Line-of-sight quantum key distribution with differential phase shift keying

Hiroyuki Endo,a,b, Toshihiko Sasaki,a,c,d, Masahiro Takeoka,e,f, Mikio Fujiwara,a,b, Masato Koashi,a,b,4 and Masahide Sasaki1,∗

1 Quantum ICT Collaboration Center, National Institute of Information and Communications Technology, Koganei, Tokyo 184-8795, Japan
2 Quantum ICT Laboratory, National Institute of Information and Communications Technology, Koganei, Tokyo 184-8795, Japan
3 Department of Applied Physics, The University of Tokyo, Bunkyo-ku, Tokyo 113-8656, Japan
4 Photon Science Center, The University of Tokyo, Bunkyo-ku, Tokyo 113-8656, Japan
5 Faculty of Science and Technology, Keio University, Yokohama, Kanagawa 223-8522, Japan
6 Advanced ICT Research Institute, National Institute of Information and Communications Technology, Koganei, Tokyo 184-8795, Japan

∗ Authors to whom any correspondence should be addressed.

E-mail: h-endo@nict.go.jp and psasaki@nict.go.jp

Keywords: quantum key distribution, free-space optical communications, satellite communications, physical-layer cryptography

Abstract

Free-space optical (FSO) links offer a practical approach to realize quantum key distribution (QKD) in a global scale. However, when one wants to further extend the distance from the geostationary orbit to the ground, currently known QKD schemes cannot realize practical key rates mainly due to the diffraction losses of a laser beam. If the facts that the FSO links are highly directional and must be used in the line-of-sight (LoS) condition are taken into account, one may impose some physical restrictions on an eavesdropping model to explore longer-distance QKD. In this paper, we propose a novel FSO secret key agreement scheme, line-of-sight QKD (LoS-QKD), based on a quantum wiretap channel. In our model, an eavesdropper can tap only a limited fraction of the FSO signal beam but perform any physically allowable operations on the tapped signals. Fading effects which are significant in the FSO links are fully taken into account. We provide a security proof for the differential phase shift (DPS) keying scheme in terms of the metric which meets the composability. We investigate numerically the performances of LoS-QKD with DPS keying, including finite-length analysis, showing that our proposed scheme can realize high-speed and long-distance secret key agreement with information-theoretic security.

1. Introduction

Quantum key distribution (QKD) [1–3] is a method for secret key agreement between two remote parties, a sender (Alice) and a receiver (Bob), connected by a quantum channel. QKD can theoretically be secure against an eavesdropper (Eve) who can launch any physically allowable attacks and have unbounded computational resources (information-theoretic security). Today QKD networks have been deployed in installed optical fibers over the metropolitan scale [4, 5] and recently in the continental scale [6, 7], based on the trusted nodes and key relay. Unfortunately, these fiber-based QKD networks cannot be extended to inter-continental configurations because submarine cables with optical fiber amplifiers cannot support QKD links.

To extend the distance to a global scale, satellite-based QKD is a promising solution. Several satellite-based communication experiments over the quantum-limited channels have successfully been demonstrated so far, to show the possibility of long-distance QKD [8–10]. The Chinese team launched the quantum science satellite in the low-earth orbit (LEO) [11] and performed a series of QKD experiments [12–15], in which a key rate of about 47.8 kbps in a passage with a distance range from 645 km to 1200 km was achieved [14] with a decoy-state BB84 scheme.
The next challenge is to increase the key rate and the distance. Unfortunately, however, improvements in the instrument level based on known QKD protocols cannot be a fundamental solution, because the theoretical upper bound on the key rate of QKD shows that it is impossible to extend the distance to a range between a geostationary (GEO) satellite and a ground station [16] with a sufficient amount of keys by practical space laser link technologies.

One possible avenue is to relax security threat assumptions in QKD over a free-space optical (FSO) link, taking into account its typical features, namely, that the link is highly directional and must be in the line-of-sight (LoS) between Alice and Bob. These features make Eve much harder to eavesdrop the signals without being detected by Alice and Bob, who could equip with link surveillance apparatuses (e.g. camera, RADAR, LIDAR). This situation can be modeled by the wiretap channel (WTCh) [17]. Based on the WTCh, one can develop modified QKD protocols to improve the key rate and the distance.

A similar concept was already exploited to develop secrecy message transmission [17, 18] and secret key agreement [19, 20] with information-theoretic security. These schemes are based on classical information theory, and referred to as physical layer security (PLS) [21, 22]. PLS schemes over the FSO links are recently studied both theoretically [16, 23–27] and experimentally [28–34].

Secret key agreement on the quantum WTCh has also been theoretically investigated in the context of satellite-to-ground QKD [35, 36]. However, there is some concern about the applicability of these theoretical studies to the realistic FSO links which suffer from atmospheric turbulence, beam wandering, and so on, resulting in fading effects (temporal variations of received signal intensity at Bob). In fact, reference [35] proposes the photon key distribution protocols over satellite-to-ground links, assuming that the legitimate parties can detect man-in-the-middle attacks. This assumption simplifies the protocol and hardware systems compared to the conventional QKD schemes. Unfortunately, however, it is unclear what kinds of channel models are assumed there: the key rate formulas shown or discussed in the paper seem inappropriate to assure the security when, for example, the channel has birefringence properties or suffers from atmospheric effects. A further careful investigation would be necessary. Reference [36] discusses secret key agreement over a linear lossy bosonic WTCh. This paper considers not only the passive-Eve scenario but also the active-Eve scenario in which Eve can insert two-mode squeezed state into the WTCh. However, this paper focuses on the restricted model in which channel’s statistical nature is independent and identically distributed (iid). For FSO links, however, this is not the case in general due to atmospheric effects, as shown in references [28, 33, 34].

In this paper, we present a novel scheme of QKD for a FSO link, that is, line-of-sight quantum key distribution (LoS-QKD) based on differential phase shift (DPS) keying. We model a ‘wiretapper’ channel between Alice and Eve by a linear beam splitter (BS) placed in front of Alice’s transmitter. Eve can perform any physically allowable operations on the beam reflected by the BS and also have unbounded computational resources. The FSO link between Alice and Bob (the main channel) can suffer from atmospheric effects. We assume that the main channel has the several properties including ‘phase insensitivity’, whose detail will be explained in section 2. Based upon this quantum WTCh model, we provide a security proof in terms of the metric which meets the composability. We study numerically the performances of LoS-QKD with DPS keying, including finite-length analysis, and show that the proposed scheme can realize high-speed and long-distance key distribution with information-theoretic security.

2. Line-of-sight quantum key distribution

In this section, we introduce the basics of LoS-QKD with DPS keying. We first present the configuration of the scheme, and discuss the assumptions imposed on the FSO-WTCh and Bob’s receiving apparatus. We then present the detailed flow of the protocol, for which we will develop a security proof in the next section.

2.1. Configuration of LoS-QKD

A basic configuration of LoS-QKD is shown in figure 1. Alice modulates coherent-state pulses from a source by DPS keying according to an input random bit sequence (RBS) from a random number generator (RNG). The optical signals are transmitted to Bob over the LoS channel, which may suffer from the atmospheric effects, and received by a one-bit-delay balanced interferometer with two on/off detectors, D0 and D1. An on/off detector reports detection when it detects photons in the designated duration, and reports no detection otherwise.

We assume that Eve stays far from the LoS channel and taps only a limited fraction of the optical signals, whose detailed models were studied by case-by-case risk analysis in section 2 of reference [33]. We model this situation by a BS in front of Alice’s transmitter. The reflectivity of this BS is generally small in the LoS communication scenario. Eve can perform any physically allowable operations on the signal reflected by the BS, and can have unbounded computational resources. We assume that the transmitted optical signals will
be affected by the atmosphere in the LoS channel before they are received by Bob, which we treat as the main channel acting on the optical pulses. After completing optical transmission of the RBS from Alice to Bob, they perform key-distillation processing with communications over an authenticated public channel.

2.2. Protocol of LoS-QKD

We here describe our proposed protocol of LoS-QKD using the configuration in figure 1.

(1) Alice generates a coherent train of weak pulses from the laser source, and modulates each pulse by adding a phase shift $0$ or $\pi$ according to a random bit generated from the RNG. Alice transmits the modulated pulses to Bob over the LoS channel.

(2) Bob measures the relative phase ($0$ or $\pi$) between adjacent pulses in the received pulse train using the one-bit-delay interferometer and the photon detectors. Whenever the detection succeeds, he records its timing and also records the measurement outcome as a bit $d$, where $d = 0$ corresponds to the relative phase $0$ and $d = 1$ to $\pi$. He concatenates all the outcome bits from the successful timings to form a raw key $d$. Let $N_{\text{raw}}$ be the length of $d$.

(3) Bob randomly chooses test bits from the $N_{\text{raw}}$ bits of the raw key $d$ to define his test sequence $\kappa_{\text{test}}^B$. Let $N_{\text{test}}$ be the length of $\kappa_{\text{test}}^B$. He concatenates the remaining $N_{\text{sift}} := N_{\text{raw}} - N_{\text{test}}$ bits in $d$ to define his sifted key $\kappa^B$.

(4) Bob announces the successful timings, the position of test bits, and his test sequence $\kappa_{\text{test}}^B$.

(5) Using Bob’s announcement and her record of the phase modulation, Alice defines her $N_{\text{sift}}$-bit sifted key $\kappa^A$ and her $N_{\text{test}}$-bit test sequence $\kappa_{\text{test}}^A$. She announces $\kappa_{\text{test}}^A$.

(6) Based on $\kappa^A_{\text{test}}$ and $\kappa^B_{\text{test}}$, Alice and Bob perform information reconciliation in the forward direction: Alice provides Bob with information on her sifted key $\kappa^A$, and Bob computes a reconciled key $\kappa^B_{\text{rec}}$ from $\kappa^B$.

(7) Alice and Bob determine the length $N_{\text{fin}}$ of the final key, and carry out privacy amplification to obtain the $N_{\text{fin}}$-bit final keys $\kappa^A_{\text{fin}}$ and $\kappa^B_{\text{fin}}$ from $\kappa^A$ and $\kappa^B_{\text{rec}}$, respectively.

After we provide assumptions on Alice’s and Bob’s devices and on the LoS channel in the next section, we will present a more specific version of the above protocol in section 4 and will prove its finite-size security.

3. Assumptions on devices and channels

In this section, we provide assumptions on Alice’s apparatus, the quantum channel from Alice to Bob, and Bob’s apparatus. At the same time, we introduce various mathematical notations, which will be used to provide more specific description of the proposed protocol in section 4.

We assume that Alice sends out $N_{\text{pul}}$ pulses in total. In the DPS keying in which a bit is encoded in the relative phase between an adjacent pair of pulses, $N_{\text{tot}} := N_{\text{pul}} - 1$ bits are encoded on these pulses. We thus index the $N_{\text{pul}}$ pulses by $(0, 1, \ldots, N_{\text{tot}})$. We denote the system of the $i$th pulse by $C_i$ ($i = 0, 1, \ldots, N_{\text{tot}}$) and the whole system of the $N_{\text{pul}}$ pulses by $C$. We denote by $\hat{n}_i$ the photon number operator for the $i$th pulse $C_i$.
3.1. Sender’s apparatus
An ideal laser source will prepare each pulse in an identical coherent state with the same mean photon number $\mu_A$ and with the same phase, namely, in a coherent state $|\sqrt{\mu_A}\rangle$. Although we will assume such a perfect source for computing key rates in section 5, our security proof given in section 4 relies only on a much weaker assumption on the laser source. The complex amplitudes of different pulses may differ, namely, the $i$th pulse may have its own value $\alpha_i$ of its complex amplitude, as long as $|\alpha_i|^2 \leq \mu_A$. Furthermore, the possibility of fluctuations and correlations in $\alpha_i$ as long as $|\alpha_i|^2 \leq \mu_A$ holds with unit probability. These assumptions are formally stated as follows.

**Assumption 1 (laser source).** Let $\mu_A > 0$ be a constant. The sender’s laser source can be equivalently replaced by the following procedure. Generate $N_{\text{pul}}$-tuple of complex numbers $\alpha$ with a probability $\Pr(\alpha)$ satisfying
$$\Pr(|\alpha_i|^2 \leq \mu_A) = 1, \quad \forall i.$$ (1)

According to $\alpha$, prepare $N_{\text{pul}}$ pulses in state $|\alpha_i\rangle_C$:
$$|\alpha\rangle_C := \bigotimes_{i=0}^{N_{\text{pul}}} |\alpha_i\rangle_C,$$ (2)
where $|\alpha_i\rangle_C$ is a coherent state with amplitude $\alpha_i$.

In the actual protocol of LoS-QKD, there is no need for Alice to know the value of $\alpha$ or the distribution $\Pr(\alpha)$. The only parameter she has to know is $\mu_A$, which is used in determining the amount of privacy amplification. Note that assumption 1 is stronger than merely requiring that the state of system $C$ is given by a density operator $\rho(\alpha) = \sum \Pr(\alpha)|\alpha\rangle\langle\alpha|$. Assumption 1 may not hold if the optical pulses have quantum correlations to other systems that Alice does not possess. A sufficient condition for assumption 1 is that system $C$ is in state $\rho(\alpha)$ and is decoupled from any other system.

