Simple security proof of coherent-one-way quantum key distribution

Rui-Qi Gao,1 Yuan-Mei Xie,1 Jie Gu,1 Wen-Bo Liu,1 Chen-Xun Weng,1 Bing-Hong Li,1 Hua-Lei Yin,1,∗ and Zeng-Bing Chen1,†

1National Laboratory of Solid State Microstructures,
School of Physics and Collaborative Innovation Center of Advanced Microstructures, Nanjing University, Nanjing 210093, China
(Dated: June 5, 2023)

Coherent-one-way quantum key distribution (COW-QKD), which requires a simple experimental setup and has the ability to withstand photon-number-splitting attacks, has been not only experimentally implemented but also commercially applied. However, recent studies have shown that the current COW-QKD system is insecure and can only distribute secret keys safely within 20 km of the optical fiber length. In this study, we propose a practical implementation of COW-QKD by adding a two-pulse vacuum state as a new decoy sequence. This proposal maintains the original experimental setup as well as the simplicity of its implementation. Utilizing detailed observations on the monitoring line to provide an analytical upper bound on the phase error rate, we provide a high-performance COW-QKD asymptotically secure against coherent attacks. This ensures the availability of COW-QKD within 100 km and establishes theoretical foundations for further applications.

I. INTRODUCTION

Quantum key distribution (QKD) [1,2], whose security is guaranteed by quantum laws, allows secret key distribution between two distant parties. Since the Bennett-Brassard 1984 (BB84) protocol [1] was first proposed, numerous QKD schemes have been developed [3–6]. To defeat detector attacks [3,6], a viable approach is measurement-device-independent QKD [7,8], which has been implemented over a long distance [9,10]. Recently, twin-field QKD [11–19] has also solved this issue and significantly improved the secret key rate. Another strong restriction in practical QKD is the photon number splitting attack [20] on the source side. For example, the coherent-state-based (non-random phase) BB84 protocol can only realize secure key transmissions over 15 km. To overcome this limitation, several approaches such as decoy-state methods [21–23], strong reference-pulse methods [24], non-orthogonal coding methods [25–27], and distributed-phase-reference methods [28–31] have been proposed.

As a type of distributed-phase-reference protocol, coherent-one-way (COW) QKD [32] has received considerable attention because of its simple and convenient experimental implementation [32–39], which has been deployed in practical quantum communication networks [40–41]. Considering the restricted types of collective attacks [42], the key rate depends linearly on the transmittance $\eta$. Additionally, a variant of COW-QKD with a security proof against general attacks was proposed in 2012 [35], and the resulting key rate “appears to” be of order $O(\eta^2)$. To date, all COW-QKD experiments [35,36,39], including long-distance experiments [35,36], still employ the original security proof [42] in which the key rate is of order $O(\eta^2)$. These experimental results demonstrate the practicability and potential of COW-QKD.

However, the so called “zero-error attack” [45,46] involves eavesdropping without breaking the coherence between adjacent non-vacuum pulses (no bit error). Consequently, COW-QKD is insecure if the key rate scales as $O(\eta^2)$; in fact, the given attack restricts the secure key rate scaling to slightly higher than $\eta^2$. Recently, a novel security proof using semidefinite programming techniques [47] showed that the transmission distance of COW-QKD using active basis choice is only 20 km. Thus, extending the secure transmission distance of COW-QKD has become an urgent issue.

In this study, we propose a practical implementation of COW-QKD and provide a security proof with precise phase error rate estimation. This proposal keeps all the experimental equipment of the original version unchanged and maintains its ease of implementation. With detailed observations on the monitoring line, we estimate the upper bound on the phase error rate instead of only checking the coherence between adjacent non-vacuum states. We show that the lower bound of the key rate is 0.005$\eta^2$, while ensuring the security within 100 kilometers. It is worth mentioning that our secure lower bound for the key rate is approximately 10 times higher than the key rate given by the COW-QKD variant in Ref. [43], considering that we effectively evaluated the impact of the vacuum states and provided an analytical expression.

