Controlled Entanglement Source for Quantum Cryptography

Qiang Zeng,[1,*] Haoyang Wang,[1,2] Huihong Yuan,[1] Yuanbin Fan,[1] Lai Zhou,[1] Yuanfei Gao,[1]
Haiqiang Ma,[2] and Zhiliang Yuan[1,†]

[1] *Beijing Academy of Quantum Information Sciences, Beijing 100193, China*
[2] *School of Science and State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China*

(Received 31 January 2023; revised 24 March 2023; accepted 21 April 2023; published 15 May 2023)

Quantum entanglement has become an essential resource in quantum information processing. Existing works employ entangled quantum states to perform various tasks, while little attention is paid to the control of the resource. In this work, we propose a simple protocol to upgrade an entanglement source with access control through phase randomization at the optical pump. The enhanced source can effectively control all users in utilizing the entanglement resource to implement quantum cryptography. In addition, we show this control can act as a practical countermeasure against memory attack on device-independent quantum key distribution at a negligible cost. To demonstrate the feasibility of our protocol, we implement an experimental setup using just off-the-shelf components and characterize its performance accordingly.

DOI: 10.1103/PhysRevApplied.19.054048

I. INTRODUCTION

Modern society operates upon reliable and secure communication. Current cryptosystems defend from eavesdropping and attacks based on computation complexity, which is however vulnerable to advancing quantum technologies [1]. Quantum key distribution (QKD) [2–7] enables distant users to establish secret keys assuming any computational power of attackers but rather based on the basic physical principles, thus guaranteeing information-theoretic security [8]. In particular, entanglement-based QKD (EB QKD) protocol [3,9] stands out compared to QKD using weak coherent pulses [10–12] for it requiring no intensity modulation [4,5] and is naturally applicable for multiusers [13–17]. Further, the ultimate form of quantum secure communication [18], device-independent QKD protocol (DI QKD) [19,20], exploits the strong correlation existing in quantum entanglement that is beyond the classical regime to eliminate fully the need of trust on the QKD users' apparatuses. The main insight behind this is that the security in DI QKD requires the exclusion of existence of the local hidden variable (LHV) model [21] of the apparatuses, while such a model can be regarded as some preset conspiracies, which cannot be distinguished in traditional QKD [22].

Indeed, a lower requirement on the level of trust comes with extra demanding requirements on the performance of the practical devices. To faithfully implement DI QKD, a high-quality entanglement resource is a prerequisite to defend against collective attack [23]. In addition, high detection efficiency from the resource to both of the users is required to ensure an unbiased statistics to defend against detection efficiency attack [24,25]. Moreover, the measurement device should be *memoryless* to prevent from leaking information by tracing the history statistics of the reused devices, which is described as memory attack [26]. Fortunately, recent progresses show the above problems can be well tackled to meet the capability of state-of-the-art equipment. Remarkably, three practical DI QKD experiments were demonstrated recently [18,27,28].

Quantum entanglement is foreseeable to serve as a useful resource in future networks as a quantum utility just like electricity and gas in today's energy grids. For instance, the dealers distribute entangled states—usually carried with a photon, as it is the best information carrier over a long distance—to users to establish secret keys. However, the topic of resource control has rarely been discussed despite its apparent significance. As illustrated in Fig. 1, a conventional entanglement server constantly distributes maximally entangled states to the communication user pairs. However, the server lacks the ability to control whether the distributed photons are indeed consumed by authorized users. Unauthorized users can tap entangled photons off the channels for their own key generation without being noticed.

Surprisingly, adding control to an entanglement source can also provide defense against memory attacks [26] for DI QKD, where the attackers can retrieve the secure keys generated in earlier sessions without being detected when

[*] zengqiang@baqis.ac.cn
[†] yuanzl@baqis.ac.cn

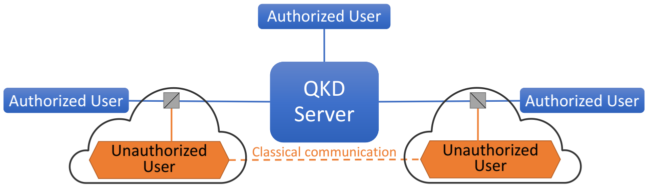

FIG. 1. Schematic of entanglement-based QKD network with both authorized and unauthorized users.

the measurement devices are reused. Existing countermeasures [26,29], including destroying the used measurement devices, strictly isolating the entanglement generation devices or using additional alternate devices, essentially prevent the attackers' access to the (possibly) recorded information, but bring considerable complexity to the system, not to mention the prohibitive cost.