As for the phase modulator, we assume that it works ideally. Given $\alpha_i$, the $i$th pulse leaves Alice either in state $|\alpha_i\rangle$ or in state $|-\alpha_i\rangle$.

3.2. Channel model
As explained in subsection 2.1, we assume that the wiretapper channel is modeled by a BS. When the open input port is in the vacuum, the action of a BS with reflectivity $\eta$ is described by an isometry $\hat{U}_{\text{BS}}(\eta)$ satisfying the following property. For an input pulse in a coherent state $|\alpha\rangle_C$ with complex amplitude $\alpha$, we have $\hat{U}_{\text{BS}}(\eta)|\alpha\rangle_C = |\sqrt{1-\eta}\alpha\rangle_C|\sqrt{\eta}\alpha\rangle_E$, where the pulse $E$ is received by Eve. The action of the BS on the $N_{\text{pul}}$ input pulses is then given by a CPTP (completely-positive trace preserving) map
$$\mathcal{E}_{\text{wtp}}(\rho) := (\hat{U}_{\text{BS}}^{(n)}\otimes N_{\text{pul}})\rho(\hat{U}_{\text{BS}}^{(n)})\otimes N_{\text{pul}}.$$(3)

Using this notation, we describe the assumption on the LoS channel as follows.

**Assumption 2 (wiretap channel model).** The channel between Alice and Bob is modeled by $\mathcal{E}_{\text{wtp}}$, which is a wiretapper channel composed of a BS with reflectivity $\eta_E$, followed by a main channel $\mathcal{E}_{\text{main}}$, as shown in figure 2.

As for the main channel $\mathcal{E}_{\text{main}}$, we do not assume a specific model but only assume a weak assumption. This allows our security proof to cover a wide range of unknown and time-varying properties of the atmosphere across which LoS-QKD is carried out. To describe our assumption, which we call phase insensitivity, we introduce a general operation of optical phase shifts on $N_{\text{pul}}$ pulses. Application of an
optical phase shift $\theta_i$ on the $i$th pulse for $i = 0, 1, \ldots, N_{\text{tot}}$ is represented by a CPTP map
\begin{equation}
\mathcal{E}_{\text{ps}}^{(\theta)}(\rho) := \hat{U}_{\text{ps}}^{(\theta)} \rho \hat{U}_{\text{ps}}^{(\theta)\dagger}
\end{equation}
with $\theta := (\theta_0, \theta_1, \ldots, \theta_{N_{\text{tot}}})$ and
\begin{equation}
\hat{U}_{\text{ps}}^{(\theta)} := \bigotimes_{i=0}^{N_{\text{tot}}} e^{i\theta_i} \hat{h}.
\end{equation}
The assumption of phase insensitivity implies that the main channel depends on neither the absolute phases nor the relative phases of the optical pulses, which is formally stated in terms of the map $\mathcal{E}_{\text{ps}}^{(\theta)}$ as follows.

**Assumption 3 (channel phase insensitivity).** The CPTP map $\mathcal{E}_{\text{main}}$ on system $C$ of $N_{\text{pul}}$ pulses satisfies
\begin{equation}
\mathcal{E}_{\text{ps}}^{(\theta)} \circ \mathcal{E}_{\text{main}} = \mathcal{E}_{\text{main}} \circ \mathcal{E}_{\text{ps}}^{(\theta)}
\end{equation}
for arbitrary $\theta$.

Note that this assumption allows the transmittance to vary for each pulse, or even to be affected by the presence of photons in the preceding pulses, as long as such correlations are insensitive to the optical phases of the input pulses. We believe that the phase insensitivity is very unlikely to be violated by natural causes in the case of DPS keying. To break phase insensitivity, the oscillating dipoles of particles in the atmosphere must memorize the phase of a pulse and affect the subsequent pulses accordingly. It implies that the dephasing time must be longer than the pulse interval (e.g. 1 ns for 1 GHz of pulse repetition rate), which normally requires a resonance of a similar bandwidth ($\sim$1 GHz). It is unlikely that such a sharp resonance coincides with the frequency of the laser used in the LoS-QKD, which makes the phase insensitivity condition reasonable for LoS-QKD with DPS keying.

### 3.3. Receiver’s apparatus
Since the optical pulses received by Bob are very weak, the measurement of the phase difference between an adjacent pair of pulses often fails, which happens when neither of the detectors reports the arrival of photons at the designated timing. Bob publicly announces the positions of such detection failure (or equivalently the positions of success) so that Alice and Bob can agree to generate sifted keys only from the pairs for which Bob’s detection has succeeded. Let us label adjacent pairs in such a way that the $j$th pair consists of the $(j-1)$th and the $j$th pulses, for $j = 1, \ldots, N_{\text{tot}}$. Define a detection index set $D \subset \{1, \ldots, N_{\text{tot}}\}$ as the set of the indices of the pairs for which Bob’s detection has succeeded. Bob’s announcement of the successful timings in step 4 of the protocol in subsection 2.2 is equivalent to announcing the set $D$.

Our security proof in this paper assumes that the statistics of detection pattern $D$ is independent of the optical phases of the $N_{\text{pul}} = N_{\text{tot}} + 1$ pulses (system $C$) received by Bob. To formally describe this property, we represent Bob’s measurement by POVM (positive operator-valued measure) $\{E_D\}_{D \subset \{1, \ldots, N_{\text{tot}}\}}$ such that, when the state of the received $N_{\text{pul}}$ pulses is $\rho$, the probability of outcome $D$ is given by $\Pr(D) = \text{Tr}(E_D \rho)$. Our assumption on Bob’s apparatus is now stated as follows.

**Assumption 4 (detection phase insensitivity).** For any state $\rho$ of system $C$, Bob’s measurement $\{E_D\}_{D \subset \{1, \ldots, N_{\text{tot}}\}}$ satisfies
\begin{equation}
\text{Tr}(E_D \rho) = \text{Tr}(E_D \mathcal{E}_{\text{ps}}^{(\theta)}(\rho)), \quad \forall \ D \subset \{1, \ldots, N_{\text{tot}}\}
\end{equation}
for arbitrary $\theta$.

This assumption holds true if the following two conditions are simultaneously met: (a) the two on/off detectors have the same detection efficiency, and (b) a double-click event, where both detectors report the arrival of photons, is regarded as a successful detection.

### 4. Security proof
In this section, we give a security proof of the proposed LoS-QKD protocol in the finite-size regime. We first clarify the goal of the security proof in subsections 4.1 and 4.2. In subsection 4.1, we refine the protocol in subsection 2.2 to be more specific by using the mathematical notations introduced in the previous section. We call it actual protocol to distinguish it from other protocols introduced in subsequent subsections. In subsection 4.2, we explain the security criteria in the finite-size regime, which are widely used for QKD protocols. Subsection 4.3 focuses on the property of the sender’s phase encoding in the protocol, and explain the basic idea used in the security proof based on complementarity. The security proof begins with subsection 4.4, which shows that the security statement of actual protocol is reduced to that of another
protocol which we call virtual protocol. It is then further reduced to a condition on classical random variables defined in yet another protocol called estimation protocol in subsection 4.5. The statistics of the random variables are analyzed in subsection 4.6, which completes the security proof and gives a formula for the finite-size final key length for a given security parameter. Technical details will be available in appendix A through appendix C.

Throughout this section, we use the following notations for defining an indexed series of variables:

\[(x_i)_{i=0}^N = (x_0, x_1, \ldots, x_N),\]
\[(x_i)_{\text{condition}} = (x_0, x_1, \ldots, x_q),\]
\[\{i_1, i_2, \ldots, i_d\} = \{i|\text{condition}\}, i_k < i_k+1.\]

### 4.1. Formal description of the LoS-QKD protocol

Here we give a specific version of the LoS-QKD protocol in subsection 2.2 such that we are able to discuss its security in the finite-size regime. We first list the protocol parameters which are shared in public by Alice and Bob prior to the run of the protocol. Let \(\mu_A\) be the bound on the mean photon number of a pulse from the laser source, which appears in assumption 1. Let \(N_{\text{pul}} = N_{\text{tot}} + 1\) be the total number of pulses transmitted from Alice to Bob, and \(p_{\text{test}} \in [0, 1]\) be the fraction of test bits. Let \(\eta_B\) be the reflectivity of the BS in the WTCh model. In addition, we define \(\Pr(C_{\text{PA}}|N_1, N_2)\) as the probability over \(N_1 \times N_2\) binary matrices \(C_{\text{PA}}\) used in the privacy amplification, and \(N_{\text{IR}}(\kappa_A^{\text{test}}, \kappa_B^{\text{test}})\) as a function to determine the length of communication used for information reconciliation from test bits \(\kappa_A^{\text{test}}\) and \(\kappa_B^{\text{test}}\).

The description of the refined protocol, which we call actual protocol, is now given as follows.

**Actual protocol**

1. Using the laser source, Alice prepares system \(C = (C_i)_{i=0}^{N_{\text{tot}}}\) of \(N_{\text{pul}}\) optical pulses in state \(\rho_C\). She generates a random bit sequence \(a := (a_i)_{i=0}^{N_{\text{tot}}}\) using the RNG. She modulates the optical pulses by adding a phase shift to the \(i\)th pulse if \(a_i = 1\) for \(i = 0, \ldots, N_{\text{tot}}\), such that the state of system \(C\) becomes

\[
\left(\bigotimes_{i=0}^{N_{\text{tot}}} (-1)^{a_i\eta_B}\right) \rho \left(\bigotimes_{i=0}^{N_{\text{tot}}} (-1)^{a_i\eta_B}\right).
\]

Alice transmits the modulated pulses to Bob over the LoS channel.

2. Bob performs a DPS measurement on the received pulses. According to the measurement outcomes for the \(N_{\text{tot}}\) adjacent pairs, he determines a detection index set \(D \subset \{1, \ldots, N_{\text{tot}}\}\) and a raw key \(d := (d_j)_{j \in D}\) by the following rule. For the \(j\)th pair, if neither of the detectors clicks, and \(j \in D\) otherwise. If only one of the detectors clicks, \(d_j\) is set to be the index of that detector (i.e. 0 or 1). If both detectors click, \(d_j\) is randomly set to 0 or 1.

3. Bob generates a test-bit index set \(D_{\text{test}}\) by performing Bernoulli sampling with sampling rate \(p_{\text{test}}\) on \(D\). He defines a sifted key set \(D_{\text{diff}} := D \setminus D_{\text{test}}\), his sifted key \(\kappa_B := (d_j)_{j \in D_{\text{diff}}}\) with a length of \(N_{\text{diff}} := |D_{\text{diff}}|\), and his test sequence \(\kappa_B^{\text{test}} := (d_j)_{j \in D_{\text{test}}}\) with a length of \(N_{\text{test}} := |D_{\text{test}}|\).

4. Bob announces \(D_{\text{diff}}, D_{\text{test}},\) and \(\kappa_B^{\text{test}}\).

5. Alice defines her raw-bit sifted key \(\kappa_A := (k_j)_{j \in D_{\text{diff}}}\) and her test-bit test sequence \(\kappa_A^{\text{test}} := (k_j)_{j \in D_{\text{test}}}\) from \(a\) by the relation \(k_j := a_j \oplus d_{j-1}\). She announces \(\kappa_A^{\text{test}}\).

6. (Information reconciliation). By using encrypted communication consuming \(N_{\text{IR}}(\kappa_A^{\text{test}}, \kappa_B^{\text{test}})\) bits of preshared key (i.e. via Vernam’s one-time pad [37]), Alice provides Bob with information on her sifted key \(\kappa_A\). Bob then computes a reconciled key \(\kappa_B^{\text{rec}}\) from \(\kappa_B\).

7. (Privacy amplification). Alice and Bob determine the length \(N_{\text{fin}}\) of the final key based on \(\mu_A, \eta_B, D_{\text{diff}},\) and \(D_{\text{test}}\). Alice chooses a \(N_{\text{diff}} \times N_{\text{fin}}\) binary matrix \(C_{\text{PA}}\) with the probability \(\Pr(C_{\text{PA}}|N_{\text{diff}}, N_{\text{fin}})\) and announces it. Alice and Bob then obtain the final keys \(\kappa_B^{\text{fin}} := \kappa_A C_{\text{PA}}\) and \(\kappa_B^{\text{fin}} := \kappa_B^{\text{rec}} C_{\text{PA}}\), respectively.

