Finite-key analysis for coherent one-way quantum key distribution

Ming-Yang Li,[1] Xiao-Yu Cao,[1] Yuan-Mei Xie,[1] Hua-Lei Yin,[2,1,*] and Zeng-Bing Chen[1,†]

[1]*National Laboratory of Solid State Microstructures and School of Physics, Collaborative Innovation Center of Advanced Microstructures, Nanjing University, Nanjing 210093, China*

[2]*Department of Physics and Beijing Key Laboratory of Opto-electronic Functional Materials and Micro-nano Devices, Key Laboratory of Quantum State Construction and Manipulation (Ministry of Education), Renmin University of China, Beijing 100872, China*

(Received 23 September 2023; accepted 11 December 2023; published 8 January 2024)

Coherent-one-way (COW) quantum key distribution (QKD) is a significant communication protocol that has been implemented experimentally and deployed in practical products due to its simple equipment requirements. However, existing security analyses of COW-QKD either provide a short transmission distance or lack immunity against coherent attacks in the finite-key regime. In this paper, we present a tight finite-key security analysis within the universally composable framework for a variant of COW-QKD, which has been proven to extend the secure transmission distance in the asymptotic case. We combine the quantum leftover hash lemma and entropic uncertainty relation to derive the key rate formula. When estimating statistical parameters, we use the recently proposed Kato's inequality to ensure security against coherent attacks and achieve a higher key rate. Our paper confirms the security and feasibility of COW-QKD for practical application and lays the foundation for further theoretical study and experimental implementation.

DOI: 10.1103/PhysRevResearch.6.013022

I. INTRODUCTION

Quantum theory has been playing a significant role in the field of communications, leading to the development of primitives such as quantum repeaters [1–3], quantum conference key agreement [4–10], quantum secret sharing [11–18], and quantum digital signatures [19–22]. Among these primitives, quantum key distribution (QKD) [23,24] has received considerable attention due to its ability to provide two remote users with a secret key with unconditional security guaranteed by the laws of quantum mechanics. Since the first QKD protocol, the Bennett-Brassard 1984 protocol [23] was proposed, various QKD schemes have been developed [25–27] to improve its practicality. Among these developments, measurement-device-independent QKD [28,29] is of vital importance for its immunity against one of the most threatening attacks, detector attacks [30], which enable experimental operations over a long distance [31,32]. However, due to channel loss, the key rates of most QKD protocols are bounded by the secret-key capacity of repeaterless QKD [33–36]. A protocol called the twin-field QKD [37] and its variants [38–43], which are based on single-photon interference instead of two-photon interference, break this bound and increase the secure distance to 833 km [44] and 1002 km [45] experimentally. Moreover, the recently proposed asynchronous measurement-device-independent QKD [46,47] (also named mode-pairing QKD) has become a practical approach for long-distance quantum communication systems [48–51] because it breaks the linear bound with its simple experimental implementation compared with twin-field QKD. The photon number splitting attack [52] is another critical limitation of practical QKD that has been overcome by several means like decoy-state methods [53–55], nonorthogonal coding methods [56–58], strong reference methods [59], and distributed-phase-reference methods [60–63], including differential-phase-shift (DPS) QKD and coherent-one-way (COW) QKD.

DPS protocol [60,61] is becoming more significant for its excellent key rate performance achieved by the simple setup of equipment. The experimental progress [64–67] shows the status of DPS-QKD as a promising protocol for realizing the quantum communication process in the real world. Theoretically, long-term security analyses of DPS-QKD have been proposed to establish a solid foundation to guarantee its unconditional security in reality. Assuming a single photon to be in each of the blocks, the analysis in Ref. [68] provided security proof of DPS-QKD, and this impractical assumption was changed to use a blockwise phase-randomized coherent photon source in later developments [69,70]. Furthermore, recently proposed proofs [71–73] give more practical analyses, removing the requirement of a special photon source and covering more general cases. Finally, Refs. [74,75] provide information-theoretic secure analyses to show the practicability of DPS-QKD in the finite-key regime, which builds a complete theoretic scheme for this protocol. We note that the

*hlyin@ruc.edu.cn
†zbchen@nju.edu.cn

security proof in Ref. [74] results in a key rate that scales in the order of $O(\eta^2)$ without relativistic constraint and has immunity against coherent attacks, which is of vital importance in realistic implementation.

COW-QKD [62] is another type of distributed-phase-reference protocol that has been implemented in practical quantum information processing [76] with its easily achievable experimental requirements [77–84], which are similar to those of DPS-QKD. Contrary to the DPS-QKD, the security proof for the COW protocol remains incomplete, primarily due to the absence of a finite-key secure analysis that simultaneously offers robust key rate performance and security against coherent attacks. Typically, the security of COW-QKD is proven by measuring the interference visibility to estimate information leakage [85,86]. However, when considering the zero-error attack [87,88], which enables eavesdropping by Eve without introducing bit errors, COW-QKD is insecure if its key rate scales as $O(\eta)$ [89], which is the scale of the key rate used in many COW-QKD experiments [79,81–84,90]. In Ref. [91], the authors introduced an innovative method for calculating the key rate of a variant of COW-QKD, resulting in an improved key rate in high-loss channels. However, the security of this protocol in the finite-key regime, particularly its immunity to coherent attacks, has yet to be proven. This is a crucial step in ensuring its practicality in real-world environments. In summary, the lack of a finite-key analysis for COW-QKD that offers both a high key rate and security against coherent attacks remains a significant challenge in enhancing the practicality of this technology. Recently, a security proof for COW-QKD was proposed [92] based on an innovative practical implementation that retains the simplicity of the original version. By estimating the upper bound on the phase error rate instead of measuring the visibility of interference, it was shown that the secure transmission distance can be over 100 km, and an analytic formula for the key rate was provided. Nevertheless, a practical QKD protocol only involves finite resources, which means only a finite number of states are sent, leading to statistical fluctuations between observed values and expected values. Consequently, before we promote this protocol into reality, finite key analysis must be completed to lay the theoretical foundation. The uncertainty relation of smooth entropies [93] has been utilized to prove the finite-key security of the BB84 protocol [94] with composable security [95] against general attacks. This entropic uncertainty relation framework has been further extended to other finite-key cases of QKD, even with imperfect light sources [96,97]. This demonstrates its robust capability to underpin finite-key security analysis for various protocols.

In this paper, we extend the security proof in Ref. [92] to the finite-key domain with composable security [95] to demonstrate its real-world applicability. We employ the quantum leftover hash lemma [98] and the entropic uncertainty relation [93,94] to derive a formula for the secure key length in the finite-key regime. When dealing with correlated random variables, we apply Kato's inequality [99] to estimate statistical fluctuations, ensuring security against coherent attacks and resulting in a higher key rate compared to Azuma's inequality [100]. We simulate the performance of the key rate under different conditions, such as varying values of misalignment error and different choices of basis, to demonstrate the flexibility of our protocol. The simulation results and comparison with existing analyses and another similar protocol confirm the advantages of our approach. Additionally, our protocol is employed to show the exceptional capability of Kato's inequality in providing significantly tighter bounds when addressing events with an extremely low probability of occurrence. The comparison of key rates with previous COW variants and a summary of differences in many aspects are presented as well, serving to clearly highlight the unique advantages of our protocol.

This paper is organized as follows: Sec. II introduces the assumptions on devices and our COW-QKD protocol scheme. Section III presents details of the key rate calculation. Numerical simulations of key rate performance under different conditions and some comparisons are shown in Sec. IV, and we conclude in Sec. V.

II. ASSUMPTIONS AND PROTOCOL DESCRIPTIONS

A. Assumptions on devices

For the completeness of this paper, the assumptions on the devices of sender Alice and receiver Bob are introduced here before we describe our variant of the COW-QKD. In this protocol, Alice encodes a random bit with a quantum state consisting of two pulses sent in adjacent time windows and extracts a string of secret bits from these states together with Bob.

1. Assumptions on Alice's devices

The assumptions on Alice's devices are presented below:

(1) Alice employs her sending equipment, which includes a mode-locked continuous-wave laser and an intensity modulator, to create weak coherent pulses. Alternatively, she can completely block the output to generate a vacuum state;

(2) In our variant of COW-QKD, Alice randomly selects her initial bit string and encodes each bit into a two-pulse state. Additionally, she randomly determines which two adjacent time windows will be used to transmit decoy states. Consequently, the probability of the emitted state being a weak coherent pulse or a vacuum state in each time window is independent of the states sent previously.

2. Assumptions on Bob's devices

The assumptions on Bob's devices are summarized as follows:

(1) Bob's detection devices receive optical pulses transmitted through a quantum channel with a transmittance of η. These incoming states are then divided into a data line or a monitoring line using a beam splitter with a transmittance of t_B. Alternatively, an optical switch can be used in place of the beam splitter, allowing Bob to actively distribute the quantum states.

(2) On the data line, the quantum states are directly transmitted to a single-photon detector which measures the arrival time of the pulses. On the monitoring line, Bob utilizes an asymmetric Mach-Zehnder interferometer, which includes a one-bit delay and two single-photon detectors, to record which detector clicks within certain time windows. We note that all

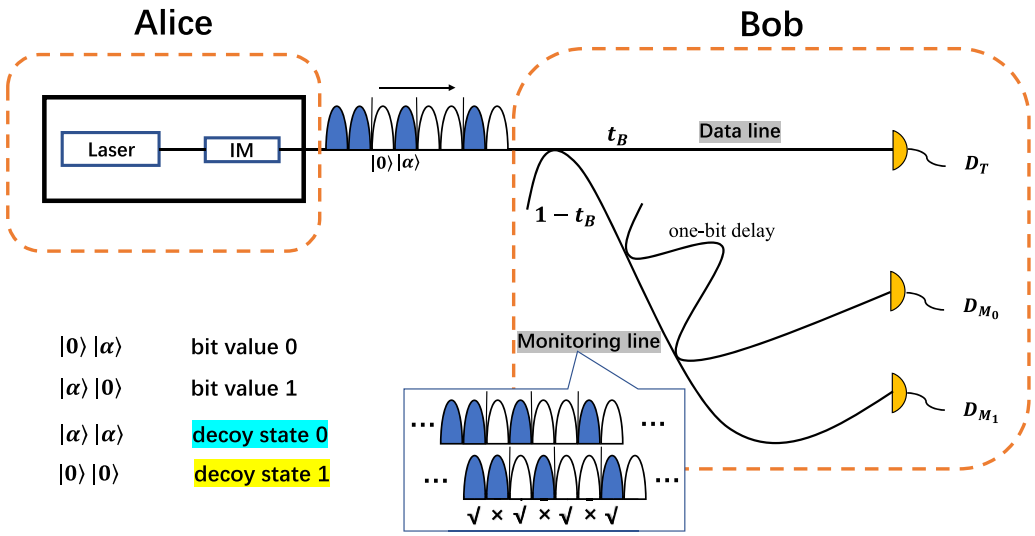

FIG. 1. Experimental implementation of COW-QKD protocol in this paper. With an intensity modulator (IM), Alice can prepare quantum states $|0\rangle$ and $|\alpha\rangle$ in each time window experimentally to randomly sends a sequence of pulses that consists of states $|0\rangle_{2k-1}|\alpha\rangle_{2k}$, $|\alpha\rangle_{2k-1}|0\rangle_{2k}$, $|\alpha\rangle_{2k-1}|\alpha\rangle_{2k}$, and $|0\rangle_{2k-1}|0\rangle_{2k}$ to Bob. After passively distributing these states into the data line or the monitoring line with a beam splitter of transmittance t_B, Bob records the detector's click in each round. D_T, D_{M_0}, and D_{M_1} are single-photon detectors. Compared to the original version of COW QKD, our protocol adds state $|0\rangle_{2k-1}|0\rangle_{2k}$ as another decoy state, which maintains the requirements for experimental equipment. We note that on the monitoring line, Bob is only required to record the clicks that occur within specific time windows. These clicks are a result of interference involving two pulses from the same round, as illustrated in the provided figure.

the single-photon detectors are threshold detectors, designed to simply determine the presence or absence of a photon.