Quantum mechanics provides an elegant solution to the control problems via quantum secret sharing (QSS) [30,31]. Its implementation, which originally required exotic multiphoton Greenberg-Horne-Zeilinger (GHZ) states [32,33], has been substantially simplified through the use of *pseudo*-GHZ states comprising just photon pairs and thus enabled a QSS demonstration based on time-bin entanglement [34]. Recently, the two-photon QSS approach was successfully extended to polarization encoding [35].

Inspired by the two-photon QSS protocol [34], we propose a simple but profoundly useful upgrade to a conventional entanglement source to have access control in which a binary pseudo randomness is introduced. By further introducing the mixed state, we show this enhanced entanglement source can effectively protect DI QKD from memory attacks at a negligible cost. We experimentally demonstrate our scheme in a time-bin encoding system.

II. PHASE MODULATION TO ENTANGLEMENT SOURCE

We first briefly review the three-party QSS protocol. Assuming a triple-qubit GHZ state $|\Psi\rangle_{\text{GHZ}} = 1/\sqrt{2}(|000\rangle + |111\rangle)$ is shared by three parties (say, Alice, Bob, and Coy). Subjected to Alice performing measurement σ_{X} or σ_{Y} locally, where σ_{X} and σ_{Y} are the Pauli matrices, the state shared between the other two parties is projected onto one of the following four possible states, based on the outcome of Alice's local measurement:

$$\text{X}_A^{\pm} \rightarrowtail |\phi^{\pm}\rangle_{BC} = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle),$$

$$\text{Y}_A^{\pm} \rightarrowtail |\psi^{\mp}\rangle_{BC} = \frac{1}{\sqrt{2}}(|00\rangle \mp i|11\rangle),$$

where $\text{X}^{\pm} = 1/\sqrt{2}(|0\rangle \pm |1\rangle)$, $\text{Y}^{\pm} = 1/\sqrt{2}(|0\rangle \pm i|1\rangle)$ are the eigenstates of σ_{X} and σ_{Y}, respectively. Alice's measurement outcome is thus required for Bob and Coy if they want to perform the conventional EB QKD protocol, and in this sense Alice can be regarded as the QKD controller, which is also known as third-man quantum cryptography [33]. Instead of using a genuine triple-qubit GHZ state, it is pointed out that the controller need not actually perform measurements on the state, but locally preparing and randomly distributing four possible two-qubit states [34,35]. Note that the choice of measurement of Alice is public information, thus only one bit of information is kept secret for each run in the practical implementation. For the purpose of control, we here note that one fixed measurement setting is enough.

In our scheme, we randomly (with equal probability) assign 0 and π relative phase to the entangled qubits, which is equivalent to performing measurement σ_{X} at the controller side, thus the source distributing a random mixture of states $|\phi^+\rangle$ and $|\phi^-\rangle$ to the end users. Note that the two states have an opposite correlation with respect to measurements σ_{X}, σ_{Y}, and the superposition $\sigma_{\text{X}\pm\text{Y}}$. The security analysis of EB QKD usually requires demonstrating violation of Bell-type inequalities (e.g., Clauser-Horne-Shimony-Holt (CHSH) inequality [36]). Specifically, the CHSH parameter [36] can be written as

$$S_{\text{CHSH}} := E(\sigma_{\text{X}}, \sigma_{\text{X+Y}}) + E(\sigma_{\text{Y}}, \sigma_{\text{X+Y}}) + E(\sigma_{\text{X}}, \sigma_{\text{X}-\text{Y}}) - E(\sigma_{\text{Y}}, \sigma_{\text{X}-\text{Y}}), \tag{1}$$