After the run of the protocol, Alice and Bob share \(N_{\text{fin}}\)-bit final keys, while they consume \(N_{\text{IR}}\) bits of a preshared key during the protocol. The net key gain \(G\) is thus given by

\[G = N_{\text{fin}} - N_{\text{IR}}.\]

### 4.2. Security criteria

We define the security of our protocol using a criterion that is widely used for conventional QKD and satisfies the universal composability [38]. Given an attack strategy by Eve, we can define the probability
Pr(\(N_{\text{fin}}\)) of the final key length and the quantum state \(\rho_{\text{AEB|N_{\text{fin}}}^\text{fin} \rangle}^\text{fin} \rangle\), which is the final state over Alice’s and Bob’s final keys and Eve’s quantum system conditioned on \(N_{\text{fin}}\). The state \(\rho_{\text{AEB|N_{\text{fin}}}^\text{fin} \rangle}^\text{fin} \rangle\) is generally written as

\[
\rho_{\text{AEB|N_{\text{fin}}}^\text{fin} \rangle}^\text{fin} \rangle = \sum_{\kappa_A^\text{fin}, \kappa_B^\text{fin} \in \{0,1\}^N_{\text{fin}}} \Pr(\kappa_A^\text{fin} \rangle, \kappa_B^\text{fin} \rangle | N_{\text{fin}}) \times \langle \kappa_A^\text{fin} \rangle (\kappa_A^\text{fin} \rangle \otimes \kappa_B^\text{fin} \rangle) (\kappa_B^\text{fin} \rangle \otimes \rho_{EB|N_{\text{fin}}} (\kappa_A^\text{fin} \rangle, \kappa_B^\text{fin} \rangle).
\]

(12)

From the above state, we define a quantum state representing the ideal final key by

\[
\rho_{\text{AEB|N_{\text{fin}}}^\text{ideal} \rangle}^\text{ideal} := \left( \sum_{\kappa \in \{0,1\}^N_{\text{fin}}} \frac{1}{2^{N_{\text{fin}}}} |\kappa\rangle \langle \kappa| \otimes |\kappa\rangle \langle \kappa| \right) \otimes \text{Tr}_{AB} \left( \rho_{\text{AEB|N_{\text{fin}}}^\text{fin} \rangle \right).
\]

(13)

The security of a protocol is stated in terms of the distance between the actual state and the ideal state. We say the protocol is \(\varepsilon_{\text{sec}}\)-secure if

\[
\frac{1}{2} \sum_{N_{\text{fin}} \geq 1} \Pr(N_{\text{fin}}) ||\rho_{\text{AEB|N_{\text{fin}}}^\text{fin} \rangle}^\text{fin} \rangle - \rho_{\text{AEB|N_{\text{fin}}}^\text{ideal} \rangle}^\text{ideal} \rangle \leq \varepsilon_{\text{sec}}
\]

holds regardless of Eve’s attack. Here, ||\(\sigma\)|| denotes the trace norm of operator \(\sigma\).

It is convenient to decompose the above condition into two separate conditions. We say a protocol is \(\varepsilon_2\)-correct if

\[
\sum_{N_{\text{fin}} \geq 1} \Pr(N_{\text{fin}}) \Pr(\kappa_A^\text{fin} \rangle \neq \kappa_B^\text{fin} \rangle | N_{\text{fin}}) \leq \varepsilon_2
\]

(15)

holds regardless of Eve’s attack. We say a protocol is \(\varepsilon_X\)-secret if

\[
\frac{1}{2} \sum_{N_{\text{fin}} \geq 1} \Pr(N_{\text{fin}}) ||\rho_{\text{AEB|N_{\text{fin}}}^\text{fin} \rangle}^\text{fin} \rangle - \rho_{\text{AEB|N_{\text{fin}}}^\text{ideal} \rangle}^\text{ideal} \rangle \leq \varepsilon_X
\]

(16)

holds regardless of Eve’s attack, where \(\rho_{\text{AEB|N_{\text{fin}}}^\text{fin} \rangle}^\text{fin} \rangle := \text{Tr}_B (\rho_{\text{AEB|N_{\text{fin}}}^\text{fin} \rangle}^\text{fin} \rangle\) and \(\rho_{\text{AEB|N_{\text{fin}}}^\text{ideal} \rangle}^\text{ideal} \rangle := \text{Tr}_B (\rho_{\text{AEB|N_{\text{fin}}}^\text{ideal} \rangle}^\text{ideal} \rangle\). When a protocol is \(\varepsilon_2\)-correct and \(\varepsilon_X\)-secret, it can be shown that it is \((\varepsilon_2 + \varepsilon_X)\)-secure. In this paper, we assume that the information reconciliation in the actual protocol guarantees the \(\varepsilon_2\)-correctness of the protocol, and focus on proving \(\varepsilon_X\)-secrecy in the subsequent subsections.

4.3. Property of the sender’s encoding and basic idea behind the security proof

Consider an entangled state between a qubit \(A\) and an optical pulse \(C\), given by

\[
|\psi(\alpha)\rangle_{AC} := \frac{1}{\sqrt{2}} \left( |0\rangle_A |\alpha\rangle_C + |1\rangle_A |\alpha\rangle_C \right),
\]

(17)

where \(|0\rangle_A, |1\rangle_A\) is an orthonormal basis of qubit \(A\), which we call the Z-basis, and \(|\alpha\rangle_C\) is the coherent state with complex amplitude \(\alpha\). Suppose that qubit \(A\) is measured on the Z-basis to produce an outcome \(a \in \{0,1\}\). With probability 1/2, \(a = 0\) and the optical pulse is in state \(|\alpha\rangle_C\). With probability 1/2, \(a = 1\) and the optical pulse is in state \(|\bar{\alpha}\rangle_C\). This is exactly the same as the procedure of choosing \(a_i\) and modulating the \(i\)th pulse in step 1 of actual protocol. To be more comprehensive, consider a quantum register of \(N_{\text{pal}}\) qubits \(A := (A_i)_{i=0}^{N_{\text{pal}}}\) and \(N_{\text{pal}}\) optical pulses \(C := (C_i)_{i=0}^{N_{\text{pal}}}\). Define an entangled state

\[
|\Psi(\alpha)\rangle_{AC} := \bigotimes_{i=0}^{N_{\text{pal}}} |\psi(\alpha_i)\rangle_{AC_i}.
\]

(18)

Under assumption 1 on the laser source, step 1 of actual protocol is equivalent to choosing \(\alpha\), preparing state \(|\Psi(\alpha)\rangle_{AC}\), and measuring the \(N_{\text{pal}}\) qubits \(A\) on the Z-basis to determine \(a\). This property will be used in constructing a virtual protocol in the next subsection.

Our security proof is based on the complementarity approach \([39]\), in which the secrecy of an observable is assessed from the uncertainty of a complementary observable. To explain the basic idea, let us go back to the simple example of state \(|\psi(\alpha)\rangle_{AC}\). Instead of measuring qubit \(A\) on the Z-basis to obtain bit \(a\), suppose that one measures it on a complementary basis \(|0\rangle_A (= |0\rangle_A + |1\rangle_A)/\sqrt{2}\), \(|1\rangle_A (= |0\rangle_A - |1\rangle_A)/\sqrt{2}\), which we call the X-basis, to obtain a bit \(x \in \{0,1\}\) as an outcome. For determining statistics of \(x\), it is convenient to consider the parity of the photon number, which is an observable complementary to
the optical phases of 0 and π. Let us define the projection operators onto the even- $(b = 0)$ and the odd- $(b = 1)$ photon-number subspaces by

$$
\Pi^{(b)}_{C} := \frac{1 + (-1)^b(-1)^{\mu}}{2},
$$

where $\hat{n}_C$ is the photon number operator for pulse C. We also rewrite $|\psi(\alpha)\rangle_{AC}$ using the relation $| - \alpha\rangle_C = (-1)^{\mu}|\alpha\rangle_C$ as

$$
|\psi(\alpha)\rangle_{AC} = \frac{1}{\sqrt{2}} \left( |0\rangle_A + |1\rangle_A(-1)^{\mu} \right) |\alpha\rangle_C.
$$

Then the probability of bit $x$ is computed as

$$
Pr(x = b) = \|A(\hat{b}|\psi(\alpha)\rangle_{AC})\|^2 = \|\Pi^{(b)}_{C}|\alpha\rangle_C\|^2.
$$

Especially for $b = 1$, we have $Pr(x = 1) = p_{ph}(|\alpha|^2)$ with

$$
p_{ph}(\mu) := \frac{1 - e^{-2\mu}}{2}.
$$

The function $p_{ph}(\mu)$ represents the probability of the photon number to be odd when it follows the Poisson distribution with mean $\mu$, and will also appear in the formula for the secure key length later. The value of $Pr(x = 1)$ is related to how secure the Z-basis outcome $a$ is from someone having access to the optical pulse C. In particular, $Pr(x = 1) = 0$ if $|\alpha| = 0$, in which case the pulse is in the vacuum and thus carries no information on bit $a$. The secrecy of $a$ can also be understood from the fact that qubit A is exactly in state $|0\rangle_A$ before the Z-basis measurement, which means no one should be able to predict the outcome $a$. In the opposite limit of $|\alpha| \rightarrow \infty$, the bit $a$ is fully leaked through the pulse, while $Pr(x = 1)$ approaches $1/2$, implying that we are completely uncertain about the value of $x$. In the general case with $0 < Pr(x = 1) < 1/2$, we may expect that this value somehow quantifies the amount of leaked information, and hence is eventually used for determining an appropriate amount of privacy amplification to make a protocol secure.

In LoS-QKD, we assume that only a fraction of the emitted pulse energy is received by Eve. After a wiretapper channel, the whole state may become

$$
|\phi(\alpha, \eta)\rangle_{ACE} := \mathcal{U}^{(o)}_{BS}|\psi(\alpha)\rangle_{AC} = \frac{1}{\sqrt{2}} \left( |0\rangle_A|\sqrt{1 - \eta}\alpha\rangle_C|\sqrt{\eta}\alpha\rangle_E + |1\rangle_A - \sqrt{1 - \eta}\alpha\rangle_C - \sqrt{\eta}\alpha\rangle_E \right) - |1\rangle_A(-1)^{\mu}(-1)^{\mu} |\sqrt{1 - \eta}\alpha\rangle_C|\sqrt{\eta}\alpha\rangle_E.
$$

Of course, the application of $\mathcal{U}^{(o)}_{BS}$ does not change the statistics of bit $x$, namely,

$$
Pr(x = 1) = \|A(\hat{1}|\phi(\alpha, \eta)\rangle_{ACE})\|^2 = p_{ph}(|\alpha|^2).
$$

But when we want to evaluate the secrecy of bit $a$ from Eve, we may argue that the optical pulse C, which is beyond Eve’s reach, can be used to reduce the uncertainty in bit $x$. For the convenience of constructing a virtual protocol in the next subsection, here we define a measurement for extracting useful information from pulse C with a minimal disturbance on its state as follows.

**Definition 1 (parity measurement).** A parity measurement on an optical pulse C produces an outcome $x' \in \{0, 1\}$ corresponding to the parity of the photon number. Let $\sigma_C$ be the state of C before the measurement, and $U^{(b)}_{C}(x' = b) (b = 0, 1) be the state of$C after the parity measurement on condition that $x' = b$. Then it holds that

$$
Pr(x' = b) = Tr(\Pi^{(b)}_C \sigma_C)
$$

and

$$
\rho^{(x' = b)}_C = \frac{\Pi^{(b)}_C \sigma_C \Pi^{(b)}_C}{Tr(\Pi^{(b)}_C \sigma_C)}.
$$

Let $\rho_C := \sum_b Pr(x' = b)\rho^{(x' = b)}_C$ be the state after the measurement averaged over the outcome $b$. It satisfies

$$
\rho_C = \sum_{b = 0, 1} \Pi^{(b)}_C \sigma_C \Pi^{(b)}_C
$$

$$
= \frac{1}{2} \left( \sigma_C + (-1)^{\mu}\sigma_C(-1)^{\mu} \right).
$$
Suppose that, for the state $|\phi(\alpha, \eta)\rangle_{\text{AC}}$, X-basis measurement is performed on qubit A and parity measurement is on pulse C to produce outcomes $x$ and $x'$, respectively. Their distribution is computed from equation (24) as
\[
Pr(x = b, x' = b') = \| \langle b | \Pi_C^{(b)} \rangle_{\text{AC}} \|_2^2
\]
\[
= \| \Pi_E^{(b') \odot b} |\sqrt{\eta}\rangle_E \|_2^2
\]
and hence
\[
Pr(x \oplus x' = c) = \sum_{b'=0,1} Pr(x = b' \oplus c, x' = b') = \| \Pi_E^{c} |\sqrt{\eta}\rangle_E \|_2^2,
\]
which is also expected from the property that the BS preserves the total number of photons. We thus obtain
\[
Pr(x \neq x') = p_{\text{ph}}(\eta|\alpha|^2),
\]
which implies that the uncertainty in $x$ given $x'$ is related to the mean photon number received by Eve.

In a rigorous proof of security, the property of equation (33) turns out to be inadequate because a bit is adopted only when the corresponding optical pulse C leads to a successful detection in Bob’s measurement. In general, such conditioning could distort the statistics, and a conditional probability of $x \neq x'$ might not be bounded by $p_{\text{ph}}(\eta|\alpha|^2)$ as in equation (33). Fortunately, we can prove that there is no such worry. As shown in appendix A, $x \oplus x'$ is independent of any random variable $W$ generated by accessing the pulse C, namely,
\[
Pr(x \oplus x' = c|W) = Pr(x \oplus x' = c) \quad (c = 0, 1).
\]

4.4. Virtual protocol
In this subsection, we present a virtual protocol, which is helpful in proving the $\varepsilon_X$-secrecy, equation (16), of actual protocol. The virtual protocol is constructed in such a way that, as far as the final state of Alice’s key and Eve’s quantum system are concerned, it is equivalent to actual protocol. Bob’s final key, which is irrelevant to the $\varepsilon_X$-secrecy, is not generated in the virtual protocol. Instead, Bob’s action is designed for making it easier to prove the $\varepsilon_X$-secrecy condition by using the complementarity of quantum mechanics.

