Unconditionally secure key distribution without quantum channel

Hua-Lei Yin[1, *]

[1] *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

(Dated: August 27, 2024)

Key distribution plays a fundamental role in cryptography [1–4]. Currently, the quantum scheme [5, 6] stands as the only known method for achieving unconditionally secure key distribution. This method has been demonstrated over distances of 508 and 1002 kilometers in the measurement-device-independent [7] and twin-field [8] configurations, respectively. However, quantum key distribution faces transmission distance issues [9] and numerous side channel attacks [10] since the basic physical picture requires the use of quantum channels between users [10–13]. Even when quantum repeater [14] and quantum constellation [15] are used, commercializing quantum cryptography on a large scale remains unattainable due to the considerable expense and significant technical hurdles associated with establishing a global quantum network and facilitating mobile quantum communication. Here, by discovering the provable quantum one-way function, we propose another key distribution scheme with unconditional security, named probability key distribution, that promises users between any two distances to generate a fixed and high secret key rate. There are no quantum channels for exchanging quantum signals between two legitimate users. Non-local entangled states can be generated, identified and measured in the equivalent virtual protocol and can be used to extract secret keys. We anticipate that this discovery presents a paradigm shift in achieving unconditionally secure cryptography, thereby facilitating its widespread application on a global scale.

Cryptography ensures the secure confidentiality, integrity, authenticity, and non-repudiation during data processing [1–4]. Modern cryptography ensures security through keys rather than unknown cryptosystems. How to distribute secret keys in the presence of an eavesdropper Eve is known as the key distribution problem. The holy grail of key distribution is unconditional security, also called information-theoretic security. To present our protocol, we outline several typical key distribution schemes in Table I. Presently, public-key cryptography [1] is the most extensively adopted and efficacious scheme, primarily due to its efficiency and no requirement on a physical channel. Unfortunately, public-key cryptography is very vulnerable to quantum computing [16]. Recently, post-quantum cryptography has been proposed to replace public-key cryptography by introducing greater mathematical complexity [17]. However, this approach can only resist some known quantum attacks and cannot ensure security against future advanced algorithms [18]. An alternative approach to resolving the key distribution predicament involves using physical laws, such as chaos key distribution [19, 20], optical (quantum) stream cipher [21], and quantum key distribution [5, 6]. These physics-based key distribution schemes require physics channels to exchange physics signals. Consequently, the key rate and transmission distance are limited by channel loss, and side channel attacks via physics channels are inevitable.

Quantum key distribution has garnered significant attentionand advancementdue to its exclusive capability to ensure unconditional security through rigorous theoretical analysis [10–13]. For instance, a space-to-ground quantum network spanning 4600 kilometers has been successfully demonstrated leveraging a quantum satellite [22]. Since the inception of the initial quantum protocol by Bennett and Brassard in 1984 [23], the ingrained physical picture involves two distant users, Alice and Bob, engaging a quantum channel for the exchange of quantum signals [10–13]. Loosely speaking, in an actual protocol or at least an equivalent virtual protocol, quantum entanglement will establish between Alice and Bob through the exchange of quantum signals. Subsequently, this entanglement serves as the foundational resource for Alice and Bob to distill a secure key via quantum laws. Owing to the inevitable loss in the quantum channel, the secret key rate are limited by the capacity of the quantum channel, such as the repeaterless bound [24, 25] and the repeater-assisted bound [26]. Envisioning a prospective global quantum communication network involves interlinking ground-based nodes via quantum repeater [14] and connecting satellite-ground and inter-satellite nodes through a quantum constellation [15]. However, quantum repeaters, for example, require a combination of efficient and high-fidelity quantum memories, gate operations, and measurements, remain an outstanding challenge. Quantum constellations not only have security compromises but also require extremely high technical difficulty and substantial financial investment.

Non-local entangled state generation

The key distribution scheme delineated herein not only pledges unconditional security but also obviates the ne-

TABLE I. A comparison of several typical key distribution schemes.

Scheme	Fundamental laws	Physics channel	Key rate	Unconditional security
Public-key cryptography	Computation complexity	No	Low	No
Post-quantum cryptography	Computation complexity	No	Low	No
Chaos key distribution	Chaos synchronization	Yes	High	No
Optical stream cipher	Semi-classical physics	Yes	High	No
Quantum key distribution	Quantum physics	Yes	Low	Yes
Probability key distribution	Probability theory and quantum physics	No	High	Yes

cessity for a physical (quantum) channel. It promises Alice and Bob in establishing a consistent and high secret key rate irrespective of distance. Prior to the specific introduction of our probability key distribution (PKD) protocol, we initially elucidate the generation of non-local entangled states, depicted in Fig. 1a. The utilization of the Hadamard gate and controlled-phase gate generates an entangled state $\frac{1}{\sqrt{2}}\left(|+z\rangle|\sqrt{\mu}e^{\mathbf{i}\theta}\rangle+|-z\rangle|-\sqrt{\mu}e^{\mathbf{i}\theta}\rangle\right)$ between the qubit and optical pulse, wherein $|\pm z\rangle$ represents the eigenstates of the Z basis. Considering the case of continuous phase randomization, the joint density matrix $\hat{\rho}$ of Alice's and Bob's systems is a mixture of states $\hat{\rho}_k$ (see Methods). Qubit systems A and B are entangled, and there is no phase shift error for each photon number k. Evidently, the virtual entangled state is nonlocally generated as both Alice and Bob possess identical and confidential random phase information. Leveraging the virtual entangled state enables Alice and Bob to extract a secret key. Now, we will elucidate how Alice and Bob can continuously exchange secret phase information θ with unconditional security by employing the following two pivotal observations.

Provable quantum one-way function

First observation: The process of generating the discrete phase-randomized weak coherent state through a random mapping rule is the provable quantum one-way function if the phase number is sufficiently large and the optical intensity remains low. Let us define our provable *quantum one-way function*, which can be regarded as the quantum version of a one-way function [3] and has rigorous one-wayness. A quantum function $qf:\vec{x}\in\{0,1\}^l\rightarrow|\phi_j(\vec{x})\rangle$ is called provable quantum one-way if the following two conditions hold: 1) easy to evaluate, enabling the generation of a quantum state $|\phi_j(\vec{x})\rangle$ in polynomial time corresponding to the input bit string $\vec{x}$; 2) *unable to invert*, preventing the derivation of any meaningful information about the bit string $\vec{x}$ from the received quantum state (Note that the received quantum state should be regarded as the mixture state instead of pure state $|\phi_j(\vec{x})\rangle$ due to missing information $\vec{x}$).

The continuous phase-randomized weak coherent state can be seen as a mixture of photon-number states [27]

$$\int_0^{2\pi}\frac{d\theta}{2\pi}|\sqrt{\mu}e^{\mathbf{i}\theta}\rangle\langle\sqrt{\mu}e^{\mathbf{i}\theta}|=\sum_{k=0}^{\infty}e^{-\mu}\frac{\mu^k}{k!}|k\rangle\langle k|,\qquad(1)$$

if Eve is not known about the phase θ of each coherent state. From the view of the right-hand side of Eq. (1), the process of generating the continuous phase-randomized coherent state is a provable quantum one-way function, where the photon number state hides the global phase information θ. The main reasons are that there are quantum fluctuations for quadrature operators of the coherent state in phase space, as shown in Fig. 1b. The phase-probability distributions of the coherent state $|\sqrt{\mu}e^{\mathbf{i}\theta}\rangle$ are shown in Figs. 1c and 1d with different intensities μ and phases θ, respectively. Measuring the phase of a continuous phase-randomized coherent state equates to measuring the Poisson-distributed mixture of the photon number state (see Methods).

The continuous phase randomization scenarios entail an infinite number of global phases. However, it is essential to consider discrete phase randomization, where one has m global phases and $\theta\in 0,2\pi/m,4\pi/m,\ldots,2\pi(m-1)/m$. We must note the important difference between the continuous and discrete phase-randomized cases. As demonstrated in Fig 1e, mapping a global phase needs $|\vec{x}|=\log_2 m=10$ bits if $m=1024$. In the traditional mapping rule, the first bits of $\vec{x}$ are always 0 and 1 for $\theta\in[0,\pi)$ and $\theta\in[\pi,2\pi)$, respectively. Noteworthy is the non-uniform phase-probability distribution of the coherent state ($\mu\neq 0$), as depicted in Fig 1c. Eve can directly deduce, with high probability, the values of the first bit as 0 and 1 when the measured global phase corresponds to $\pi/2$ and $3\pi/2$, respectively. Consequently, the discrete phase-randomized coherent state even with $m=1024$ is not a rigorous quantum one-way function if the traditional mapping rule is utilized. Note that this will become the rigorous quantum one-way function if $m\rightarrow\infty$ because a few bits of information is no meaning for an infinitely long bit string $|\vec{x}|=\log_2 m\rightarrow\infty$. Here, we eliminate the probability difference of the bit value by exploiting the *random mapping* rule, as shown in Fig. 1f.

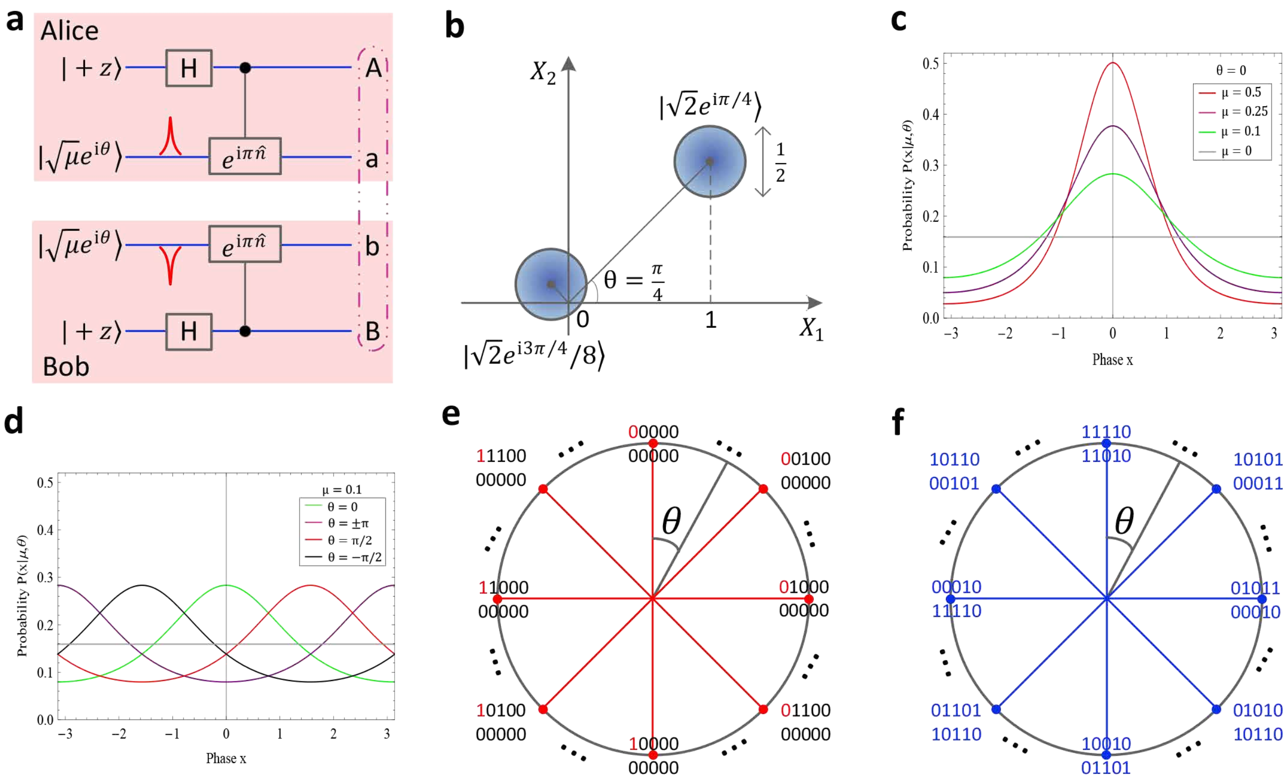


FIG. 1. **Basic idea behind non-local entangled state generation.** **a**, Alice (Bob) exploits a Hadamard gate to qubit A (B) and a controlled-phase gate $|{+z}\rangle\langle{+z}| \otimes \hat{\mathbf{I}} + |{-z}\rangle\langle{-z}| \otimes e^{\mathbf{i}\pi\hat{n}}$ to qubit A (B) as a control and optical pulse a (b) as a target. If the global phase θ of Alice's and Bob's optical pulses are identical and randomized, qubit A and qubit B will be entangled from the view of Eve. **b**, Fluctuations of the quadrature operators $\hat{X}_1 = (\hat{a}^\dagger + \hat{a})/2$ and $\hat{X}_2 = \mathbf{i}(\hat{a}^\dagger - \hat{a})/2$ of the coherent state in phase space. This means that given a coherent state, the measured phase will fluctuate. **c**, **d**, Phase-probability distributions of coherent states with different intensities and global phases. It is clearly observed that the higher the intensity of the coherent state is, the smaller the variance of the phase. The gray line represents the vacuum state where the phase is uniformly random and the probability is equal to $\frac{1}{2\pi}$. **e**, Traditional mapping rule, where Eve knows the mapping rule and is fixed in all sessions. The global phase is directly generated according to the value of the 10-bit string $\vec{x}$, i.e., $\theta = 2\pi j/1024$, where j is the decimal value of the 10-bit string $\vec{x}$. The 10-bit $\vec{x} = 1111011010$ ($j = 986$) corresponds to the $\theta = 2\pi \times 986/1024$ phase in all the sessions. **f**, Random mapping rule in one session, where Eve has no knowledge of the mapping rule and is changed in each session. The 10-bit $\vec{x} = 1111011010$ corresponds to phase $\theta = 0$ in this special session.

The phase $\theta = 0$ does not just correspond to only one 10-bit string $\vec{x} = 0000000000$ anymore but to all 1024 feasible 10-bit strings $\vec{x} \in \{0,1\}^{10}$. Each global phase uniformly and randomly correlates with all possible 10-bit strings. Hence, under the random mapping rule, Eve can not steal any information of $\vec{x}$ even he has the discrete phase-randomized weak coherent state (details see Supplementary Information).

Random information negotiation

Second observation: Alice and Bob can share themselves-generated quantum random numbers in many communication rounds with unconditional security via a fixed but long secret key and a per-update but short secret key if these quantum random numbers are not leaked to Eve when they are used. Let us define the unconditional security of a communication round where Alice and Bob transmit ciphertext to share plaintext via key and algorithm over an authentic channel. We call the communication round unconditionally secure when Eve cannot steal any plaintext information even if she uses unlimited computational resources. To elaborate, Eve can merely guess the plaintext at random; even if she guessed the plaintext correctly, she could not find any difference between the correct plaintext and the other wrong plaintext.