II. PROTOCOL DESCRIPTION

In the original COW protocol, sender Alice encodes logic bits 0 and 1 into a pair of coherent states (non-random phase) $|\alpha_k\rangle = |0\rangle_{2k-1}|\alpha\rangle_{2k}$ and $|1_k\rangle =
FIG. 1: Schematic of COW-QKD in our work. Alice randomly sends a sequence of states $|0\rangle_{2k-1} |\alpha\rangle_{2k}, |\alpha\rangle_{2k-1} |0\rangle_{2k}$ to Bob. Then, a beam-splitter of transmittance $t_B$ distributes incoming pulses into the data line and monitoring line at the receiving side, Bob. The quantum states can be experimentally realized by Alice by modulating $|0\rangle$ or $|\alpha\rangle$ using an intensity modulator (IM) in each time bin. Compared with the original version, where the sequences of states can be prepared in a similar manner, there is no extra technical requirement in our modification. $D_T$, $D_{M_0}$, and $D_{M_1}$ are the single-photon detectors.

$|\alpha\rangle_{2k-1} |0\rangle_{2k}$ at two time points $2k - 1$ and $2k$ ($k = 1, 2, \ldots, K$), where $|0\rangle$ is the vacuum state and $|\alpha\rangle$ is a coherent state with mean photon number $\mu = |\alpha|^2$. Additionally, Alice sends a two-pulse sequence $|\alpha\rangle_{2k-1} |\alpha\rangle_{2k}$, which is defined as a decoy sequence. Because all non-vacuum pulses share a common phase, Alice can use a mode-locked continuous-wave laser followed by an intensity modulator to prepare weak coherent pulses.

The pulses are then transmitted to the receiver, Bob, through a quantum channel characterized by $\eta$. Bob employs an asymmetric beam-splitter with a transmission coefficient $t_B$ (passive basis choice) to split the incoming pulses into the data line and the monitoring line. We note that Bob can also use an optical switch (active basis choice) instead of the beam-splitter. On the data line, Bob obtains the raw key by measuring the arrival time of each pair of pulses using detector $D_T$. On the monitoring line, Bob checks the coherence between adjacent non-vacuum pulses by observing the measurement outcome of a Mach-Zehnder interferometer with two detectors, $D_{M_0}$ and $D_{M_1}$. Information leakage can be detected by broken coherence, which can be reflected by the visibility $V = [P(D_{M_0}) - P(D_{M_1})] / [P(D_{M_0}) + P(D_{M_1})]$, where $P(D_{M_0})$ and $P(D_{M_1})$ is the probability that the detector $D_{M_0}$ and $D_{M_1}$ clicks. Alice and Bob also use a random subset of data on the data line to test the bit error rate $E_b$.

The security proof and secure key rate of COW-QKD are provided based on these two parameters, $E_b$ and $V$ [42].

Nevertheless, recent studies introduced the so-called zero-error attack [43,49]. On the one hand, since the signals sent by Alice are linearly independent, Eve can adopt an unambiguous state discrimination measurement to distinguish each signal sent by Alice without introducing error on the data line. On the other hand, the vacuum state in the signals naturally breaks the coherence between adjacent pulses. Taking advantage of this property, Eve can resend to Bob blocked signal sequences that preserve coherence among consecutive non-empty pulses. Thus, all the security proofs of COW-QKD, which rely on coherence analysis, appear to be unreliable.

As shown in figure 1, we propose a practical implementation of COW-QKD by adding a two-pulse vacuum state $|0\rangle_{2k-1} |0\rangle_{2k}$ as decoy sequence 2. When evaluating the secure key rate, Alice no longer estimates the visibility $V$ to quantify leaked information. Instead, she calculates the gains $Q_{0i}^{M_1}, Q_{i0}^{M_1}, Q_{\alpha i}^{M_1}$ and $Q_{i0}^{M_1}$ ($i = 0$ or 1) to estimate the phase error rate, where the superscript $M_i$ represents the clicking detector $D_{M_i}$ on the monitoring line announced by Bob, the subscript refers to the corresponding sequence $|0\rangle_{2k-1} |\alpha\rangle_{2k}, |\alpha\rangle_{2k-1} |0\rangle_{2k}, |\alpha\rangle_{2k-1} |\alpha\rangle_{2k}$ and $|0\rangle_{2k-1} |0\rangle_{2k}$ sent by Alice. Here, we clarify that if multiple detectors click corresponding to every pair of states, Bob regards this event as one of these detectors clicking randomly [43, 49].

