{E}}^{(1)}$ are diagonal, Eq. (107) can be simplified by replacing von Neuman entropy S with the classical Shannon entropy H

$$S\left(q_0\hat{\rho}_{\mathrm{E}}^{(0)} + q_1\hat{\rho}_{\mathrm{E}}^{(1)}\right) = H\left(\left\{q_0\langle n|\hat{\rho}_{\mathrm{E}}^{(0)}|n\rangle + q_1\langle n|\hat{\rho}_{\mathrm{E}}^{(1)}|n\rangle\right\}_{n=0}^{+\infty}\right), \quad (108)$$

$$S\left(\hat{\rho}_{\mathrm{E}}^{(a)}\right) = H\left(\left\{\langle n|\hat{\rho}_{\mathrm{E}}^{(a)}|n\rangle\right\}_{n=0}^{+\infty}\right), \quad (109)$$

where the Shannon entropy of a probability distribution $\left\{w_j\right\}_j$ is defined as $H\left(\{w_j\}_j\right) = -\sum_j w_j \log_2\left(w_j\right)$.

4.4 Correlations

Stealing a proportion r_{E} of a coherent signal pulse $|\gamma\rangle$ provides Eve with a state $|\sqrt{r_{\mathrm{E}}}\gamma\rangle$ uncorrelated with $|\gamma\rangle$, as the state of the joint system is described by product $|\sqrt{1-r_{\mathrm{E}}}\gamma\rangle\otimes|\sqrt{r_{\mathrm{E}}}\gamma\rangle$. This is, however, not the case when the signal pulse is subject to optical amplification, turning a pure coherent state into a mixture of coherent states: now, by splitting off same r_{E}-fraction of this mixture, Eve gets a correlated state containing more information about the sent bit. Therefore, contrary to one's executions, for Eve standing right next to Alice may be less effective than somewhere further along the line—provided that the noise from the optical amplifiers does not overweight the benefits of correlations. Assuming that Eve performs the beam splitter attack, we quantify the correlation between Eve's and Bob's measurement results by calculating the Pearson correlation coefficient [59,60]

$$R_{\mathrm{BE}} = \frac{\langle\langle n_{\mathrm{B}} n_{\mathrm{E}}\rangle\rangle}{\sigma_{n_{\mathrm{B}}}\cdot\sigma_{n_{\mathrm{E}}}}, \quad (110)$$

where $\langle\langle\ldots\rangle\rangle$ stands for irreducible correlator, $\sigma_{n_{\mathrm{B(E)}}}$ is the standard variance. The values are defined as follows

$$\langle\langle n_{\mathrm{B}} n_{\mathrm{E}}\rangle\rangle = \langle n_{\mathrm{B}} n_{\mathrm{E}}\rangle_{\hat{\rho}_{\mathrm{BE}}} - \langle n_{\mathrm{B}}\rangle_{\hat{\rho}_{\mathrm{B}}}\cdot\langle n_{\mathrm{E}}\rangle_{\hat{\rho}_{\mathrm{E}}}, \quad (111)$$

$$\sigma_{n_{\mathrm{B}}} = \sqrt{\left\langle n_{\mathrm{B}}^2\right\rangle_{\hat{\rho}_{\mathrm{B}}} - \langle n_{\mathrm{B}}\rangle_{\hat{\rho}_{\mathrm{B}}}^2}, \quad \sigma_{n_{\mathrm{E}}} = \sqrt{\left\langle n_{\mathrm{E}}^2\right\rangle_{\hat{\rho}_{\mathrm{E}}} - \langle n_{\mathrm{E}}\rangle_{\hat{\rho}_{\mathrm{E}}}^2}. \quad (112)$$