For an encryption system, it has been proven that one-time pad can provide unconditional security [28], where the ciphertext $\vec{c}$ is the XOR value between the plaintext $\vec{m}$ and the key $\vec{k}$, i.e., $\vec{c} = \vec{m} \oplus \vec{k}$. For one-time pad, the key $\vec{k}$ should be completely random and up-dated in each round (i.e., one key can only used once) while there is no any requirement on the plaintext for different rounds [2]. Here we exchange the above requirements of the key and plaintext in our random information negotiation. Let plaintext be a quantum random number $\vec{r}$, which is completely random and up-dated in different round. Let key $\vec{d}$ is generated by using a fixed but long secret key $\vec{K}_{\text{fix}}$ and a up-date but short secret key $\vec{K}_{\text{upd}}$ in each round. The length of the fixed secret key $\vec{K}_{\text{fix}}$ can not be shorter than $|\vec{d}|$, which ensures that the generated key $\vec{d}$ is completely random in the first round. Then Alice and Bob utilize the generated key $\vec{d}$ to share the quantum random number $\vec{r}$ via XOR algorithm $\vec{c} = \vec{r} \oplus \vec{d}$. If we can ensure that the used quantum random number $\vec{r}$ does not leak any information to Eve (it is true in provable quantum one-way function), who can only implement ciphertext-only attack and no other plaintext-dependent attacks. Therefore, the shared quantum random number $\vec{r}$ and key $\vec{d}$ (as well as key $\vec{K}_{\text{fix}}$) are all unknown to Eve in the first communication round since observation of the ciphertext provides no plaintext information whatsoever to Eve. Based on this, Alice and Bob can repeat the above process in many communication rounds, where the unconditional security is always maintain even key $\vec{K}_{\text{fix}}$ is reused (see Supplementary Information for detail).

Probability key distribution protocol

Based on the above two observations, we propose our actual PKD protocol, as shown in Fig. 2a. The fixed but long secret key $\vec{K}_{\text{fix}}$ is reused many times before it is discarded. Alice and Bob exploit $\vec{K}_{\text{fix}} \in \{0,1\}^{s+t-1}$ to build the Toeplitz matrix $\mathbf{H}_{st}$ with s rows and t columns. The per-update but short secret key $\vec{K} \in \{0,1\}^{s}$ will change in each PKD session. For each PKD session, five steps were performed as follows.

(i) Alice prepares weak coherent state optical pulse pairs (signal pulse and reference pulse) $|\sqrt{\mu}e^{\mathrm{i}\varphi_a}\rangle_a \otimes |\sqrt{\mu}\rangle_a$, where μ is the intensity of each pulse and $\varphi_a = \theta_a + r_a\pi$ is the phase of the signal pulse. $r_a \in \{0,1\}$ is the random bit value. The random global phase $\theta_a \in \{0, 2\pi/m, 4\pi/m, \ldots, 2\pi(m-1)/m\}$ is determined by the quantum random number string $\vec{x}_a \in \{0,1\}^{\log_2 m}$. There are m global phases and each $\log_2 m$-bit map to a global phase. Bob does the same. Instead of the fixed mapping rule, the global phase is determined by random mapping. The random mapping rule is shared between Alice and Bob through one-time pad by consuming $m \log_2 m$ bits of the pre-shared secret key. They repeat step (i) for N rounds. (ii) Alice performs single-photon interference measurement for the prepared pulse pairs. If and only if one of detectors D_{aL} and D_{aR} clicks represents a successful detection event. Alice keeps r_a as the raw key and announces the successful detection event and the corresponding detector when there is a successful detection event. Bob does the same. The numbers of successful detection events for Alice and Bob are both n for one PKD session. (iii) Alice and Bob obtain the data string $\vec{D} = \vec{K}_{\text{upd}} \cdot \mathbf{H}_{st}$, where $\vec{D}$ has t bits and $t \geq n \log_2 m$. Let the first $n \log_2 m$ bits in $\vec{D}$ constitute the data string $\vec{D}_n$. For n successful detection events of Alice, let $\vec{R}_n(\vec{x}_a) \in \{0,1\}^{n \log_2 m}$ be the random bit string corresponding to Alice's global phases. Alice sends ciphertext $\vec{R}_n(\vec{x}_a) \oplus \vec{D}_n$ to Bob, who decrypts ciphertext with data string $\vec{D}_n$ to obtain quantum random numbers $\vec{R}_n(\vec{x}_a)$ and thus acquires the global phase of Alice θ_a according to the above random mapping rule. According to the phase θ_a of each event, Bob rearranges his raw key and detector click order to ensure that $\theta_b = \theta_a$. If $\{D_{aL}, D_{bR}\}$ or $\{D_{aR}, D_{bL}\}$ click, Bob flips his raw key bit. Finally, Alice and Bob obtain the raw key strings $\vec{Z}_a$ and $\vec{Z}_b$, respectively. (iv) Bob acquires an estimation $\hat{\vec{Z}}_b$ of $\vec{Z}_a$ in the error correction scheme by revealing at most λ bits of information. Then, Alice and Bob perform an error verification to ensure identical keys by publishing $\log_2(2/\varepsilon_{\text{cor}})$-bit [29, 30]. (v) Alice and Bob perform privacy amplification by applying a random universal$_2$ hash function [31] to extract length ℓ bits of secret key.

Note that the sharing $\vec{R}_n(\vec{x}_a)$ scheme in step (iii) is a special way in our random information negotiation. For the actual protocol, the global phase of the reference pulse can be known to Eve. Thus, Alice (Bob) can utilize another laser to prepare the reference pulse with zero phase and performs the single-photon interference measurement, which can be called the prepare-and-measure virtual protocol 1, as shown in Fig. 2b. Furthermore, the entanglement-based virtual protocol 2 in Fig. 2c is equivalent to the prepare-and-measure virtual protocol 1. The phase error of the joint qubit system of Alice and Bob is always zero (see Methods).

The PKD protocol is ε_{sec}-secret and ε_{cor}-correct if the secret key length of one session is satisfied (see the Supplementary Information).

$$\ell \leq n - \lambda - \log_2 \frac{2}{\varepsilon_{\text{cor}}} - 2\log_2 \frac{3}{2\varepsilon_{\text{sec}}}, \tag{2}$$

where the leaked information is $\lambda = nfh(E)$ due to error correction. The Shannon entropy function is $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$. $E \approx 25\%$ and $f = 1.05$ are the bit error rate and the error correction efficiency, respectively. Here, we can set the intensity $\mu = 0.1$, the phase number $m = 1024$, the detection efficiency $\eta_d = 0.8$, the dark count rate $p_d = 10^{-8}$, $\varepsilon_{\text{cor}} = 10^{-15}$ and $\varepsilon_{\text{sec}} = 10^{-10}$. Considering a gigahertz system and $N = 10^9$ for one second in one PKD session, the net remaining secret key rate is $R = \ell - s - m\log_2 m \approx 20$ Mbps if we ignore the reused secret key string $\vec{K}_{\text{fix}}$ and let $|\vec{K}_{\text{upd}}| = s = 10^4$.

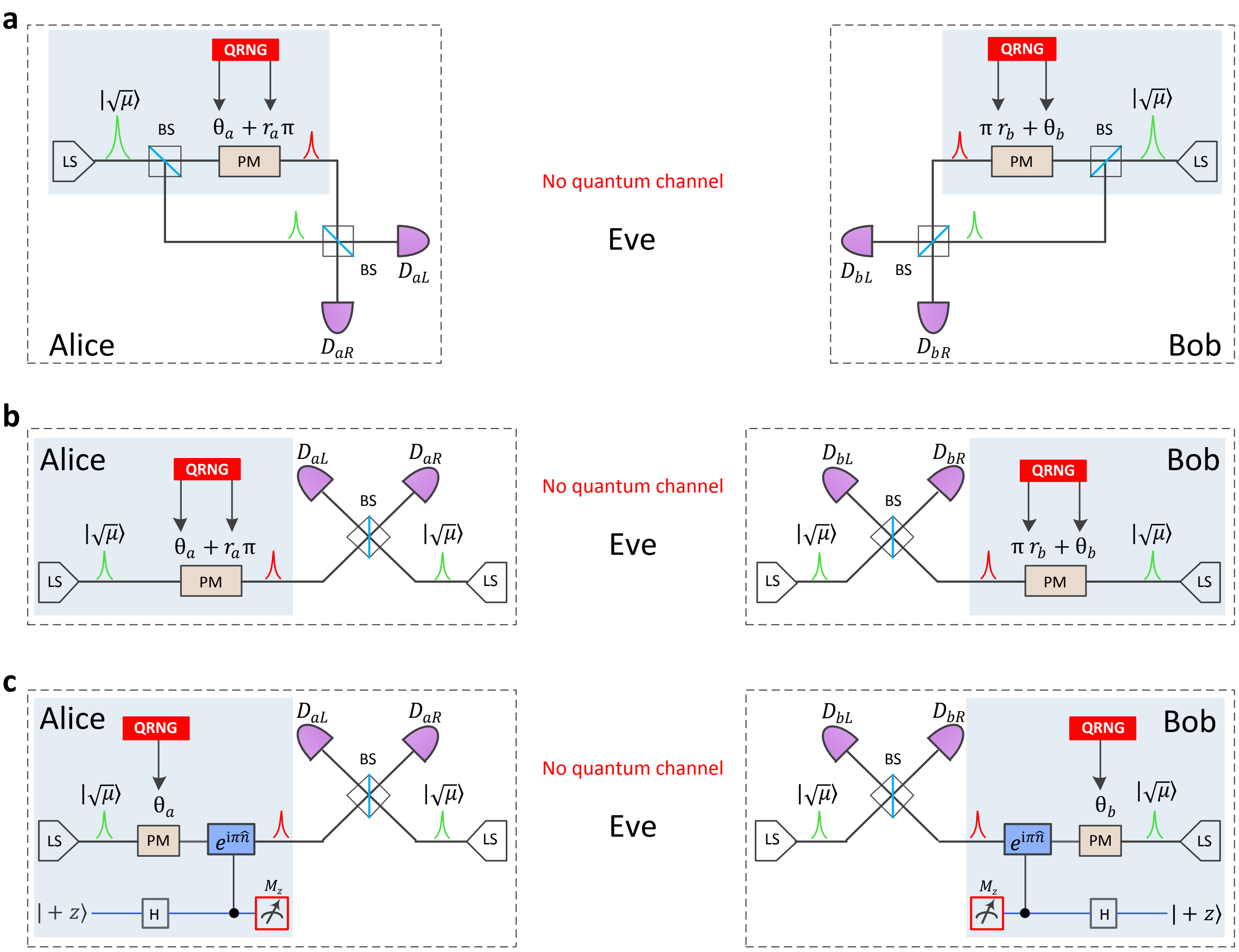


FIG. 2. **Optical realization of the PKD protocol.** **a**, Actual protocol: Alice (Bob) exploits a laser (LS) and a beam splitter (BS) to generate optical pulse pairs (called the signal pulse and reference pulse, respectively). She (he) utilizes a phase modulator (PM) to modulate the phase of the signal pulse $\theta_a + r_a\pi$ $(\theta_b + r_b\pi)$, where θ_a (θ_b) are random global phases and r_a, r_b are binary random numbers generated by quantum random number generation (QRNG). Then, Alice (Bob) performs single-photon interference measurements for the pulse pairs through a BS and two detectors, D_{aL} and D_{aR} (D_{bL} and D_{bR}, respectively). **b**, Virtual protocol 1: Alice (Bob) exploits one laser to prepare the signal pulse and another laser to generate the reference pulse. **c**, Virtual protocol 2: Alice (Bob) generates an entangled state between the qubit and optical modes instead of an signal pulse. Alice and Bob measure their qubit to obtain the raw key by using the Z basis after they announce the successful detection event.

Conclusion and discussion

Overall, we have proven the unconditional security of PKD by introducing the concepts of a rigorous quantum one-way function and random information negotiation. Our proposal allows any two distant users to extract secure keys at a high-speed rate as long as they can pre-share some of the secret keys. Based on the random mapping rule, our provable quantum one-way function does not reveal even a single bit information to Eve, which is completely different from the previous definition of the quantum one-way function [32]. We remark that our random information negotiation is not an encryption scheme since the communication data between Alice and Bob are quantum random numbers (generated by only Alice and Bob themselves) rather than messages. Moreover, shared quantum random numbers cannot be used as keys for encrypting another message. Otherwise, quantum random numbers could potentially be leaked to Eve, which leads to our random information negotiation that is not secure. Fortunately, shared quantum random numbers can be used to map the global phase of the coherent state when one constructs the quantum one-way function. These quantum random numbers do not leak to Eve due to the rigorous one-wayness inherent in our provable quantum one-way function.

The existence of classical one-way functions remains an unresolved inquiry. Should they exist, this can resolve the paramount unsolved query within theoretical computer science, namely, the complexity classes P and NP are distinct [3]. We have proven that the phase-randomized weak coherent state with a random mapping rule is a provable quantum one-way function with rigorous one-wayness. This function safeguards the phase information within quantum states, rendering it unrecoverable by Eve. As an example, we utilized this provable quantum one-way function to propose an unconditionally secure key distribution scheme. We expect that our quantum one-way function will be widely used to construct information-theoretically secure privacy protection protocols, such as quantum zero-knowledge proof and quantum secure multiparty computation. Actually, the steps required to prepare and measure quantum state within our PKD protocol are unnecessary and it will greatly simplify the cost and increase the bit rate, which will be discussed in our next work.

METHODS

Joint density matrix

For continuous phase randomization, the joint density matrix (including qubit systems A, B and optical modes a, b) is $\hat{\rho}=\sum_{k=0}^{\infty}\frac{e^{-2\mu}(2\mu)^k}{k!}\hat{\rho}_k$, where the state $\hat{\rho}_k$ can be given by

$$\begin{cases} \hat{P}\left(\frac{|\phi^-\rangle_{AB}|+\rangle_{ab}^{\otimes k}+|\psi^-\rangle_{AB}|-\rangle_{ab}^{\otimes k}}{\sqrt{2}}\right), & \text{if } k \text{ is odd,} \\ \hat{P}\left(\frac{|\phi^+\rangle_{AB}|+\rangle_{ab}^{\otimes k}+|\psi^+\rangle_{AB}|-\rangle_{ab}^{\otimes k}}{\sqrt{2}}\right), & \text{if } k \text{ is even.} \end{cases} \tag{3}$$

Let $\hat{P}(|x\rangle)=|x\rangle\langle x|$, states $|\phi^{\pm}\rangle=\frac{1}{\sqrt{2}}(|+z\rangle|+z\rangle\pm|-z\rangle|-z\rangle)$ and $|\psi^{\pm}\rangle=\frac{1}{\sqrt{2}}(|+z\rangle|-z\rangle\pm|-z\rangle|+z\rangle)$ be four Bell states. States $|\pm\rangle_{ab}=\frac{1}{\sqrt{2}}(|10\rangle_{ab}\pm|01\rangle_{ab})=\frac{\hat{a}^{\dagger}\pm\hat{b}^{\dagger}}{\sqrt{2}}|00\rangle_{ab}$ is a superposition single-photon state with a and b modes. $|\pm\rangle_{ab}^{\otimes k}=\frac{1}{\sqrt{2^k k!}}\left(\hat{a}^{\dagger}\pm\hat{b}^{\dagger}\right)^k|00\rangle_{ab}$ is the k-photon state, i.e., k identical photons with state $|\pm\rangle_{ab}$.