(3) We assume the detection efficiency η_d and dark-count rate p_d of each detector to be the same and reasonable values of them are employed in Sec. IV to numerically present the performance of our protocol.

B. Detailed steps

In COW-QKD protocol, sender Alice uses two-pulse states $|0_k\rangle = |0\rangle_{2k-1}|\alpha\rangle_{2k}$ and $|1_k\rangle = |\alpha\rangle_{2k-1}|0\rangle_{2k}$ at two time windows $2k-1$ and $2k$ $(k = 1, 2, \ldots, N)$ to encode logic bits 0 and 1 in the kth round, respectively. Here we use $|0\rangle$ to denote the vacuum state and $|\alpha\rangle$ to denote the coherent state whose mean photon number is $\mu = |\alpha|^2$. As shown in Fig. 1, the COW-QKD scheme used in this paper takes both the two-pulse coherent state $|\alpha\rangle_{2k-1}|\alpha\rangle_{2k}$ and two-pulse vacuum state $|0\rangle_{2k-1}|0\rangle_{2k}$ as decoy states to estimate the phase error rate instead of using visibility to reflect the broken coherence.

The detailed steps of this scheme are:

(1) Alice randomly sends a sequence of pulses that consists of states $|0\rangle_{2k-1}|\alpha\rangle_{2k}$, $|\alpha\rangle_{2k-1}|0\rangle_{2k}$, $|\alpha\rangle_{2k-1}|\alpha\rangle_{2k}$, and $|0\rangle_{2k-1}|0\rangle_{2k}$ with probability p_z, p_z, p_{d_1}, and p_{d_2}, respectively, to Bob where $p_z = \frac{1}{2}(1 - p_{d_1} - p_{d_2})$. She records her choice of sending in each round. This step is repeated for N rounds so we have $k = 1, 2, \ldots, N$.

(2) Bob uses a beam splitter of transmittance t_B to passively distribute incoming states into the data line or the monitoring line. On the data line, he measures the click time of each signal to determine which logic bit Alice encodes in this round and gets the raw key. On the monitoring line, he records which detector clicks in each round. As illustrated in Fig. 1, the clicks that are recorded are specifically those resulting from interference involving two pulses from the same round. Any other clicks should be disregarded. Here we note that if multiple detectors click in one round, Bob records one of these detector clicks randomly.

(3) Bob announces in which round he records a click on the data line. Alice only keeps her logic bits in those rounds and discards the rest to get the raw key.

(4) Bob announces his click records of the monitoring line. Alice calculates the following click counts: $n_{0\alpha}^{M_i}$, $n_{\alpha 0}^{M_i}$, $n_{\alpha\alpha}^{M_i}$, and $n_{00}^{M_i}$ $(i = 0$ or $1)$. $n_u^{M_i}(u = 0\alpha, \alpha 0, \alpha\alpha, 00)$ are the click counts of states $|0\rangle_{2k-1}|\alpha\rangle_{2k}$, $|\alpha\rangle_{2k-1}|0\rangle_{2k}$, $|\alpha\rangle_{2k-1}|\alpha\rangle_{2k}$, and $|0\rangle_{2k-1}|0\rangle_{2k}$, respectively, where the superscript M_i refers to the clicking detectors on the monitoring line. By applying Kato's inequality, she can estimate the upper bound on phase error rate $\overline{E_p}$. The bit error rate E_z can be calculated by revealing some bits from the raw key. If either $\overline{E_p}$ or E_z exceeds the preset values, the protocol aborts.

(5) After an error correction step is performed, at most leak_{EC} bits of information are revealed. Then Alice and Bob verify whether the error correction step succeeds and perform privacy amplification to get the final key string.

III. THE KEY-LENGTH FORMULA

A. Security definition

Before we present the security proof in the finite-key regime, we introduce the universally composable framework of QKD [95]. Typically, performing a QKD protocol either generates a pair of bit strings $\hat{S}_A$ and $\hat{S}_B$ for Alice and Bob, respectively, or aborts so $\hat{S}_A = \hat{S}_B = \varnothing$. A secure QKD protocol must satisfy the two criteria below.

The first is the correctness criterion which is met if two bit strings are the same, i.e., $\hat{S}_A = \hat{S}_B$. In practical experiments, however, as it is not always possible to perfectly satisfy the

correctness criterion, a small degree of error is typically allowed. Instead, we require that the probability of the two bit strings not being identical does not exceed a predetermined value, denoted as ε_{cor}, In this case, we say that the protocol is ε_{cor}-correct.

The second is the secrecy criterion which is met if there is no correlation between the system of the eavesdropper Eve and the bit strings of Alice. We assume the orthonormal basis which consists of Alice's quantum system and corresponds to each possible bit string of Alice to be $\{|s\rangle\}_s$. The secrecy criterion requires the joint quantum state of Alice and Eve to be $\rho_{\text{AE}} = \rho_{\text{AE}}^{\text{ideal}} \equiv U_{\text{A}} \otimes \rho_{\text{E}}$, where $U_{\text{A}} = \sum_s \frac{1}{|\mathcal{S}|} |s\rangle\langle s|$ is a uniform mixture which indicates that the probability of generating each possible bit string of Alice is uniformly distributed, and ρ_{E} is Eve's system, which does not correlate with Alice's system. However, it is not always possible to perfectly satisfy this criterion in practice. This means that a small deviation between the actual joint quantum state of Alice and Eve and the ideal state is permissible. The trace distance measures the difference and we say the protocol is ε_{sec}-secret if the trace distance between the actual joint quantum state ρ_{AE} and the ideal state $\rho_{\text{AE}}^{\text{ideal}}$ does not exceed Δ, i.e.,

$$\tfrac{1}{2} \left\| \rho_{\text{AE}} - \rho_{\text{AE}}^{\text{ideal}} \right\|_1 \leqslant \Delta, \tag{1}$$

and $(1 - p_{\text{abort}})\Delta \leqslant \varepsilon_{\text{sec}}$, where p_{abort} is the probability for aborting this protocol and $\| \cdot \|_1$ denotes the trace norm.

Finally, a protocol is ε_{s}-secure if it is both ε_{cor}-correct and ε_{sec}-secret with $\varepsilon_{\text{cor}} + \varepsilon_{\text{sec}} \leqslant \varepsilon_{\text{s}}$.

B. Security proof

Here, a virtual entanglement-based protocol is introduced to obtain the secure key rate in the finite-key regime, which is based on the virtual entanglement-based protocol in Ref. [92]. To simplify the presentation, we ignore the label k and express the state sent in the kth round as $|0_z\rangle$ and $|1_z\rangle$. Let $|0_x\rangle = (|0_z\rangle + |1_z\rangle)/\sqrt{N^+}$ and $|1_x\rangle = (|0_z\rangle - |1_z\rangle)/\sqrt{N^-}$ be the logic bits 0 and 1 in the X basis, where $N^{\pm} = 2(1 \pm e^{-\mu})$ are the normalization factors. In the virtual entanglement-based protocol, Alice prepares K pairs of the entangled state

$$\begin{aligned} |\phi\rangle &= \frac{1}{\sqrt{2}} (|+z\rangle_A |0_z\rangle_{A'} + |-z\rangle_A |1_z\rangle_{A'}) \\ &= \frac{\sqrt{N^+}}{2} |+x\rangle_A |0_x\rangle_{A'} + \frac{\sqrt{N^-}}{2} |-x\rangle_A |1_x\rangle_{A'}, \end{aligned} \tag{2}$$

where $|\pm x\rangle$ and $|\pm z\rangle$ are the eigenstates of the Pauli matrices X and Z, respectively, and subscripts A and A' denote different quantum systems possessed by Alice. Then Alice measures the qubits in the system A randomly in the Pauli X or Z basis to obtain the raw key $\hat{X}_A$ from the X basis and $\hat{Z}_A$ from the Z basis. Bob's experimental implementation is the same as the practical COW-QKD. He obtains his raw key $\hat{Z}_B$ of the Z basis on the data line by measuring the click time just like the original protocol. He also records a bit value 0(1) in the X basis when detector $D_{M_0}(D_{M_1})$ on the monitoring line clicks to obtain the raw key $\hat{X}_B$. $\hat{Z}_A$ and $\hat{Z}_B$ are used to extract the final key so the error-correction step and error-verification step are performed to them. If these steps succeed, Alice and Bob obtain the same bit string which we denote as $\hat{Z}$. All the information that the eavesdropper Eve possesses up to the error-correction step and error-verification step is denoted as E'. The smooth min-entropy $H_{\min}^{\varepsilon}(\hat{Z}|E')$ characterizes the mean probability that Eve can guess $\hat{Z}$ successfully with all information she owns using the optimal strategy [101]. The smooth max-entropy $H_{\max}^{\varepsilon}(\hat{Z}_A|\hat{Z}_B)$ quantifies the number of bits required to reconstruct $\hat{Z}_A$ from $\hat{Z}_B$ [102].