In what follows, we present the detailed flow of the virtual protocol. In addition to the protocol parameters for actual protocol, we define a probability $Pr(C_{\text{ph}}|N_1, N_2)$ over $N_1 \times N_2$ full-rank binary matrices $C_{\text{ph}}$. Construction of a set $T_{\text{ph}} \subset \{0, 1\}^{N_{\text{ph}}}$ will be given in the subsequent subsections. Probability $Pr(\alpha)$ appearing in assumption 1 is also used.

Virtual protocol
1. Alice generates $N_{\text{pal}}$-tuple of complex numbers $\alpha := (\alpha_0, \alpha_1, \ldots, \alpha_{N_{\text{pal}}})$ with probability $Pr(\alpha)$ and prepares quantum register $A$ of $N_{\text{pal}}$ qubits and system $C$ of $N_{\text{pal}}$ optical pulses in state $|\Psi(\alpha)\rangle_{\text{AC}}$ defined in equation (18). She then sends system $C$ to the wiretapper channel $E_{\text{wtp}}$, while keeping quantum register $A$.
2. Bob generates a test-bit index set $D_{\text{test, all}}$ by performing Bernoulli sampling with sampling rate $p_{\text{test}}$ on $\{1, \ldots, N_{\text{tot}}\}$. He defines a pulse index set $P_{\text{test, all}}$ as
\[
P_{\text{test, all}} := \{i \in \{0, 1, \ldots, N_{\text{tot}}\} \} (i \in D_{\text{test, all}}) \lor (i + 1 \in D_{\text{test, all}}) \}.
\]
3. After the wiretapper channel $E_{\text{wtp}}^{(ij)}$, Bob performs the parity measurement (definition 1) on the $i$th pulse whenever $i \notin P_{\text{test, all}}$ to obtain an outcome $x_i$. He then sends all the $(N_{\text{tot}} + 1)$ pulses to the main channel $E_{\text{main}}$.
4. Bob performs DPS measurement on the received pulses after the main channel $E_{\text{main}}$. According to the measurement outcomes for the $N_{\text{tot}}$ adjacent pairs, he determines a detection index set $D \subset \{1, \ldots, N_{\text{tot}}\}$ and a raw key $d := (d_j)_{j \in D}$ by the following rule. For the $j$th pair, $j \notin D$ if neither of the detectors clicks, and $j \in D$ otherwise. If only one of the detectors clicks, $d_j$ is set to be the index of that detector (i.e. 0 or 1). If both detectors click, $d_j$ is randomly set to 0 or 1.
5. Bob defines sets $D_{\text{left}} := D \setminus D_{\text{test}}$ and $D_{\text{test}} := D \cap D_{\text{test, all}}$. Bob also defines his test sequence $\alpha_{\text{test}}^{(ij)} := (d_j)_{j \in D_{\text{test}}}$ with a length of $N_{\text{test}} := |D_{\text{test}}|$. Bob announces $D_{\text{left}}$, $D_{\text{test}}$, and $\alpha_{\text{test}}^{(ij)}$. 
(6) Bob announces $P_{\text{test}}$, all and $(x'_j)_{j \in P_{\text{test}}}$.
(7) For $i \in P_{\text{test}}$, Alice performs a projection measurement on qubit $A_i$ on the Z-basis $\{|0\rangle, |1\rangle\}$ to determine the bit $a_i$. She defines her $N_{\text{test}}$-bit test sequence $\kappa^A_{\text{test}} := (a_i \oplus a_{j-1})_{i \in P_{\text{test}}}$ and announces it.
(8) For $i \notin P_{\text{test}}$, Alice applies $Z$-rotation operation $Z \equiv |0\rangle\langle 0| - |1\rangle\langle 1|$ on qubit $A_i$, if $x'_i = 1$.

(9) Alice applies a CNOT gate operation on $A_{j-1}$ and $A_j$, in which $A_{j-1}$ is a control and $A_j$ is a target, in descending order of $j \in D_{\text{diff}}$. She then defines a sifted key register as $A^{\text{sift}} := (A_i)_{i \in D_{\text{diff}}}$, which consists of $N_{\text{diff}} := |D_{\text{diff}}|$ qubits. Alice renames the indices to $(1, 2, \ldots, N_{\text{diff}})$ such that $A^{\text{sift}} = (A_i^\text{diff})_{i = 1}^{N_{\text{diff}}}$.

(10) (Privacy amplification). Alice determines the length $N_{\text{fin}}$ of the final key based on $\mu_A, \eta_A, D_{\text{diff}},$ and $D_{\text{test}}$. Alice extracts a $N_{\text{diff}} \times N_{\text{fin}}$ fullrank binary matrix $C_{PA}$ with the probability $\Pr(C_{PA}|N_{\text{diff}}, N_{\text{fin}})$, and announces its partial matrix $C_{PA} \equiv C_{PA}[I_{N_{\text{fin}}}O]^T$. She applies a unitary operation on $A^{\text{diff}}$.

(11) Alice measures $(A_i^\text{diff})_j = N_{\text{fin}} + 1$ on $X$ basis to obtain a $(N_{\text{diff}} - N_{\text{fin}})$-bit sequence. She chooses a $N_{\text{diff}}$-bit sequence $e^A_{\text{ph}} \in T_{\text{ph}}$ such that the last $(N_{\text{diff}} - N_{\text{fin}})$ bits of $e^A_{\text{ph}}(C_{PA}^{-1})^T$ coincide with the measured sequence. If she cannot find such a sequence, she sets $e^A_{\text{ph}} = 0$. Using a $N_{\text{fin}} \times N_{\text{fin}}$ matrix $\tilde{H} := [I_{N_{\text{fin}}}0]C_{PA}$, Alice applies a $Z$-rotation operation

$$\hat{U}_X(e^A_{\text{ph}}, \tilde{H}) := \sum_{x \in \{0, 1\}^{N_{\text{fin}}}} |x \oplus e^A_{\text{ph}}\tilde{H}|^T \langle x |$$

on the unmeasured sifted key register $A^{\text{fin}} := (A_i^\text{fin})_{i = 1}^{N_{\text{fin}}}$.

(12) Alice measures $A^{\text{fin}}$ on $Z$ basis to obtain her final key $\kappa^A_{\text{fin}}$.

Using assumptions 1–4 and a proper condition on the probability $\Pr(C_{PA}|N_1, N_2)$, we can show that actual protocol and virtual protocol leave Alice’s final key and Eve’s quantum system in the same state. More precisely, suppose that an attack strategy by Eve to actual protocol leads to a probability $\Pr(C_{PA}|N_{\text{fin}})$ and final states $\rho_{AE|N_{\text{fin}}}^{\text{fin}}$. Since all the announcements $(D_{\text{diff}}, D_{\text{test}}, \kappa^B_{\text{test}}, \kappa^A_{\text{test}}, C_{PA})$ in actual protocol are also made in virtual protocol, Eve can apply the same attack strategy to virtual protocol. Note that she ignores any other announcements that are only made in virtual protocol. Then, as shown in appendix B, virtual protocol also leads to the same probability $\Pr(C_{PA}|N_{\text{fin}})$ and the same final states $\rho_{AE|N_{\text{fin}}}^{\text{fin}}$. It then follows that $\varepsilon_X$-secrecy of virtual protocol implies $\varepsilon_X$-secrecy of actual protocol.

A crucial advantage in introducing virtual protocol is that it is much easier to prove its $\varepsilon_X$-secrecy. Let $\sigma^{\text{fin}}$ be the state of the $N_{\text{fin}}$ qubits $A^{\text{fin}}$ after step 11. Let $\langle 0 \rangle$ bet the state vector for $A^{\text{fin}}$ where every qubit is in state $|0\rangle$. If $\sigma^{\text{fin}} = \langle 0 \rangle \langle 0 |$ strictly held, the $Z$-basis measurement in step 12 would result in $\rho_{AE|N_{\text{fin}}}^{\text{fin}} = \rho_{AE|N_{\text{fin}}}^{\text{ideal}}$. We thus expect that, if $\sigma^{\text{fin}}$ is close to $\langle 0 \rangle \langle 0 |$, the final state $\rho_{AE|N_{\text{fin}}}^{\text{fin}}$ will also be close to $\rho_{AE|N_{\text{fin}}}^{\text{ideal}}$. In fact, it is known [40] that if

$$\sum_{N_{\text{fin}} \geq 1} \Pr(N_{\text{fin}})(1 - \langle 0 |\sigma^{\text{fin}}| 0 \rangle) \leq \delta$$

holds for $\delta > 0$, we have

$$\frac{1}{2} \sum_{N_{\text{fin}} \geq 1} \Pr(N_{\text{fin}})\|\rho_{AE|N_{\text{fin}}}^{\text{fin}} - \rho_{AE|N_{\text{fin}}}^{\text{ideal}}\| \leq \sqrt{2\delta}.$$
by classical computation to faithfully simulate the statistics of $x^*$. We call it estimation protocol and it is defined as follows.

Estimation protocol
Steps 1 through 7 are the same as those of virtual protocol.

(8) Alice measures qubits $(A_i)_{i \in \mathcal{D}_{\text{shift}}}$ on $X$ basis to obtain a bit sequence $(x_i)_{i \in \mathcal{D}_{\text{shift}}}$. She computes a bit sequence $e := (e_i)_{i \in \mathcal{D}_{\text{shift}}}$ by the following relations:

$$e_i := \begin{cases} x_i \oplus x_i & \text{if } i \not\in \mathcal{P}_{\text{test,all}} \\ x_i & \text{if } i \in \mathcal{P}_{\text{test,all}} \end{cases} \quad (41)$$

(9) Alice computes a bit sequence $e_{\text{ph}} := (e_{\text{ph},i})_{i \in \mathcal{D}_{\text{shift}}}$ by using the following relations in the descending order of $j \in \mathcal{D}_{\text{shift}}$.

$$e_{\text{ph},j} := \begin{cases} e_j + e_{\text{ph}, j+1} & \text{if } j + 1 \in \mathcal{D}_{\text{shift}} \\ e_j & \text{if } j + 1 \not\in \mathcal{D}_{\text{shift}} \end{cases} \quad (42)$$

(10) Alice determines the length $N_{\text{fin}}$ of the final key based on $\mu_{ph}$, $e_{\text{ph}}$, $\mathcal{D}_{\text{shift}}$, and $\mathcal{D}_{\text{test}}$. Alice extracts a $N_{\text{shift}} \times N_{\text{shift}}$ fullrank binary matrix $\tilde{C}_{\text{ph}}$ with the probability $\text{Pr}(\tilde{C}_{\text{ph}}|N_{\text{shift}}, N_{\text{fin}})$. She defines a $N_{\text{shift}} \times N_{\text{shift}}$ matrix $H := [\tilde{I}_{N_{\text{fin}}} \tilde{C}_{\text{ph}}]$ and a $(N_{\text{shift}} - N_{\text{fin}}) \times N_{\text{shift}}$ matrix $H := [O_{N_{\text{shift}} - N_{\text{fin}}} \tilde{C}_{\text{ph}}]^{-1}$.

(11) Alice chooses a $N_{\text{shift}}$-bit sequence $e_{\text{ph}}^* \in \mathcal{T}_{\text{ph}}$ satisfying $e_{\text{ph}}^*H^T = e_{\text{ph}}H^T$. If she cannot find such a sequence, she sets $e_{\text{ph}}^* = 0$. Alice then computes

$$x^* := (e_{\text{ph}} \oplus e_{\text{ph}}^*)H^T. \quad (43)$$

By comparing steps 8 through 11 to the corresponding steps in virtual protocol, it is easy to see that the $x^*$ are generated in the same way in both protocols. Our goal is thus to prove an inequality of the form

$$\text{Pr}(N_{\text{fin}} \geq 1, x^* \neq 0) \leq \delta, \quad (44)$$

which then implies that actual protocol is $\sqrt{2\delta}$-secret.

4.6. Completion of proof and formula for final key length
The remaining task of the security proof is to determine a final key length $N_{\text{fin}}$ such that equation (44) holds true. Here we provide a sketch of the proof, and leave technical details to appendix C.

Suppose that we find a set $\mathcal{T}_{\text{ph}}$ such that $e_{\text{ph}} \in \mathcal{T}_{\text{ph}}$ holds with a probability close to unity. We may choose a final key length to satisfy $N_{\text{fin}} \leq N_{\text{shift}} - \log_2|\mathcal{T}_{\text{ph}}| - s$ with $s > 0$, so that the length $(N_{\text{shift}} - N_{\text{fin}})$ of the bit sequence $e_{\text{ph}}H^T$ is slightly larger than $\log_2|\mathcal{T}_{\text{ph}}|$. Then, with a high probability, the sequence $e_{\text{ph}}^*H^T$ is unique to $e_{\text{ph}}$, namely, there is no other element $e_{\text{ph}}' \in \mathcal{T}_{\text{ph}} (e_{\text{ph}}' \neq e_{\text{ph}})$ that satisfies $e_{\text{ph}}'H^T = e_{\text{ph}}H^T$. This leads to equation (44) with a small $\delta$. Obviously, the final key length will be larger if the size of the set $\mathcal{T}_{\text{ph}}$ is smaller.