For the case of discrete phase randomization, the initial joint density matrix of Alice's and Bob's can be written as

$$\hat{\rho}^{\text{dis}}(m)=\sum_{k=0}^{m-1}P_m^{2\mu}(k)\hat{\rho}_{\lambda_k}, \tag{4}$$

which is the mixture of states $\hat{\rho}_{\lambda_k}$ with probability $P_m^{2\mu}(k)=e^{-2\mu}\sum_{l=0}^{\infty}\frac{(2\mu)^{lm+k}}{(lm+k)!}$. The density matrix of $\hat{\rho}_{\lambda_k}$ can be given by

$$\begin{cases} \hat{P}\left(\frac{|\phi^-\rangle_{AB}|\lambda_k^+\rangle_{ab}+|\psi^-\rangle_{AB}|\lambda_k^-\rangle_{ab}}{\sqrt{2}}\right), & \text{if } k \text{ is odd,} \\ \hat{P}\left(\frac{|\phi^+\rangle_{AB}|\lambda_k^+\rangle_{ab}+|\psi^+\rangle_{AB}|\lambda_k^-\rangle_{ab}}{\sqrt{2}}\right), & \text{if } k \text{ is even,} \end{cases} \tag{5}$$

where the quantum state $|\lambda_k^{\pm}\rangle_{ab}$ is denoted as

$$|\lambda_k^{\pm}\rangle_{ab}=\frac{e^{-\mu}}{\sqrt{P_m^{2\mu}(k)}}\sum_{l=0}^{\infty}\frac{(\sqrt{2\mu})^{lm+k}}{\sqrt{(lm+k)!}}|\pm\rangle_{ab}^{\otimes lm+k}. \tag{6}$$

If the phase number m approaches infinity, the discrete phase randomization case will become a continuous case. According to Eqs. (3) and (5), two qubit systems A and B can only be in the subspace spanned by Bell state $|\phi^-\rangle$ and $|\psi^-\rangle$ ($|\phi^+\rangle$ and $|\phi^+\rangle$) if k is odd (even), no matter whether Eve performs any quantum measurements for optical modes a and b. Obviously, there may have bit error but not phase error when Alice and Bob measure the qubit systems A and B, respectively.

Quantum measurement

Given a coherent state with intensity μ and phase θ, there is a phase-probability distribution that can be written as [33, 34]

$$P(x|\mu,\theta)=\lim_{l\to\infty}\frac{1}{2\pi}\left|\sum_{k=0}^{l}e^{-\mathbf{i}(x-\theta)k}\frac{e^{-\mu/2}\mu^{k/2}}{\sqrt{k!}}\right|^2, \tag{7}$$

where $x\in[0,2\pi)$ represents the measured phase, $P(x|\mu,\theta)$ is the corresponding probability and $\int_0^{2\pi}P(x|\mu,\theta)dx=1$. The average probability of the measured phase x for a given uniformly distributed phase $\theta\in[0,2\pi)$ is

$$\frac{1}{2\pi}\int_0^{2\pi}P(x|\mu,\theta)d\theta\equiv\frac{1}{2\pi},\quad\forall\ \mu \text{ and } x, \tag{8}$$

which means that the measured phase x is completely random. If the intensity is zero (vacuum state), the phase-probability distribution is uniform, i.e., $P(x|\mu=0,\theta)=1/(2\pi)$. Actually, for all photon number states $|k\rangle$, the phase-probability distribution is uniform. Measuring the phase of a continuous phase-randomized coherent state is equivalent to measuring the mixture of the photon number state with the Poisson distribution.

For the discrete phase randomization $m=1024$ case, the average probability of the measured phase x can be given by

$$\frac{1}{1024}\sum_{j=0}^{1023}P\left(x|\mu=0.1,\theta=\frac{2\pi j}{1024}\right)\simeq\frac{1}{2\pi},\quad\forall\ x, \tag{9}$$

which is equivalent to the continuous phase randomization case with negligible difference in probability. The discrete phase-randomized coherent state can be written as a mixture of the pseudo photon-number state $|\lambda_k\rangle$ [35, 36]

$$\frac{1}{m}\sum_{j=0}^{m-1}|\sqrt{\mu}e^{\mathbf{i}\frac{2\pi j}{m}}\rangle\langle\sqrt{\mu}e^{\mathbf{i}\frac{2\pi j}{m}}| = \sum_{k=0}^{m-1}P_m^{\mu}(k)|\lambda_k\rangle\langle\lambda_k|, \tag{10}$$

where one has probability $P_m^{\mu}(k) = e^{-\mu}\sum_{l=0}^{\infty}\frac{\mu^{lm+k}}{(lm+k)!}$ and state $|\lambda_k\rangle = \frac{e^{-\mu/2}}{\sqrt{P_m^{\mu}(k)}}\sum_{l=0}^{\infty}\frac{(\sqrt{\mu})^{lm+k}}{\sqrt{(lm+k)!}}|lm+k\rangle$. The discrete case will become the continuous case if $m \to \infty$, i.e., $\lim_{m\to\infty}|\lambda_k\rangle \equiv |k\rangle$ and $\lim_{m\to\infty}P_m^{\mu}(k) \equiv e^{-\mu}\mu^k/k!$. For a microcosmic coherent state and a sufficiently large m, the discrete case is almost identical to the continuous case. The trace distance between $|\lambda_k\rangle$ and $|k\rangle$ can be given by

$$\begin{aligned} D(|\lambda_k\rangle, |k\rangle) &= \frac{1}{2}\mathrm{tr}\big||\lambda_k\rangle\langle\lambda_k| - |k\rangle\langle k|\big| \\ &< \sqrt{\sum_{l=1}^{\infty}\frac{\mu^{lm}k!}{(lm+k)!}} \approx \sqrt{\mu^m/m!}. \end{aligned} \tag{11}$$

For a discrete phase-randomized coherent state, the optimum unambiguous state discrimination measurement probability can be written as [37, 38]

$$\begin{aligned} P_{\mathrm{USD}} &= \min_{r=0,1,\ldots,m-1}\sum_{j=0}^{m-1}e^{-\mathbf{i}2\pi jr/m}e^{\mu\left(e^{\mathbf{i}2\pi j/m}-1\right)} \\ &\approx \frac{m\mu^{m-1}}{(m-1)!}, \end{aligned} \tag{12}$$

where the second equation works if the intensity μ is small. If Eve implements the minimum error discrimination measurement, the minimum error probability is [39, 40]

$$P_{\min} = 1 - \frac{1}{m^2}\left|\sum_{r=0}^{m-1}\sqrt{\sum_{k=0}^{m-1}e^{-\mu(1-e^{\mathbf{i}2\pi k/m})+\mathbf{i}2\pi kr/m}}\right|^2. \tag{13}$$

For the case of intensity $\mu = 0.1$ and phase number $m = 1024$, the trace distance $D(|\lambda_k\rangle, |k\rangle) \approx \sqrt{\mu^m/m!} = 1.36 \times 10^{-1832}$. The optimum unambiguous state discrimination probability is $P_{\mathrm{USD}} \approx m\mu^{m-1}/(m-1)! = 1.94 \times 10^{-3657}$, which means that Eve cannot successfully implement an unambiguous state discrimination attack. The minimum error probability is $P_{\min} = 99.83\%$, which is approximately equal to the random guessing case in which the error probability is $1 - 1/m = 99.90\%$.

Acknowledgements

We gratefully acknowledge the support from the National Natural Science Foundation of China (No. 12274223).

* hlyin@ruc.edu.cn

[1] Menezes, A. J., van Oorschot, P. C. & Vanstone, S. A. *Handbook of applied cryptography* (CRC press, 1996).

[2] Stinson, D. R. *Cryptography: theory and practice* (CRC Press, 1995).

[3] Goldreich, O. *Foundations of Cryptography: Basic Techniques* (Cambridge University Press, 2001).

[4] Yin, H.-L. *et al.* Experimental quantum secure network with digital signatures and encryption. *Natl. Sci. Rev.* **10**, nwac228 (2023).

[5] Bennett, C. H. & Brassard, G. Quantum cryptography: public key distribution and coin tossing. *In Proc. Int. Conf. on Computers, Systems and Signal Processing* 175–179 (1984).

[6] Ekert, A. K. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.* **67**, 661–663 (1991).

[7] Zhou, L. *et al.* Experimental quantum communication overcomes the rate-loss limit without global phase tracking. *Phys. Rev. Lett.* **130**, 250801 (2023).

[8] Liu, Y. *et al.* Experimental twin-field quantum key distribution over 1000 km fiber distance. *Phys. Rev. Lett.* **130**, 210801 (2023).

[9] Diamanti, E., Lo, H.-K., Qi, B. & Yuan, Z. Practical challenges in quantum key distribution. *npj Quantum Inf.* **2**, 1–12 (2016).

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

[11] Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145–195 (2002).

[12] Scarani, V. *et al.* The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301 (2009).

[13] Portmann, C. & Renner, R. Security in quantum cryptography. *Rev. Mod. Phys.* **94**, 025008 (2022).

[14] Sangouard, N., Simon, C., de Riedmatten, H. & Gisin, N. Quantum repeaters based on atomic ensembles and linear optics. *Rev. Mod. Phys.* **83**, 33–80 (2011).

[15] Lu, C.-Y., Cao, Y., Peng, C.-Z. & Pan, J.-W. Micius quantum experiments in space. *Rev. Mod. Phys.* **94**, 035001 (2022).

[16] Shor, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review* **41**, 303–332 (1999).

[17] Bernstein, D. J. & Lange, T. Post-quantum cryptography. *Nature* **549**, 188–194 (2017).

[18] MATZOV. Report on the security of lwe: Improved dual lattice attack. *https://doi.org/10.5281/zenodo.6493704* (2022).

[19] Argyris, A. *et al.* Chaos-based communications at high bit rates using commercial fibre-optic links. *Nature* **438**, 343–346 (2005).

[20] Soriano, M. C., García-Ojalvo, J., Mirasso, C. R. & Fischer, I. Complex photonics: Dynamics and applications of delay-coupled semiconductors lasers. *Rev. Mod. Phys.* **85**, 421–470 (2013).

[21] Barbosa, G. A., Corndorf, E., Kumar, P. & Yuen, H. P. Secure communication using mesoscopic coherent states. *Phys. Rev. Lett.* **90**, 227901 (2003).

[22] Chen, Y.-A. *et al.* An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature* **589**, 214–219 (2021).

[23] Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing? *Theor. Comput. Sci.* **560**, 7–11 (2014).

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

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

[26] Pirandola, S. End-to-end capacities of a quantum communication network. *Commun. Phys.* **2**, 51 (2019).

[27] van Enk, S. J. & Fuchs, C. A. Quantum state of an ideal propagating laser field. *Phys. Rev. Lett.* **88**, 027902 (2001).

[28] Shannon, C. E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **28**, 656–715 (1949).

[29] Wegman, M. N. & Carter, J. L. New hash functions and their use in authentication and set equality. *J. Comput. Syst. Sci.* **22**, 265–279 (1981).

[30] Krawczyk, H. Lfsr-based hashing and authentication. In *Annual International Cryptology Conference*, 129–139 (Springer, 1994).

[31] Bennett, C. H., Brassard, G., Crépeau, C. & Maurer, U. M. Generalized privacy amplification. *IEEE Transactions on Information theory* **41**, 1915–1923 (1995).

[32] Buhrman, H., Cleve, R., Watrous, J. & De Wolf, R. Quantum fingerprinting. *Phys. Rev. Lett.* **87**, 167902 (2001).

[33] Pegg, D. T. & Barnett, S. M. Phase properties of the quantized single-mode electromagnetic field. *Phys. Rev. A* **39**, 1665–1675 (1989).

[34] Bužek, V., Wilson-Gordon, A. D., Knight, P. L. & Lai, W. K. Coherent states in a finite-dimensional basis: Their phase properties and relationship to coherent states of light. *Phys. Rev. A* **45**, 8079–8094 (1992).

[35] Cao, Z., Zhang, Z., Lo, H.-K. & Ma, X. Discrete-phase-randomized coherent state source and its application in quantum key distribution. *New J. Phy.* **17**, 053014 (2015).

[36] Shao, S.-F. *et al.* Phase-matching quantum key distribution without intensity modulation. *Phys. Rev. Appl.* **20**, 024046 (2023).

[37] Chefles, A. & Barnett, S. M. Optimum unambiguous discrimination between linearly independent symmetric states. *Phys. Lett. A* **250**, 223–229 (1998).

[38] Van Enk, S. Unambiguous state discrimination of coherent states with linear optics: Application to quantum cryptography. *Phys. Rev. A* **66**, 042313 (2002).

[39] Barnett, S. M. & Croke, S. Quantum state discrimination. *Adv. Opt. Photonics* **1**, 238–278 (2009).

[40] Wallden, P., Dunjko, V. & Andersson, E. Minimum-cost quantum measurements for quantum information. *J. Phys. A: Math. and Theor.* **47**, 125303 (2014).

Supplementary Information for "Unconditionally secure key distribution without quantum channel"

Hua-Lei Yin[1, *]

[1] *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*

(Dated: August 27, 2024)

I. REVIEW OF QUANTUM MEASUREMENTS

No quantum measurement can perfectly discriminate between non-orthogonal quantum states. Here, we first provide a brief review of two highly effective quantum measurements for m symmetric coherent states. The first is the optimal unambiguous state discrimination (USD) measurement [1, 2], and the second is the minimum error discrimination measurement [2, 3].

A. Unambiguous state discrimination

For N linearly independent pure state $\{|\psi_j\rangle\}$, $j = 0, 1, \ldots, N-1$, there is a positive operator-valued measure (POVM) $\{\hat{E}_j\}_{j=0}^{N}$ with $N+1$ elements that can realize unambiguous state discrimination measurement. These POVM elements can be given by [1]

$$\begin{cases} \hat{E}_j & = \frac{P_j}{|\langle\psi_j|\psi_j^{\perp}\rangle|^2}\left|\psi_j^{\perp}\right\rangle\left\langle\psi_j^{\perp}\right|, \quad \forall j = 0, 1, \ldots, N-1, \\ \\ \hat{E}_N & = \hat{E}_? = \hat{\mathbf{I}} - \sum_{j=0}^{N-1}\hat{E}_j, \end{cases} \tag{S1}$$

where $\hat{\mathbf{I}}$ is the unit operator and $\hat{E}_j \geq 0$ is the positive operator. Operator $\hat{E}_?$ leads to a failure of the state discrimination measurement. Thereinto, for all $i, j = 0, 1, \ldots, N-1$, we have

$$\begin{cases} \langle\psi_i|\hat{E}_j|\psi_i\rangle & = P_i\delta_{ij}, \\ \\ \langle\psi_i|\psi_j^{\perp}\rangle & = \langle\psi_j|\psi_j^{\perp}\rangle\delta_{ij}, \end{cases} \tag{S2}$$

where $\delta_{ij} = 1$ if $i = j$, otherwise, $\delta_{ij} = 0$. The result j is obtained only if the state is $|\psi_j\rangle$ and the probability of occurrence is $0 \leq P_j \leq 1$. The state $\left|\psi_j^{\perp}\right\rangle$ is orthogonal to all allowed states except for the state $|\psi_j\rangle$.