III. SECURITY ANALYSIS

To provide a security proof for COW-QKD, we introduce a virtual entanglement-based protocol as follows: Here, we redefine the $k$-th optical modes $|0_i\rangle = |0\rangle_{2k-1} |\alpha\rangle_{2k}$ and $|1_i\rangle = |\alpha\rangle_{2k-1} |0\rangle_{2k}$, where we omit the label $k$ to simplify the presentation. Let $|0_x\rangle =
\( (|0_z\rangle + |1_z\rangle)/\sqrt{N^+} \) and \( |1_z\rangle = (|0_z\rangle - |1_z\rangle)/\sqrt{N^-} \) be two nonclassical optical modes, where \( N^\pm = 2(1 \pm e^{-\mu}) \) are the normalization factors. We introduce an ancillary qubit, where \( |\pm z\rangle \) and \( |\pm x\rangle \) are the eigenstates of the Pauli operators \( Z \) and \( X \) of the qubit, respectively. Alice prepares \( K \) pairs of entangled state

\[
\begin{align*}
|\psi\rangle &= \frac{1}{\sqrt{2}} (|+z\rangle_A |0_z\rangle_{A'} - |z\rangle_A |1_z\rangle_{A'}) \\
&= \frac{\sqrt{N^+}}{2} |+x\rangle_A |0_x\rangle_{A'} + \frac{\sqrt{N^-}}{2} |-x\rangle_A |1_x\rangle_{A'} ,
\end{align*}
\]

where the subscript \( A \) denotes the ancillary qubit maintained by Alice, and \( A' \) represents the optical mode sent to Bob. Alice randomly measures the ancillary qubit in the \( Z \) or \( X \) basis and then acquires the raw keys \( \tilde{Z}_A \) from the \( Z \) basis and \( \tilde{X}_A \) from the \( X \) basis. Then, she sends optical modes to Bob in an insecure quantum channel. Similar to the practical COW protocol, the optical modes are detected randomly on the data or monitoring line. When observing that the detector \( D_T \) clicks at the previous moment \( T_0 \) (the latter moment \( T_1 \)), Bob records the bit value 0 (1) as the raw key in \( \tilde{Z}_B \). In addition, the raw key \( \tilde{X}_B \) is obtained by Bob observing the monitoring line. A detector \( D_{M_0} (D_{M_1}) \) click denotes a bit value of 0 (1).

Let \( H^e_{\text{min}} (\tilde{Z}_A | E) \) be the smooth min-entropy characterizing the average probability that Eve guesses \( \tilde{Z}_A \) correctly using the optimal strategy with access to the correlations stored in her quantum memory. Let \( H^e_{\text{max}} (\tilde{Z}_A | \tilde{Z}_B) \) be the smooth max-entropy corresponding to the number of extra bits required to reconstruct the value of \( Z_A \) using \( Z_B \), up to a failure probability of \( \epsilon \). For later use, we denote the binary Shannon entropy as \( h(a) = -a \log_2 a - (1-a) \log_2 (1-a) \), and the size of \( \tilde{Z}_A \) as \( n_z \). \( X_A' \) is the bit string that Alice would have obtained if she had measured in the \( X \) basis in virtual protocol, which is actually measured in the \( Z \) basis. Therefore, we have a smooth max-entropy \( H^e_{\text{max}} (\tilde{X}_A' | \tilde{Z}_B) \leq n_z h(E_z) \) in the asymptotic limit, where \( E_z \) is the bit error rate in the \( X \) basis. By exploiting the uncertainty relation method for smooth entropies, the asymptotic secret key rate of the virtual entanglement-based protocol can be expressed as