Instead of directly finding a set $\mathcal{T}_{\text{ph}}$, it is much easier to find a set $\mathcal{T}$ such that $e \in \mathcal{T}$ holds with a probability close to unity, because the sequence $e$ follows simpler statistics. Once we find such a set $\mathcal{T}$, choosing a final key length to satisfy $N_{\text{fin}} \leq N_{\text{shift}} - \log_2|\mathcal{T}| - s$ leads to equation (44). To see this, notice that at step 9 of estimation protocol, $e_{\text{ph}}$ is uniquely determined if $e$ is given. Let us denote this functional dependence by $e_{\text{ph}} = f_{\text{shift}}(e)$, and define $\mathcal{T}_{\text{ph}} := f_{\text{shift}}(\mathcal{T})$. Since $|\mathcal{T}_{\text{ph}}| \leq |\mathcal{T}|$, we have $N_{\text{fin}} \leq N_{\text{shift}} - \log_2|\mathcal{T}_{\text{ph}}| - s$.

Since $e \in \mathcal{T}$ implies $e_{\text{ph}} \in \mathcal{T}_{\text{ph}}$, the latter also holds with a probability close to unity, leading to equation (44).

To analyze the behavior of the sequence $e := (e_i)_{i \in \mathcal{D}_{\text{shift}}}$ defined in equation (41) of step 8, let us divide the set $\mathcal{D}_{\text{shift}}$ into two disjoint subsets as $\mathcal{D}_{\text{shift}} = \mathcal{D}_0 \cup \mathcal{D}_1$ with $\mathcal{D}_0 := \mathcal{D}_{\text{shift}} \cap \mathcal{P}_{\text{test,all}}$ and $\mathcal{D}_1 := \mathcal{D}_{\text{shift}} \setminus \mathcal{P}_{\text{test,all}}$. The sequence $e$ is also divided into two parts, $e' := (e_i)_{i \in \mathcal{D}_0}$ and $e'' := (e_i)_{i \in \mathcal{D}_1}$.

From equations (33) and (44) with assumptions 1 and 2, we see that, for $i \in \mathcal{D}_0$, the probability of $e_i = 1$ is at most $p_{\text{ph}}(\eta | H_{i\mu_{\text{ph}}})$. The number of 1’s in the sequence $e''$ is thus expected to be at most

$$|\mathcal{D}_0|p_{\text{ph}}(\eta | H_{i\mu_{\text{ph}}}) + \Delta,$$

where a parameter $\Delta > 0$ allows for statistical fluctuations. For the sequence $e'$ of length $|\mathcal{D}_1| = N_{\text{shift}} - |\mathcal{D}_0|$, we have no condition to restrict its behavior. We may thus expect that there exists a good set $\mathcal{T}$ with its size satisfying

$$\log_2|\mathcal{T}| \leq N_{\text{shift}} - |\mathcal{D}_0| + |\mathcal{D}_0|h(p_{\text{ph}}(\eta | H_{i\mu_{\text{ph}}}) + \Delta) \quad (45)$$

with

$$h(x) := \begin{cases} -x \log_2 x - (1 - x) \log_2 (1 - x) & (x < 1/2) \\ 1 & (x \geq 1/2) \end{cases} \quad (46)$$
Hence, the target condition of equation (44) is expected to be fulfilled if the final key length is chosen to satisfy
\[ N_{\text{fin}} \leq |D_0| (1 - h(p_{\text{ph}}(\eta_E, \mu_A) + \Delta)) - s. \] (47)

A rigorous proof along this line is given in appendix C, in which the fluctuations in the right-hand side of equation (47) are analyzed in detail to determine a formula for \( N_{\text{fin}} \) and find quantitative relation to \( \delta \) in equation (44). The derived key length formula is given by
\[ N_{\text{fin}} = \max \left\{ 0, \frac{N_{\text{rec}}}{M_U(N_{\text{rec}}, p_{\text{ph}}(\eta_E, \mu_A), \epsilon)} \right\} - s, \] (48)
where
\[ M_U(n, p, \epsilon) := \max \left\{ k \leq n \mid k \leq np \land \epsilon < 2^{-D(k/n,p)} \right\}, \] (49)
\[ D(p||q) := p \log_2 \frac{p}{q} + (1 - p) \log_2 \frac{1 - p}{1 - q}, \] (50)
\[ N_{\text{rec}} := N_{\text{sift}} - N_{\text{sift-tes}} - M_U(N_{\text{cand}}, p_{\text{test}}, \epsilon), \] (51)
\[ N_{\text{sift-tes}} := |D'_{\text{sift}} \cap D_{\text{test}}|, \] (52)
\[ N_{\text{cand}} := |D'_{\text{sift}} \setminus D|, \] (53)
\[ D'_{\text{sift}} := \{ i \in \{1, 2, \ldots, N_{\text{tot}} \} \mid i - 1 \in D_{\text{sift}} \}, \] (54)
which guarantees
\[ \Pr(N_{\text{fin}} \geq 1, x^* \neq 0) \leq 2\epsilon + 2^{-s}. \] (55)

Hence, we conclude that the actual protocol is \( \sqrt{2(2\epsilon + 2^{-s})} \)-secret with the choice of the final key length according to equation (48).

5. Numerical calculation of secure key rate

In this section, we present numerical calculations on the performances of LoS-QKD for the asymptotic and the finite-length regimes. Although the security proof in the previous section covers the general case of the LoS channel including non-iid channels, we here use a simplified model of the linear lossy bosonic channel as described in figure 3, and show potential performances of LoS-QKD for high-speed and long-distance secret key agreement. We also assume that the laser source prepares each pulse in \(|\sqrt{\mu_A}\rangle\), where the parameter \( \mu_A \) is to be optimized for maximizing the key rate.

The main channel is modeled by the BS with reflectivity \( \eta_{\text{env}} \), which corresponds to the total optical loss to the environment due to the laser beam divergence and the absorption in the atmosphere and the receiver. For simplicity, we include the common quantum efficiency of the detectors to \( \eta_{\text{env}} \). We also define the total transmittance of the channel between Alice and Bob as \( \eta_B := (1 - \eta_E)(1 - \eta_{\text{env}}) \).

In what follows, \( T \) and \( \nu_d \) denotes the pulse interval and the dark count rate of Bob’s on/off detectors. We set \( T = 1 \) ns (the pulse repetition rate of 1 GHz) and \( \nu_d = 1000 \) cps (counts per second), which are typical values in the current technology level.
5.1. Asymptotic key rate

We refer to the key rate in the asymptotic regime as the asymptotic key rate $R_{K,A}$, and define it as

$$R_{K,A} := \lim_{N_{\text{tot}} \to \infty} \left( \max_{\mu_A} \left[ \frac{N_{\text{fin}} - N_{\text{IR}}}{N_{\text{tot}}} \right] \right).$$  \hspace{1cm} (56)

In the asymptotic regime where $N_{\text{tot}}$ is infinitely long, $N_{\text{test}}/N_{\text{tot}} \to 0$, $N_{\text{sift}}/N_{\text{tot}} \to 0$, $N_{\text{cand}}/N_{\text{tot}} \to 0$, and $M_{\text{test}}(N_{\text{rec}}^0, p_{\text{ph}}(\eta_E \mu_A), \epsilon) \to p_{\text{ph}}(\eta_E \mu_A)$. \hspace{1cm} (57)

Hereafter, we simply write $p_{\text{ph}}(\eta_E \mu_A)$ as $p_{\text{ph}}$ and call this quantity the phase error rate. In addition, Alice and Bob can use the error correction code achieving the Shannon limit, namely,

$$N_{\text{IR}} = N_{\text{sift}} h(p_{\text{bit}}),$$ \hspace{1cm} (58)

where $p_{\text{bit}}$ denotes the quantum bit error rate (QBER), and is given as

$$p_{\text{bit}} = \frac{1 + \exp(-\mu_A \eta_B - \nu_d T)(1 - \exp(-\nu_d T))}{2p_{\text{det}}},$$ \hspace{1cm} (59)

as explained in appendix D. Hence, we obtain

$$\frac{N_{\text{fin}} - N_{\text{IR}}}{N_{\text{tot}}} \to p_{\text{det}}(1 - h(p_{\text{bit}}) - h(p_{\text{ph}})),\hspace{1cm} (60)$$

where $p_{\text{det}} := N_{\text{sift}}/N_{\text{test}}$ is the photon detection rate at Bob, and given as

$$p_{\text{det}} = 1 - \exp(-\mu_A \eta_B - 2\nu_d T),$$ \hspace{1cm} (61)

as explained in appendix D. Then, the asymptotic key rate $R_{K,A}$ in equation (56) turns into

$$R_{K,A} = \max_{\mu_A} \left[ p_{\text{det}}(1 - h(p_{\text{bit}}) - h(p_{\text{ph}})) \right].$$ \hspace{1cm} (62)

We plot the asymptotic key rate $R_{K,A}$ as a function of the channel loss $\eta^{-1}_B$ in figure 4 (red solid lines). For $\eta_E = 10^{-6}$, $R_{K,A}$ remains 1 Gbps at around $\eta^{-1}_B = 50$ dB (the flat region), then starts to decrease as $\eta^{-1}_B$ increases (the decreasing region), and finally drops to zero (the outage point) when $\eta^{-1}_B$ goes beyond 100 dB. The outage point corresponds to the channel loss at which the photon detection rate at Bob becomes comparable with the dark count rate of his on/off detectors. The asymptotic key rate $R_{K,A}$ still attains 1 kbps even at $\eta^{-1}_B = 100$ dB, which can cover a sufficient link budget for GEO-satellite-to-ground links assuming currently available technologies of optical antenna and PAT (pointing, tracking, and acquisition) system.

The asymptotic key rate $R_{K,A}$ deteriorates as $\eta_E$ increases. For $\eta_E = 10^{-4}$, the flat region becomes narrower. For $\eta_E = 10^{-2}$ or higher, the flat region disappears. The outage point in $\eta^{-1}_B$ also becomes smaller accordingly. The curve for $\eta_E = 1 - \eta_B$ is for the case where Eve can collect all photons Bob loses.
For comparison, we also plot the curves for known DPS-QKD (Waks’ scheme [41] and Mizutani’s scheme [42]), and decoy-state BB84 with the same link and noise conditions. Mizutani’s scheme is secure against the coherent attack (the most general attack in QKD), but its key rate decreases rapidly (blue one-dotted line). Waks’ scheme is secure against a limited family of attacks, i.e. the individual attack, and can reach 40 dB (blue dashed line). This curve shows almost the same performance as LoS-QKD with \( \eta_B = 1 - \eta_E \). Decoy-state BB84 can reach 50 dB which corresponds to a maximum link budget of LEO-satellite-to-ground communication (green dotted line). Unfortunately, these three schemes cannot cover a range of GEO-satellite-to-ground links, which should correspond to a channel loss of 60 dB or hopefully 80 dB (see the last paragraph in subsection 5.2). In appendix F, we also compare the asymptotic key rates of LoS-QKD and PLS scheme over FSO links (FSO-PLS) with DPS keying to show how the assumption on Eve affects the performances.

Now we discuss characteristic features of the LoS-QKD performances and the mechanisms behind. The crossover behavior from the flat region to the decreasing region is the common characteristic of secure transmission rates in PLS schemes, i.e. secrecy message rates in reference [16] and key rates in references [33, 34]. For example, the curves of the secrecy message rate versus the channel loss also consist of the flat region and the decreasing region as shown in figure 7 of reference [16]. The flat region and the decreasing regions in the \( R_{K,A} - \eta_B^{-1} \) curve are particularly referred to as ‘the loss-independent region’ and ‘the noise-limited regions’, respectively. In the loss-independent region, the received signal power is large enough compared to the noise power, and hence the signal can be discriminated in an error-free manner. In the noise-limited region, on the other hand, the received signal power becomes comparable with or less than the noise power, and hence the discrimination of the signal suffers from errors due to the noises, resulting in the monotonic decrease of the rate \( R_{K,A} \) as the channel loss \( \eta_B^{-1} \) increases. The observed behavior in the LoS-QKD is explained in a similar manner, if we ascribe the hardness in discrimination to the indistinguishability of quantum signals, which is often interpreted as quantum noise or shot noise inherent in a set of non-orthogonal quantum states.

Figure 5(a) presents the optimized mean photon number \( \mu_A \) at Alice versus the channel loss \( \eta_B^{-1} \). The optimized \( \mu_A \) monotonically increases in the loss-independent region, and then reaches a plateau in the noise-limited region. This very fact that Alice can increase \( \mu_A \) in the loss-independent region is a striking difference from the conventional QKD schemes in which the signal intensity at Alice must be at the single photon level. This is brought by the strong assumption on Eve that she can tap only the limited fraction \( \eta_E \) of the signal via the BS.