Considering that the prior probability of state $|\psi_j\rangle$ is p_j, thus the density matrix of the system is $\hat{\rho} = \sum_{j=0}^{N-1} p_j|\psi_j\rangle\langle\psi_j|$. The USD probability $P_{\rm USD}^{(N)}$ is defined as the total probability of correctly identifying the state,

$$\begin{aligned} P_{\rm USD}^{(N)} &= \sum_{j=0}^{N-1}\mathrm{tr}(\hat{E}_j\hat{\rho}) = \sum_{j=0}^{N-1} p_j\langle\psi_j|E_j|\psi_j\rangle \\ &= \sum_{j=0}^{N-1} p_j P_j. \end{aligned} \tag{S3}$$

One can implement unambiguous state discrimination measurements since m symmetric coherent states are linearly independent quantum states. For N symmetric coherent states $\left\{\left|\sqrt{\mu}e^{\mathbf{i}2\pi j/N}\right\rangle\right\}_{j=0}^{N-1}$ with a uniform priori probability $p_j = 1/N$, the optimal USD probability can be written as [1]

$$P_{\rm USD}^{(N)} = \min_{r=0,1,\ldots,N-1}\sum_{j=0}^{N-1} e^{-\mathbf{i}2\pi jr/N} e^{\mu\left(e^{\mathbf{i}2\pi j/N}-1\right)}. \tag{S4}$$

Considering the special case $N = 2$, the optimal probability $P^{(2)}_{\text{USD}} = \min\{1 + e^{-2\mu}, 1 - e^{-2\mu}\} = 1 - e^{-2\mu}$, which is identical to the analytical two pure-state conclusion [4] $P^{(2)}_{\text{USD}} = 1 - |\langle -\sqrt{\mu}|\sqrt{\mu}\rangle| = 1 - e^{-2\mu}$. Note that Eq. (S4) usually does not yield analytical results; we can only calculate them numerically. However, for small intensity μ, we can use an approximate analytical formula [5]

$$\begin{aligned} P^{(N)}_{\text{USD}} &= \min_{r=0,1,\ldots,N-1} \sum_{j=0}^{N-1} e^{-\mathbf{i}2\pi jr/N} e^{\mu\left(e^{\mathbf{i}2\pi j/N}-1\right)} \\ &\approx \frac{N\mu^{N-1}}{(N-1)!}. \end{aligned} \tag{S5}$$

B. Minimum error discrimination

For N possible states $\{\hat{\rho}_j\}_{j=0}^{N-1}$ with associated a priori probabilities $\{p_j\}_{j=0}^{N-1}$, there is a POVM $\{E_j\}_{j=0}^{N-1}$ with N elements that can achieve minimum error discrimination. The sufficient and necessary conditions of this POVM can be written as [2]

$$\begin{cases} \sum_{i=0}^{N-1} p_i\hat{\rho}_i\hat{E}_i - p_j\hat{\rho}_j & \geq 0, \quad \forall j = 0, 1, \ldots, N-1, \\ \hat{E}_i(p_i\hat{\rho}_i - p_j\hat{\rho}_j)\hat{E}_j & = 0, \quad \forall i, j = 0, 1, \ldots, N-1. \end{cases} \tag{S6}$$

Note that the two conditions are not independent; i.e., the second condition may be derived from the first condition. The minimum error discrimination probability is defined as

$$P_{\text{min}} = \sum_{j=0}^{N-1} p_j \sum_{i\neq j} \text{tr}(\hat{\rho}_j\hat{E}_i). \tag{S7}$$

For many cases, the minimum error discrimination measurement is the square-root measurement. In addition, there is an important conclusion for square-root measurements; i.e., for any set of pure states, there is at least one set of prior probabilities such that the minimum error discrimination measurement for this set of states is the square root measurement. The POVM elements of the square-root measurement can be given by [2]

$$\hat{E}_j = p_j\hat{\rho}^{-1/2}\hat{\rho}_j\hat{\rho}^{-1/2}, \tag{S8}$$

where $\hat{\rho} = \sum_{j=0}^{N-1} p_j\hat{\rho}_j$. Obviously, the above operator E_j is positive, and $\sum_{j=0}^{N-1}\hat{E}_j = \hat{\mathbf{I}}$. The square-root measurement is the minimum error discrimination measurement for symmetric coherent states. Considering N symmetric coherent states $\left\{|\psi_j\rangle = \left|\sqrt{\mu}e^{\mathbf{i}2\pi j/N}\right\rangle\right\}_{j=0}^{N-1}$ with a uniform priori probability of $p_j = 1/N$. The Gram matrix of the states we are trying to distinguish between is an $N \times N$ matrix, where the matrix element $G_{i,j}$ of the i-th row and j-th column can be defined as

$$\begin{aligned} G_{i,j} &= \langle\psi_i|\psi_j\rangle = \langle\sqrt{\mu}e^{\mathbf{i}2\pi i/N}|\sqrt{\mu}e^{\mathbf{i}2\pi j/N}\rangle \\ &= e^{-\mu\left[1-e^{\mathbf{i}2\pi(j-i)/N}\right]}, \end{aligned} \tag{S9}$$

where $i, j = 0, 1, \ldots, N-1$. Note that we let the matrix start with zero rows and zero columns instead of one row and one column for consistency. Obviously, the Gram matrix G is a circulant matrix since it relies only on the difference $j - i$. It can be diagonalized with the unitary discrete Fourier transform. The eigenvalue λ_r of Gram matrix G can be given by

$$\lambda_r = \sum_{k=0}^{N-1} c_k\omega^{kr} \tag{S10}$$

where we have $r = 0, 1, \ldots, N-1$, $\omega = e^{\mathbf{i}2\pi/N}$ and $c_k = e^{-\mu\left(1-e^{\mathbf{i}2\pi k/N}\right)}$. The optimal minimum error discrimination probability $P_{\min}$ can be written as [3]

$$\begin{aligned} P_{\min} &= 1 - \frac{1}{N^2}\left|\sum_{r=0}^{N-1}\sqrt{\lambda_r}\right|^2 \\ &= 1 - \frac{1}{N^2}\left|\sum_{r=0}^{N-1}\sqrt{\sum_{k=0}^{N-1} e^{-\mu(1-e^{\mathrm{i}2\pi k/N})+\mathrm{i}2\pi kr/N}}\right|^2 . \end{aligned} \tag{S11}$$

II. PROOF OF THE FIRST OBSERVATION

First observation: The process of generating the discrete phase-randomized weak coherent state through a random mapping rule is the provable quantum one-way function if the phase number is sufficiently large and the optical intensity remains low.

Each weak coherent state $\left|\sqrt{\mu}e^{\mathrm{i}\theta}\right\rangle$ is actively generated through phase modulation, where the electrical signal is determined by the bit substring $\vec{x}$. According to the definition of the provable quantum one-way function provided in the main text, an attacker Eve cannot obtain any information about $\vec{x}$ if Eve only have access to the quantum state. This quantum system will be considered as a mixture state rather than the pure state due to the absence of phase information.

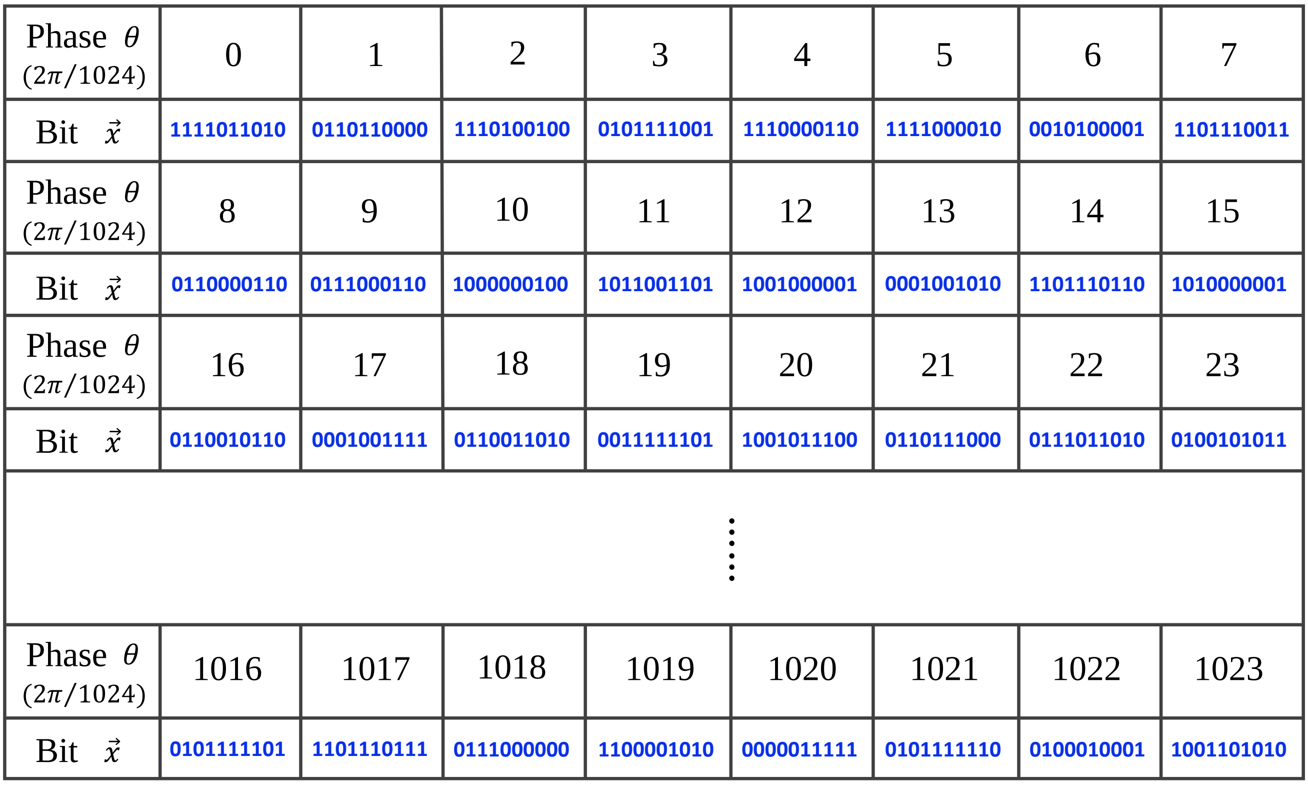
To demonstrate the validity of this assertion, we will show that the density matrix of the discrete phase-randomized weak coherent state is equivalent to a *pseudo* photon number mixture state. This *pseudo* photon number mixture state is ϵ-close (ϵ being an exponentially small number close to zero) to the Poisson-distributed photon number mixture state, which is uncorrelated with the global phase θ. The Poisson-distributed photon number mixture state is identical to the continuous phase-randomized coherent state. Therefore, unambiguous state discrimination cannot be utilized, and each state can only be guessed randomly.

Furthermore, using the random mapping rule, each phase interval (e.g., $[0,\pi)$) also corresponds to random bit substrings, with each bit of the substrings having a 50% probability of being zero. Thus, Eve cannot derive any information about $\vec{x}$ even through phase interval estimation via quantum measurement. It is important to note that $\vec{x}$ must be a true random number generated by quantum or other physical random number generation methods. Consequently, each phase of the weak coherent state is independent and random.

A. Random mapping rule

For m global phases $\theta \in \{0, 2\pi/m, 4\pi/m, \ldots, 2\pi(m-1)/m\}$, there are $m!$ possible mapping rules. In each probability key distribution (PKD) session, the mapping rule that links the global phase θ to the bit substring $\vec{x}$ is random and determined by a truly random bit string $\vec{C}$. Various methods can generate these random mapping rules. Here, we describe a straightforward, albeit non-optimal, method involving true random numbers. Traditionally, true random number resources have been relatively accessible. Recent advancements in quantum random number generation have made it possible to easily generate tens of gigabits per second of quantum random numbers.

As illustrated in Fig. S1, consider one user, such as Alice, who sorts a total of m phases, ranging from 0 to $2\pi(m-1)/m$, into a sequence ordered from smallest to largest. Each phase corresponds to a $\log_2 m$-bit value. Given a true random number string $\vec{B}$ with a sufficiently large number of bits, $O(10m\log_2 m)$, Alice treats each $\log_2 m$-bit of $\vec{B}$ segment as a bit substring. The bit substring is then filled into $\vec{C}$ according to the order in which each $\log_2 m$-bit substring first appears in $\vec{B}$. For instance, if $m = 1024$, then $\log_2 m = 10$, and the random bit string $\vec{B} \in \{0,1\}^{10^5}$ is divided into 10^4 bit substrings. Suppose the first six bit substrings are $\vec{B}_1 = 1111011010$, $\vec{B}_2 = 0110110000$, $\vec{B}_3 = 1110100100$, $\vec{B}_4 = 0101111001$, $\vec{B}_5 = 0110110000$ and $\vec{B}_6 = 1110000110$. In this case, $\vec{B}_5$ is discarded since it is a duplicate of $\vec{B}_2$, which already appeared earlier. Following this method, the bit string that determines the random mapping rule is $\vec{C} = \vec{c}_0||\vec{c}_1||\vec{c}_2||\cdots||\vec{c}_{m-1}$, where $\vec{c}_0 = \vec{B}_1 = 1111011010$, $\vec{c}_1 = \vec{B}_2 = 0110110000$, $\vec{c}_2 = \vec{B}_3 = 1110100100$, $\vec{c}_3 = \vec{B}_4 = 0101111001$, $\vec{c}_4 = \vec{B}_6 = 1110000110$, and so forth. Consequently, the bit substring $\vec{x} = 1111011010 = \vec{c}_0$ (which is 968 in decimal notation) corresponds to global phase $\theta = 0$, the bit substring $\vec{x} = 0110110000 = \vec{c}_1$ corresponds to phase $\theta = 2\pi/1024 \times 1$, the bit substring $\vec{x} = 1110100100 = \vec{c}_2$ corresponds to global phase $\theta = 2\pi/1024 \times 2$, the bit substring $\vec{x} = 0101111001 = \vec{c}_3$ corresponds to global phase $\theta = 2\pi/1024 \times 3$, and the bit substring $\vec{x} = 1110000110 = \vec{c}_4$ corresponds to global phase $\theta = 2\pi/1024 \times 4$. The bit substring $\vec{x} = \vec{c}_j$



Phase θ $(2\pi/1024)$	0	1	2	3	4	5	6	7
Bit $\vec{x}$	1111011010	0110110000	1110100100	0101111001	1110000110	1111000010	0010100001	1101110011
Phase θ $(2\pi/1024)$	8	9	10	11	12	13	14	15
Bit $\vec{x}$	0110000110	0111000110	1000000100	1011001101	1001000001	0001001010	1101110110	1010000001
Phase θ $(2\pi/1024)$	16	17	18	19	20	21	22	23
Bit $\vec{x}$	0110010110	0001001111	0110011010	0011111101	1001011100	0110111000	0111011010	0100101011
					⋮			
Phase θ $(2\pi/1024)$	1016	1017	1018	1019	1020	1021	1022	1023
Bit $\vec{x}$	0101111101	1101110111	0111000000	1100001010	0000011111	0101111110	0100010001	1001101010

FIG. S1: The random mapping rule of some one PKD session. The basic unit of the phase row is $2\pi/1024$; thus, 1023 denotes that the phase $\theta = 2\pi/1024 \times 1023$. The bit substring $\vec{x} = 1111011010 = \vec{c}_0$ is the first to appear, so it corresponds to phase $\theta = 0$. The bit substring $\vec{x} = 1001101010 = \vec{c}_{1023}$ is the last to appear, so it corresponds to the phase $\theta = 2\pi/1024 \times 1023$.

corresponds to global phase $\theta = 2\pi/1024 \times j$. The detailed mapping rule for a particular session is shown in Fig. S1. In each PKD session, $m \log_2 m$ bits (which is greater than $\log_2(m!)$) are used to determine a specific random mapping rule, and these rules vary with each session.