\[
\begin{align*}
\hat{R} &= \frac{1}{P_z K} [H^e_{\text{min}} (\tilde{Z}_A | E) - H^e_{\text{max}} (\tilde{Z}_A | \tilde{Z}_B) ] \\
&= \frac{1}{P_z K} [n_z - h(E_z) - n_z f h(E_z)] \\
&= Q_z \left[ 1 - h(E_z) - f h(E_z) \right],
\end{align*}
\]

where \( Q_z = n_z/(P_z K) = (Q_{z_0}^{T_0} + Q_{z_1}^{T_1} + Q_{z_0}^{T_0} + Q_{z_1}^{T_1})/2 \) is the gain that Alice measures in the \( Z \) basis and Bob detects on the data line, and \( P_z \) is the probability that Alice measures in the \( Z \) basis and Bob measures on the data line. Here, \( f \) denotes the efficiency of error correction and \( E_z \) is the bit error rate in the \( Z \) basis. Moreover, when using the entropic uncertainty relation, the signals detected by Bob’s device should be independent of Alice and Bob’s basis choices. This requirement can naturally be satisfied when using active basis choice, but it needs to be cautiously considered when applying the passive basis choice. Using passive basis choice, Eve can apply classical wavelength attacks to partially control Bob’s basis selection and cause weak basis-choice flaws. Nevertheless, the secure key rate decreases only slightly when the wavelength is carefully characterized to minimize this effect. Recently, passive basis
choice has been widely utilized in various QKD protocols \cite{64,63}. In this study, using passive basis choice, we assume that the beam-splitter is not controlled by the eavesdropper and use the squashing model \cite{48,19} in the measurement setup.

In fact, the virtual entanglement-based protocol can be converted to an equivalent prepare-and-measure nonclassical protocol, that is, Alice directly prepares optical modes rather than preparing entangled states and measuring the ancillary qubit system. When Alice chooses the \( Z \) basis, she directly sends the optical modes \( |0_z\rangle \) and \( |1_z\rangle \) with probability 1/2. If Alice selects the \( X \) basis, she directly sends nonclassical optical modes \( |0_x\rangle \) and \( |1_x\rangle \) with probabilities \( N^+ /4 \) and \( N^- /4 \), respectively.

The above facts can be directly seen from the density matrices of the \( Z \) and \( X \) bases, which are equal in the nonclassical protocol, that is,

\[
\rho = \frac{1}{2} (|0_z\rangle \langle 0_z| + |1_z\rangle \langle 1_z|) = (N^+ |0_x\rangle \langle 0_x| + N^- |1_x\rangle \langle 1_x|) /4. \tag{3}
\]

Therefore, the bit error rate \( E_z \) can be obtained directly from the observed gain as follows:

\[
E_z = \frac{Q_{T_w}^T + Q_{T_0}^T}{Q_{T_0}^T + Q_{T_1}^T + Q_{T_0}^{T_1} + Q_{T_1}^{T_1}}, \tag{4}
\]

where \( Q_{T_w}^T \) represents the gain of the event that Alice sends optical mode \( |w_z\rangle \) (\( w = 0 \) or 1) and Bob obtains a click at the \( T_j \) (\( j = 0 \) or 1) moment on the data line, and

\[
Q_z = \left( Q_{T_0}^{T_0} + Q_{T_1}^{T_0} + Q_{T_0}^{T_1} + Q_{T_1}^{T_1} \right) /2. \text{ Similarly, the bit error rate of the X basis is given by}
\]

\[
E_x = \frac{N^+ Q_{M_0}^M + N^- Q_{M_1}^M}{N^+ (Q_{M_0}^{M_0} + Q_{M_1}^{M_1}) + N^- (Q_{M_0}^{M_0} + Q_{M_1}^{M_1})} = \frac{N^+ Q_{M_0}^M + \left[ 2 \left( Q_{M_0}^{M_0} + Q_{M_1}^{M_0} \right) - N^+ Q_{M_0}^M \right]}{2 \left( Q_{M_0}^{M_0} + Q_{M_1}^{M_0} + Q_{M_1}^{M_1} \right)}, \tag{5}
\]