According to the quantum leftover hashing lemma [98], a Δ-secret key of length l can be extracted from $\hat{Z}$ when a random universal$_2$ hash function to $\hat{Z}$, where parameter Δ satisfies

$$\Delta = 2\varepsilon + \tfrac{1}{2}\sqrt{2^{l - H_{\min}^{\varepsilon}(\hat{Z}|E')}}. \tag{3}$$

Letting $\varepsilon_0 = \frac{1}{2}\sqrt{2^{l - H_{\min}^{\varepsilon}(\hat{Z}|E')}}$, the length l of the secret key is [103]

$$l = H_{\min}^{\varepsilon}(\hat{Z}|E') - 2\log_2\left(\frac{1}{2\varepsilon_0}\right). \tag{4}$$

A chain-rule inequality for these smooth entropies is used to describe the error-correction step and error-verification step. That is,

$$\begin{aligned} H_{\min}^{\varepsilon}(\hat{Z}|E') &\geqslant H_{\min}^{\varepsilon}(\hat{Z}_A|E) - H_{\max}^{\varepsilon}(\hat{Z}_A|\hat{Z}_B) \\ &= H_{\min}^{\varepsilon}(\hat{Z}_A|E) - \text{leak}_{\text{EC}} - \log_2\left(\frac{2}{\varepsilon_{\text{cor}}}\right), \end{aligned} \tag{5}$$

where leak_{EC} and $\log_2(\frac{2}{\varepsilon_{\text{cor}}})$ are the numbers of bits that are revealed during the error-correction and error-verification procedure, respectively, to generate a ε_{cor}-correct key, and $\hat{E}$ denotes all the information that Eve possesses before the error-correction step and error-verification step. The lower bound on the smooth min-entropy can be obtained by the entropic uncertainty relation [93]. We denote the binary Shannon entropy as $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$. Let $\hat{X}'_A$ and $\hat{X}'_B$ be the bit strings that Alice and Bob would have obtained if Alice had measured in the X basis, which is actually measured in the Z basis in the virtual protocol. So, we have $H_{\max}^{\varepsilon}(\hat{X}'_A|\hat{X}'_B) \leqslant n_z h(E_x)$, where n_z is the size of $\hat{Z}_A$ and E_x is the bit error rate in the X basis. By exploiting the the entropic uncertainty relation, we have

$$H_{\min}^{\varepsilon}(\hat{Z}_A|E) \geqslant n_z - H_{\max}^{\varepsilon}(\hat{X}'_A|\hat{X}'_B) \geqslant n_z[1 - h(E_x)], \tag{6}$$

and the final key length is

$$l \geqslant n_z[1 - h(E_x)] - \text{leak}_{\text{EC}} - \log_2\left(\frac{2}{\varepsilon_{\text{cor}}}\right) - 2\log_2\left(\frac{1}{2\varepsilon_0}\right). \tag{7}$$

C. Phase error rate

The phase error rate formula is derived by the same method in Ref. [92]. For the completeness of this paper, a brief deduction is presented here. We consider a prepare-and-measure protocol which is equivalent to the entanglement-based protocol in Sec. III B. In this protocol, when Alice prepares her optical signals, she randomly chooses the Z or X basis. If she chooses the Z basis, she prepares states $|0_z\rangle$ and $|1_z\rangle$ with the same probability. If she chooses the X basis, she prepares states $|0_x\rangle$ and $|1_x\rangle$ with probability $\frac{N^+}{4}$ and $\frac{N^-}{4}$, respectively.

She sends her states to Bob, and Bob uses the same implementation as the practical protocol to measure these states in the Z basis (data line) or in the X basis (monitoring line) distributed by a beam splitter.

It is obvious that the density matrices of the X and Z basis are the same. That is,

$$\begin{aligned}\rho &= (|0_z\rangle\langle 0_z| + |1_z\rangle\langle 1_z|)/2 \\ &= (N^+ |0_x\rangle\langle 0_x| + N^- |1_x\rangle\langle 1_x|)/4. \end{aligned} \tag{8}$$

Therefore, the bit error rate of the X basis can be obtained as follows:

$$\begin{aligned} E_x &= \frac{N^+ Q_{0_x}^{M_1} + N^- Q_{1_x}^{M_0}}{N^+\left(Q_{0_x}^{M_0} + Q_{0_x}^{M_1}\right) + N^-\left(Q_{1_x}^{M_0} + Q_{1_x}^{M_1}\right)} \\ &= \frac{N^+\left(Q_{0_x}^{M_1} - Q_{0_x}^{M_0}\right) + 2\left(Q_{0_z}^{M_0} + Q_{1_z}^{M_0}\right)}{2\left(Q_{0_z}^{M_0} + Q_{0_z}^{M_1} + Q_{1_z}^{M_0} + Q_{1_z}^{M_1}\right)}, \end{aligned} \tag{9}$$

which is equal to the bit error rate in the virtual entanglement-based protocol, where $Q_{s_{x(z)}}^{M_i}$ refers to the gain of the event which Alice prepares state $|s_{x(z)}\rangle$ $(s = 0, 1)$ and Bob get a click with detector $D_{M_i}(i = 0, 1)$ on the monitoring line. The relation $\frac{N^-}{4}Q_{1x}^{M_i} + \frac{N^+}{4}Q_{0x}^{M_i} = \frac{1}{2}(Q_{1z}^{M_i} + Q_{0z}^{M_i})$ is used in the second equation, which can be obtained from Eq. (8). Because the density matrices of the Z basis and X basis are the same, the eavesdropper Eve cannot distinguish whether the prepare-and-measure protocol or the practical COW-QKD protocol is actually performed by Alice and Bob. The phase error rate in the practical COW-QKD protocol is equal to the bit error rate of the X basis in the prepare-and-measure protocol.

In practical COW-QKD protocol, states $|0_x\rangle$ and $|1_x\rangle$ are not sent, so we cannot calculate $Q_{0_x}^{M_1}$ and $Q_{0_x}^{M_0}$ directly. The decoy states $|\alpha\rangle_{2k-1}|\alpha\rangle_{2k}$ and $|0\rangle_{2k-1}|0\rangle_{2k}$ are used to estimate $\overline{Q_{0_x}^{M_1}}$ and $\underline{Q_{0_x}^{M_0}}$, where $\overline{O}$ and $\underline{O}$ are the upper and lower bounds on value O, respectively. The expressions are

$$\begin{aligned}\overline{Q_{0x}^{M_1}} &= \frac{1}{N^+}\left(e^{\frac{\mu}{2}}\sqrt{Q_{\alpha\alpha}^{M_1}} + e^{-\frac{\mu}{2}}\sqrt{Q_{00}^{M_1}}\right)^2 \\ &\quad + \frac{N^-}{N^+}\left(\frac{e^{\mu}N^-}{4} + e^{\mu}\sqrt{Q_{\alpha\alpha}^{M_1}} + \sqrt{Q_{00}^{M_1}}\right) \end{aligned} \tag{10}$$

and

$$\begin{aligned}\underline{Q_{0x}^{M_0}} &= \frac{1}{N^+}\left(e^{\mu}Q_{\alpha\alpha}^{M_0} + e^{-\mu}Q_{00}^{M_0} - 2\sqrt{Q_{00}^{M_0}Q_{\alpha\alpha}^{M_0}}\right) \\ &\quad - \frac{N^-}{N^+}\left(e^{\mu}\sqrt{Q_{\alpha\alpha}^{M_0}} + \sqrt{Q_{00}^{M_0}}\right), \end{aligned} \tag{11}$$

where $Q_w^{M_i}(w = \alpha\alpha, 00)$ denotes the gain of the event which Alice sends state $|\alpha\rangle|\alpha\rangle$ or $|0\rangle|0\rangle$, respectively, where we also omit the subscripts of states $|\alpha\rangle_{2k-1}|\alpha\rangle_{2k}$ and $|0\rangle_{2k-1}|0\rangle_{2k}$ and Bob gets a click with detector $D_{M_i}(i = 0, 1)$. The details of how to obtain Eqs. (10) and (11) can be found in Ref. [92].

D. Statistical fluctuations

Given the impact of finite-key effects, it is crucial to ensure the security of our protocol within the finite-key regime if we want to facilitate the practical application of this technology. This involves taking into account the statistical fluctuations between observed and expected values and estimating the lower bound of the final key length using a concentration inequality [99,100].

Typically, Azuma's inequality [100] is applied to convert observed values to the upper or lower bound on corresponding expected values and vice versa. As shown in Ref. [74], it can be concluded that a loose bound will be obtained when using Azuma's inequality to estimate the statistical fluctuations of events that occur with a very small probability. Specifically, the estimation of the gains of decoy states $|0\rangle_{2k-1}|0\rangle_{2k}$ is loose when using Azuma's inequality. Instead, we use a concentration inequality named Kato's inequality [99] to make our estimation tighter so a higher key rate can be obtained. Here we introduce the general form of Kato's inequality which has been employed in some finite key analyses [74,104]. Let $n_1, n_2, \ldots, n_k$ be a sequence of random variables which satisfies $0 \leqslant n_i \leqslant 1, (i = 1, 2, \ldots, k)$. Let $\Gamma_i = \sum_{u=1}^{i} n_u$ and f_i be the σ-algebra generated by $\{n_1, n_2, \ldots, n_k\}$, which is called the natural filtration of this sequence of random variables. For any $k, a \in \mathbb{R}$ and any b s.t. $b \geqslant |a|$, according to Kato's inequality we have that

$$\begin{aligned}&\Pr\left[\sum_{u=1}^{k} E(n_u|f_{u-1}) - \Gamma_k \geqslant \left[b + a\left(\frac{2\Gamma_k}{k} - 1\right)\right]\sqrt{k}\right] \\ &\leqslant \exp\left[\frac{-2(b^2 - a^2)}{\left(1 + \frac{4a}{3\sqrt{k}}\right)^2}\right], \end{aligned} \tag{12}$$

where $E(\cdot)$ refers to the expected value. Another form of Kato's inequality can be derived by replacing $n_i \to 1 - n_i$ and $a \to -a$, which is

$$\begin{aligned}&\Pr\left[\Gamma_k - \sum_{u=1}^{k} E(n_u|f_{u-1}) \geqslant \left[b + a\left(\frac{2\Gamma_k}{k} - 1\right)\right]\sqrt{k}\right] \\ &\leqslant \exp\left[\frac{-2(b^2 - a^2)}{\left(1 - \frac{4a}{3\sqrt{k}}\right)^2}\right]. \end{aligned} \tag{13}$$

The details of how to use Kato's inequality to accomplish parameter estimation tasks are shown in the Appendix. In the description below, we let O^* be the expected value of O.