Averaging over a density matrix $\hat{\rho}$ is denoted here as $\langle\ldots\rangle_{\hat{\rho}}$. As follows from Eq. (79), the Bob-Eve density matrix can be written as

$$\hat{\rho}_{\mathrm{BE}} = \int d^2\alpha\ P\left(\alpha, \sqrt{T_1}\gamma, G_1\right)\int d^2\beta\ P\left(\beta, \sqrt{T_2(1-r_{\mathrm{E}})}\alpha, G_2\right) \times \int_0^{2\pi}\frac{d\varphi}{2\pi}\ |\sqrt{1-r_{\mathrm{E}}}\alpha e^{i\varphi}\rangle\langle\sqrt{1-r_{\mathrm{E}}}\alpha e^{i\varphi}|_{\mathrm{B}}\otimes|\sqrt{r_{\mathrm{E}}}\alpha e^{i\varphi}\rangle\langle\sqrt{r_{\mathrm{E}}}\alpha e^{i\varphi}|_{\mathrm{E}}, \quad (113)$$

$$\hat{\rho}_{\mathrm{B}} = \mathrm{tr}_{\mathrm{E}}\left[\hat{\rho}_{\mathrm{BE}}\right], \quad \hat{\rho}_{\mathrm{E}} = \mathrm{tr}_{\mathrm{B}}\left[\hat{\rho}_{\mathrm{BE}}\right], \quad (114)$$

where the effective amplification coefficients G_1, G_2 and transmission probabilities T_1, T_2 are defined by Eqs. (71) and (72). The average photon numbers of Bob's and Eve's subsystems are

$$\langle n_{\mathrm{B}}\rangle_{\hat{\rho}_{\mathrm{B}}} = \int d^2\alpha\ P\left(\alpha, \sqrt{T_1}\gamma, G_1\right)\int d^2\beta\ P\left(\beta, \sqrt{T_2(1-r_{\mathrm{E}})}\alpha, G_2\right)\cdot|\beta|^2 = (1-r_{\mathrm{E}})\cdot\left(|\gamma|^2 + G_1 - 1\right) + G_2 - 1, \quad (115)$$

$$\langle n_{\mathrm{E}}\rangle_{\hat{\rho}_{\mathrm{E}}} = \int d^2\alpha\ P\left(\alpha, \sqrt{T_1}\gamma, G_1\right)\cdot|\sqrt{r_{\mathrm{E}}}\alpha|^2 = r_{\mathrm{E}}\cdot\left(|\gamma|^2 + G_1 - 1\right). \quad (116)$$

The average product value is

$$\langle n_{\mathrm{B}} n_{\mathrm{E}}\rangle_{\hat{\rho}_{\mathrm{BE}}} = r_{\mathrm{E}}(G_2-1)\cdot\left(|\gamma|^2 + G_1 - 1\right) + r_{\mathrm{E}}(1-r_{\mathrm{E}})\cdot\left(2(G_1-1)^2 + 4|\gamma|^2(G_1-1) + |\gamma|^4\right). \quad (117)$$

Hence, the expression for the irreducible correlator depends only on $|\gamma|^2$, r_{E} and G_1:

$$\langle\langle n_{\mathrm{B}} n_{\mathrm{E}}\rangle\rangle = r_{\mathrm{E}}(1-r_{\mathrm{E}})\cdot(G_1-1)\cdot\left(2|\gamma|^2 + G_1 - 1\right). \quad (118)$$

Here, we utilized the fact that $\langle n\rangle_{|\alpha\rangle\langle\alpha|} = |\alpha|^2$. In turn, the variances are obtained using the fact that $\langle n^2\rangle_{|\alpha\rangle\langle\alpha|} = |\alpha|^4 + |\alpha|^2$:

$$\sigma_{\mathrm{B}}^2 = (1-r_{\mathrm{E}})\cdot\left(|\gamma|^2 + G_1 - 1\right)\cdot(1 + 2(G_2-1)) + (1-r_{\mathrm{E}})^2\cdot(G_1-1)\cdot\left(2|\gamma|^2 + G_1 - 1\right) + G_2(G_2-1), \quad (119)$$

$$\sigma_{\mathrm{E}}^2 = r_{\mathrm{E}}\left(|\gamma|^2 + G_1 - 1\right) + r_{\mathrm{E}}^2(G_1-1)\left(2|\gamma|^2 + G_1 - 1\right). \quad (120)$$

Substituting Eqs. (118–120) and Eqs. (71, 72) into Eq. (110) yields the dependence of R_{BE} on D_{AE}. Function $R_{\mathrm{BE}}(D_{\mathrm{AE}})$ is monotonically growing which shows that with Eve approaching Bob, their measurement results become more and more correlated. As expected, if $G_1 = 1$—corresponding to the case where Eve is right next to Alice—$R_{\mathrm{BE}}(D_{\mathrm{AE}})$ vanishes, meaning zero correlations.