where \( Q_{w(z)} \) represents the gain of the event that Alice sends optical mode \( |w_z\rangle \) and \( |0_x\rangle \) or \( |1_x\rangle \) and \( |\alpha\rangle \) or \( |\alpha\rangle \), respectively. The eavesdropper Eve cannot distinguish this step from the following virtual step: Alice prepares an entangled state \( |\psi\rangle \) and measures the ancillary qubit in the \( Z \) basis. Consequently, Alice’s raw key is identical to \( Z_A \). The secret key rate in the asymptotic limit can be written as

\[
R = Q \left[ 1 - h(E_p^a) - f h(E_b) \right], \tag{6}
\]

where \( Q = Q_z \) and \( E_b = E_z \) are the gain and bit error rate, respectively. The phase error rate \( E_p^a \) is the upper bound on the average error probability \cite{64}, which Bob guesses as Alice’s bit string \( X_A^T \) in the virtual entanglement-based protocol. This is equal to the upper
bound on the bit error rate of the X basis in the nonclassical protocol. In practice, Alice does not measure qubits in the X basis, which means that one cannot directly acquire the gains \( Q_{0x}^M \) and \( Q_{1x}^M \) in the nonclassical protocol. However, we can exploit the gains of the other quantum states \( |\alpha\rangle_{2k-1} |\alpha\rangle_{2k} \) and \( |0\rangle_{2k-1} |0\rangle_{2k} \) which can be directly attained in the COW-QKD protocol to estimate the upper bound \( Q_{0x}^M \) and the lower bound \( Q_{0x}^M \).

The phase error rate \( E^u_p \) can be expressed as

\[
E^u_p = \frac{N^+ Q_{0x}^M + [2 (Q_{0x}^M + Q_{1x}^M) - N^+ Q_{0x}^M]}{2 (Q_{0x}^M + Q_{1x}^M + Q_{1x}^M + Q_{1x}^M)},
\]

where we use the relation for gain between the nonclassical protocol and the COW-QKD protocol, that is, \( Q_{0x}^M = Q_{0x}^M \) and \( Q_{1x}^M = Q_{1x}^M \). Under collective attacks, we have the upper bound \( Q_{0x}^M \) and lower bound \( Q_{0x}^M \), using the method described in Refs. [36, 63]. The details can be found in Appendix B. Using Azuma’s inequality [66], we remark that the security of COW-QKD can be extended against coherent attacks because the estimation of the phase-error rate will yield consistent results in the asymptotic limit. Security against coherent attacks is presented in Appendix [35].

### IV. NUMERICAL SIMULATION

In our simulation, we assume a dark-count rate of \( p_d = 10^{-8} \) and detection efficiency of \( \eta_d = 80\% \). The correction efficiency, \( f \), was set to 1.1. The linear lossy channel is characterized by a transmittance of \( \eta = 10^{-0.02L} \). The transmission coefficient \( t_B \) of the asymmetric beam-splitter is given by the optimization algorithm.

We present the secret key rate of COW-QKD using passive-basis choice with different misalignment errors in figure [3]. Compared with \( \eta^2 \) and the Pirandola-Laurenza-Ottaviani-Banchi bound (PLOB bound) [67, 68] (\( R_{\text{PLOB}} = - \log_2 (1 - \eta) \)), the lower bound on the key rate scales is of the order of \( O(\eta^2) \), which is consistent with the result in Ref. [45]. The secret key rate can still be transmitted over 100 km through the optical fiber when misalignment error \( e_a = 0 \). The secret key rate using active basis choice on the receiving side is also considered. The numerical results of the secret key rate using passive basis choice and active basis choice are presented in figure [3]. Figure [3] also presents the upper bound on the phase error rate \( E^u_p \) using active basis choice.

In figure [4], we show the key rate of the nonclassical protocol using passive basis choice. Comparing the results of the nonclassical protocol with the decoy-state BB84 protocol [22, 23] and the PLOB bound [67, 68], we find that the nonclassical protocol also achieves the key rate of order \( O(\eta) \).