After performing the COW-QKD protocol, observed values $n_{\alpha\alpha}^{M_i}$ and $n_{00}^{M_i}$ $(i = 0, 1)$ are obtained, which stand for the total click counts of detector M_i when state $|0\rangle|0\rangle$ or $|\alpha\rangle|\alpha\rangle$ is sent, respectively. $Q_{s_z}^{M_i}(s = 0, 1)$ and the click count of detector D_T, which we express as n_z, can be directly calculated as well. First, we use these four observed values to estimate their upper bounds on corresponding expected values by Kato's inequality as follows:

$$n_w^{M_i*} \leqslant \overline{n_w^{M_i*}} = n_w^{M_i} + \Delta_w^{M_i}, \tag{14}$$

where $w = 00, \alpha\alpha$ and $i = 0, 1$. The statistical fluctuation parameters here are obtained in the way presented in the Appendix. Similarly, two lower bounds $\underline{n_w^{M_0*}}$ $(w = 00, \alpha\alpha)$ need to be calculated as follows:

$$n_w^{M_0*} \geqslant \underline{n_w^{M_0*}} = n_w^{M_0} - \Delta_w^{M_0\prime}. \tag{15}$$

We set the failure probability for estimating each of the six bounds above to be ε_1. The total number of rounds performed is set to be N. So, we can denote the number of state $|\alpha\rangle|\alpha\rangle$

sent by Alice as $N_{\alpha\alpha} = N \times p_{d_1}$ and the number of state $|0\rangle\,|0\rangle$ as $N_{00} = N \times p_{d_2}$. We calculate the upper and lower bounds on gains of each event as follows:

$$\overline{Q_w^{M_i*}} = \overline{n_w^{M_i*}}/n_w, \tag{16}$$

$$\underline{Q_w^{M_0*}} = \underline{n_w^{M_0*}}/n_w. \tag{17}$$

Then, by applying Eqs. (10) and (11) in the expected case, we obtain the expected values as follows:

$$\overline{Q_{0x}^{M_1*}} = \frac{1}{N^+}\left(e^{\frac{\mu}{2}}\sqrt{\overline{Q_{\alpha\alpha}^{M_1*}}} + e^{-\frac{\mu}{2}}\sqrt{\overline{Q_{00}^{M_1*}}}\right)^2 + \frac{N^-}{N^+}\left(\frac{e^{\mu}N^-}{4} + e^{\mu}\sqrt{\overline{Q_{\alpha\alpha}^{M_1*}}} + \sqrt{\overline{Q_{00}^{M_1*}}}\right), \tag{18}$$

$$\underline{Q_{0x}^{M_0*}} = \frac{1}{N^+}\left(e^{\mu}\underline{Q_{\alpha\alpha}^{M_0*}} + e^{-\mu}\underline{Q_{00}^{M_0*}} - 2\sqrt{\overline{Q_{00}^{M_0*}} \times \overline{Q_{\alpha\alpha}^{M_0*}}}\right) - \frac{N^-}{N^+}\left(e^{\mu}\sqrt{\overline{Q_{\alpha\alpha}^{M_0*}}} + \sqrt{\overline{Q_{00}^{M_0*}}}\right). \tag{19}$$

Finally, by applying Eq. (9) and considering the bit error rate in the X basis to be equal to the phase error rate in the Z basis in the expected value case [32], the expected upper bound on the phase error rate is

$$\overline{E_p^*} = \overline{E_x^*} = \frac{N^+\left(\overline{Q_{0x}^{M_1*}} - \underline{Q_{0x}^{M_0*}}\right) + 2\left(Q_{0_z}^{M_0} + Q_{1_z}^{M_0}\right)}{2\left(Q_{0_z}^{M_0} + Q_{0_z}^{M_1} + Q_{1_z}^{M_0} + Q_{1_z}^{M_1}\right)}. \tag{20}$$

We use Kato's inequality again but in a different form which is explained in the Appendix to calculate the upper bound on phase error rate in the observed value case. The expected number of clicks corresponding to phase errors is $\overline{n_p^*} = N \times \overline{E_p^*}$. So, the upper bound on the observed value is

$$n_p \leqslant \overline{n_p} = \overline{n_p^*} + \Delta_p, \tag{21}$$

where $\Delta_p = \sqrt{\frac{1}{2}n_z \ln \varepsilon_2^{-1}}$ and ε_2 is the failure probability for estimating $\overline{n_p}$. So, the upper bound on the phase error rate is

$$\overline{E_p} = \overline{n_p}/n_z. \tag{22}$$

E. Composable security

Considering the failure probability for estimating the statistical fluctuations described in Sec. III D, the practical protocol has a total secrecy of $\varepsilon_{\text{sec}} = 2\varepsilon + \varepsilon_0 + 6\varepsilon_1 + \varepsilon_2$, where we take $\varepsilon = \varepsilon_0 = \varepsilon_1 = \varepsilon_2 = \varepsilon_{\text{sec}}/10$. So, the final key length is denoted as

$$l \geqslant n_z[1 - h(\overline{E_p})] - \text{leak}_{\text{EC}} - \log_2\left(\frac{2}{\varepsilon_{\text{cor}}}\right) - 2\log_2\left(\frac{5}{\varepsilon_{\text{sec}}}\right), \tag{23}$$

and the COW-QKD protocol in this paper is ε_s-secret, where $\varepsilon_s = \varepsilon_{\text{cor}} + \varepsilon_{\text{sec}}$.

IV. NUMERICAL SIMULATION AND DISCUSSION

To numerically simulate the key rate performance of our protocol in the finite-key regime, we assume that the dark-count rate is $p_d = 2 \times 10^{-8}$ and the efficiency of the photon detectors is $\eta_d = 70\%$. The number of bits that are revealed in the error-correction step leak_{EC} is $f n_z h(E_z)$, where the correction efficiency f is set to 1.1. The transmittance of the optical fiber with length L is expressed by $\eta = 10^{-0.016L}$. For finite-key analysis, the security bounds of correctness and secrecy are fixed to $\varepsilon_{\text{cor}} = 10^{-15}$ and $\varepsilon_{\text{sec}} = 10^{-10}$. Other experimental parameters such as the mean photon number $\mu = |\alpha|^2$ and the transmittance of the beam-splitter used to distribute incoming states are decided by an optimization algorithm.

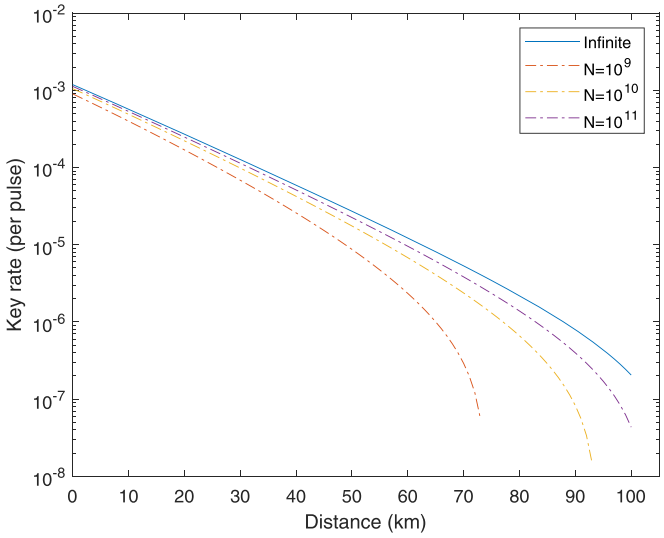

FIG. 2. Secret key rate with different values of the total number of rounds, $N = 10^9$, 10^{10}, and 10^{11}, using passive basis choice. The misalignment error e_d is set to 1%. When $N = 10^{11}$, which is reasonable in experimental implementation, the key rate is quite close to the performance in the asymptotic case. The key rate performance also shows that the security of our protocol ensures a secure distance exceeding 100km for COW-QKD in practical implementation.

We present the performance of the key rate of COW-QKD with different total numbers of rounds compared with the key rate of infinite limit [92], where the misalignment error rate is fixed to $e_d = 1\%$. As shown in Fig. 2, we can conclude that if the state-sending step of our protocol is repeated for $N = 10^{11}$ rounds, the key rate is close to that of infinite limit, showing the practicality of our protocol in the finite-key regime. When choosing $N = 10^{11}$, a 3-Mbit key can be obtained through 34 km fiber by Alice and Bob if they run our protocol with a laser operating at 1 GHZ for only 30 seconds, which presents the superiority of this protocol in short-distance communication. The results also demonstrate that our security analysis guarantees an unconditionally secure communication range exceeding 100 km for COW-QKD, given its straightforward experimental setup.

We demonstrate the flexibility of our protocol by presenting its key rate performance under different conditions. First, the beam splitter used to passively distribute optical pulses into the data or monitoring lines can be replaced by an optical switch that actively divides incoming states into different lines. This is referred to as the passive and active basis choice, respectively. A comparison of the key rate between passive and active basis choice is presented in Fig. 3, along with the estimated upper bound on the phase error rate $\overline{E_p}$ when using an active basis, demonstrating the applicability of our analysis

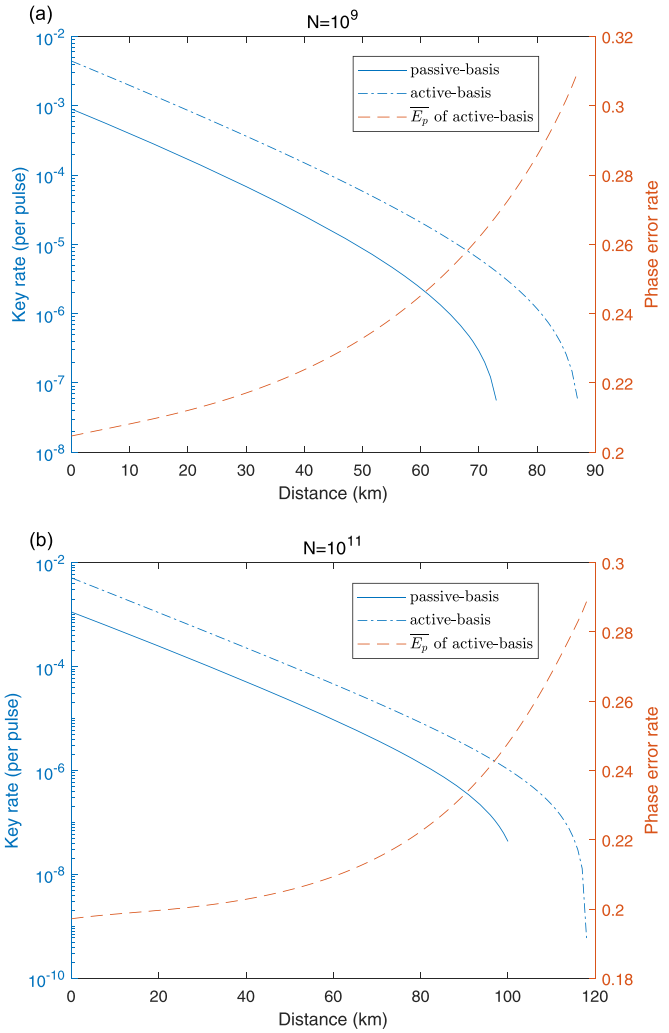

FIG. 3. Comparison of key rates using passive basis and active basis when $N = 10^9$ and $N = 10^{11}$. The upper bound on the phase error rate $\overline{E_p}$ using active basis choice is presented by the dashed red line. The misalignment error e_d is set to 1%. (a) The total number of rounds is $N = 10^9$. (b) The total number of rounds is $N = 10^{11}$.