NOTE 5. Phase encoding

In this note, we study the phase encoding scheme. We perform our analysis along the same lines as in the case of the photon number encoding.

5.1 Bob's information

For self-evident reasons, phase randomization approach is inapplicable in case of phase encoding-based protocol. The density matrix describing the tripartite system right before Bob's measurement is

$$\hat{\rho}_{\mathrm{AS}}^{\to\mathrm{Bob}} = \frac{1}{2}\sum_{a=0,1}|a\rangle\langle a|_{\mathrm{A}}\otimes\int d^2\alpha\ P(\alpha, \sqrt{T_1}\gamma_a, G_1) \times\left(\int d^2\beta\ P\left(\beta, \sqrt{(1-r_{\mathrm{E}})T_2}\alpha, G_2\right)\cdot|\beta\rangle\langle\beta|_{\mathrm{S}}\right). \quad (121)$$

Given that Alice sent bit $a\in\{0,1\}$, the probability that Bob's measurement outcome is $b\in\{0,1\}$ can be written as

$$p(b|a) = \int\frac{d^2\alpha}{\pi(G_1-1)}\cdot\exp\left(-\frac{|\alpha-\gamma_a|^2}{G_1-1}\right) \times\int\frac{d^2\beta}{\pi(G_2-1)}\exp\left(-\frac{\left|\beta-\sqrt{1-r_{\mathrm{E}}}\alpha\right|^2}{G_2-1}\right)\cdot\langle\beta|\hat{E}_b|\beta\rangle. \quad (122)$$

The overlap between coherent state $|\beta\rangle$ and the state with a particular value of the $\hat{q}-$quadrature is

$$|\langle q|\beta\rangle|^2 = \sqrt{\frac{2}{\pi}}\cdot\exp\left(-2\left(\mathrm{Re}[\beta]-q\right)^2\right). \quad (123)$$

For conclusive measurement results on the Bob's side we have

$$\langle\beta|\hat{E}_0|\beta\rangle = \frac{1}{2}\int_{\theta_1'}^{\theta_2'}dq\ e^{-2(\mathrm{Re}[\beta]-q)^2}, \quad \langle\beta|\hat{E}_1|\beta\rangle = \frac{1}{2}\int_{-\theta_2'}^{-\theta_1'}dq\ e^{-2(\mathrm{Re}[\beta]-q)^2}. \quad (124)$$

The expression for conditional probabilities $p(b|a)$ can be determined analytically

$$p(b|a) = \frac{1}{2}\mathrm{erf}\left(\frac{\sqrt{2}\left(\theta_2' + (-1)^{a+b}\cdot\gamma\sqrt{1-r_{\mathrm{E}}}\right)}{\sqrt{1+2(G_2-1)+2(1-r_{\mathrm{E}})(G_1-1)}}\right) - \frac{1}{2}\mathrm{erf}\left(\frac{\sqrt{2}\left(\theta_1' + (-1)^{a+b}\cdot\gamma\sqrt{1-r_{\mathrm{E}}}\right)}{\sqrt{1+2(G_2-1)+2(1-r_{\mathrm{E}})(G_1-1)}}\right). \quad (125)$$

Since $p(\checkmark|0) = p(\checkmark|1)$, the mutual information between Alice and Bob is

$$I(\mathrm{A},\mathrm{B}) = S(\mathrm{A}) - S(\mathrm{A}|\mathrm{B}) = 1 - h_2\left(\frac{p(1|0)}{p_\checkmark}\right). \quad (126)$$

As a result, we obtain the explicit form of the expression $S(\mathrm{A}) - S(\mathrm{A}|\mathrm{B})$ which we substitute into Eg. (6) of the main text.