Figure 5(b) shows the received mean photon number \( \mu_B := \eta_B \mu_A \) at Bob versus the channel loss \( \eta_B^{-1} \). The curve of \( \mu_B \) gradually decreases in the loss-independent region, and then decreases more rapidly in the noise-limited region. In the loss-independent region, \( \mu_B \) is greater than the single photon level, and hence Bob’s detection almost always succeeds. The crossover occurs when \( \mu_B \) reaches the single photon level. For \( \eta_B = 10^{-6} \), for example, the crossover point is at around \( \eta_B^{-1} = 50 \) dB. Once \( \eta_B^{-1} \) goes beyond the crossover point, \( \mu_B \) becomes smaller than the single photon level, and Bob’s detection succeeds less frequently. Alice cannot increase the mean photon number \( \mu_A \) further in this region because the signal leaked to Eve is already strong, as seen in figure 5(c). The crossover point can also be expressed by the relation \( \eta_B^{-1} \sim 10 \eta_E^{-1} \), where Eve’s received mean photon number \( \mu_E = \eta_E \mu_A \) reaches 0.1 photons, and the information leakage to Eve becomes a matter. Finally, when \( \eta_B^{-1} \) is close to the outage point, Bob’s receiver becomes dark-count-noise limited, namely, the received count rate becomes comparable with the dark count rate, and the QBER increases. In this region, the optimized strategy is not to increase \( \mu_A \) to reduce QBER, but to suppress \( \mu_A \) to reduce the wiretapping risk. So, the optimized \( \mu_A \) drops at the end of each curve in figure 5(a). These behaviors are closely related to QBER \( p_{\text{bit}} \) and the phase error rate \( p_{\text{ph}} \) (see appendix E).

### 5.2. Finite-length key rate

We refer to the secure key rate in the finite-length regime as the *finite-length key rate* \( R_{K,F} \), and define it as

\[
R_{K,F} := \max_{\mu_A} \frac{N_{\text{fin}} - N_{\text{IR}}}{N_{\text{tot}}},
\]

for a fixed \( N_{\text{tot}} \). To evaluate \( N_{\text{fin}} \), we set \( N_{\text{diff}} \), \( N_{\text{diff-test}} \), and \( N_{\text{cand}} \) as

\[
N_{\text{diff}} = N_{\text{tot}} P_{\text{det}} (1 - p_{\text{test}}),
\]

\[
N_{\text{diff-test}} = N_{\text{tot}} P_{\text{det}}^2 (1 - p_{\text{test}}) p_{\text{test}},
\]

\[
N_{\text{cand}} = N_{\text{tot}} P_{\text{det}} (1 - p_{\text{det}}) (1 - p_{\text{test}}),
\]

respectively. In addition, we set

\[
N_{\text{IR}} = \int_0^\infty N_{\text{diff}} h(p_{\text{bit}}),
\]

where

\[
N_{\text{IR}}
\]

respectively. In addition, we set

\[
N_{\text{IR}} = \int_0^\infty N_{\text{diff}} h(p_{\text{bit}}),
\]
Figure 5. (a) Optimized mean photon number $\mu_A$ at Alice giving $R_{K,A}$ for the curves of LoS-QKD in figure 4. The right axis shows corresponding optical power, assuming that the center wavelength of optical pulse is 1550 nm. The required transmission power is far less than 1 mW even for $\eta_E = 10^{-6}$. (b) Corresponding mean photon number $\mu_B$ at Bob. (c) Corresponding mean photon number $\mu_E$ at Eve. Parameters: $\nu_d = 1000$ cps, $T = 1$ ns.

where $f_{EC} \geq 1$ denotes the error correction efficiency.

Figure 6 shows the finite-length key rate $R_{K,F}$ as a function of channel loss $\eta_{E}^{-1}$. For each $\eta_E$, we calculate $R_{K,F}$ with four values of $N_{tot}$, $10^9$ (solid line), $10^8$ (dashed line), $10^7$ (chain line), and $10^6$ (dotted line), as well as the asymptotic key rate $R_{K,A}$ (blue solid line) for comparison. Here remember that $N_{tot}$ is the number of optical pulses at Alice used for generating the final key. We choose $p_{test} = 0.06$, which is the same as the previous experiments of FSO-PLS scheme [28, 34]. We set the security parameter $\epsilon_X$ as $10^{-11}$. To ensure the relation $\epsilon_X := \sqrt{2(\epsilon + 2^{-7})}$ holds, we set

$$\epsilon = \frac{\epsilon_X^2}{4},$$

$$s = 2 \log_2 \frac{2}{\epsilon_X}.$$  

We set $f_{EC} = 1.1$.

In the loss-independent region, the finite-length key rates $R_{K,F}$ are slightly smaller than the asymptotic key rate $R_{K,A}$. This reduction is due to spending the test bits and the finite error correction efficiency. In the noise-limited region, the gap between $R_{K,F}$ and $R_{K,A}$ gets larger as $\eta_{E}^{-1}$ increases, and the outage point moves to the lower loss side as $N_{tot}$ decreases. Roughly speaking, the outage point decreases by about 20 dB when $N_{tot}$ decreases from $10^9$ to $10^6$.

Now a typical link budget between GEO-satellite-to-ground links is 80 dB. Practical link budgets between the satellite and the ground usually vary by 10 dB to 20 dB in the time scale of minutes due to atmospheric fading. Then the results of figure 6 imply that LoS-QKD for GEO-satellite-to-ground links is possible in the case of $\eta_E = 10^{-6}$, by taking $N_{tot}$ larger than $10^8$. The key rate of 1 Mbps could be achieved in the best condition in principle. Technical challenge is to implement key-distillation processing for $N_{tot} \geq 10^8$ with limited computing resources in satellite. This task could be feasible by careful modification of current architectures of software-based key-distillation processing, combined with advanced space-qualified CPUs and memories.
6. Conclusion

In this paper, we proposed the novel QKD scheme, LoS-QKD with DPS keying, for the FSO link modeled by the quantum WTC\textit{h}. Eve can tap only the limited fraction of the FSO signal beam, as modeled by the BS with the reflectivity \( \eta_E \) in front of Alice’s transmitter, but can perform any physically allowable operations on the tapped signals. The main channel between Alice and Bob may be affected by atmospheric fading effects. Thanks to the complementarity approach, we proved the composable security of LoS-QKD.

We numerically evaluated the performances of LoS-QKD based on the asymptotic and finite-length analyses. We also compared the asymptotic key rates with existing schemes, DPS-QKD and FSO-PLS (SKA). We showed how key agreement performances can be improved as Eve’s wiretapping ability is weakened. If we can assume that Eve’s wiretapping ratio \( \eta_E \) can be as small as \( \eta_E = 10^{-4} \sim 10^{-6} \), LoS-QKD can potentially realize GEO-satellite-to-ground secret key agreement under the practical conditions (i.e. total number of transmitted pulses, security parameter, error correction efficiency, and fraction of test bits) available in current technology. It would be an interesting open problem how to extend the concept of LoS-QKD to other protocols, such as measurement-assisted relaying schemes with a satellite, including measurement-device-independent QKD [43], and twin-field QKD [44].

A big remaining question is how one can certify the assumption that Eve’s wiretapping ability can be restricted to the BS model. It should be an involved task in practice. One should employ channel estimation techniques with signal and beacon beams as well as additional channel surveillance apparatuses (e.g. camera, RADAR, LIDAR). Unfortunately, there might be no single strong physical mechanism to certify our WTC\textit{h} model, but various physical mechanisms accompanied with the highly directional nature and LoS of the FSO links need to be employed.

Nevertheless, our results, at least, imply a way how to relate cryptographic schemes with information-theoretic security to each other, providing a unified design chart as the tradeoff relation between security level (adversarial assumptions) and usability (performances of key rate and distance). Based on our results, one can select appropriate schemes according to the use cases, the performance and security requirements: for higher security even against the active attack, DPS-QKD should be only the solution; for longer transmission distance and higher secure key rate, LoS-QKD or FSO-PLS could be an option. We believe that such a hybrid secret key agreement system is possible because these secret key agreement schemes can be implemented with almost the same technological platform.

Acknowledgments

The authors thank Professor R Matsumoto for the theoretical discussion. This work was partly supported by ‘Research and Development of the Quantum Cryptography Technology for Satellite Communications (JPJ007462)’ in ‘Research and Development of Information and Communications Technology (JPMI00316)’ of Ministry of Internal Affairs and Communication (MIC), Japan. This work was also funded in part by JSPS KAKENHI Grant No. 21K14163.
Data availability statement

No new data were created or analysed in this study.

Appendix A. Independence of variable $x \oplus x'$

Consider the state of pulse C after the X-basis and the parity measurement on the condition that $x \oplus x' = c$, and denote it by $\rho_C^{[x \oplus x' = c]}$ for $c = 0, 1$. This conditional state is written as

$$
\Pr(x \oplus x' = c)\rho_C^{[x \oplus x' = c]} = \sum_{b'=0,1} \text{Tr} \left[ A \left( \rho_C^{[x \oplus c]} \Pi_C^{(b')} |\phi(\alpha, \eta)\rangle \langle \phi(\alpha, \eta)| \Pi_C^{(b')} |\rho_C^{[x \oplus c]} \right) \right] \tag{A.1}
$$

and

$$
||\Pi_E^{(c')} |\sqrt{\eta} \alpha \rangle \|^2 \left[ \sum_{b'=0,1} \Pi_C^{(b')} |\sqrt{1 - \eta} \alpha\rangle \langle \sqrt{1 - \eta} \alpha| \right] , \tag{A.2}
$$

which means

$$
\rho_C^{[x \oplus x' = 0]} = \rho_C^{[x \oplus x' = 1]} . \tag{A.3}
$$

This implies that the random variable $x \oplus x'$ is independent of the state of the optical pulse C, and hence of any random variable W generated by accessing the pulse C.

Appendix B. Relation between actual protocol and virtual protocol

We assume that the probability $\Pr(\tilde{C}_{PA}|N_1, N_2)$ is related to the probability $\Pr(C_{PA}|N_1, N_2)$ in actual protocol by

$$
\sum_{\tilde{C}_{PA}, \tilde{C}_{PA}} \Pr(\tilde{C}_{PA}|N_1, N_2) = \Pr(C_{PA}|N_1, N_2), \tag{B.1}
$$

where $I_N$ denotes the identity matrix of order N and $O$ denotes the $N \times (N_1 - N_2)$ zero matrix. This ensures that, given $N_{\text{diff}}$ and $N_{\text{fin}}$, the announcement of $C_{PA}$ in actual protocol and that in virtual protocol are equivalent.

We then focus on virtual protocol and analyze Alice’s procedure of emitting optical pulses, receiving ($D_{\text{diff}}, D_{\text{test}}$) from Bob, announcing ($\kappa_{\text{test}}^{\text{fin}}, C_{PA}$), and creating the final key $\kappa_{\text{fin}}^{\text{test}}$. Since the Z-rotations in step 11 do not affect the Z-basis measurement in step 12, step 11 is redundant. Since the CNOT gates in step 9 and the unitary operation in step 10 are permutations in the Z-basis, step 8 is also redundant. Then, by comparing steps 1, 7, 9, 10, and 12 of virtual protocol and steps 1, 5, and 7 of actual protocol under assumption 1 and the source equivalence discussed in subsection 4.3, it is easy to see that Alice’s procedure is the same in the two protocols.

We next investigate the equivalence of Bob’s procedure of announcing ($D_{\text{diff}}, D_{\text{test}}, \kappa_{\text{test}}^{\text{fin}}$). Since step 8 is already found to be redundant, the outcome $x_1'$ of parity measurement can be discarded. Then, action of the parity measurement on the optical pulse is equivalent to random phase modulation (0 or $\pi$) as shown in equation (28). Assumption 3 on phase insensitivity of the main channel further implies that we may assume the random phase modulation is applied after the main channel $E_{\text{main}}$. This has two implications. One is that the parity measurements do not affect the detection pattern $D$, thanks to assumption 4 on the detection phase insensitivity. It is also easy to confirm that $D_{\text{test}}$ can be regarded as a Bernoulli sampling from $D$. Thus, $D_{\text{diff}}$ and $D_{\text{test}}$ are equivalent in the two protocols. Another implication is that the parity measurements do not affect the pulses for $\mathcal{P}_{\text{test, all}}$. Since $\kappa_{\text{test}}^{\text{fin}}$ is generated from measurements only involving the pulses for $\mathcal{P}_{\text{test, all}}$, $\kappa_{\text{test}}^{\text{fin}}$ is also equivalent in the two protocols.

From the above, we conclude that virtual protocol leads to the same probability $\Pr(N_{\text{fin}})$ and the same final states $\rho_{\text{fin}}^{\text{AE}}$ as actual protocol, which is true for any attack strategy to actual protocol.