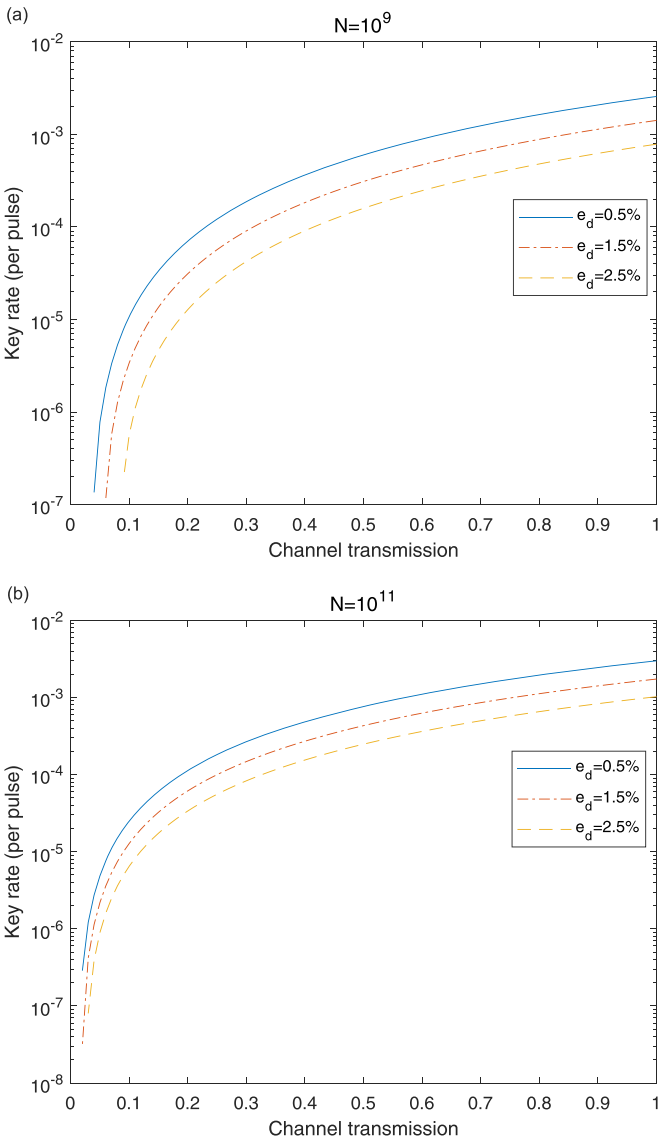

FIG. 4. Secret key rate simulation in the finite-key case with different values of misalignment error when using passive basis. When a large misalignment error is employed, the key rates do not drop significantly, which is an important advantage in constructing quantum information systems. (a) The total number of rounds is $N = 10^9$. (b) The total number of rounds is $N = 10^{11}$.

with an active basis. Our protocol also exhibits robustness when faced with varying values of the misalignment error rate, as shown in Fig. 4. The results show that even with a large misalignment error, the key rates are not significantly affected. This indicates the practicality of our protocol in constructing quantum communication systems under different experimental conditions.

We compare our protocol with DPS-QKD [71], whose equipment requirements are similar to that of COW-QKD. The finite-key security analysis of it in Ref. [74] shows a tighter bound on phase error rate can be obtained by Kato's inequality. To simulate under the same experimental conditions, we follow the choice in Ref. [74] and fix the security bounds of both correctness and secrecy to 2^{-28} to get a total secrecy of $2^{-27} \approx 10^{-8.1}$. The misalignment error e_d is set to 0.01 and the dark-count rate is 0, so we can ensure the bit error rate is 1% as chosen in Ref. [74]. The correction efficiency f is 1.16, and we have simulated the key rate under varying values of overall channel transmittance, taking into account both optical fiber loss and detection efficiency. We note that in our COW-QKD protocol, Alice sends two pulses in each round, whereas the DPS-QKD protocol requires three pulses. For comparison, we need to ensure that the total number of pulses N_{pulse} is the same for both protocols. We compare the key rates of the two protocols when N_{pulse} is set to 3×10^{11} and 3×10^{12}, so one of the results for DPS-QKD is consistent with that reported in Ref. [74]. The simulation is shown in Fig. 5. The results reveal that the key rates of our protocol are significantly higher than those reported in Ref. [74].

Following the approach proposed in Ref. [74], our protocol demonstrates an enhancement of Kato's inequality over Azuma's inequality as well. In our protocol, the gain of the decoy states $|0\rangle_{2k-1}|0\rangle_{2k}$, represented as $Q_{00}^{M_i}$, is

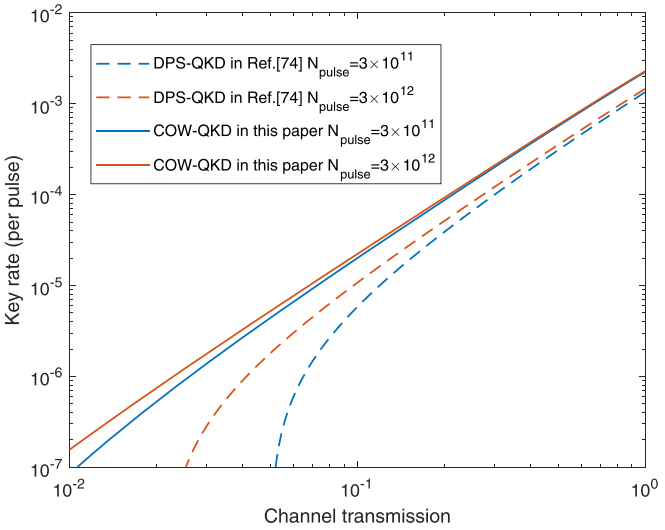

FIG. 5. Comparison of key rates of our protocol and the DPS-QKD protocol in Ref. [74]. Two protocols have similar experimental settings and both belong to the distributed-phase-reference QKD protocols. The bit error rate is 1% and the correction efficiency f is 1.16. For convenience, the security bounds of both correctness and secrecy are fixed to 2^{-28} as in Ref. [74]. We compare the key rates when the numbers of pulses are $N_{\text{pulse}} = 3 \times 10^{11}$ and $N_{\text{pulse}} = 3 \times 10^{12}$ and conclude that our protocol has advantages on the secure transmission distance and key rate performance.

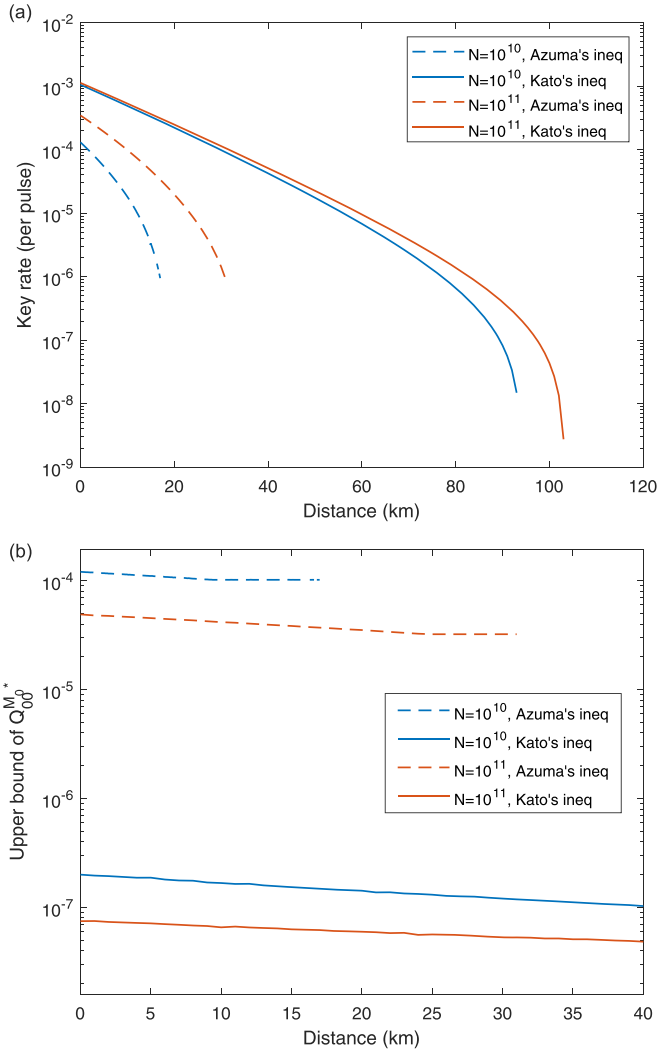

FIG. 6. (a) Finite secret key rate simulation of our protocol using Azuma's or Kato's inequalities to estimate the upper bound on $Q_{00}^{M_0*}$ with $N = 10^{10}$ and $N = 10^{11}$. The misalignment error e_d is set to 1%. It can be concluded that significantly higher key rates are obtained by utilizing Kato's inequality. (b) The detailed estimated values of $\overline{Q_{00}^{M_0*}}$ when applying Azuma's or Kato's inequalities. Statistical fluctuations dominate the estimation of the upper bound, leading to significantly higher values. Consequently, higher phase error rates are calculated as per Eqs. (18)–(20) and result in lower key rates.

entirely attributed to the nonzero dark count rate, which is approximately on the scale of 10^{-8}. However, the fluctuations estimated by Azuma's inequality between observed and expected values exhibit a linear dependence on $\sqrt{N_{00}}$. These statistical fluctuations dominate the estimation of the upper limit on $Q_{00}^{M_i*}$, resulting in a decrease in $\underline{Q_{0x}^{M_0*}}$ and an increase in $\overline{Q_{0x}^{M_1*}}$ according to Eqs. (18) and (19). This gives rise to a higher phase error rate as per Eq. (20), consequently leading to a diminished key rate. To compare the results, we conduct a numerical simulation of our protocol's key rates, using Azuma's or Kato's inequalities to estimate the upper bound on $Q_{00}^{M_i*}$. The results are depicted in Fig. 6 together with a detailed comparison of the upper bounds on $Q_{00}^{M_0*}$ obtained by two inequalities.

Compared with other security analyses of previous variants of COW-QKD, our protocol has notable advantages because its key rate performance is better when considering the highest security standard, i.e., the security against both zero-error attack and coherent attacks. For the completeness of this paper, in Fig. 7 we compare the key rates in the asymptotic case of our COW protocol with the variants proposed in Refs. [86,89] that have the immunity against these two attacks. To fairly compare, the parameter choices in Refs. [86,89] are adopted, which fix the dark count rate p_d to 10^{-7} and set the detection efficiency η_d to 99%. In our numerical simulation of the variant presented in Ref. [86], we opt for a scenario where each three-signal block, comprising six optical pulses, shares the same phase. This modification to the experimental setup has inevitably altered the simplicity of the original protocol. Both of these previous variants are simulated with an active basis choice. It can be concluded that our protocol not only outperforms in terms of key rates and transmission distance but also preserves the original simplicity of the COW-QKD setting.