The specific random mapping rule $\vec{C}$ in each session is known only to Alice. To share this rule with Bob, Alice must encrypt it and transmit it using a one-time pad, which requires an $m \log_2 m$-bit pre-shared secret key. Additionally, to ensure that the mapping rules have not been tampered with by Eve, it is necessary to use information-theoretically secure authentication methods [6, 7]. To reduce the amount of secret key required for message authentication, Alice and Bob can authenticate multiple mapping rules from several PKD sessions simultaneously. Since the random mapping rule is determined by true random numbers, all possible mapping rules occur with equal probability. Consequently, from the view of Eve, each global phase θ is uniformly and randomly associated with all possible $\log_2 m$-bit substrings.

B. Discrete phase-randomized coherent state

We now quantitatively analyze the relationship between discrete and continuous phase-randomized coherent states. First, we demonstrate that the continuous phase-randomized coherent state $\left|\sqrt{\mu}e^{\mathrm{i}\theta}\right\rangle$ can be considered uncorrelated with the global phase θ. For the discrete phase-randomized coherent state $\left|\sqrt{\mu}e^{\mathrm{i}\theta}\right\rangle$, where $\theta \in \{0, 2\pi/m, 4\pi/m, \ldots, 2\pi(m-1)/m\}$, the discrete case approaches the continuous case as $m \to \infty$. Specifically, the discrete phase values θ will cover the continuous range $[0, 2\pi)$ in the limit of large m. The density matrix of the continuous phase-randomized weak coherent state can be given by

$$\hat{\rho}^{\mathrm{con}} = \frac{1}{2\pi}\int_0^{2\pi} \left|\sqrt{\mu}e^{\mathrm{i}\theta}\right\rangle\left\langle\sqrt{\mu}e^{\mathrm{i}\theta}\right| d\theta = \sum_{k=0}^{\infty} e^{-\mu}\frac{\mu^k}{k!}|k\rangle\langle k| = \sum_{k=0}^{\infty} P^{\mu}(k)|k\rangle\langle k|, \tag{S12}$$

where $P^{\mu}(k) = e^{-\mu}\mu^k/k!$ represents the Poisson distribution for the Fock state $|k\rangle$, and the right-hand side of Eq. (S12) is a mixture of these Poisson-distributed Fock states. The density matrix is identical in both cases, making them indistinguishable. Clearly, the global phase of a Fock state has no physical significance; the statistics of measurements predicted for $e^{\mathbf{i}\theta}|k\rangle$ and $|k\rangle$ are the same. Thus, from an observational perspective, the states $e^{\mathbf{i}\theta}|k\rangle$ and $|k\rangle$ are equivalent. Consequently, for Eve, the global phase is independent of the continuous phase-randomized weak coherent state. In other words, without knowledge of the phase information, the continuous phase-randomized quantum weak coherent state appears as a photon number mixture state. For Eve, this means the global phase is entirely random, and no useful information can be extracted from it. This is what we refer to as the source of rigorous one-wayness. Conversely, the preparator perceives the system as a pure state rather than a photon number mixture state, given that they generated it.

To show this more intuitively, we introduce the normalized quantum phase operator [8, 9]

$$e^{\mathbf{i}\hat{\phi}_\theta} = \lim_{l\to\infty}\sum_{j=0}^{l} e^{\mathbf{i}\theta_j}|\theta_j\rangle\langle\theta_j|, \tag{S13}$$

where $j = 0, 1, \ldots, l$ and phase state $|\theta_j\rangle$ is the eigenstate of phase operator $\hat{\phi}_\theta$, since we can prove that $e^{\mathbf{i}\hat{\phi}_\theta}|\theta_j\rangle = e^{\mathbf{i}\theta_j}|\theta_j\rangle$ and $\hat{\phi}_\theta = \lim_{l\to\infty}\sum_{j=0}^{l}\theta_j|\theta_j\rangle\langle\theta_j|$. The phase state $|\theta_j\rangle$ is defined in $l+1$ dimension Fock state space

$$|\theta_j\rangle = \lim_{l\to\infty}\frac{1}{\sqrt{l+1}}\sum_{k=0}^{l} e^{\mathbf{i}k\theta_j}|k\rangle, \tag{S14}$$

where phase $\theta_j = \theta_0 + 2\pi j/(l+1)$ and θ_0 is the reference state. The phase state satisfies the complete orthogonal condition $\langle\theta_j|\theta_h\rangle = \delta_{jh}$ and $\hat{\mathbf{I}}_{l+1} = \sum_{j=0}^{l}|\theta_j\rangle\langle\theta_j|$. Therefore, for $k \le l$, one can expand the Fock state $|k\rangle$ with a phase state

$$|k\rangle = \lim_{l\to\infty}\frac{1}{\sqrt{l+1}}\sum_{j=0}^{l} e^{-\mathbf{i}k\theta_j}|\theta_j\rangle, \tag{S15}$$

which means that each Fock state $|k\rangle$ is a uniform superposition of phase states θ_j. Therefore, one obtained phase via any quantum measurement will be completely random given the mixture of the Fock state.

For m discrete global phases, the density matrix of the discrete phase-randomized weak coherent state can be written as [10, 11]

$$\hat{\rho}^{\mathrm{dis}}(m) = \frac{1}{m}\sum_{j=0}^{m-1}\left|\sqrt{\mu}e^{\mathbf{i}\frac{2\pi}{m}j}\right\rangle\left\langle\sqrt{\mu}e^{\mathbf{i}\frac{2\pi}{m}j}\right| = \sum_{k=0}^{m-1} P_m^{\mu}(k)|\lambda_k\rangle\langle\lambda_k|, \tag{S16}$$

which can be regarded as the mixture of pseudo photon-number states $|\lambda_k\rangle$ with probability $P_m^{\mu}(k)$. The probability $P_m^{\mu}(k)$ and pseudo photon-number state $|\lambda_k\rangle$ can be given by

$$\begin{aligned} P_m^{\mu}(k) &= e^{-\mu}\sum_{l=0}^{\infty}\frac{\mu^{lm+k}}{(lm+k)!}, \\ |\lambda_k\rangle &= \frac{e^{-\mu/2}}{\sqrt{P_m^{\mu}(k)}}\sum_{l=0}^{\infty}\frac{(\sqrt{\mu})^{lm+k}}{\sqrt{(lm+k)!}}|lm+k\rangle. \end{aligned} \tag{S17}$$

Obviously, the probability will become the Poisson distribution, and state λ_k will become the Fock state if $m\to\infty$, i.e., $\lim_{m\to\infty} P_m^{\mu}(k) \equiv e^{-\mu}\mu^k/k!$ and $\lim_{m\to\infty}|\lambda_k\rangle \equiv |k\rangle$. In the asymptotic limit case, we have $m = 2\pi/d\theta$; thus,

$$\lim_{m\to\infty}\frac{1}{m}\sum_{j=0}^{m-1}\left|\sqrt{\mu}e^{\mathbf{i}\frac{2\pi}{m}j}\right\rangle\left\langle\sqrt{\mu}e^{\mathbf{i}\frac{2\pi}{m}j}\right| = \frac{1}{2\pi}\int_0^{2\pi}\left|\sqrt{\mu}e^{\mathbf{i}\theta}\right\rangle\left\langle\sqrt{\mu}e^{\mathbf{i}\theta}\right|d\theta. \tag{S18}$$

For finite m, we can calculate the probability difference $\Delta(\mu, m, k)$ and trace distance $D(|\lambda_k\rangle, |k\rangle)$ between the Fock state and the pseudo photon-number state. For $0 \le k \le m-1$, we have the probability difference

$$\Delta(\mu, m, k) = \frac{P_m^{\mu}(k) - P^{\mu}(k)}{P^{\mu}(k)} = \sum_{l=1}^{\infty}\frac{\mu^{lm}k!}{(lm+k)!}. \tag{S19}$$

For $0 \le k \le m-1$, we have the trace distance

$$\begin{aligned} D(|\lambda_k\rangle, |k\rangle) &= \frac{1}{2}\mathrm{tr}||\lambda_k\rangle\langle\lambda_k| - |k\rangle\langle k|| = \sqrt{1 - F(|\lambda_k\rangle, |k\rangle)^2} \\ &= \sqrt{1 - \frac{1}{1 + \sum_{l=1}^{\infty} \frac{\mu^{lm} k!}{(lm+k)!}}} = \sqrt{1 - \frac{1}{1 + \Delta(\mu, m, k)}} \\ &< \sqrt{\Delta(\mu, m, k)} = \sqrt{\sum_{l=1}^{\infty} \frac{\mu^{lm} k!}{(lm+k)!}}. \end{aligned} \tag{S20}$$

Obviously, for $\Delta(\mu, m, k) \le \Delta(\mu, m, 0)$, we have $\Delta(0.1, 1024, 0) = 1.85 \times 10^{-3664}$.

For the phase-randomized coherent state, we consider that the purification of this system

$$|\psi\rangle_{AE} = \frac{1}{\sqrt{m}} \sum_{j=0}^{m-1} |j\rangle_A \big|\sqrt{\mu} e^{\mathbf{i}\theta_j}\big\rangle_E, \tag{S21}$$

where $\theta_j = 2\pi j/m$, only Alice owns the qudit system A, and Eve can access the optical mode E. Deterministic phase information θ_j can be obtained by measuring qudit $|j\rangle_A$, i.e., from the view of Alice, the optical mode will become the pure state $\big|\sqrt{\mu} e^{\mathbf{i}\theta_j}\big\rangle_E$. However, Eve does not have access to the qudit system. From the view of Eve, the optical mode becomes the mixed state

$$\hat{\rho}_E^{\mathrm{dis}}(m) = \mathrm{tr}_A |\psi\rangle_{AE}\langle\psi|_{AE} = \frac{1}{m} \sum_{j=0}^{m-1} \left|\sqrt{\mu} e^{\mathbf{i}\frac{2\pi}{m}j}\right\rangle_E \left\langle \sqrt{\mu} e^{\mathbf{i}\frac{2\pi}{m}j}\right|. \tag{S22}$$

Since $\lim_{m\to\infty} \hat{\rho}_E^{\mathrm{dis}}(m) = \hat{\rho}_E^{\mathrm{con}} = \sum_{k=0}^{\infty} e^{-\mu}\mu^k/k! \times |k\rangle_E\langle k|$, the system of the Eve is completely decoupled from the phase information θ_j of Alice if $m \to \infty$. In other words, Eve can only randomly guess the phase if he or she has $\hat{\rho}_E^{\mathrm{con}}$. However, $\hat{\rho}_E^{\mathrm{dis}}(m) \neq \hat{\rho}_E^{\mathrm{con}}$ for finite m, which leads Eve to obtain some phase information. For example, for $m = 2$, the probability of obtaining an optimum unambiguous state discrimination measurement is $P_{\mathrm{USD}}^{(2)} = 1 - e^{-2\mu}$. Fortunately, the amount of leaked to Eve's information decreases exponentially with increasing m.

To define the secrecy of a phase, we consider the quantum state $\hat{\rho}_E$, which describes the correlation between Alice's phase information and the eavesdropper Eve (for any given attack strategy). The phase is called ϵ-secret from Eve if it is ϵ-close to a uniformly distributed phase that is uncorrelated with the eavesdropper, that is, if

$$\frac{1}{2}\left\|\hat{\rho}_E - \hat{\rho}_E^{\mathrm{ideal}}\right\|_1 \le \epsilon, \tag{S23}$$

where $\|\cdot\|_1$ is the trace norm and $\hat{\rho}_E^{\mathrm{ideal}}$ is the ideal state that is completely decoupled from Alice's phase. According to this definition, the quantum state is $\hat{\rho}_E = \hat{\rho}_E^{\mathrm{dis}}(m)$ for m symmetric coherent states, and the ideal state is $\hat{\rho}_E^{\mathrm{ideal}} = \hat{\rho}_E^{\mathrm{con}}$. Let λ_n be the n-th eigenvalue of $\hat{\rho}_E^{\mathrm{dis}}(m) - \hat{\rho}_E^{\mathrm{con}}$; the trace distance can be given by

$$\begin{aligned} D\left(\hat{\rho}_E^{\mathrm{dis}}(m), \hat{\rho}_E^{\mathrm{con}}\right) &= \frac{1}{2}\left\|\hat{\rho}_E^{\mathrm{dis}}(m) - \hat{\rho}_E^{\mathrm{con}}\right\|_1 \\ &= \frac{1}{2}\mathrm{tr}\left|\hat{\rho}_E^{\mathrm{dis}}(m) - \hat{\rho}_E^{\mathrm{con}}\right| \\ &= \frac{1}{2}\sum_{n=0}^{\infty} |\lambda_n|. \end{aligned} \tag{S24}$$

The above formula can be calculated numerically only. This process is highly complicated because there is an infinite number of photons. Here, we consider the photon number truncated to $m-1$; the density matrices $\hat{\rho}_E^{\mathrm{dis}}(m)$ and $\hat{\rho}_E^{\mathrm{con}}$

are all $m \times m$ diagonal matrices. Thus, we have the approximate result

$$\begin{aligned}\epsilon = D\left(\hat{\rho}_E^{\rm dis}(m), \hat{\rho}_E^{\rm con}\right) &= \frac{1}{2}\left|\left|\hat{\rho}_E^{\rm dis}(m) - \hat{\rho}_E^{\rm con}\right|\right|_1 \\ &\approx \frac{1}{2}\sum_{k=0}^{m-1}\Delta(\mu, m, k)P^{\mu}(k) \\ &= \frac{e^{-\mu}}{2}\sum_{k=0}^{m-1}\sum_{l=1}^{\infty}\frac{\mu^{lm+k}}{(lm+k)!} \\ &\approx \frac{e^{-\mu}\mu^m}{2(m!)}.\end{aligned} \tag{S25}$$

where we assume that m is large enough, for example, $m \geq 100$. If $m = 1024$ and $\mu = 0.1$, we have $\epsilon = 8.35 \times 10^{-3665}$.