5.2 Eve's information

The density matrix of the Alice-Bob-Eve system given that Bob obtained conclusive measurement result is

$$\hat{\rho}^{\mathrm{f}}_{\mathrm{ABE}} = \frac{1}{2}\sum_{a=0,1}\frac{1}{p(\checkmark|a)}\,|a\rangle\langle a|_{\mathrm{A}} \otimes \sum_{b=0,1}|b\rangle\langle b|_{\mathrm{B}} \otimes \int d^2\alpha\; P(\alpha,\sqrt{T_1}\gamma_a,G_1)$$
$$\times \int d^2\beta\; P\left(\beta,\sqrt{(1-r_{\mathrm{E}})T_2}\alpha,G_2\right)\langle\beta|\hat{E}_b|\beta\rangle\,|\sqrt{r_{\mathrm{E}}}\alpha\rangle\langle\sqrt{r_{\mathrm{E}}}\alpha|_{\mathrm{E}}\,. \quad (127)$$

To estimate the conditional entropy $S(\mathrm{A}|\mathrm{E})$ one has to calculate the reduced Alice-Eve density matrix by tracing out Bob's subsystem:

$$\hat{\rho}^{\mathrm{f}}_{\mathrm{AE}} = \mathrm{tr}_{\mathrm{B}}\left[\hat{\rho}^{\mathrm{f}}_{\mathrm{ABE}}\right] = \frac{1}{2}\sum_{a=0,1}\frac{1}{p(\checkmark|a)}\,|a\rangle\langle a|_{\mathrm{A}} \otimes \int d^2\alpha\; P\left(\alpha,\sqrt{T_1}\gamma_a,G_1\right)$$
$$\times \int d^2\beta\; P\left(\beta,\sqrt{(1-r_{\mathrm{E}})T_2}\alpha,G_2\right)\langle\beta|\hat{E}_\checkmark|\beta\rangle\,|\sqrt{r_{\mathrm{E}}}\alpha\rangle\langle\sqrt{r_{\mathrm{E}}}\alpha|_{\mathrm{E}}\,. \quad (128)$$

It can be rewritten as

$$\hat{\rho}^{\mathrm{f}}_{\mathrm{AE}} = \int d^2\alpha\; Q_\checkmark[\alpha]\cdot\hat{\rho}^{\mathrm{f}}_{\mathrm{AE}}[\alpha]\,, \quad (129)$$

where

$$Q_\checkmark[\alpha] = \frac{P\left(\alpha;\sqrt{T_1}\gamma,G_1\right)}{p_\checkmark}\int d^2\beta\; P\left(\beta;\alpha\sqrt{(1-r_{\mathrm{E}})T_2},G_2\right)\langle\beta|\hat{E}_\checkmark|\beta\rangle\,, \quad (130)$$

$$\hat{\rho}^{\mathrm{f}}_{\mathrm{AE}}[\alpha] = \frac{1}{2}\sum_{a=0,1}|a\rangle\langle a|_{\mathrm{A}} \otimes \left|(-1)^a\sqrt{r_{\mathrm{E}}}\alpha\right\rangle\left\langle(-1)^a\sqrt{r_{\mathrm{E}}}\alpha\right|_{\mathrm{E}}. \quad (131)$$

Mutual information between the eavesdropper and Alice after the post-selection procedure is

$$I(\mathrm{A},\mathrm{E}) = S(\mathrm{A}) - S(\mathrm{A}|\mathrm{E}) = 1 - S(\mathrm{A}|\mathrm{E}). \quad (132)$$

The lower bound on the entropy $S(\mathrm{A}|\mathrm{E})$ may be found by exploiting the concavity of conditional quantum entropy

$$S(\mathrm{A}|\mathrm{E}) \geq \int d^2\alpha\; Q_\checkmark[\alpha]\cdot S_{\hat{\rho}^{\mathrm{f}}_{\mathrm{AE}}[\alpha]}(\mathrm{A}|\mathrm{E})$$
$$= \int d^2\alpha\; Q_\checkmark[\alpha]\cdot\left[1 - h_2\left(\frac{1+\left|\langle-\sqrt{r_{\mathrm{E}}}\alpha|\sqrt{r_{\mathrm{E}}}\alpha\rangle\right|}{2}\right)\right]$$
$$= 1 - \int d^2\alpha\; Q_\checkmark[\alpha]\cdot h_2\left(\frac{1+\exp\left(-2r_{\mathrm{E}}|\alpha|^2\right)}{2}\right), \quad (133)$$