Additionally, we compare the COW-QKD of this study with the variants of COW-QKD [43, 47] in figure [5]. The variant in Ref. [43] is considered in the case where all different 3-signal blocks (including 6 optical pulses) share the same phase and Bob applies the active basis choice setup. The variant in Ref. [47] is considered in the case where the decoy sequence keeps the original setting as \( |\alpha\rangle_{2k-1} |\alpha\rangle_{2k} \). In figure [6], the dark count rate \( p_d \) is set to \( 10^{-7} \) and the detection efficiency \( \eta_d \) is set to 99%. The results reveal that the lower bound on the key rate for the COW-QKD using passive basis choice and active basis choice are both tighter than the result given by the variant in Ref. [43]. The secure key distribution in this work also achieves a longer transmittance distance compared with the variant in Ref. [47]. We also almost maintain the original setting of the COW protocol.

Table [I] summarizes the performance of this study with the variants of the COW-QKD protocol [43, 47]. The asymptotic security of all these COW-typed QKD protocols has been proven against coherent attacks. Compared with this work, the variant of COW-QKD in Ref. [45] also extends the secure key distribution over 90 km using active basis choice; however, it changed the original protocol a lot (coding with m-signal blocks). The variant in Ref. [47] almost maintains the setting of the original COW protocol as in this work. However, its secret keys can only be distributed within 20 km using active basis choice (Here, we consider the variant protocol in Ref. [47], maintaining the original COW-QKD decoy sequence \( |\alpha\rangle_{2k-1} |\alpha\rangle_{2k} \)). Our work using passive basis choice also shows good performance, which is presented in parentheses.

### V. CONCLUSION

In this study, we provide an asymptotic security proof for the practical implementation of COW-QKD under coherent attacks and derive the lower bound on the secure key rate. The security proof no longer relies on coherence between adjacent pulses to detect eavesdrop-
ping. Instead, we sort the observed quantities to estimate the upper bound on the phase error rate. Our result is tighter than the lower bound on the key rate of the variant COW-QKD because we calculate the component of the vacuum states more carefully. Maintaining all current experimental apparatus and techniques, we extend the secure key distribution to 100 km, which paves the way for the secure implementation of COW-QKD.

Acknowledgments

We thank Charles Ci Wen Lim, Nicolas Gisin, and Ignatius William Primaatmaja for enlightening the discussions and making the security proof of this work more rigorous. We thank Amine Iggidr for helping us find and correct an incorrect expression $c_5$ given in appendix A of the previous version. We gratefully acknowledge support from National Natural Science Foundation of China (No. 61801420), Natural Science Foundation of Jiangsu Province (No. BK20211145), Fundamental Research Funds for the Central Universities (No. 020414380182), Key Research and Development Program of Nanjing Jiangbei New Area (No. ZDYD20210101), Key-Area Research and Development Program of Guangdong Province (No. 2020B0303040001). R.-G. Q. and Y.-M. X. contributed equally to this work.

Appendix A: Upper bound on phase error rate

Here, we first consider the case in which Bob applies a passive basis choice to distribute incoming pulses into the data and monitoring lines. The gain of the state $|\phi\rangle$ heralded by detector $D_M_i$ ($i = 0$ or 1) clicking can be given by

$$Q_{\phi}^{M_i} = \langle \phi | \hat{M}^+_i \hat{M}_i | \phi \rangle,$$

(A1)

where $\hat{M}_i$ is the Kraus operator corresponding to detector $D_M_i$.

In the nonclassical protocol, the gains of the states $|0_x\rangle$ and $|1_x\rangle$ detected by detector $D_M_i$ on the monitoring line, that is, $Q_{0_x}^{M_i}$ and $Q_{1_x}^{M_i}$, can be written as $Q_{0_x}^{M_i} = Q_{1_x}^{M_i} = (1 - p_d) e^{-t_{a_b}p_{\mu}} c_1 (1 - c_1)$, where $c_1 = (1 - p_d) e^{-(1-t_{a_b})p/2}$. The gains $Q_{0_x}^{M_i}$ and $Q_{1_x}^{M_i}$ of the nonclassical states $|0_x\rangle$ on the monitoring line are $Q_{0_x}^{M_0} = \frac{2}{N^2} (1 - p_d)^3 (1 - c_1) e^{-((1-t_{a_b})p/2) c_2 + e^{-(1-t_{a_b})p/2} c_3}$ and $Q_{1_x}^{M_0} = \frac{2}{N^2} (1 - p_d)^2 c_1 e^{(1-t_{a_b})p/2} [c_4 - (1 - p_d) c_2] + c_3 (1 - c_1)$, where the parameters $c_2 = e^{(1-t_{a_b})p(1-n)/2} + e^{-(1-t_{a_b})p(1-n)/2}$, $c_3 = e^{(1-t_{a_b})p - e^{(1-t_{a_b})p}}$ and $c_4 = e^{(1-t_{a_b})p/2} + e^{-(1-t_{a_b})p/2}$.