Furthermore, we can use the USD and the minimum error discrimination measurements for analysis from another perspective. If $m = 1024$ and $\mu = 0.1$, the optimal USD probability and minimum error discrimination measurement probability can be given by

$$P_{\rm USD}^{(m)} = \frac{m\mu^{m-1}}{(m-1)!} = 1.94 \times 10^{-3657}, \tag{S26}$$

and

$$P_{\rm min} = 1 - \frac{1}{m^2}\left|\sum_{r=0}^{m-1}\sqrt{\sum_{k=0}^{m-1} e^{-\mu(1-e^{\mathrm{i}2\pi k/m})+\mathrm{i}2\pi kr/m}}\right|^2 = 99.83\%. \tag{S27}$$

Obviously, it is impossible for Eve to know with certainty what the phase of one optical pulse is through the USD measurement. If Eve does not exploit the received quantum state, he can randomly guess the phase, and the error probability of random guessing is 1 − 1/1024 = 99.90%. Compared with the error probabilities of minimum error discrimination measurement and random guessing, one can find that the quantum states received by Eve offer almost no advantage for large m and small μ.

III. PROOF OF THE SECOND OBSERVATION

Second observation: Alice and Bob can share themselves-generated quantum random numbers in many communication rounds with unconditional security via a fixed but long secret key and a per-update but short secret key if these quantum random numbers are not leaked to Eve when they are used.

It is well established that the one-time pad is the only information-theoretically secure encryption system. The one-time pad requires two conditions: the secret key used for encryption must be updated for each use and must be at least as long as the message, and the key must be truly random and kept entirely secret by the communicating parties. Importantly, sharing a true random number rather than the message in the second observation is not an actual encryption process but rather a negotiation of random information. Hence, we remark that the second observation does not contradict the conclusion about the one-time pad.

To further clarify our second observation, we will first review various types of attacks in cryptanalysis [12], explain why the one-time pad is an information-theoretically secure encryption scheme, and contrast it with why a (non-one-time pad) stream cipher does not offer the same level of security.

A. Types of attack utilized in cryptanalysis

The goal of cryptanalysis is to efficiently and fully recover plaintext from ciphertext, and it often involves deducing the decryption key used for past or future messages. The four most important types of attacks are as follows:

1. *Ciphertext-only attack*: Cryptanalysts attempt to deduce the decryption key or plaintext using only the available ciphertext. This is the most challenging scenario for cryptanalysts, as the only information they have is the ciphertext itself.

2. *Known-plaintext attack*: Cryptanalysts try to uncover the decryption key or algorithm by combining intercepted ciphertext with known plaintext-ciphertext pairs. Executing this attack is typically only slightly more challenging than a ciphertext-only attack.

3. *Chosen-plaintext attack*: Cryptanalysts can select specific plaintexts and obtain their corresponding ciphertexts through the encryption system. This type of attack is more potent than a known-plaintext attack but requires additional resources.

4. *Chosen-ciphertext attack*: Cryptanalysts can choose ciphertexts and obtain the corresponding plaintexts. If they have access to decryption equipment (though not necessarily the decryption key), they can use this attack to deduce plaintexts from various ciphertexts without direct access to the decryption key. This attack is the most powerful and is primarily used against public key cryptosystems, though it is traditionally the most challenging to implement.

In addition to the four attacks mentioned, there are other types such as adaptive chosen-plaintext attacks and adaptive chosen-ciphertext attacks. Powerful techniques like differential cryptanalysis and linear cryptanalysis typically belong to known-plaintext attacks. Similarly, a brute-force search attack, even with unlimited computational resources, relies on known plaintext-ciphertext pairs to verify its results, thus also being categorized as a known-plaintext attack.

B. One-time pad encryption and perfect secrecy

Information-theoretical security, also known as unconditional security, ensures that a cryptosystem maintains its security even if the eavesdropper possesses unlimited computational resources. Unconditional security in cryptosystems is referred to as perfect secrecy. To define perfect secrecy, let $\vec{m}$, $\vec{m}_0$, and $\vec{m}_1$ represent arbitrary plaintexts, and let $\mathcal{M}$ denote the plaintext space. Let $\vec{c}$ be an arbitrary ciphertext, and $\mathcal{C}$ denote the ciphertext space. Let $\vec{k}$ be an arbitrary key, and $\mathcal{K}$ represent the key space. $\mathrm{Enc}_{\vec{k}}(\vec{m})$ $(\mathrm{Dec}_{\vec{k}}(\vec{m}))$ denotes the encryption (decryption) algorithm using key $\vec{k}$ and message $\vec{m}$.

Perfect secrecy: for $\forall\ \vec{m}_0, \vec{m}_1 \in \mathcal{M}$ $(|\vec{m}_0| = |\vec{m}_1|)$ and $\forall\ \vec{c} \in \mathcal{C}$, we call a symmetric encryption system with the property of perfect secrecy if we have

$$\Pr\left[\mathrm{Enc}_{\vec{k}}(\vec{m}_0) = \vec{c}\right] = \Pr\left[\mathrm{Enc}_{\vec{k}}(\vec{m}_1) = \vec{c}\right], \tag{S28}$$

where $\vec{k} \in \mathcal{K}$ is uniformly random. The probability of obtaining the ciphertext $\vec{c}$ from the encryption of any two plaintexts within the plaintext space $\mathcal{M}$ is identical. This implies that no information is disclosed by the ciphertext, meaning that an attacker cannot determine which plaintext corresponds to the given ciphertext $\vec{c}$, even if they use unlimited computational resources to enumerate all possible keys in the key space $\mathcal{K}$.

One-time pad: For each encryption session, let $\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0,1\}^n$, $\vec{m} \in \mathcal{M}$, $\vec{k} \in \mathcal{K}$ and $\vec{c} \in \mathcal{C}$; the encryption and decryption algorithms are

$$\begin{aligned} \mathrm{Enc}_{\vec{k}}(\vec{m}) &: \vec{c} = \vec{m} \oplus \vec{k}, \\ \mathrm{Dec}_{\vec{k}}(\vec{m}) &: \vec{m} = \vec{c} \oplus \vec{k}, \end{aligned} \tag{S29}$$

where the random key $\vec{k}$ must be used only once. Obviously, the one-time pad has the property of perfect secrecy since, given $\vec{c}$, for any one $\vec{m}$, there is only one corresponding $\vec{k}$. Eq. (S28) is naturally satisfied in one-time pad.

Shannon law: Let $(\mathrm{Enc}_{\vec{k}}(\vec{m}), \mathrm{Dnc}_{\vec{k}}(\vec{m}))$ be a symmetric encryption scheme defined on $(\mathcal{K}, \mathcal{M}, \mathcal{C})$; if it is a perfect secrecy, then $|\mathcal{K}| \geq |\mathcal{M}|$. Thus, $|\mathcal{K}| = |\mathcal{M}|$ of one-time pad is the optimal scheme.

We highlight the following points. First, perfect secrecy is concerned with ciphertext-only attacks, meaning the attacker only has access to the eavesdropped ciphertext. Second, since the key is used only once and is updated in each session, the plaintexts, keys, and ciphertexts from other sessions are irrelevant to any single session attack. Consequently, attacks such as known-plaintext attacks are ineffective. Specifically, in a one-time pad scheme, other types of attacks are futile because they provide no useful information to the attacker. A brute-force search attack, even with unlimited computational resources, is also ineffective, as the correctness of the attack results cannot be verified. For instance, if an attacker correctly enumerates a key and obtains the correct plaintext, they cannot distinguish it from other plaintexts. As a result, the attacker is left with no option but to make a completely random guess.

Stream ciper: Let G be an efficient computable deterministic function

$$G(\vec{k}): \ \vec{k} \in \{0,1\}^n \to \vec{\mathrm{k}}_{\mathrm{pse}} \in \{0,1\}^N, \quad n << N, \tag{S30}$$

where the extended pseudorandom key $\vec{\mathrm{k}}_{\text{pse}}$ is used in a streaming manner across numerous encryption sessions. The encryption and decryption algorithms also include the XOR operation

$$\begin{aligned} \mathrm{Enc}_{\vec{k}}(\vec{m}) &: \vec{c} = \vec{m} \oplus G(\vec{k}), \\ \mathrm{Dec}_{\vec{k}}(\vec{m}) &: \vec{m} = \vec{c} \oplus G(\vec{k}). \end{aligned} \tag{S31}$$

Note that in a stream cipher, a short key seed $\vec{k}$ is used for many encryption sessions. According to Shannon's law, a stream cipher cannot achieve perfect secrecy because $|\vec{k}| \ll |\vec{m}|$. An obvious vulnerability is the known-plaintext attack, as the pseudorandom keys $\vec{\mathrm{k}}_{\text{pse}}$ used in different encryption sessions are not completely independent but related. Consequently, known plaintext-ciphertext pairs can provide useful information to verify the correctness of results in brute-force search attacks. Immunity to known-plaintext attacks is a crucial factor in determining whether a cryptosystem possesses perfect secrecy.

C. The security of random information negotiation with $\vec{R}_n(\vec{x}_a)$

With the above knowledge, we can now easily prove our second observation. Let us first look at the concrete implementation in the main text. Given a fixed but long secret key $\vec{K}_{\text{fix}} \in \{0,1\}^{s+t-1}$, a fully random Toeplitz matrix $\mathbf{H}_{st}$ with $s \times t$ ($s << t$) can be constructed by using the secret key $\vec{K}_{\text{fix}} = [h_0, h_1, \cdots, h_{s+t-1}]$, as follows:

$$\mathbf{H}_{st} = \begin{bmatrix} h_{s-1} & h_s & h_{s+1} & \cdots & h_{s+t-3} & h_{s+t-2} \\ h_{s-2} & h_{s-1} & h_s & \cdots & h_{s+t-4} & h_{s+t-3} \\ h_{s-3} & h_{s-2} & h_{s-1} & \cdots & h_{s+t-5} & h_{s+t-4} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ h_1 & h_2 & h_3 & \cdots & h_{t-1} & h_t \\ h_0 & h_1 & h_2 & \cdots & h_{t-2} & h_{t-1} \end{bmatrix}. \tag{S32}$$

Note that $\mathbf{H}_{st}$ will be reused in many PKD sessions, for example, 10^4 sessions. For each PKD session, a short but per-update secret key $\vec{K} \in \{0,1\}^s$ is exploited to generate the data string $\vec{D} \in \{0,1\}^t$,

$$\vec{D} = \vec{K} \cdot \mathbf{H}_{st}. \tag{S33}$$

Let $\vec{K} = [k_0, k_1, \cdots, k_{s-1}]$ and $\vec{D} = [d_0, d_1, \cdots, d_{t-1}]$ be the row vector; thus, we have

$$\begin{aligned} d_j &= k_0 h_{s+j-1} \oplus k_1 h_{s+j-2} \oplus k_2 h_{s+j-3} \oplus \cdots \oplus k_{s-1} h_j \\ &= \sum_{i=0}^{s-1} \oplus k_i h_{s+j-i-1}, \end{aligned} \tag{S34}$$

where $j = 0, 1, \cdots, t-1$. Note that in each PKD session, both Alice and Bob share the same secret keys $\vec{K}_{\text{fix}}$ and $\vec{K}$, resulting in the identical data string $\vec{D}$. According to Eq. (S34), each bit d_j of $\vec{D}$ in the first PKD session is independent and random. Consequently, from Eve's perspective, the data string $\vec{D}$ in the first PKD session appears as a random t-bit string. In other words, the value of the bit string $\vec{D}$ can be all 2^t cases from the bit string $00\cdots0$ to $00\cdots0$ with equal probability.

In the first PKD session, the data string $\vec{D}$ is a random bit string since $\mathbf{H}_{st}$ has not been utilized. Let the first $n\log_2 m$ bits in $\vec{D}$ form bit string $\vec{D}_n$, i.e., $\vec{D}_n = [d_0, d_1, \cdots, d_{n\log_2 m}] \subseteq \vec{D}$. Let $\vec{R}_n(\vec{x}_a) \in \{0,1\}^{n\log_2 m}$ represent the random bit string used for discrete phase modulation. Alice shares the random bit string $\vec{R}_n(\vec{x}_a)$ with Bob by sending the XOR result $\vec{c}_n = \vec{R}_n(\vec{x}_a) \oplus \vec{D}_n$. Bob retrieves the random bit string $\vec{R}_n(\vec{x}_a)$ via the XOR operation $\vec{R}_n(\vec{x}_a) = \vec{c}_n \oplus \vec{D}_n$. The random bit string $\vec{R}_n(\vec{x}_a)$ is generated solely by Alice and is not the message itself. Although bit string $\vec{R}_n(\vec{x}_a)$ is also used for discrete phase modulation, the corresponding discrete phase-randomized weak coherent state with a random mapping rule does not leak information to Eve due to the rigorous one-wayness of provable quantum one-way function. Additionally, $\vec{R}_n(\vec{x}_a)$ is used to generated quantum state only once and will be updated in the next PKD session. Therefore, Eve can only exploit ciphertext-only attacks, with no other attack types being viable. In the first PKD session, Eve only has access to the ciphertext $\vec{c}_n$ and lacks knowledge of $\vec{R}_n(\vec{x}_a)$ or $\vec{D}_n$, which ensures perfect secrecy since $|\vec{R}_n(\vec{x}_a)|$=$|\vec{D}_n|$. Consequently, $\mathbf{H}_{st}$ remains completely random and non-informative to Eve even after the first PKD session.

In the second PKD session, all procedures are identical to those of the first PKD session, except that the unknown Toeplitz matrix $\mathbf{H}_{st}$ is reused. Note that $\mathbf{H}_{st}$ remains entirely random from Eve's perspective in the second PKD session. Consequently, only ciphertext-only attacks are feasible for Eve, with no other attack methods being effective. Eve has no knowledge of $\vec{R}_n(\vec{x}_a)$ or $\vec{D}_n$, ensuring that the sharing of $\vec{R}_n(\vec{x}_a)$ maintains perfect secrecy. Indeed, subsequent PKD sessions follow the same protocol as the second session. Thus, we conclude that Alice and Bob achieve information-theoretical security when sharing the random bit string $\vec{R}_n(\vec{x}_a)$ in all PKD sessions.