Appendix C. Rigorous analysis of statistics in estimation protocol

As can be seen from steps 7 and 8 of estimation protocol, the statistics of various bits in $e := (e_i)_{i \in D_{\text{diff}}}$ are quite different for $i \in \mathcal{P}_{\text{test, all}}$ and for $i \notin \mathcal{P}_{\text{test, all}}$. Our first goal is thus to find a lower bound on the size of set

$$
\overline{D_0} := D_{\text{diff}} \setminus \mathcal{P}_{\text{test, all}} \tag{C.1}
$$
in terms of variables available also in actual protocol. Since $|\mathcal{D}_0| = N_{\text{diff}} - |\mathcal{D}_0|$ with

$$\mathcal{D}_0 := \mathcal{D}_{\text{diff}} \cap \mathcal{P}_{\text{test}, \text{all}},$$

we focus on the size of $\mathcal{D}_0$. Since $\mathcal{D}_{\text{diff}} \cap \mathcal{P}_{\text{test}, \text{all}} = \emptyset$, we see from equation (35) that

$$\mathcal{D}_0 = \{i \in \{0, 1, \ldots, N_{\text{tot}} - 1\} | (i \in \mathcal{D}_{\text{diff}}) \cap (i + 1 \in \mathcal{P}_{\text{test}, \text{all}}) \}. \quad (C.3)$$

We also define a shifted version of $\mathcal{D}_0$ by

$$\mathcal{D}'_0 = \{i \in \{1, 2, \ldots, N_{\text{tot}}\} | (i - 1 \in \mathcal{D}_{\text{diff}}) \cap (i \in \mathcal{P}_{\text{test}, \text{all}}) \}$$

where

$$\mathcal{D}'_{\text{diff}} := \{i \in \{1, 2, \ldots, N_{\text{tot}}\} | i - 1 \in \mathcal{D}_{\text{diff}} \}. \quad (C.5)$$

It is obvious that $|\mathcal{D}_0| = |\mathcal{D}'_0|$. A subset $\mathcal{D}'_{\text{diff}} \cap \mathcal{P}_{\text{test}} \subset \mathcal{D}'_0$ implies two consecutive successful detection events with the earlier one assigned to $\mathcal{D}_{\text{diff}}$ and the other one to $\mathcal{P}_{\text{test}}$. This subset is available in actual protocol and its size is

$$N_{\text{diff} - \text{test}} := |\mathcal{D}'_{\text{diff}} \cap \mathcal{P}_{\text{test}}|. \quad (C.6)$$

We thus only need to estimate the number of the remaining elements in $\mathcal{D}'_0$, namely, the size of

$$\mathcal{D}_1 := \mathcal{D}'_{\text{diff}} \cap (\mathcal{P}_{\text{test}, \text{all}} \setminus \mathcal{P}_{\text{test}}). \quad (C.7)$$

Since $\mathcal{P}_{\text{test}} = \mathcal{D} \cap \mathcal{P}_{\text{test, all}}$, we can rewrite $\mathcal{D}_1$ as

$$\mathcal{D}_1 = \mathcal{D}_{\text{cand}} \cap \mathcal{P}_{\text{test, all}},$$

where

$$\mathcal{D}_{\text{cand}} := \mathcal{D}'_{\text{diff}} \setminus \mathcal{D} \quad (C.9)$$

and its size

$$N_{\text{cand}} := |\mathcal{D}'_{\text{diff}} \setminus \mathcal{D}| \quad (C.10)$$

are available in actual protocol.

To derive a bound on $|\mathcal{D}_1|$, notice that $\mathcal{D}_{\text{cand}}$ is uniquely determined from $\mathcal{D}$ and $\mathcal{P}_{\text{test}}$. We denote that relation as $\mathcal{D}_{\text{cand}} = f(\mathcal{D}, \mathcal{P}_{\text{test}})$. Then, for any sets $S_0, S_1$ and $S_2$ with $S_0 = f(S_1, S_2)$, we have

$$\Pr(\mathcal{D}_1 | \mathcal{D}_{\text{cand}} = S_0, \mathcal{D} = S_1, \mathcal{P}_{\text{test}} = S_2)$$

$$= \Pr(S_0 \cap \mathcal{D}_{\text{test, all}} | \mathcal{D} = S_1, S_1 \cap \mathcal{P}_{\text{test, all}} = S_2) \quad (C.11)$$

$$= \Pr(S_0 \cap \mathcal{D}_{\text{test, all}} | S_1 \cap \mathcal{D}_{\text{test, all}} = S_2) \quad (C.12)$$

$$= \Pr(S_0 \cap \mathcal{D}_{\text{test, all}}), \quad (C.13)$$

where we used the facts that $\mathcal{D}_{\text{test, all}}$ and $\mathcal{D}$ are statistically independent and that $S_0 \cap \mathcal{D}_{\text{test, all}}$ and $S_1 \cap \mathcal{D}_{\text{test, all}}$ are statistically independent because $S_0 \cap S_1 = \emptyset$. This equation means that, given $N_{\text{cand}}$, $|\mathcal{D}_1|$ follows a binomial distribution. Hence we can use Chernoff–Hoeffding theorem to obtain

$$\Pr(|\mathcal{D}_1| \leq M^U(N_{\text{cand}}, p_{\text{test, all}})) \geq 1 - \epsilon, \quad (C.14)$$

where

$$M^U(n, p, \epsilon) := \max \left\{ k \leq n | k \leq np \lor \epsilon < 2^{-n \log_2(1/p)} \right\} \quad (C.15)$$

with

$$D(p||q) := p \log_2 \frac{p}{q} + (1 - p) \log_2 \frac{1 - p}{1 - q}. \quad (C.16)$$

Since

$$|\mathcal{D}_0| = N_{\text{diff}} - |\mathcal{D}_0| = N_{\text{diff}} - |\mathcal{D}'_0| = N_{\text{diff}} - N_{\text{diff} - \text{test}} - |\mathcal{D}_1|, \quad (C.17)$$

we have

$$\Pr\left( N^L_{\text{rec}} \leq |\mathcal{D}_0| \right) \geq 1 - \epsilon \quad (C.18)$$

with

$$N^L_{\text{rec}} := N_{\text{diff}} - N_{\text{diff} - \text{test}} - M^U(N_{\text{cand}}, p_{\text{test, all}}). \quad (C.19)$$
The set $T_{ph}$ in virtual protocol and estimation protocol is constructed as follows. A set $D_{rec}$ with $|D_{rec}| = N^{l}_{rec}$ is chosen such that $D_{rec} \subseteq \overline{D_{0}}$ if $N^{l}_{rec} \leq |\overline{D_{0}}|$, and $D_{rec} \subset D_{fin}$ otherwise. From this set, we define a weight of an $N_{fin}$-bit sequence $s = (s_i)_{i \in D_{fin}}$ by

$$w(s; D_{rec}) := \sum_{i \in D_{rec}} s_i.$$  

(C.20)

From the property of the source given in equation (34) of subsection 4.3, we see that for $i \notin P_{test, all}$, the random variable $e_i := x_i \oplus x'_i$ is independent of other variables when conditioned on $\alpha_i$. We thus have

$$\Pr(e_{i(k)}|D_{rec} = \{i(1), i(2), \ldots, i(N^{l}_{rec})\}, e_{i(1)}, \ldots, e_{i(k-1)}, N^{l}_{rec} \leq |\overline{D_{0}}|, \alpha) = \Pr(e_{i(k)}|\alpha_i),$$

which amounts to requiring that $\Pr(e_i|\alpha_i) = \Pr(e_i|\alpha_i)$ for $i \notin P_{test, all}$. On the other hand, $N^{l}_{rec} \leq |\overline{D_{0}}|$ implies $D_{rec} \cap P_{test, all} = \emptyset$ because $D_{rec} \subset \overline{D_{0}} = D_{fin}\setminus P_{test, all}$ by construction. We thus obtain

$$\Pr(w(e; D_{rec}) \leq M^{U}(N^{l}_{rec}, p_{ph}(\eta|\mu_A), \epsilon) | D_{rec}, N^{l}_{rec} \leq |\overline{D_{0}}|) \geq 1 - \epsilon.$$  

(C.23)

We define a set $T$ of $N_{fin}$-bit sequences by

$$T := \{s = (s_i)_{i \in D_{fin}} | w(s; D_{rec}) \leq M^{U}(N^{l}_{rec}, p_{ph}(\eta|\mu_A), \epsilon)\}.$$  

(C.24)

Then it satisfies

$$\Pr(e \in T|N^{l}_{rec} \leq |\overline{D_{0}}|) \geq 1 - \epsilon$$  

(C.25)

and

$$\log_2|T| \leq N_{fin} - N^{l}_{rec} + N^{l}_{rec} h\left(\frac{M^{U}(N^{l}_{rec}, p_{ph}(\eta|\mu_A), \epsilon)}{N^{l}_{rec}}\right),$$

where the function $h(x)$ is defined in equation (46). In estimation protocol, $e_{ph}$ is uniquely determined if $e$ is given. Let us denote this functional dependence by $e_{ph} = f_{est}(e)$, and define $T_{ph} := f_{est}(T)$. Then we have $|T_{ph}| \leq |T|$. Since $e \in T$ implies $e_{ph} \in T_{ph}$, we see from equations (C.18) and (C.25) that

$$\Pr(e_{ph} \in T_{ph}) \geq 1 - 2\epsilon$$  

(C.27)

holds true.

We assume that the selection of matrix $H$ in step 10 is sufficiently random to meet the condition of universal2 hashing, i.e.

$$\Pr(y_1H^T = y_2H^T|N_{diff}, N_{fin}) \leq 2^{-(N_{fin} - N_{fin})},$$

\forall y_1, y_2 \in \{0, 1\}^{N_{fin} - N_{fin}} \text{ with } y_1 \neq y_2,$$

which amounts to requiring that $\Pr(C_{ph}|N_1, N_2)$ in the actual protocol be dual universal2 hashing [45]. Then we have

$$\Pr(e_{ph}^{\ast} \neq e_{ph}|N_{diff}, N_{fin}, T_{ph}, e_{ph} \in T_{ph}) \leq 2^{-(N_{fin} - N_{fin})}|T_{ph}| \leq 2^{-(N_{fin} - N_{fin})}|T|.$$  

(C.28)

We thus adopt the length of the final key to be

$$N_{fin} = \left[ N^{l}_{rec} \left[ 1 - h\left(\frac{M^{U}(N^{l}_{rec}, p_{ph}(\eta|\mu_A), \epsilon)}{N^{l}_{rec}}\right) \right] - z \right]$$

(C.31)

whenever it is positive. Then we have $\Pr(e_{ph}^{\ast} \neq e_{ph}|e_{ph} \in T_{ph}) \leq 2^{-z}$ and hence

$$\Pr(N_{fin} \geq 1, x^{\ast} \neq 0) \leq 2\epsilon + 2^{-z}.$$  

(C.32)
Appendix D. Derivation of \( p_{\text{det}} \) and \( p_{\text{bit}} \)

In this appendix, we derive the photon detection rate \( p_{\text{det}} \) in equation (61) and the QBER \( p_{\text{bit}} \) in equation (59).

We start with the photon detection rate \( p_{\text{det}} \), which is the probability that at least one of Bob’s detectors clicks. It suffices to consider only the case that Alice transmits bit 0 thanks to the symmetry of the protocol on input bits. So, \( p_{\text{det}} \) is given as
\[
p_{\text{det}} = 1 - P_{D0}(\text{off})P_{D1}(\text{off}), \tag{D.1}
\]
where \( P_{D0}(\text{off}) \) and \( P_{D1}(\text{off}) \) are the probabilities that Bob’s on/off detectors D0 and D1 do not click, respectively. Assuming that the photon number distribution follows a Poisson distribution, they are given as
\[
P_{D0}(\text{off}) = \exp(-\mu A \eta_B - \nu_d T), \tag{D.2}
\]
\[
P_{D1}(\text{off}) = \exp(-\nu_d T). \tag{D.3}
\]
Substituting equations (D.2) and (D.3) into equation (D.1), we have
\[
p_{\text{det}} = 1 - \exp(-\mu A \eta_B - \nu_d T) \exp(-\nu_d T) = 1 - \exp(-\mu A \eta_B - 2\nu_d T), \tag{D.4}
\]
which is we want to obtain.

Next, we derive the QBER \( p_{\text{bit}} \), which is the probability that the unintended detector clicks. As with \( p_{\text{det}} \), we only consider the case that Alice transmits bit 0. So, \( p_{\text{det}} \) is given as
\[
p_{\text{bit}} = \frac{P_{D0}(\text{off})(1 - P_{D1}(\text{off})) + \frac{1}{2}(1 - P_{D0}(\text{off}))(1 - P_{D1}(\text{off}))}{p_{\text{det}}}, \tag{D.5}
\]
where the second term of the numerator reflects the fact that we set 0 or 1 randomly to a raw key bit when both detectors click. Using equations (D.2) and (D.3), we have
\[
p_{\text{bit}} = \frac{(1 + \exp(-\mu A \eta_B - \nu_d T))(1 - \exp(-\nu_d T))}{2p_{\text{det}}}, \tag{D.6}
\]
which is we want to obtain.

Appendix E. Behaviors of \( p_{\text{bit}} \) and \( p_{\text{ph}} \)

In this appendix, we present the behaviors of QBER \( p_{\text{bit}} \) and the phase error rate \( p_{\text{ph}} \). In figures E1(a) and (b), we present these quantities for the asymptotic rates \( R_{SKA} \) of LoS-QKD in figure 4 as a function of \( \eta_B^{-1} \).