In the COW protocol, because the nonclassical state $|0_x\rangle$ cannot be acquired, we cannot directly estimate the gain $Q_{0_x}^{M_i} = \langle 0_x | \hat{M}^+_i \hat{M}_i | 0_x \rangle$. We express $|0_x\rangle$ using the states $|0, 0\rangle$, $|\alpha, \alpha\rangle$, and $|\beta, \beta\rangle$ as follows:

$$|0_x\rangle = \frac{e^{-\mu} |0, 0\rangle + |\alpha, \alpha\rangle - (1 - e^{-\mu}) |\beta, \beta\rangle}{\sqrt{2(1 + e^{-\mu})}},$$

(A2)

where the state $|\beta\rangle = (|\alpha\rangle - e^{-\mu/2} |0\rangle)/\sqrt{1 - e^{-\mu}}$ denotes the normalized non-vacuum part of the state $|\alpha\rangle$. The pairs of states $|0, 0\rangle$ and $|\alpha, \alpha\rangle$ correspond to decoy sequences sent by Alice. Thus, we can rewrite the gain $Q_{0_x}^{M_i}$ as

$$\langle 0_x | \hat{M}^+_i \hat{M}_i | 0_x \rangle = \sum_{i, k} s_i s_k \langle \phi_i | \hat{M}^+_i \hat{M}_i | \phi_k \rangle,$$

(A3)

where $\langle \phi_i | \hat{M}^+_i \hat{M}_i | \phi_k \rangle \leq |s_i s_k| \sqrt{\langle \hat{M}_i | \phi_i \rangle^2 \langle \hat{M}_i | \phi_k \rangle^2}$.

Appendix B: Security against coherent attacks

Here, we extend the security of COW-QKD against coherent attacks. We consider a process in which a pair of states is sent at two time points, $2k - 1$ and $2k$ ($k = 1, 2, \ldots, K$) as one round, and the entire process of the COW protocol is performed by repeating this
round \( K \) times. Following a similar security analysis as in the main text, we assume an equivalent prepare-and-measure nonclassical protocol. Let the Kraus operator \( \mathcal{M}_i^l \) correspond to the announcement of detector \( D_M \) associated with the \( l \)-th round \((l = 1, 2, \ldots, K)\). We denote the probability of the event that Alice decides to send the nonclassical optical mode \( |0_x\rangle \) as \( p_{0_x} \). For any arbitrary small quantity \( \epsilon \geq 0 \), according to Azuma’s inequality, we have that

\[
\left| \sum_{i=1}^{K} p_{0_x} Q_{0_x}^{l,M_i} - N_{0_x}^{l,M_i} \right| < \epsilon |K| \tag{B1}
\]

holds, except for the minuscule probability, \( 2e^{-K\epsilon^2/2} \). Here, \( Q_{0_x}^{l,M_i} \) corresponds to the probability that the nonclassical optical mode \( |0_x\rangle \) is detected by the detector \( D_M \) on the monitoring line associated with the \( l \)-th round. \( N_{0_x}^{l,M_i} \), as an observed quantity, is the actual number of events that the nonclassical optical mode \( |0_x\rangle \) sent by Alice is detected by the detector \( D_M \) on the monitoring line. When \( K \) tends to infinity in the asymptotic limit, we can deduce from Eq. \( \tag{B1} \) that

\[
\frac{N_{0_x}^{l,M_i}}{K} \approx \frac{\sum_{l=1}^{K} p_{0_x} Q_{0_x}^{l,M_i}}{K} \tag{B2}
\]

Here, \( Q_{0_x}^{l,M_i} \) satisfies Eq. \( \tag{A5} \), and all gains of the COW-QKD protocol in Eq. \( \tag{A5} \) are associated with the \( l \)-th round (which corresponds to the condition of the security proof against collective attacks). Combining this result with the upper bound on the phase error rate derived from Eq. \( \tag{7} \) in the main text, we find that the estimation result of the phase error rate is consistent in the asymptotic limit when considering collective and coherent attacks. Thus, the asymptotic security of COW-QKD against coherent attacks is proven.