It is crucial to emphasize that the primary reason Eve cannot exploit the correlation of $\vec{D}$ across different PKD sessions is that $\vec{R}_n(\vec{x}_a)$ is a true random number rather than a message. Random bit string $\vec{R}_n(\vec{x}_a)$ used to generate quantum system can be proven to maintain rigorous one-wayness (no information is leaked in provable quantum one-way function). Eve does not have access to $\vec{R}_n(\vec{x}_a)$ for each PKD session, meaning she lacks any known plaintext-ciphertext pairs. Consequently, brute-force search attacks using unlimited computational resources are ineffective. The method for generating the unknown data string $\vec{D}$, as outlined by Eqs. (S32) and (S33), is not unique. The generation process must satisfy one condition: the data string $\vec{D}$ must appear completely random to Eve in each session, i.e., $\vec{D}$ must yield all possible bit strings. It is important to note that our random information negotiation method is not suitable for cryptosystems designed to transmit messages, as it would essentially function as a stream cipher in such cases. Obviously, message may be leaked to Eve. In that scenario, Eve could potentially acquire known plaintext-ciphertext pairs and use brute-force search attacks to verify correctness and try to find the fixed secret key $\vec{K}_{\text{fix}} \in \{0,1\}^{s+t-1}$.

Here, to aid in understanding why the repeated use of a single key can still achieve unconditional security, let us recall the unconditionally secure authentication by using random universal$_2$ hashing, for example linear-feedback-shift-register-based (LFSR-based) Toeplitz matrix [7]. The LFSR-based Toeplitz matrix is determined by an irreducible polynomial $p(x) = x_n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ of degree n over the Galois field GF(2) and n-bit random initial vector. The LFSR-based Toeplitz hashing operation can be written as $h_{\vec{p},\vec{s}}(M)= H_{nm} \cdot \vec{M} = \vec{Hash}$, where $\vec{p} = (a_{n-1}, a_{n-2}, ..., a_1, a_0)$ represents an irreducible polynomial and $\vec{s} = (b_n, b_{n-1}, ..., b_2, b_1)^T$ is the initial column vector. $\vec{p}$ and $\vec{s}$ are random and determine the Toeplitz matrix H_{nm} with n rows and m columns. $\vec{M} = (M_1, M_2...M_m)^T$ is the message and known by Eve in the form of an m-bit column vector. Note that the tag of the authentication communication is encrypted by one-time pad i.e., $\vec{Tag} = h_{\vec{p},\vec{s}}(\vec{M}) \oplus \vec{Key}$. In each authentication communication round, Eve cannot obtain any information of the LFSR-based Toeplitz hash function and the hash value due to $\vec{Key}$ is random. Therefore the initial vector $\vec{s}$ and irreducible polynomial $\vec{p}$ can be reused to generated the LFSR-based Toeplitz matrix H_{nm} in many authentication communication round. As a counterpart, in our random information negotiation, $\vec{R}_n(\vec{x}_a)$ is totally random (provable quantum one-way function does not leak any information) and updated in each session.

IV. SECRET KEY RATE

A. Proof of zero phase error

Here, we first introduce entanglement-based virtual protocol 2 in the main text, where Alice and Bob do not directly generate a weak coherent state but rather prepare an entangled state between the qubit and the signal optical mode.

(i) Alice exploits a light source and phase modulator to generate a signal optical pulse $\left|\sqrt{\mu}e^{\mathbf{i}\theta_a}\right\rangle$. She utilizes a Hadamard gate to qubit A to generate the state $\left|+x\right\rangle_A = \frac{1}{\sqrt{2}}(\left|+z\right\rangle_A + \left|-z\right\rangle_A)$. Then, Alice exploits a controlled-phase gate $\left|+z\right\rangle\left\langle+z\right|\otimes\hat{\mathbf{I}}+\left|-z\right\rangle\left\langle-z\right|\otimes e^{\mathbf{i}\pi\hat{n}}$ to qubit A as a control and signal optical pulse a as a target to generate the entangled state $\left|\varphi\right\rangle_{Aa}^{\theta_a} = \frac{1}{\sqrt{2}}\left(\left|+z\right\rangle_A\left|\sqrt{\mu}e^{\mathbf{i}\theta_a}\right\rangle_a + \left|-z\right\rangle_A\left|-\sqrt{\mu}e^{\mathbf{i}\theta_a}\right\rangle_a\right)$. The random global phase $\theta_a \in \{0, 2\pi/m, 4\pi/m, \ldots, 2\pi(m-1)/m\}$ is determined by the random bit substring $\vec{x}_a \in \{0,1\}^{\log_2 m}$. There are m global phases and each $\log_2 m$-bit map to a global phase. Bob does the same. Instead of the fixed mapping rule, the global phase is determined by random mapping rule. The random mapping rule is shared between Alice and Bob through one-time pad encryption by consuming $m \log_2 m$ bits of the pre-shared secret key. Alice (Bob) keeps the qubits A (B) in quantum memory. Alice and Bob repeat step (i) for N rounds.

(ii) Alice (Bob) utilizes another laser to generate the reference pulse. Alice (Bob) performs the single-photon interference measurement for the signal optical pulse a (b) and reference pulse by using a beam splitter and two detectors, D_{aL} and D_{aR} (D_{bL} and D_{bR}). If and only if one of the D_{aL} and D_{aR} (D_{bL} and D_{bR}) detector clicks represents a successful detection event. The number of successful detection events for Alice's signal optical pulse and Bob's signal optical pulse are both n for one PKD session. They announce the successful detection event and the corresponding detector. Alice (Bob) keeps the corresponding qubit A (B) of her (his) successful detection event and discards the others.

(iii) Alice and Bob obtain the data string $\vec{D} = \vec{K} \cdot \mathbf{H}_{st}$, where $\vec{D}$ has t bits and $t \geq n \log_2 m$. Let the first $n \log_2 m$ bits in $\vec{D}$ constitute the data string $\vec{D}_n$. For n successful detection events of Alice, let $\vec{R}_n(\vec{x}_a) \in \{0,1\}^{n \log_2 m}$ be the random bit string corresponding to Alice's global phases. Alice sends ciphertext $\vec{R}_n(\vec{x}_a) \oplus \vec{D}_n$ to Bob, who decrypts ciphertext with data string $\vec{D}_n$ to obtain quantum random numbers $\vec{R}_n(\vec{x}_a)$ and thus acquires the global phase of Alice θ_a according to the same random mapping rule. According to the phase θ_a of each event, Bob rearranges his qubit system B and detector click order to ensure that $\theta_b = \theta_a$. If $\{D_{aL}, D_{bR}\}$ or $\{D_{aR}, D_{bL}\}$ click, Bob performs a bit flip about his qubit B. Then, Alice and Bob exploit the Z basis to measure qubit systems A and B to acquire the raw key, respectively. Finally, Alice and Bob obtain the raw key strings $\vec{Z}_a$ and $\vec{Z}_b$, respectively.

(iv) Bob acquires an estimation $\vec{\mathrm{Z}}_b$ of $\vec{Z}_a$ in the error correction scheme by revealing at most λ bits of information. Then, Alice and Bob perform an error verification to ensure identical keys by publishing the $\log_2(2/\varepsilon_{\rm cor})$-bit.

(v) Alice and Bob perform privacy amplification by applying a random universal$_2$ hash function to extract length ℓ bits of the secret key.

Obviously, Alice's and Bob's local measurements for the qubit system commute with their measurements for optical modes. The entanglement-based protocol is equivalent to the prepare-and-measure protocol since the local Z basis measurement can be securely moved to step (i). If Alice measures $|{+z}\rangle_A$, she records bit 0 and sends an optical pulse $\left|\sqrt{\mu}e^{\mathrm{i}\theta_a}\right\rangle$. If Alice measures $|{-z}\rangle_A$, she records bit 1 and sends an optical pulse $\left|-\sqrt{\mu}e^{\mathrm{i}\theta_a}\right\rangle$. Actually, from the view of Eve, the nonlocal entangled state will be generated if Alice and Bob have identical and confidential random phase information $\theta_a = \theta_b$. Alice and Bob can exploit the virtual entangled state to extract the secret key. Alice and Bob can measure two-qubit systems A and B by using the Z and X bases, respectively. The results of the Z basis are used as the raw key. The quantum bit error rate of the X basis quantifies the phase error rate. As follows, we will show that the quantum bit error rate of the X basis is always zero. Thus, we do not need to actually measure the X basis and obtain the zero-phase error conclusion.

The four Bell states can be written as

$$\begin{aligned}
|\phi^+\rangle &= \frac{1}{\sqrt{2}}\left(|{+z+z}\rangle + |{-z-z}\rangle\right) = \frac{1}{\sqrt{2}}\left(|{+x+x}\rangle + |{-x-x}\rangle\right), \\
|\phi^-\rangle &= \frac{1}{\sqrt{2}}\left(|{+z+z}\rangle - |{-z-z}\rangle\right) = \frac{1}{\sqrt{2}}\left(|{+x-x}\rangle + |{-x+x}\rangle\right), \\
|\psi^+\rangle &= \frac{1}{\sqrt{2}}\left(|{+z-z}\rangle + |{-z+z}\rangle\right) = \frac{1}{\sqrt{2}}\left(|{+x+x}\rangle - |{-x-x}\rangle\right), \\
|\psi^+\rangle &= \frac{1}{\sqrt{2}}\left(|{+z-z}\rangle - |{-z+z}\rangle\right) = \frac{1}{\sqrt{2}}\left(|{-x+x}\rangle - |{+x-x}\rangle\right),
\end{aligned} \tag{S35}$$

where $|\pm z\rangle$ and $|\pm x\rangle$ are the eigenstates of the Z and X bases. The entangled states generated by Alice and Bob with random phases θ_a and θ_b can be written as

$$\begin{aligned}
|\varphi\rangle_{Aa}^{\theta_a} &= \frac{1}{\sqrt{2}}\left(|{+z}\rangle_A\left|\sqrt{\mu}e^{i\theta_a}\right\rangle_a + |{-z}\rangle_A\left|-\sqrt{\mu}e^{i\theta_a}\right\rangle_a\right), \\
|\varphi\rangle_{Bb}^{\theta_b} &= \frac{1}{\sqrt{2}}\left(|{+z}\rangle_B\left|\sqrt{\mu}e^{i\theta_b}\right\rangle_b + |{-z}\rangle_B\left|-\sqrt{\mu}e^{i\theta_b}\right\rangle_b\right).
\end{aligned} \tag{S36}$$

Let us consider the special case with $m \to \infty$ and $\theta_b = \theta_a = \theta$. The initial joint quantum state between Alice and Bob can be given by

$$\begin{aligned}
\rho &= \frac{1}{2\pi}\int_0^{2\pi} |\psi\rangle_{Aa}^{\theta}\langle\psi| \otimes |\psi\rangle_{Bb}^{\theta}\langle\psi| d\theta = \frac{1}{2\pi}\int_0^{2\pi} \hat{P}\left(|\psi\rangle_{Aa}^{\theta}|\psi\rangle_{Bb}^{\theta}\right) d\theta \\
&= \sum_{k=0}^{\infty} \frac{e^{-2\mu}}{2}\left[\frac{(2\mu)^{2k+1}}{(2k+1)!}\hat{P}\left(|\phi^-\rangle_{AB}|+\rangle_{ab}^{\otimes 2k+1} + |\psi^-\rangle_{AB}|-\rangle_{ab}^{\otimes 2k+1}\right) + \frac{(2\mu)^{2k}}{(2k)!}\hat{P}\left(|\phi^+\rangle_{AB}|+\rangle_{ab}^{\otimes 2k} + |\psi^+\rangle_{AB}|-\rangle_{ab}^{\otimes 2k}\right)\right] \\
&= \sum_{k=0}^{\infty} e^{-2\mu}\left[\frac{(2\mu)^{2k+1}}{(2k+1)!}\hat{P}\left(\frac{|\phi^-\rangle_{AB}|+\rangle_{ab}^{\otimes 2k+1} + |\psi^-\rangle_{AB}|-\rangle_{ab}^{\otimes 2k+1}}{\sqrt{2}}\right) + \frac{(2\mu)^{2k}}{(2k)!}\hat{P}\left(\frac{|\phi^+\rangle_{AB}|+\rangle_{ab}^{\otimes 2k} + |\psi^+\rangle_{AB}|-\rangle_{ab}^{\otimes 2k}}{\sqrt{2}}\right)\right] \\
&= \sum_{k=0}^{\infty} e^{-2\mu}\frac{(2\mu)^k}{k!}\rho_k,
\end{aligned} \tag{S37}$$

which is the mixture of ρ_k with probability $e^{-2\mu}\frac{(2\mu)^k}{k!}$. We have $\hat{P}(|x\rangle)=|x\rangle\langle x|$ and $|\pm\rangle_{ab}=\frac{1}{\sqrt{2}}(|10\rangle_{ab}\pm|01\rangle_{ab})=\frac{\hat{a}^\dagger\pm\hat{b}^\dagger}{\sqrt{2}}|00\rangle_{ab}$, which is a superposition single-photon state with a and b modes. $|\pm\rangle_{ab}^{\otimes k}=\frac{1}{\sqrt{2^k k!}}\left(\hat{a}^\dagger\pm\hat{b}^\dagger\right)^k|00\rangle_{ab}$ is the k-photon state, i.e., k identical photons with state $|\pm\rangle_{ab}$. The density matrix of ρ_k can be written as

$$\rho_k=\begin{cases}\hat{P}\left(\frac{|\phi^-\rangle_{AB}|+\rangle_{ab}^{\otimes k}+|\psi^-\rangle_{AB}|-\rangle_{ab}^{\otimes k}}{\sqrt{2}}\right), & \text{if } k \text{ is odd,}\\[2ex] \hat{P}\left(\frac{|\phi^+\rangle_{AB}|+\rangle_{ab}^{\otimes k}+|\psi^+\rangle_{AB}|-\rangle_{ab}^{\otimes k}}{\sqrt{2}}\right), & \text{if } k \text{ is even.}\end{cases} \tag{S38}$$

From Eq. (S38), no matter what we do with the optical signal modes a and b, we can see that the measurement outcomes of the X basis by Alice's qubit A and Bob's qubit B are always perfect anticorrelation (positive correlation) if k is odd (even). Note that the global phase $\theta_a=\theta$ is random due to our first observation and the second observation. Each state ρ_k can be regarded as the tagged state, where Alice and Bob can know with certainty what joint quantum state they are sending in each round. After announcing the successful detection of Alice's signal optical pulse and Bob's signal optical pulse, considering that Alice and Bob measure their kept qubit systems on the X basis instead of the Z basis, the quantum bit error rate is always zero for each state ρ_k. Therefore, the phase error rate must be zero even though Alice and Bob do not perform the X basis measurement.