In the loss-independent region, \( p_{\text{bit}} \) shows the error floor which is determined by the dark count rate of Bob’s on/off detectors, while \( p_{\text{ph}} \) monotonically increases. In the noise-limited region, \( p_{\text{bit}} \) monotonically increases, while \( p_{\text{ph}} \) shows a plateau \( (p_{\text{ph}} = 0.09) \), irrelevant to the value of \( \eta_B \). This value of \( p_{\text{ph}} \) corresponds to Eve’s received mean photon number \( \mu_E \) of 0.29. We note that the behavior of \( p_{\text{ph}} \) shown in figure E1(b) is similar to that of Eve’s received mean photon number \( \mu_E \) in figure 5(c). Actually,
\[
p_{\text{ph}}(\mu_E) = \frac{1 - e^{-2\mu_E}}{2} \sim \mu_E \tag{E.1}
\]
holds for small \( \mu_E \).

Appendix F. LoS-QKD versus FSO-PLS with DPS keying

In this appendix, we compare the asymptotic key rate of FSO-PLS (SKA) with DPS keying to that of LoS-QKD. To this end, we start with deriving the asymptotic key rate of FSO-PLS with DPS keying.

We consider the configuration shown in figure F1 as the model for the FSO-PLS with DPS keying. The main channel is the linear lossy bosonic channel modeled by the BS with reflectivity \( \eta_{\text{env}} \) as with the model for LoS-QKD shown in figure 3. However, opposed to LoS-QKD, we explicitly specify Eve’s wiretapping scheme. Namely, she also equips with the one-bit-delay balanced interferometer and two on/off detectors to perform the DPS measurement onto the tapped photons. To consider the conservative situation, Eve’s on/off detectors have ideally no dark counts.
Figure E1. (a) Quantum bit error rate $p_{\text{bit}}$ and (b) phase error rate $p_{\text{ph}}$ for the asymptotic rates $R_{K,A}$ of LoS-QKD in figure 4. Parameters: $\nu_d = 1000$ cps, $T = 1$ ns.

Figure F1. Schematic diagram of the configuration of FSO-PLS with DPS keying.

Also, in the information reconciliation step of the key-distillation processing, we adopt the reverse reconciliation where Bob provides Alice with information on his sifted key $\kappa_B$ via the authenticated public channel. Therefore, the asymptotic key rate formula for FSO-PLS is given as

$$R_{K,\text{PLS}} = I(X; Y) - I(Y; Z), \quad (F.1)$$

where $I(\cdot; \cdot)$ denotes the Shannon mutual information, and $X$, $Y$, and $Z$ are the random variables at Alice, Bob, and Eve, respectively. The first term of equation (F.1) corresponds to the information rate shared by Alice and Bob after the reconciliation and the second term of equation (F.1) corresponds to the information rate leaked to Eve in the reverse reconciliation [33].

The mutual information $I(X; Y)$ in equation (F.1) is evaluated as

$$I(X; Y) = \sum_x \sum_y P_X(x) W_B(y|x) \log_2 \frac{W_B(y|x)}{\sum_{x'} P_X(x') W_B(y|x')} . \quad (F.2)$$

In the equation, $P_X(x)$ denotes the input probability of Alice’s bit, and $P_X(0) = P_X(1) = 1/2$ since Alice sends a random bit sequence. Also, $W_B(y|x)$ denotes the transition probability of the main channel. Since the bit detection failure and the bit error occur in the main channel, the main channel is modeled into the
binary symmetric erasure channel shown in figure F2(a), and the transition probability $W_B(y|x)$ is given as

$$W_B(0|0) = W_B(1|1) = p_{\text{det}}(1 - p_{\text{bit}}),$$  \hspace{1cm} (F.3)
$$W_B(0|1) = W_B(1|0) = p_{\text{det}}p_{\text{bit}},$$  \hspace{1cm} (F.4)
$$W_B(?)|0) = W_B(?)|1) = (1 - p_{\text{det}}),$$  \hspace{1cm} (F.5)

where ‘?’ denotes an erasure symbol. Substituting these transition probabilities into equation (F.2), we obtain

$$I(X; Y) = p_{\text{det}}(1 - h(p_{\text{bit}})).$$  \hspace{1cm} (F.6)

Similarly, the mutual information $I(Y; Z)$ in equation (F.1) is evaluated as

$$I(Y; Z) = \sum_y \sum_z P_Y(y)W_{EB}(z|y)\log_2 \frac{W_{EB}(z|y)}{\sum_y P_Y(y)W_{EB}(z|y)},$$  \hspace{1cm} (F.7)

where $P_Y(y)$ denotes the probability of Bob’s bit and $W_{EB}(z|y)$ denotes the transition probability of the channel from Bob to Eve. Since Bob’s bits are output of the main channel which takes Alice’s bit as an input, $P_Y(y)$ is given as

$$P_Y(0) = P_Y(1) = \frac{p_{\text{det}}}{2},$$  \hspace{1cm} (F.8)
$$P_Y(?) = (1 - p_{\text{det}}).$$  \hspace{1cm} (F.9)

The channel from Bob to Eve is the concatenation of the channel from Bob to Alice and the wiretapper channel, as shown in figure F2(b). The channel from Bob to Alice is the reverse version of the main channel, and its transition probabilities $W_{AB}(x|y)$ are calculated as

$$W_{AB}(0|0) = W_{AB}(1|1) = 1 - p_{\text{bit}},$$  \hspace{1cm} (F.10)
$$W_{AB}(0|1) = W_{AB}(1|0) = p_{\text{bit}},$$  \hspace{1cm} (F.11)
$$W_{AB}(0|?) = W_{AB}(1|?) = \frac{1}{2},$$  \hspace{1cm} (F.12)

with Bayes’ theorem. Since Eve has the ideal on/off detectors without dark counts, the wiretapper channel becomes the binary erasure channel with the transition probabilities

$$W_E(0|0) = W_E(1|1) = 1 - p_{\text{fail},E},$$  \hspace{1cm} (F.13)
Figure F3. (a) Asymptotic key rates and (b) optimum mean photon number $\mu_A$ in input pulses of LoS-QKD (red lines) and FSO-PLS (blue lines). Parameters: $\nu_d = 1000$ cps, $T = 1$ ns.

where

$$W_E(\cdot|0) = W_E(\cdot|1) = p_{\text{fail,E}}, \quad \text{(F.14)}$$

Consequently, the channel from Bob to Eve becomes the three-input-three-output channel with the transition probabilities

$$W_{EB}(0|0) = W_{EB}(1|1) = (1 - p_{\text{bit}})(1 - p_{\text{fail,E}}), \quad \text{(F.16)}$$

$$W_{EB}(0|1) = W_{EB}(1|0) = p_{\text{bit}}(1 - p_{\text{fail,E}}), \quad \text{(F.17)}$$

$$W_{EB}(\cdot|0) = W_{EB}(\cdot|1) = W_{EB}(\cdot|\cdot) = p_{\text{fail,E}}, \quad \text{(F.18)}$$

$$W_{EB}(0|\cdot) = W_{EB}(1|\cdot) = \frac{1}{2} - p_{\text{fail,E}}. \quad \text{(F.19)}$$

Using these probabilities, we obtain

$$I(Y; Z) = p_{\text{det}}(1 - p_{\text{fail,E}})(1 - h(p_{\text{bit}})). \quad \text{(F.20)}$$

Finally, from equations (F.6) and (F.20), the asymptotic key rate of FSO-PLS with DPS keying is given as

$$R_{K,\text{PLS}} = p_{\text{det}}p_{\text{fail,E}}(1 - h(p_{\text{bit}})). \quad \text{(F.21)}$$

Now, we compare the asymptotic key rate of two schemes. Figures F3(a) and (b) show the asymptotic key rates $R_{K,A}$ and the mean photon number $\mu_A$ of the input pulses for LoS-QKD (red lines) and FSO-PLS (blue lines), respectively. The asymptotic key rate of the FSO-PLS is also characterized by the loss-independent and noise-limited regions. Actually, the behaviors of the optimized mean photon number $\mu_A$ are almost the same between these schemes. However, the plateau of the loss-independent region of FSO-PLS is wider than that of LoS-QKD. This is because $\mu_A$ can be larger in FSO-PLS than in LoS-QKD owing to the additional assumption that Eve’s apparatus is explicitly specified. Moreover, $R_{K,A}$ of the PLS (SKA) monotonically decreases and never drops as opposed to LoS-QKD, because the PLS (SKA) adopts the reverse reconciliation scheme.

Thus, by specifying Eve’s detection strategy as the similar kind as Bob’s one, we can further improve the performances in the noise-limited region. If, however, users should worry about possibilities of store-now-and-decrypt-later attacks using future quantum technologies including quantum memory and so on, then LoS-QKD is recommended.

ORCID iDs

Toshihiko Sasaki https://orcid.org/0000-0003-0745-6791
Masahide Sasaki https://orcid.org/0000-0002-9508-570X

References

[1] Bennett C H and Brassard G 1984 Quantum cryptography: public-key distribution and coin tossing Proc. on Int. Conf. on Computers, Systems and Signal Processing pp 175–9
[2] Ekert A K 1991 Phys. Rev. Lett. 67 661–3
[3] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Rev. Mod. Phys. 74 145–95
[4] Peet M et al 2009 New J. Phys. 11 075001
[5] Sasaki M et al 2011 Opt. Express 19 10387–409
[6] Courtland R 2016 IEEE Spectr. 53 11–2
[7] Tang Y L et al 2016 Phys. Rev. X 6 011024
[8] Takenaka H, Carrasno–Casado A, Fujiwara M, Kitamura M, Sasaki M and Toyoshima M 2017 Nat. Photon. 11 502
[9] Günthner K et al 2017 Optica 4 611–6
[10] Liao S K et al 2017 Chin. Phys. Lett. 34 090302
[11] Yin J et al 2017 Science 356 1140–4
[12] Liao S K et al 2017 Nat. Photon. 11 509
[13] Liao S K et al 2018 Phys. Rev. Lett. 120 030501
[14] Chen Y A et al 2021 Nature 589 214–9
[15] Yin J et al 2020 Nature 582 501–5
[16] Endo H, Han T S, Aoki T and Sasaki M 2015 IEEE Photon. J. 7 7903418
[17] Wyner A D 1975 Bell Syst. Tech. J. 54 1355–87
[18] Csiszár I and Körner J 1978 IEEE Trans. Inf. Theory 24 339–48
[19] Maurer U M 1993 IEEE Trans. Inf. Theory 39 733–42
[20] Ahlswede R and Csiszar I 1993 IEEE Trans. Inf. Theory 39 1121–32
[21] Zhou X, Yan Z and Lingyang S 2016 Physical Layer Security in Wireless Communications (Boca Raton, FL: CRC Press)
[22] Schaefer R F, Boche H, Khisti A and Poor H V 2017 Information Theoretic Security and Privacy of Information Systems (Cambridge: Cambridge University Press)
[23] Wang N, Song X, Cheng J and Leung V C M 2014 J. Opt. Commun. Netw. 6 1072–81
[24] Lopez-Martinez F J, Gomez G and Garrido-Balsells J M 2015 IEEE Photon. J. 7 7901014
[25] Sun X and Djordjevic I B 2016 IEEE Photon. J. 8 7901110
[26] Zou D and Xu Z 2016 IEEE Photon. J. 8 7804809
[27] Chen C and Yang H 2018 Opt. Express 26 16422–41
[28] Endo H et al 2016 Opt. Express 24 8940–55
[29] Wang T L, Gariano J A and Djordjevic I B 2018 IEEE Photon. J. 10 7907113
[30] Wang T L and Djordjevic I B 2018 IEEE Photon. J. 10 7908611
[31] Ji J, Huang Q, Chen X and Sun I 2019 IEEE Photon. J. 11 7903240
[32] Fujiwara M et al 2018 Opt. Express 26 19513–23
[33] Endo H, Fujiwara M, Kitamura M, Tsuzuki O, Ito T, Shimizu R, Takeoka M and Sasaki M 2018 Opt. Express 26 23305–32
[34] Endo H, Fujiwara M, Kitamura M, Tsuzuki O, Shimizu R, Takeoka M and Sasaki M 2020 OSA Contin. 3 2525–43
[35] Vergoossen T, Bedington R, Grieve J A and Ling A 2019 Entropy 21 387
[36] Pan Z, Seshadreesan K P, Clark W, Adcock M R, Djordjevic I B, Shapiro J H and Guha S 2020 Phys. Rev. Appl. 14 024044
[37] Vernam G S 1926 Trans. Am. Inst. Electr. Eng. 45 295–301
[38] Muller-Quade J and Renner B 2009 New J. Phys. 11 085006
[39] Koashi M 2009 New J. Phys. 11 045018
[40] Matsuura T, Sasaki T and Koashi M 2019 Phys. Rev. A 99 042303
[41] Waks E, Takesue H and Yamamoto Y 2006 Phys. Rev. A 73 012344
[42] Mizutami A, Sasaki T, Kato G, Takeuchi Y and Tamaki K 2017 Quantum Sci. Technol. 3 014003
[43] Lo H K, Curty M and Qi B 2012 Phys. Rev. Lett. 108 130503
[44] Lucamarini M, Yuan Z L, Dynes J F and Shields A J 2018 Nature 557 400–3
[45] Tsurumaru T and Hayashi M 2013 IEEE Trans. Inf. Theory 59 4700–17