where

$$E(\alpha, \beta) := p_{\alpha,\beta}^{++} + p_{\alpha,\beta}^{--} - p_{\alpha,\beta}^{+-} - p_{\alpha,\beta}^{-+} \tag{2}$$

is the correlation function comprising the probabilities of four possible outcome combinations given the measurements α and β. The correlation function E quantifies the correlation of the photon pairs, assuming that the coincidence from output "++" and "−−" signify correlated; and "+−" and "−+" signify anticorrelated. S_{CHSH} is upper bounded at 2 under the assumption of *locality* in the classical regime. However in the quantum regime, entangled states are strongly correlated surpassing the locality restriction [37] with the upper bound of $2\sqrt{2}$. Thus $S_{\text{CHSH}} > 2$ ensures that the source is genuinely quantum (or more generally, no signaling [20]) and not manipulated by attackers.

For state $|\phi^+\rangle$ the expected value of S_{CHSH} it is $2\sqrt{2}$, while for $|\phi^-\rangle$ is $-2\sqrt{2}$. Thus the uniform mixture of $|\phi^+\rangle$ and $|\phi^-\rangle$ results in $S_{\text{CHSH}} = 0$, if the two states are not properly identified. In other words, how well the two users know about the exact correlation of each state determines whether the violation can be certified. We leave the quantification of the effect of phase modulation to the subsequent section.

The above scheme has one main technical problem: how to efficiently deliver the modulation information to the legitimate users. In a faithful execution of the QSS protocol, the raw key held by the dealer corresponds to the modulation information, which has an equal size to the raw key held by each user. This forces the controller to actively participate in the implementation and record a phase bit for each coincidence event the users detect, thereby adding to implementation complexity. More preferably, the controller can preshare a string of modulation information with legitimate users and they select the bit, which coincides with a photon detection. This however requires the string to be much longer than the final raw key to offset the significant loss *en route*. One may expect that repeating a fixed-length random binary string can work as the preshared modulation string. However, as we explain in Appendix A, the unauthorized users can always collaborate and reveal the pattern given any finite-size preshared modulation string. As the source needs to generate random bits throughout the session, a practical solution is to use a block cipher algorithm [e.g., Advanced Encryption Standard (AES) [38]] working in stream encryption mode, which is commonly used for bit expansion in prepare-and-measure QKD implementations [39]. In this way, only a small size of preshared randomness is required as the seed.

III. GENUINE PHASE RANDOMIZATION AND DEFENSE AGAINST MEMORY ATTACK

The above scheme though prevents unwanted usage, cannot directly apply to the defense against memory attack [26], in which the attacker is able to learn fully about the measurement choices and outcomes of users. If the attackers combine the data of key generation that was recorded in the previous session, as we discuss in Appendix A, due to the correspondence of measurement results and modulation bits, they know immediately the modulation string according to the raw key. The question is whether it is possible to protect the modulation information from revealing even when the raw key is fully exposed. We show in the following that this is indeed achievable.

The basic idea is to hide the detectable binary pseudo randomness in genuine randomness. Operationally, we choose to apply a random phase with a probability of p to the maximally entangled states so as to destroy the phase correlation. This is practically equivalent to distributing a mixed state to the users, which can be written as

$$\hat{R} = (|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |1\rangle\langle 1| \otimes |1\rangle\langle 1|)/2. \qquad (3)$$

Thus, the source now randomly distributes three possible states to the users: $|\phi^+\rangle$, $|\phi^-\rangle$, and $\hat{R}$ with respective probabilities of $(1-p)/2$, $(1-p)/2$, and p. With the local states at each user unchanged ($\mathbb{1}/2$), the malicious devices cannot reveal the control string from the measurement outcomes because it is impossible to retrieve a specific form of decomposition out of a mixed state without sufficient ancillary information. Even if the devices recorded the raw key and managed to send it out, the eavesdropper still cannot obtain the secure key in previous sessions because the key generation process is encrypted. More precisely, the effective raw key is obtained by sifting out the genuinely random bits from the measurement results. We note that the measurement results should be transferred to and post-processed on isolated and trusted computers, which hold the modulation information.

IV. CONTROLLED ENTANGLEMENT SOURCE PROTOCOL

We now give a detailed description of how our protocol proceeds.