Now, we can easily generalize the conclusion to a finite phase number m and an arbitrary phase difference $\delta\theta$. For a given $\delta\theta=\theta_b-\theta_a$, the initial joint quantum state between Alice and Bob can be written as

$$\begin{aligned}\rho^{\delta\theta}&=\frac{1}{m}\sum_{\theta_a}|\psi\rangle_{Aa}^{\theta_a}\langle\psi|\otimes|\psi\rangle_{Bb}^{\theta_a+\delta\theta}\langle\psi|\\&=\sum_{k=0}^{m-1}P_m^{2\mu}(k)\rho_{\lambda_k}^{\delta\theta},\end{aligned} \tag{S39}$$

which is the mixture of $\rho_{\lambda_k}^{\delta\theta}$ with probability $P_m^{2\mu}(k)=e^{-2\mu}\sum_{l=0}^{\infty}\frac{(2\mu)^{lm+k}}{(lm+k)!}$. The density matrix of $\rho_{\lambda_k}^{\delta\theta}$ can be given by

$$\rho_{\lambda_k}^{\delta\theta}=\begin{cases}\hat{P}\left(\frac{|\phi^-\rangle_{\tilde{a}\tilde{b}}\left|\lambda_k^{+\delta\theta}\right\rangle_{ab}+|\psi^-\rangle_{\tilde{a}\tilde{b}}\left|\lambda_k^{-\delta\theta}\right\rangle_{ab}}{\sqrt{2}}\right), & \text{if } k \text{ is odd,}\\[2ex] \hat{P}\left(\frac{|\phi^+\rangle_{\tilde{a}\tilde{b}}\left|\lambda_k^{+\delta\theta}\right\rangle_{ab}+|\psi^+\rangle_{\tilde{a}\tilde{b}}\left|\lambda_k^{-\delta\theta}\right\rangle_{ab}}{\sqrt{2}}\right), & \text{if } k \text{ is even,}\end{cases} \tag{S40}$$

where the quantum state $\left|\lambda_k^{\pm\delta\theta}\right\rangle_{ab}$ is denoted as

$$\left|\lambda_k^{\pm\delta\theta}\right\rangle_{ab}=\frac{e^{-\mu}}{\sqrt{P_m^{2\mu}(k)}}\sum_{l=0}^{\infty}\frac{(\sqrt{2\mu})^{lm+k}}{\sqrt{(lm+k)!}}|\pm\delta\theta\rangle_{ab}^{\otimes lm+k}. \tag{S41}$$

Quantum state $|\pm\delta\theta\rangle_{ab}^{\otimes k}=\frac{1}{\sqrt{2^k k!}}\left(\hat{a}^\dagger\pm e^{\mathbf{i}\delta\theta}\hat{b}^\dagger\right)^k|00\rangle_{ab}$ represents the k identical photon with state $|\pm\delta\theta\rangle_{ab}=\frac{1}{\sqrt{2}}(|10\rangle_{ab}\pm e^{\mathbf{i}\delta\theta}|01\rangle_{ab})$. Like in the special case, each state $\rho_{\lambda_k}^{\delta\theta}$ can be regarded as the tagged state due to our first and second observations. From Eq. (S40) and the above argument, the phase error rate is also zero even if Eve carries out any attacks. Finally, since the phase difference $\delta\theta$ can be arbitrary and even known by Eve, we conclude that the phase error rate of the PKD protocol is always zero.

B. Universally composable framework

Here, we note that our PKD protocol meets the universally composable framework [13]. For each PKD session, our protocol either outcomes a pair of key strings $\vec{S}_a$ and $\vec{S}_b$ with $|\vec{S}_a|=|\vec{S}_b|=\ell$ or aborts. For a secure protocol, the key strings should satisfy the correctness and secrecy criteria as follows. Specifically, a protocol is ε_{tot}-secure if it is ε_{cor}-correct and ε_{sec}-secret with $\varepsilon_{\text{cor}}+\varepsilon_{\text{sec}}\leq\varepsilon_{\text{tot}}$.

Correctness criterion: a protocol is ε_{cor}-correct if the error-verification step is passed, where we have $\Pr[\vec{S}_a \neq \vec{S}_b] \leq \varepsilon_{\text{cor}}$, i.e., the probability that two key strings are not identical does not surpass ε_{cor}.

Secrecy criterion: an ideal protocol in which the generated key string $\vec{S}_a$ of Alice is independent of Eve's system ρ_E, i.e., the joint classical-quantum state between Alice and Eve

$$\begin{aligned}\rho_{AE}^{\text{ideal}} &= U_A \otimes \rho_E \\ &= \frac{1}{2^\ell} \sum_{\vec{s}_a} |\vec{s}_a\rangle\langle\vec{s}_a| \otimes \rho_E,\end{aligned} \tag{S42}$$

where $\vec{s}_a \in \{0,1\}^\ell$ is the bit value and $U_A = \frac{1}{2^\ell}\sum_{\vec{s}_a} |\vec{s}_a\rangle\langle\vec{s}_a|$ is the uniform mixture of all possible values of the key string $\vec{S}_a$. The ideal case is never perfectly satisfied and should be the nonideal case in the experiment. The corresponding state can be defined as $\rho_{AE} = \sum_{\vec{s}_a} p_{\vec{s}_a} |\vec{s}_a\rangle\langle\vec{s}_a| \otimes \rho_E^{\vec{s}_a}$. A protocol is ε_{sec}-secret after the privacy amplification step if we have

$$\frac{1}{2}(1 - p_{\text{about}})\|\rho_{AE} - U_A \otimes \rho_E\|_1 \leq \varepsilon_{\text{sec}}, \tag{S43}$$

where p_{abort} is the probability that the protocol will abort.

C. Entropic uncertainty relation

Note that the prepare-and-measure PKD is equivalent to the entanglement-based protocol. The entropic uncertainty relations [14] can be utilized to estimate the smooth min-entropy of the raw key conditioned on Eve's information. Up to the error-correction step is complete, let $\mathbf{E}'$ denote all the information that is acquired from Eve about the raw key $\vec{Z}_a$ of Alice. Let $H_{\text{min}}^{\epsilon}(\vec{Z}_a|\mathbf{E}')$ be the smooth min-entropy that quantifies the average probability of Eve correctly guessing $\vec{Z}_a$. According to the quantum leftover hash lemma, one can exploit a random universal$_2$ hash function to $\vec{Z}_a$, and a ε_{sec}-secret key of length ℓ from $\vec{Z}_a$ can be extracted

$$2\epsilon + \frac{1}{2}\sqrt{2^{\ell - H_{\text{min}}^{\epsilon}(\vec{Z}_a|\mathbf{E}')}} \leq \varepsilon_{\text{sec}}, \tag{S44}$$

Let $\varepsilon_{\text{PA}} = \frac{1}{2}\sqrt{2^{\ell - H_{\text{min}}^{\epsilon}(\vec{Z}_a|\mathbf{E}')}}$ be a security parameter related to privacy amplification; the secret key of length ℓ is

$$\ell = \left\lfloor H_{\text{min}}^{\epsilon}(\vec{Z}_a|\mathbf{E}') - 2\log_2 \frac{1}{2\varepsilon_{\text{PA}}} \right\rfloor. \tag{S45}$$

During the error-correction step and error-verification step, a total of $\lambda + \log_2(2/\varepsilon_{\text{cor}})$-bit will be published to Eve. Using the chain-rule inequality for smooth entropies, the smooth min-entropy can be bounded by

$$H_{\text{min}}^{\epsilon}(\vec{Z}_a|\mathbf{E}') \geq H_{\text{min}}^{\epsilon}(\vec{Z}_a|\mathbf{E}) - \lambda - \log_2 \frac{2}{\varepsilon_{\text{cor}}}, \tag{S46}$$

where $\mathbf{E}$ is the information learned by Eve before error correction. We have proven that the phase error rate ϕ_z is strictly zero. According to the uncertainty relation for smooth entropies, the smooth min-entropy $H_{\text{min}}^{\epsilon}(\vec{Z}_a|\mathbf{E})$ can be written as

$$H_{\text{min}}^{\epsilon}(\vec{Z}_a|\mathbf{E}) \geq n[1 - h(\phi_{\text{z}})] = n. \tag{S47}$$

Finally, we let $\epsilon = \varepsilon_{\text{PA}} = \varepsilon_{\text{sec}}/3$ and $2\epsilon + \varepsilon_{\text{PA}} = \varepsilon_{\text{sec}}$, and we can obtain the secret key rate by combining Eqs. (S45)-(S47),

$$\ell = n - \lambda - \log_2 \frac{2}{\varepsilon_{\text{cor}}} - 2\log_2 \frac{3}{2\varepsilon_{\text{sec}}}, \tag{S48}$$

where n is the length of the raw key and $\lambda = nfh(E)$ is the revealed information in the error-correction step.

V. SIMULATION FORMULA

When Alice prepares the optical pulse pairs $\left|\sqrt{\mu}e^{\mathbf{i}(\theta_a+r_a\pi)}\right\rangle_a \otimes \left|\sqrt{\mu}\right\rangle_a$ and performs the single-photon measurement, the gains Q_{aL} and Q_{aR} can be given by

$$Q_{aL}=\left\{1-(1-p_d)e^{-\mu\eta_d[1+\cos(\theta_a+r_a\pi)]}\right\}(1-p_d)e^{-\mu\eta_d[1-\cos(\theta_a+r_a\pi)]}, \tag{S49}$$

and

$$Q_{aR}=\left\{1-(1-p_d)e^{-\mu\eta_d[1-\cos(\theta_a+r_a\pi)]}\right\}(1-p_d)e^{-\mu\eta_d[1+\cos(\theta_a+r_a\pi)]}, \tag{S50}$$

where Q_{aL} (Q_{aR}) represents that detector D_{aL} (D_{aR}) has a click and D_{aR} (D_{aL}) does not have a click. p_d and η_d are the dark count rate and detection efficiency of the detector, respectively.

When Bob prepares the optical pulse pairs $\left|\sqrt{\mu}e^{\mathbf{i}(\theta_b+r_b\pi)}\right\rangle_b \otimes \left|\sqrt{\mu}\right\rangle_b$ and performs the single-photon measurement, the gains Q_{bL} and Q_{bR} can be given by

$$Q_{bL}=\left\{1-(1-p_d)e^{-\mu\eta_d[1+\cos(\theta_b+r_b\pi)]}\right\}(1-p_d)e^{-\mu\eta_d[1-\cos(\theta_b+r_b\pi)]}, \tag{S51}$$

and

$$Q_{bR}=\left\{1-(1-p_d)e^{-\mu\eta_d[1-\cos(\theta_b+r_b\pi)]}\right\}(1-p_d)e^{-\mu\eta_d[1+\cos(\theta_b+r_b\pi)]}, \tag{S52}$$

where Q_{bL} (Q_{bR}) represents that detector D_{bL} (D_{bR}) has a click and D_{bR} (D_{bL}) does not have a click.

For one PKD session, the total number of successful detection events can be given by

$$\begin{aligned} n &= \frac{N}{m}\sum_{\theta_a=0}^{2\pi(m-1)/m}(Q_{aL}+Q_{aR}) = \frac{N}{m}\sum_{\theta_b=0}^{2\pi(m-1)/m}(Q_{bL}+Q_{bR}) \approx \frac{N}{2\pi}\int_0^{2\pi}(Q_{aL}+Q_{aR})d\theta_a, \\ &= 2N\left[(1-p_d)e^{-\mu\eta_d}I_0(\mu\eta_d)-(1-p_d)^2e^{-2\mu\eta_d}\right], \end{aligned} \tag{S53}$$

where $I_0(x)$ is the modified Bessel function of the first kind. After the raw key rearrangement, the global phases of the Alice signal pulse and the Bob signal pulse are always the same as $\theta_a=\theta_b=\theta$. Therefore, we have $Q_L = \left[1-(1-p_d)e^{-\mu\eta_d(1+\cos\theta)}\right](1-p_d)e^{-\mu\eta_d(1-\cos\theta)}$ and $Q_R = \left[1-(1-p_d)e^{-\mu\eta_d(1-\cos\theta)}\right](1-p_d)e^{-\mu\eta_d(1+\cos\theta)}$. An error will occur if $r_a=r_b$ and detectors $\{D_{aL},D_{bR}\}$ ($\{D_{aR},D_{bL}\}$) click or if $r_a\neq r_b$ and detectors $\{D_{aL},D_{bL}\}$ ($\{D_{aR},D_{bR}\}$) click. The results for the discrete phase-randomized cases are almost the same as those for the continuous phase-randomized cases; thus, the bit error rate can be written as

$$\begin{aligned} E &= \frac{1}{2\pi}\int_0^{2\pi}\frac{2Q_LQ_R}{(Q_L+Q_R)^2}d\theta \\ &= \frac{1}{2\pi}\int_0^{2\pi}\frac{2(1-p_d)^2e^{-2\mu\eta_d}\left[1-(1-p_d)e^{-\mu\eta_d(1+\cos\theta)}\right]\left[1-(1-p_d)e^{-\mu\eta_d(1-\cos\theta)}\right]}{\left[(1-p_d)e^{-\mu\eta_d}(e^{-\mu\eta_d\cos\theta}+e^{\mu\eta_d\cos\theta})-2(1-p_d)^2e^{-2\mu\eta_d}\right]^2}d\theta. \end{aligned} \tag{S54}$$

For $\mu=0.1$, $\eta_d=0.8$ and $p_d=10^{-8}$, the bit error rate is $E\approx 25\%$.

* Electronic address: hlyin@ruc.edu.cn

[1] Chefles, A. & Barnett, S. M. Optimum unambiguous discrimination between linearly independent symmetric states. *Phys. Lett. A* **250**, 223–229 (1998).

[2] Barnett, S. M. & Croke, S. Quantum state discrimination. *Adv. Opt. Photonics* **1**, 238–278 (2009).

[3] Wallden, P., Dunjko, V. & Andersson, E. Minimum-cost quantum measurements for quantum information. *J. Phys. A: Math. and Theor.* **47**, 125303 (2014).

[4] Tang, Y.-L. *et al.* Source attack of decoy-state quantum key distribution using phase information. *Phys. Rev. A* **88**, 022308 (2013).

[5] Van Enk, S. Unambiguous state discrimination of coherent states with linear optics: Application to quantum cryptography. *Phys. Rev. A* **66**, 042313 (2002).

[6] Wegman, M. N. & Carter, J. L. New hash functions and their use in authentication and set equality. *J. Comput. Syst. Sci.* **22**, 265–279 (1981).

[7] Krawczyk, H. Lfsr-based hashing and authentication. In *Annual International Cryptology Conference*, 129–139 (Springer, 1994).

[8] Pegg, D. T. & Barnett, S. M. Phase properties of the quantized single-mode electromagnetic field. *Phys. Rev. A* **39**, 1665–1675 (1989).

[9] Bužek, V., Wilson-Gordon, A. D., Knight, P. L. & Lai, W. K. Coherent states in a finite-dimensional basis: Their phase properties and relationship to coherent states of light. *Phys. Rev. A* **45**, 8079–8094 (1992).

[10] Cao, Z., Zhang, Z., Lo, H.-K. & Ma, X. Discrete-phase-randomized coherent state source and its application in quantum key distribution. *New J. Phy.* **17**, 053014 (2015).

[11] Shao, S.-F. *et al.* Phase-matching quantum key distribution without intensity modulation. *Phys. Rev. Appl.* **20**, 024046 (2023).

[12] Menezes, A. J., van Oorschot, P. C. & Vanstone, S. A. *Handbook of applied cryptography* (CRC press, 1996).

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

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