Straightforward calculations allows us to find

$$\left\langle\exp\left(-2r_{\mathrm{E}}|\alpha|^2\right)\right\rangle_{Q_\checkmark} = \int d^2\alpha\; Q_\checkmark[\alpha]\cdot e^{-2r_{\mathrm{E}}|\alpha|^2} = \frac{\exp\left(\frac{-2r_{\mathrm{E}}|\gamma|^2}{1+2r_{\mathrm{E}}(G_1-1)}\right)}{2p_\checkmark\,(1+2r_{\mathrm{E}}(G_1-1))}$$
$$\times\left[\sum_{x=0,1}\mathrm{erf}\left(\frac{\theta'_2\cdot[1+2r_{\mathrm{E}}(G_1-1)]+(-1)^x\sqrt{(1-r_{\mathrm{E}})}\gamma}{\zeta\cdot\sqrt{1+2r_{\mathrm{E}}(G_1-1)}}\right)\right.$$
$$\left.-\sum_{x=0,1}\mathrm{erf}\left(\frac{\theta'_1\cdot[1+2r_{\mathrm{E}}(G_1-1)]+(-1)^x\sqrt{(1-r_{\mathrm{E}})}\gamma}{\zeta\cdot\sqrt{1+2r_{\mathrm{E}}(G_1-1)}}\right)\right], \quad (136)$$

where $S_{\hat{\rho}^{\mathrm{f}}_{\mathrm{AE}}[\alpha]}(\mathrm{A}|\mathrm{E})$ denotes conditional entropy for Alice-Eve density matrix described by Eq. (131). Utilizing Jensen's inequality,

$$\langle h_2(x)\rangle \leq h_2\left(\langle x\rangle\right), \quad (134)$$

we bound Eve's information as

$$I(\mathrm{A},\mathrm{E}) \leq h_2\left(\frac{1+\left\langle\exp\left(-2r_{\mathrm{E}}|\alpha|^2\right)\right\rangle_{Q_\checkmark}}{2}\right). \quad (135)$$

where $\zeta = \sqrt{G_1+G_2+2r_{\mathrm{E}}(G_1-1)(G_2-1)-3/2}$. By substituting Eq. (136) into Eq. (135) we obtain the upper bound for Eve's information (I(A:E) in the Eq. (6) of the main text).

References

53. Holstein, T. & Primakoff, H. Field dependence of the intrinsic domain magnetization of a ferromagnet. *Phys. Rev.* **58**, 1098 (1940).

54. Sanguinetti, B., Pomarico, E., Sekatski, P., Zbinden, H. & Gisin, N. Quantum cloning for absolute radiometry. *Phys. Rev. Lett.* **105**, 080503 (2010).

55. Vogel, W., Welsch, D. & Wallentowitz, S. *Quantum Optics: An Introduction* (Wiley, 2001).

56. Sekatski, P., Sanguinetti, B., Pomarico, E., Gisin, N. & Simon, C. Cloning entangled photons to scales one can see. *Phys. Rev. A* **82**, 053814 (2010).

57. Zhao, Y., Qi, B. & Lo, H.-K. Experimental quantum key distribution with active phase randomization. *Appl. Phys. Lett.* **90**, 044106 (2007).

58. Abramowitz M. & Stegun I. A., editors *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables* (US Government printing office, 1964).

59. Lee Rodgers, J. & Nicewander, W. A. Thirteen ways to look at the correlation coefficient. *The American Statistician* **42**, 59–66 (1988).

60. Pearson, K. VII. Mathematical contributions to the theory of evolution.—III. Regression, heredity, and panmixia. *Philos. Trans. R. Soc.r*, ser. A **187**, 253–318 (1896).