Moreover, we have summarized the differences with several previous works on COW-QKD in aspects such as experimental setting and key rate performance in Table I. As previously discussed, our protocol exhibits superior key rate performance compared to variants [86,89] that share an equivalent security level. A method for calculating the lower bound on the secure key rate of a COW variant was proposed in Ref. [91] recently, which shows significantly improved key rate performance. However, the absence of finite-key regime analysis and immunity against coherent attacks pose significant challenges to the practical

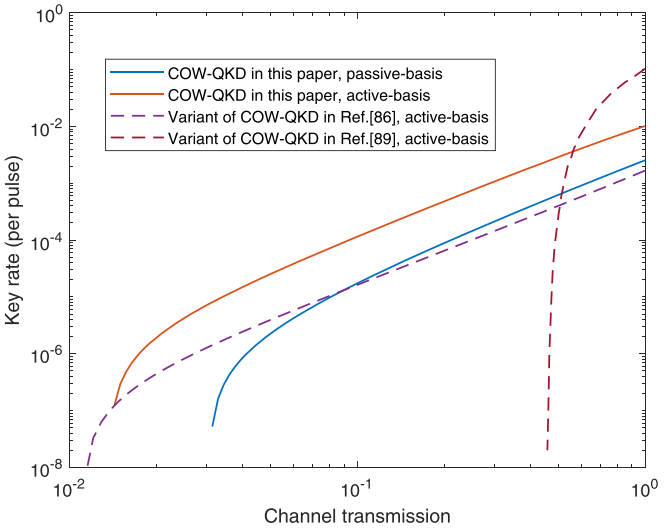

FIG. 7. Secret key rates of our protocol compared with previous variants in Refs. [86,89]. The dark count rate p_d is fixed to 10^{-7} and the efficiency of detectors is set to 99%. The experimental requirements for the variant in Ref. [86] are more complex compared to the original protocol. However, both the variant in Ref. [89] and our protocol maintain the simplicity of the setup. Under certain channel transmission values, our protocol with passive basis choice can still outperform the previous variants that use active basis choice in terms of key rate performance.

implementation of this theoretical protocol. Earlier works such as Refs. [80,85] presented security proofs that could achieve high key rates scaling as $O(\eta)$. However, these variants have been demonstrated to be insecure when confronting zero-error attacks [87,88]. Since our security proof provides the analytical formulas of the key rate, the extension of analyzing performance with finite key length can be completed as presented in Sec. III. With the help of Kato's inequality, our analysis gives a tight bound on the key rate and guarantees security against coherent attacks, establishing foundations for further practical applications.

V. CONCLUSION

In this paper, we present a finite-key analysis for the COW-QKD protocol proposed in Ref. [92]. We apply the quantum leftover hashing lemma and entropic uncertainty relation to derive an analytic formula for the key length. When dealing with correlated random variables, we use Kato's inequality to ensure security against coherent attacks and achieve a higher key rate. By considering the failure probabilities for estimating statistical fluctuations between observed and expected values, we complete the security proof within the universally composable framework. Our finite-key analysis shows that the key transmission distance can exceed 100 km in specific cases, providing a feasible approach for the secure implementation of quantum communication processes. In short-distance communication, the numerical simulation in Fig. 2 has shown that our protocol can generate a 3-Mbit secret key over 34 km fiber by running this protocol for only 30 seconds with a photon source operating at 1 GHZ repetition rate. We also present numerical simulations of key rates under different conditions, demonstrating the practicality and flexibility of our protocol. Compared to the finite-key analysis of DPS-QKD in Ref. [74], our protocol obtains a significantly higher key rate with almost the same experimental setup. Additionally, we show that our COW-QKD protocol can also be used to show the superiority of Kato's inequality when estimating events with a small probability of occurrence. Furthermore, we present the comparison of key rates with previous COW variants in the asymptotic scenario and summarize the differences in many aspects to clearly illustrate the distinct advantages of our protocol. In conclusion, our protocol lays a theoretical foundation for applying COW-QKD in real-world scenarios by offering both a high key rate and unconditional security against coherent attacks and completes the intact security proof for this protocol. Our protocol may be employed in future quantum communication with minuscule devices like chips and quantum information networks due to the simple experimental setup and excellent key rate performance.

TABLE I. The differences between our protocol and several variants of COW-QKD. Here, state $|0\rangle\,|\alpha\rangle$ is abbreviated expression of state $|0\rangle_{2k-1}\,|\alpha\rangle_{2k}$ and other states have similar meanings. States $|0\rangle\,|0\rangle\,|\alpha\rangle$, $|0\rangle\,|\alpha\rangle\,|0\rangle$, and $|0\rangle\,|\beta\rangle\,|\beta\rangle$ are three-pulse states used in Ref. [91]. EUR stands for entropic uncertainty relation and SDP stands for semidefinite programming techniques.

	Branciard *et al.* (2008) [85]	Moroder *et al.* (2012) [86]	Korzh *et al.* (2015) [80]	Wang *et al.* (2019) [89]	Lavie *et al.* (2022) [91]	This paper
Signal states	$\|0\rangle\,\|\alpha\rangle$, $\|\alpha\rangle\,\|0\rangle$	$\|0\rangle\,\|\alpha\rangle$, $\|\alpha\rangle\,\|0\rangle$[a]	$\|0\rangle\,\|\alpha\rangle$, $\|\alpha\rangle\,\|0\rangle$	$\|0\rangle\,\|\alpha\rangle$, $\|\alpha\rangle\,\|0\rangle$	$\|0\rangle\,\|0\rangle\,\|\alpha\rangle$, $\|0\rangle\,\|\alpha\rangle\,\|0\rangle$	$\|0\rangle\,\|\alpha\rangle$, $\|\alpha\rangle\,\|0\rangle$
Decoy states	$\|\alpha\rangle\,\|\alpha\rangle$	$\|\alpha\rangle\,\|\alpha\rangle$[a]	$\|\alpha\rangle\,\|\alpha\rangle$	$\|\alpha\rangle\,\|\alpha\rangle$	$\|0\rangle\,\|\beta\rangle\,\|\beta\rangle$	$\|\alpha\rangle\,\|\alpha\rangle$, $\|0\rangle\,\|0\rangle$
Attack model	Collective[b]	Coherent	Collective	Coherent	Collective	Coherent
Key rate	$O(\eta)$	$O(\eta^2)$	$O(\eta)$	$O(\eta^2)$	$O(\eta^2)$	$O(\eta^2)$
Security framework	EUR	SDP	EUR	SDP	SDP	EUR
Against zero-error attack	NO	YES	NO	YES	YES	YES
Finite feasibility	NO	NO	YES	NO	NO	YES

[a]This protocol needs three states to be sent in a group with the same phase, making the setup more complicated.
[b]This protocol only considers restricted types of collective attacks.

ACKNOWLEDGMENTS

This work is supported by the National Natural Science Foundation of China (No. 12274223), the Natural Science Foundation of Jiangsu Province (No. BK20211145), the Fundamental Research Funds for the Central Universities (No. 020414380182), and the Program for Innovative Talents and Entrepreneurs in Jiangsu (No. JSSCRC2021484).

APPENDIX: KATO'S INEQUALITY

Kato's inequality [99] is used to deal with the correlated random variables in this paper when estimating parameters. Here we introduce how to use Kato's inequality to complete the estimation in the main text.

We can use Eq. (12) to estimate the upper bounds on expected values from the corresponding observed values. In the estimation of QKD protocols, the random variables n_i, $i = 1, 2, \ldots, k$, which indicate whether the detector clicks in the ith round, respectively, are Bernoulli random variables. If the detector clicks in the uth round, $n_u = 1$, and if it doesn't click, $n_u = 0$. So, we have $E(n_u|f_{u-1}) = \Pr(n_u = 1|f_{u-1})$. Γ_k is an observed value that denotes the total number of detector click during k rounds.

To get the tightest bound, one should choose the optimal values for a and b to minimize the deviation $[b + a(\frac{2\Gamma_k}{k} - 1)]\sqrt{k}$ by solving an optimization problem. To demonstrate, we let ε_a be the failure probability for estimating the upper bounds, i.e., $\exp[\frac{-2(b^2-a^2)}{(1+\frac{4a}{3\sqrt{k}})^2}] = \varepsilon_a$, and the optimization problem which is denoted as $\min_{a,b\geqslant|a|}[b + a(\frac{2\Gamma_k}{k} - 1)]\sqrt{k}$.

This is solved by Ref. [104] and the solutions are

$$a_1 = a_1(\Gamma_k, k, \varepsilon_a) = \frac{3(72\sqrt{k}\Gamma_k(k-\Gamma_k)\ln\varepsilon_a - 16k^{3/2}\ln^2\varepsilon_a + 9\sqrt{2}(k-2\Gamma_k)\sqrt{-k^2\ln\varepsilon_a(9\Gamma_k(k-\Gamma_k) - 2k\ln\varepsilon_a)})}{4(9k - 8\ln\varepsilon_a)(9\Gamma_k(k-\Gamma_k) - 2k\ln\varepsilon_a)}, \tag{A1}$$

$$b_1 = b_1(a_1, k, \varepsilon_a) = \frac{\sqrt{18a_1^2k - \left(16a_1^2 + 24a_1\sqrt{k} + 9k\right)\ln\varepsilon_a}}{3\sqrt{2k}}. \tag{A2}$$

With the fixed values a_1 and b_1, we get the upper bound on expected value as follows according to Eq. (12):

$$\Gamma_k^* \leqslant \overline{\Gamma_k^*} = \Gamma_k + \Delta_1(a_1, b_1, k, \Gamma_k), \tag{A3}$$

where $\Delta_1(a_1, b_1, k, \Gamma_k) = [b_1 + a_1(\frac{2\Gamma_k}{k} - 1)]\sqrt{k}$ and we use the expected value Γ_k^* to denote $\sum_{u=1}^{k} E(n_u|f_{u-1})$.

Similarly, Eq. (13) can be applied to estimate the lower bound on expected values, where we need to solve another optimization problem. That is, $\min_{a,b\geqslant|a|}[b + a(\frac{2\Gamma_k}{k} - 1)]\sqrt{k}$, where $\exp[\frac{-2(b^2-a^2)}{(1-\frac{4a}{3\sqrt{k}})^2}] = \varepsilon_a$.