(1) Similar to traditional EB QKD protocols, the distributor and users reconcile the configuration of their respective setups including the synchronization of the clocks [13], but with an extra parameter, the token of the preshared seed.

(2) The selected seed is locally extended to a continuous random string via the same block cipher algorithm working in stream encryption mode. Under a certain rule the (most likely binary) random string is transformed into ternary, in which the proportion of trit “2” is properly set. The rule can be quite simple. For instance, to check every two consecutive bits of the random string, one assigns “2” to the resulting ternary random string if the two consecutive bits are “11,” otherwise assigns “00,” “01,” or “10,” if “00,” “01,” or “10,” respectively. According to the ternary random string, the controller constantly distributes one of the three element state $|\phi^+\rangle$ (trit “0”), $|\phi^-\rangle$ (trit “1”), and $\hat{R}$ (trit “2”) to the users.

(3) The users randomly pick measurement bases to their devices, and obtain a binary outcome (“+” or “−”) upon a photon detection. Note that the measurement choice and the corresponding outcomes could be recorded and leaked if the memory attack is applied.

(4) Given sufficiently many rounds, the controller stops distribution and does not take part in the subsequent procedures. Meanwhile the users publicly announce their measurement bases and sift out the unwanted combination of bases for the protocol.

(5) Among the remaining results, the users choose to publicly announce part of the outcomes of the measurements that are related to security analysis, for instance, measurement σ_{X}, σ_{Y}, and $\sigma_{\mathrm{X}\pm\mathrm{Y}}$. The outcomes of each measurement combination form a classical bit string $\mathbf{T}_O^{1(2)}$ at each side, where the superscripts denote the users. As the clocks are synchronized, a decoding string $\mathbf{T}_D$ can be deduced out of the local random string prepared in stage (1), according to the time of the photon detection—if the user is legitimate. By further omitting trit “2” in $\mathbf{T}_D$, and the corresponding bit in $\mathbf{T}_O^{1(2)}$, the security can be certified

with either user computing the CHSH function from the statics of $\mathbf{T}_O^1 \oplus \mathbf{T}_D$ and $\mathbf{T}_O^2$, or $\mathbf{T}_O^1$ and $\mathbf{T}_O^2 \oplus \mathbf{T}_D$. During this stage, unauthorized users will fail the test, as they will not hold a valid $\mathbf{T}_D$.

To have this more concrete, it is convenient to assume that the user actually holds a string $\mathbf{T}_U$, and we define the effectiveness of control using the correlation between $\mathbf{T}_U$ and $\mathbf{T}_D$:

$$U := \sum_{j \in \mathbf{T}}^{N} \frac{(-1)^j}{N}, \tag{4}$$

where $\mathbf{T} = \mathbf{T}_U \oplus \mathbf{T}_D$ with trits "2" omitted, and N is the length of $\mathbf{T}$. Note that the correlation of mixed state $\hat{R}$ is always zero, and the probability of picking entangled elements is $(1-p)$. Thus with modulation the correlation function can be written as

$$E_{\mathrm{mod}} = U(1-p)E, \tag{5}$$

where E is defined in Eq. (2). For example, if $T_D =$ "01010101," and $T_U =$ "00000000," then $U = 0$. In such a case, the users cannot distinguish completely the correct correlation that should be adopted, which will result in $E_{\mathrm{mod}} = 0$, therefore the obtained $S_{\mathrm{CHSH}} = 0$ (after modulation), and they will have to abort to avoid security risks. For a general T_D, in Appendix B we derive the optimal U for unauthorized users, which is far below the requirement for demonstrating inequality violation, given a reasonably long modulation string.

(6) Once the security is certified, the users can implement the conventional error correction and privacy amplification method to obtain the final secure key, based on the outcomes that are acquired in the same measurement bases. This however means that if the outcomes are exposed, the attacker can always generate the identical key as the method of error correction and privacy amplification are tacitly open, which is exactly how memory attack breaches. By introducing the mixed state, a certain proportion of the raw outcomes are noncorrelated and are omitted at both sides in the postprocessing stage, which is unknowable to the attackers. Thus the secure key deduced from the raw outcomes at the attacker's side is noneffective, despite the same correction and amplification method. The proportion of the mixed state, however, comes with a tradeoff, since the mixed state carries no information but is to interfere the attacks. We note that the setting of p varies depending on the practical situation, such as the channel loss.