[1] C. H. Bennett and G. Brassard, in Proceedings of the Conference on Computers, Systems and Signal Processing (IEEE Press, New York, 1984), p. 175.
[2] A. K. Ekert, Phys. Rev. Lett. 67, 661 (1991).
[3] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. 81, 1301 (2009).
[4] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Rev. Mod. Phys. 92, 025002 (2020).
[5] S. Pirandola, U. L. Andersen, L. Banchi, M. Bertani, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, et al., Adv. Opt. Photon. 12, 1012 (2020).
[6] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics 4, 686 (2010).
[7] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. 108, 130503 (2012).
[8] S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. 108, 130502 (2012).
[9] Y.-H. Zhou, Z.-W. Yu, and X.-B. Wang, Phys. Rev. A 93, 042324 (2016).
[10] 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, et al., Phys. Rev. Lett. 117, 190501 (2016).
[11] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Nature 557, 400 (2018).
[12] X. Ma, F. Zeng, and H. Zhou, Phys. Rev. X 8, 031043 (2018).
[13] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, Phys. Rev. A 98, 062323 (2018).
[14] J. Lin and N. Lütkenhaus, Phys. Rev. A 98, 042332 (2018).
[15] H.-L. Yin and Y. Fu, Sci. Rep. 9, 3045 (2019).
[16] M. Curty, K. Azuma, and H.-K. Lo, npj Quantum Inf. 5, 64 (2019).
[17] C. Cui, Z.-Q. Yin, R. Wang, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, Phys. Rev. Applied 11, 034053 (2019).
[18] H.-L. Yin and Z.-B. Chen, Sci. Rep. 9, 14918 (2019).
[19] M. Minder, M. Pittaluga, G. Roberts, M. Lucamarini, J. Dynes, Z. Yuan, and A. Shields, Nat. Photonics 13, 334 (2019).
[20] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. 85, 1330 (2000).
[21] W.-Y. Hwang, Phys. Rev. Lett. 91, 057901 (2003).
[22] X.-B. Wang, Phys. Rev. Lett. 94, 230503 (2005).
[23] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. 94, 230504 (2005).
[24] M. Koashi, Phys. Rev. Lett. 93, 120501 (2004).
[25] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, Phys. Rev. Lett. 92, 057901 (2004).
[26] K. Tamaki and H.-K. Lo, Phys. Rev. A 73, 010302 (2006).
[27] H.-L. Yin, Y. Fu, Y. Mao, and Z.-B. Chen, Sci. Rep. 6, 29482 (2016).
[28] K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. 89, 037902 (2002).
[29] K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. A 68, 022317 (2003).
[30] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, Appl. Phys. Lett. 87, 194108 (2005).
[31] T. Sasaki, Y. Yamamoto, and M. Koashi, Nature 509, 475 (2014).
[32] D. Stucki, C. Barreiro, S. Fasel, J.-D. Gautier, O. Gay, N. Gisin, R. Thew, Y. Thoma, P. Trinkler, F. Vannel, et al., Opt. Express 17, 13326 (2009).
[33] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. Towery, and S. Ten, New J. Phys. 11, 075003 (2009).
[34] N. Walenta, A. Burg, D. Caselunghe, J. Constantin, N. Gisin, O. Guinnard, R. Houlmann, P. Junod, B. Korzh, N. Kulesza, et al., New J. Phys. 16, 013047 (2014).
[35] B. Korzh, C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, Nat. Photonics 9, 163 (2015).
[36] P. Silson, C. Erven, M. Godfrey, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan, et al., Nat. Commun. 8, 2041 (2017).