The solutions are

$$a_2 = a_2(\Gamma_k, k, \varepsilon_a) = -\frac{3(72\sqrt{k}\Gamma_k(k-\Gamma_k)\ln\varepsilon_a - 16k^{3/2}\ln^2\varepsilon_a - 9\sqrt{2}(k-2\Gamma_k)\sqrt{-k^2\ln\varepsilon_a(9\Gamma_k(k-\Gamma_k) - 2k\ln\varepsilon_a)})}{4(9k - 8\ln\varepsilon_a)(9\Gamma_k(k-\Gamma_k) - 2k\ln\varepsilon_a)}, \tag{A4}$$

$$b_2 = b_2(a_2, k, \varepsilon_a) = \frac{\sqrt{18a_2^2k - \left(16a_2^2 - 24a_2\sqrt{k} + 9k\right)\ln\varepsilon_a}}{3\sqrt{2k}}, \tag{A5}$$

and we get the lower bound

$$\Gamma_k^* \geqslant \underline{\Gamma_k^*} = \Gamma_k - \Delta_2(a_2, b_2, k, \Gamma_k), \tag{A6}$$

where $\Delta_2(a_2, b_2, k, \Gamma_k) = [b_2 + a_2(\frac{2\Gamma_k}{k} - 1)]\sqrt{k}$. With the methods above, the estimations of $\overline{n_w^{M_i*}}$ and $\underline{n_w^{M_0*}}$ in the main text can be done, where $w = 00, \alpha\alpha$ and $i = 0, 1$. The failure probability for each estimation is ε_a, which is considered when explaining the composable security of our protocol.

When converting expected values to observed values, Kato's inequality is available as well. However, to get specific values of the optimal a_i, b_i and the deviation Δ_i where $i = 1, 2$, the observed value Γ_k needs to be employed, which is not known. So, we follow the method used in Ref. [104]. Let $a = 0$ and set the failure probabilities in Eqs. (12) and (13) to be ε_b. We obtain the inequalities below:

$$\sum_{u=1}^{k} E(n_u|f_{u-1}) \leqslant \Gamma_k + \Delta, \tag{A7}$$

$$\sum_{u=1}^{k} E(n_u|f_{u-1}) \geqslant \Gamma_k - \Delta, \tag{A8}$$

where $\Delta = \sqrt{\frac{1}{2}k\ln\varepsilon_b^{-1}}$. This is how the estimation procedure of Eq. (21) is done.

[1] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, Long-distance quantum communication with atomic ensembles and linear optics, Nature (London) **414**, 413 (2001).

[2] K. Azuma, K. Tamaki, and H.-K. Lo, All-photonic quantum repeaters, Nat. Commun. **6**, 6787 (2015).

[3] C.-L. Li, Y. Fu, W.-B. Liu, Y.-M. Xie, B.-H. Li, M.-G. Zhou, H.-L. Yin, and Z.-B. Chen, All-photonic quantum repeater for multipartite entanglement generation, Opt. Lett. **48**, 1244 (2023).

[4] K. Chen and H.-K. Lo, Multi-partite quantum cryptographic protocols with noisy GHZ states, Quantum Inf. Comput. **7**, 689 (2007).

[5] Y. Fu, H.-L. Yin, T.-Y. Chen, and Z.-B. Chen, Long-distance measurement-device-independent multiparty quantum communication, Phys. Rev. Lett. **114**, 090501 (2015).

[6] S. Zhao, P. Zeng, W.-F. Cao, X.-Y. Xu, Y.-Z. Zhen, X. Ma, L. Li, N.-L. Liu, and K. Chen, Phase-matching quantum cryptographic conferencing, Phys. Rev. Appl. **14**, 024010 (2020).

[7] X.-Y. Cao, J. Gu, Y.-S. Lu, H.-L. Yin, and Z.-B. Chen, Coherent one-way quantum conference key agreement based on twin field, New J. Phys. **23**, 043002 (2021).

[8] Z. Li, X.-Y. Cao, C.-L. Li, C.-X. Weng, J. Gu, H.-L. Yin, and Z.-B. Chen, Finite-key analysis for quantum conference key agreement with asymmetric channels, Quantum Sci. Technol. **6**, 045019 (2021).

[9] A. I. Fletcher and S. Pirandola, Continuous variable measurement device independent quantum conferencing with postselection, Sci. Rep. **12**, 17329 (2022).

[10] C.-L. Li, Y. Fu, W.-B. Liu, Y.-M. Xie, B.-H. Li, M.-G. Zhou, H.-L. Yin, and Z.-B. Chen, Breaking universal limitations on quantum conference key agreement without quantum memory, Commun. Phys. **6**, 122 (2023).

[11] M. Hillery, V. Bužek, and A. Berthiaume, Quantum secret sharing, Phys. Rev. A **59**, 1829 (1999).

[12] R. Cleve, D. Gottesman, and H.-K. Lo, How to share a quantum secret, Phys. Rev. Lett. **83**, 648 (1999).

[13] K.-J. Wei, H.-Q. Ma, and J.-H. Yang, Experimental circular quantum secret sharing over telecom fiber network, Opt. Express **21**, 16663 (2013).

[14] J. Gu, X.-Y. Cao, H.-L. Yin, and Z.-B. Chen, Differential phase shift quantum secret sharing using a twin field, Opt. Express **29**, 9165 (2021).

[15] B. P. Williams, J. M. Lukens, N. A. Peters, B. Qi, and W. P. Grice, Quantum secret sharing with polarization-entangled photon pairs, Phys. Rev. A **99**, 062311 (2019).

[16] A. Shen, X.-Y. Cao, Y. Wang, Y. Fu, J. Gu, W.-B. Liu, C.-X. Weng, H.-L. Yin, and Z.-B. Chen, Experimental quantum secret sharing based on phase encoding of coherent states, Sci. China Phys. Mech. Astron. **66**, 260311 (2023).

[17] M. de Oliveira, I. Nape, J. Pinnell, N. TabeBordbar, and A. Forbes, Experimental high-dimensional quantum secret sharing with spin-orbit-structured photons, Phys. Rev. A **101**, 042303 (2020).

[18] C.-L. Li, Y. Fu, W.-B. Liu, Y.-M. Xie, B.-H. Li, M.-G. Zhou, H.-L. Yin, and Z.-B. Chen, Breaking the rate-distance limitation of measurement-device-independent quantum secret sharing, Phys. Rev. Res. **5**, 033077 (2023).

[19] V. Dunjko, P. Wallden, and E. Andersson, Quantum digital signatures without quantum memory, Phys. Rev. Lett. **112**, 040502 (2014).

[20] H.-L. Yin, Y. Fu, and Z.-B. Chen, Practical quantum digital signature, Phys. Rev. A **93**, 032316 (2016).

[21] J.-Q. Qin, C. Jiang, Y.-L. Yu, and X.-B. Wang, Quantum digital signatures with random pairing, Phys. Rev. Appl. **17**, 044047 (2022).

[22] H.-L. Yin, Y. Fu, C.-L. Li, C.-X. Weng, B.-H. Li, J. Gu, Y.-S. Lu, S. Huang, and Z.-B. Chen, Experimental quantum secure network with digital signatures and encryption, Natl. Sci. Rev. **10**, nwac228 (2023).

[23] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, Theor. Comput. Sci. **560**, 7 (2014).

[24] A. K. Ekert, Quantum cryptography based on Bell's theorem, Phys. Rev. Lett. **67**, 661 (1991).

[25] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301 (2009).

[26] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, Rev. Mod. Phys. **92**, 025002 (2020).

[27] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, Advances in quantum cryptography, Adv. Opt. Photon. **12**, 1012 (2020).

[28] H.-K. Lo, M. Curty, and B. Qi, Measurement-device-independent quantum key distribution, Phys. Rev. Lett. **108**, 130503 (2012).

[29] S. L. Braunstein and S. Pirandola, Side-channel-free quantum key distribution, Phys. Rev. Lett. **108**, 130502 (2012).

[30] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, Nat. Photon. **4**, 686 (2010).

[31] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, Measurement-device-independent quantum key distribution over a 404 km optical fiber, Phys. Rev. Lett. **117**, 190501 (2016).

[32] Y.-H. Zhou, Z.-W. Yu, and X.-B. Wang, Making the decoy-state measurement-device-independent quantum key distribution practically useful, Phys. Rev. A **93**, 042324 (2016).

[33] S. Pirandola, R. García-Patrón, S. L. Braunstein, and S. Lloyd, Direct and reverse secret-key capacities of a quantum channel, Phys. Rev. Lett. **102**, 050503 (2009).

[34] M. Takeoka, S. Guha, and M. M. Wilde, Fundamental rate-loss tradeoff for optical quantum key distribution, Nat. Commun. **5**, 5235 (2014).

[35] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, Nat. Commun. **8**, 15043 (2017).

[36] S. Das, S. Bäuml, M. Winczewski, and K. Horodecki, Universal limitations on quantum key distribution over a network, Phys. Rev. X **11**, 041016 (2021).

[37] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the rate-distance limit of quantum key distribution without quantum repeaters, Nature (London) **557**, 400 (2018).

[38] X. Ma, P. Zeng, and H. Zhou, Phase-matching quantum key distribution, Phys. Rev. X **8**, 031043 (2018).

[39] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, Twin-field quantum key distribution with large misalignment error, Phys. Rev. A **98**, 062323 (2018).
[40] H.-L. Yin and Y. Fu, Measurement-device-independent twin-field quantum key distribution, Sci. Rep. **9**, 3045 (2019).
[41] J. Lin and N. Lütkenhaus, Simple security analysis of phase-matching measurement-device-independent quantum key distribution, Phys. Rev. A **98**, 042332 (2018).
[42] C. Cui, Z.-Q. Yin, R. Wang, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, Twin-field quantum key distribution without phase postselection, Phys. Rev. Appl. **11**, 034053 (2019).
[43] M. Curty, K. Azuma, and H.-K. Lo, Simple security proof of twin-field type quantum key distribution protocol, npj Quantum Inf. **5**, 64 (2019).
[44] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, W. Chen, Y.-G. Zhu, P. V. Morozov, A. V. Divochiy, Z. Zhou, G.-C. Guo, and Z.-F. Han, Twin-field quantum key distribution over 830-km fibre, Nat. Photon. **16**, 154 (2022).
[45] Y. Liu, W.-J. Zhang, C. Jiang, J.-P. Chen, C. Zhang, W.-X. Pan, D. Ma, H. Dong, J.-M. Xiong, C.-J. Zhang, H. Li, R.-C. Wang, J. Wu, T.-Y. Chen, L. You, X.-B. Wang, Q. Zhang, and J.-W. Pan, Experimental twin-field quantum key distribution over 1000 km fiber distance, Phys. Rev. Lett. **130**, 210801 (2023).
[46] Y.-M. Xie, Y.-S. Lu, C.-X. Weng, X.-Y. Cao, Z.-Y. Jia, Y. Bao, Y. Wang, Y. Fu, H.-L. Yin, and Z.-B. Chen, Breaking the rate-loss bound of quantum key distribution with asynchronous two-photon interference, PRX Quantum **3**, 020315 (2022).
[47] P. Zeng, H. Zhou, W. Wu, and X. Ma, Mode-pairing quantum key distribution, Nat. Commun. **13**, 3903 (2022).
[48] H.-T. Zhu, Y. Huang, H. Liu, P. Zeng, M. Zou, Y. Dai, S. Tang, H. Li, L. You, Z. Wang, Y.-A. Chen, X. Ma, T.-Y. Chen, and J.-W. Pan, Experimental mode-pairing measurement-device-independent quantum key distribution without global phase locking, Phys. Rev. Lett. **130**, 030801 (2023).
[49] L. Zhou, J. Lin, Y.-M. Xie, Y.-S. Lu, Y. Jing, H.-L. Yin, and Z. Yuan, Experimental quantum communication overcomes the rate-loss limit without global phase tracking, Phys. Rev. Lett. **130**, 250801 (2023).
[50] J.-L. Bai, Y.-M. Xie, Y. Fu, H.-L. Yin, and Z.-B. Chen, Asynchronous measurement-device-independent quantum key distribution with hybrid source, Opt. Lett. **48**, 3551 (2023).
[51] Y.-M. Xie, J.-L. Bai, Y.-S. Lu, C.-X. Weng, H.-L. Yin, and Z.-B. Chen, Advantages of asynchronous measurement-device-independent quantum key distribution in intercity networks, Phys. Rev. Appl. **19**, 054070 (2023).
[52] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Limitations on practical quantum cryptography, Phys. Rev. Lett. **85**, 1330 (2000).
[53] W.-Y. Hwang, Quantum key distribution with high loss: toward global secure communication, Phys. Rev. Lett. **91**, 057901 (2003).
[54] X.-B. Wang, Beating the photon-number-splitting attack in practical quantum cryptography, Phys. Rev. Lett. **94**, 230503 (2005).
[55] H.-K. Lo, X. Ma, and K. Chen, Decoy state quantum key distribution, Phys. Rev. Lett. **94**, 230504 (2005).
[56] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations, Phys. Rev. Lett. **92**, 057901 (2004).
[57] K. Tamaki and H.-K. Lo, Unconditionally secure key distillation from multiphotons, Phys. Rev. A **73**, 010302(R) (2006).
[58] H.-L. Yin, Y. Fu, Y. Mao, and Z.-B. Chen, Security of quantum key distribution with multiphoton components, Sci. Rep. **6**, 29482 (2016).
[59] M. Koashi, Unconditional security of coherent-state quantum key distribution with a strong phase-reference pulse, Phys. Rev. Lett. **93**, 120501 (2004).
[60] K. Inoue, E. Waks, and Y. Yamamoto, Differential phase shift quantum key distribution, Phys. Rev. Lett. **89**, 037902 (2002).
[61] K. Inoue, E. Waks, and Y. Yamamoto, Differential-phase-shift quantum key distribution using coherent light, Phys. Rev. A **68**, 022317 (2003).
[62] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, Fast and simple one-way quantum key distribution, Appl. Phys. Lett. **87**, 194108 (2005).
[63] T. Sasaki, Y. Yamamoto, and M. Koashi, Practical quantum key distribution protocol without monitoring signal disturbance, Nature (London) **509**, 475 (2014).
[64] H. Takesue, E. Diamanti, T. Honjo, C. Langrock, M. M. Fejer, K. Inoue, and Y. Yamamoto, Differential phase shift quantum key distribution experiment over 105 km fibre, New J. Phys. **7**, 232 (2005).
[65] E. Diamanti, H. Takesue, C. Langrock, M. M. Fejer, and Y. Yamamoto, 100 km differential phase shift quantum key distribution experiment with low jitter up-conversion detectors, Opt. Express **14**, 13073 (2006).
[66] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors, Nat. Photon. **1**, 343 (2007).
[67] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, Field test of quantum key distribution in the tokyo QKD network, Opt. Express **19**, 10387 (2011).
[68] K. Wen, K. Tamaki, and Y. Yamamoto, Unconditional security of single-photon differential phase shift quantum key distribution, Phys. Rev. Lett. **103**, 170503 (2009).
[69] K. Tamaki, M. Koashi, and G. Kato, Unconditional security of coherent-state-based differential phase shift quantum key distribution protocol with block-wise phase randomization, arXiv:1208.1995.
[70] A. Mizutani, T. Sasaki, G. Kato, Y. Takeuchi, and K. Tamaki, Information-theoretic security proof of differential-phase-shift quantum key distribution protocol based on complementarity, Quantum Sci. Technol. **3**, 014003 (2018).
[71] A. Mizutani, T. Sasaki, Y. Takeuchi, K. Tamaki, and M. Koashi, Quantum key distribution with simply

characterized light sources, npj Quantum Inf. **5**, 87 (2019).

[72] A. Mizutani, Quantum key distribution with any two independent and identically distributed states, Phys. Rev. A **102**, 022613 (2020).

[73] H. Endo, T. Sasaki, M. Takeoka, M. Fujiwara, M. Koashi, and M. Sasaki, Line-of-sight quantum key distribution with differential phase shift keying, New J. Phys. **24**, 025008 (2022).

[74] A. Mizutani, Y. Takeuchi, and K. Tamaki, Finite-key security analysis of differential-phase-shift quantum key distribution, Phys. Rev. Res. **5**, 023132 (2023).

[75] M. Sandfuchs, M. Haberland, V. Vilasini, and R. Wolf, Security of differential phase shift QKD from relativistic principles, arXiv:2301.11340.

[76] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, The secoqc quantum key distribution network in Vienna, New J. Phys. **11**, 075001 (2009).

[77] D. Stucki, C. Barreiro, S. Fasel, J.-D. Gautier, O. Gay, N. Gisin, R. Thew, Y. Thoma, P. Trinkler, F. Vannel, and H. Zbinden, Continuous high speed coherent one-way quantum key distribution, Opt. Express **17**, 13326 (2009).

[78] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres, New J. Phys. **11**, 075003 (2009).

[79] N. Walenta, A. Burg, D. Caselunghe, J. Constantin, N. Gisin, O. Guinnard, R. Houlmann, P. Junod, B. Korzh, N. Kulesza, M. Legré, C. W. Lim, T. Lunghi, L. Monat, C. Portmann, M. Soucarros, R. T. Thew, P. Trinkler, G. Trolliet, F. Vannel, and H. Zbinden, A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing, New J. Phys. **16**, 013047 (2014).

[80] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, Provably secure and practical quantum key distribution over 307 km of optical fibre, Nat. Photon. **9**, 163 (2015).

[81] P. Sibson, C. Erven, M. Godfrey, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan, R. H. Hadfield, J. L. O'Brien, and M. G. Thompson, Chip-based quantum key distribution, Nat. Commun. **8**, 13984 (2017).

[82] P. Sibson, J. E. Kennard, S. Stanisic, C. Erven, J. L. O'Brien, and M. G. Thompson, Integrated silicon photonics for high-speed quantum key distribution, Optica **4**, 172 (2017).

[83] G. L. Roberts, M. Lucamarini, J. F. Dynes, S. J. Savory, Z. L. Yuan, and A. J. Shields, Modulator-free coherent-one-way quantum key distribution, Laser Photonics Rev. **11**, 1700067 (2017).

[84] J. Dai, L. Zhang, X. Fu, X. Zheng, and L. Yang, Pass-block architecture for distributed-phase-reference quantum key distribution using silicon photonics, Opt. Lett. **45**, 2014 (2020).

[85] C. Branciard, N. Gisin, and V. Scarani, Upper bounds for the security of two distributed-phase reference protocols of quantum cryptography, New J. Phys. **10**, 013031 (2008).

[86] T. Moroder, M. Curty, Charles Ci Wen Lim, L. P. Thinh, H. Zbinden, and N. Gisin, Security of distributed-phase-reference quantum key distribution, Phys. Rev. Lett. **109**, 260501 (2012).

[87] J. González-Payo, R. Trényi, W. Wang, and M. Curty, Upper security bounds for coherent-one-way quantum key distribution, Phys. Rev. Lett. **125**, 260510 (2020).

[88] R. Trényi and M. Curty, Zero-error attack against coherent-one-way quantum key distribution, New J. Phys. **23**, 093005 (2021).

[89] Y. Wang, I. W. Primaatmaja, E. Lavie, A. Varvitsiotis, and C. C. W. Lim, Characterising the correlations of prepare-and-measure quantum networks, npj Quantum Inf. **5**, 17 (2019).

[90] I. De Marco, R. I. Woodward, G. L. Roberts, T. K. Paraïso, T. Roger, M. Sanzaro, M. Lucamarini, Z. Yuan, and A. J. Shields, Real-time operation of a multi-rate, multi-protocol quantum key distribution transmitter, Optica **8**, 911 (2021).

[91] E. Lavie and Charles C.-W. Lim, Improved coherent one-way quantum key distribution for high-loss channels, Phys. Rev. Appl. **18**, 064053 (2022).

[92] R.-Q. Gao, Y.-M. Xie, J. Gu, W.-B. Liu, C.-X. Weng, B.-H. Li, H.-L. Yin, and Z.-B. Chen, Simple security proof of coherent-one-way quantum key distribution, Opt. Express **30**, 23783 (2022).

[93] M. Tomamichel and R. Renner, Uncertainty relation for smooth entropies, Phys. Rev. Lett. **106**, 110506 (2011).

[94] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Tight finite-key analysis for quantum cryptography, Nat. Commun. **3**, 634 (2012).

[95] J. Müller-Quade and R. Renner, Composability in quantum cryptography, New J. Phys. **11**, 085006 (2009).

[96] Y. Wang, W.-S. Bao, C. Zhou, M.-S. Jiang, and H.-W. Li, Tight finite-key analysis of a practical decoy-state quantum key distribution with unstable sources, Phys. Rev. A **94**, 032335 (2016).

[97] Y. Wang, W.-S. Bao, C. Zhou, M.-S. Jiang, and H.-W. Li, Finite-key analysis of practical decoy-state measurement-device-independent quantum key distribution with unstable sources, J. Opt. Soc. Am. B **36**, B83 (2019).

[98] R. Renner, Security of quantum key distribution, Int. J. Quantum Inform. **06**, 1 (2008).

[99] G. Kato, Concentration inequality using unconfirmed knowledge, arXiv:2002.04357.

[100] K. Azuma, Weighted sums of certain dependent random variables, Tohoku Math. J. **19**, 357 (1967).

[101] R. Konig, R. Renner, and C. Schaffner, The operational meaning of min- and max-entropy, IEEE Trans. Inf. Theory **55**, 4337 (2009).

[102] J. M. Renes and R. Renner, One-shot classical data compression with quantum side information and the distillation of common randomness or secret keys, IEEE Trans. Inf. Theory **58**, 1985 (2012).

[103] H.-L. Yin and Z.-B. Chen, Finite-key analysis for twin-field quantum key distribution with composable security, Sci. Rep. **9**, 17113 (2019).

[104] G. Currás-Lorenzo, Á. Navarrete, K. Azuma, G. Kato, M. Curty, and M. Razavi, Tight finite-key security for twin-field quantum key distribution, npj Quantum Inf. **7**, 22 (2021).