We acknowledge that the security against memory attack ultimately derives from the classical secret and the QKD protocol produces no extra permanently secure data. Thus we emphasize that to ensure the long-term reliability of the protocol, the controller needs to communicate regularly (say daily with a small fraction of time) with other users for refreshing the seed rather than using a fixed preshared seed. It is worth mentioning that the controller though controls the QKD implementation, does not gain any information about users' secure key.

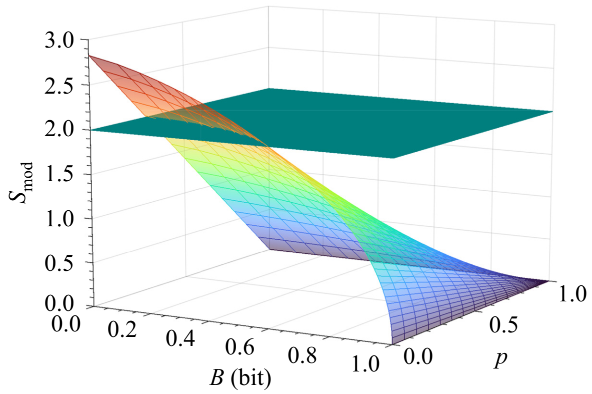

FIG. 2. Diagram of S_{CHSH} being a function with respect to B the binary entropy and p the proportion of the mixed state.

We name the above scheme *controlled entanglement source (CES)* protocol, under which the estimated relation of S_{mod} versus U and p is

$$S_{\mathrm{mod}} = 2\sqrt{2}(1-p)U, \tag{6}$$

which is a direct deduction from Eq. (5). As in the practical implementation, one cares only about the absolute value of S_{CHSH}, we introduce $B = h((1+U)/2)$ to reduce S_{mod} to positive axis for simplicity, where $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary entropy function. Note that B per se has a clear physical meaning, that is, the amount of uncertainty that is to be eliminated for the user to retrieve the correlation. The expression of S_{mod} is visualized in Fig. 2 forming a curved surface. The green plane denotes the threshold of CHSH violation, and the intersection indicates how much information (or how well the mixed state can be distinguished) is needed for the users to demonstrate the violation. For instance, the violation is possible should the entropy B is less than 0.6 bit, according to the intersection point in the (x, z) plane (corresponding to no mixed state is involved), which is equivalent to that over 85.3 % of users' decoding string is identical to the modulation string (or its complement).

V. EXPERIMENTAL SETUP AND RESULTS

To demonstrate the feasibility of our protocol, we implement an experimental setup using off-the-shelf components as schematically shown in Fig. 3. At the dealer's side, a train of phase-modulated [40] pump pulses is sent to a silicon waveguide chip [41,42], in which the time-bin

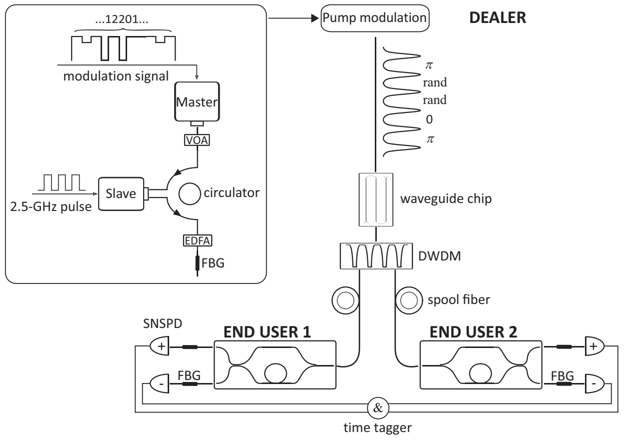

FIG. 3. Experimental setup of controlled entanglement source. Note that digit “2” in the modulation string refers to genuine randomized phase. VOA, variable optical attenuator; EDFA, erbium-doped fiber amplifier; FBG, fiber Bragg grating; SNSPD, superconducting nanowire single-photon detector.

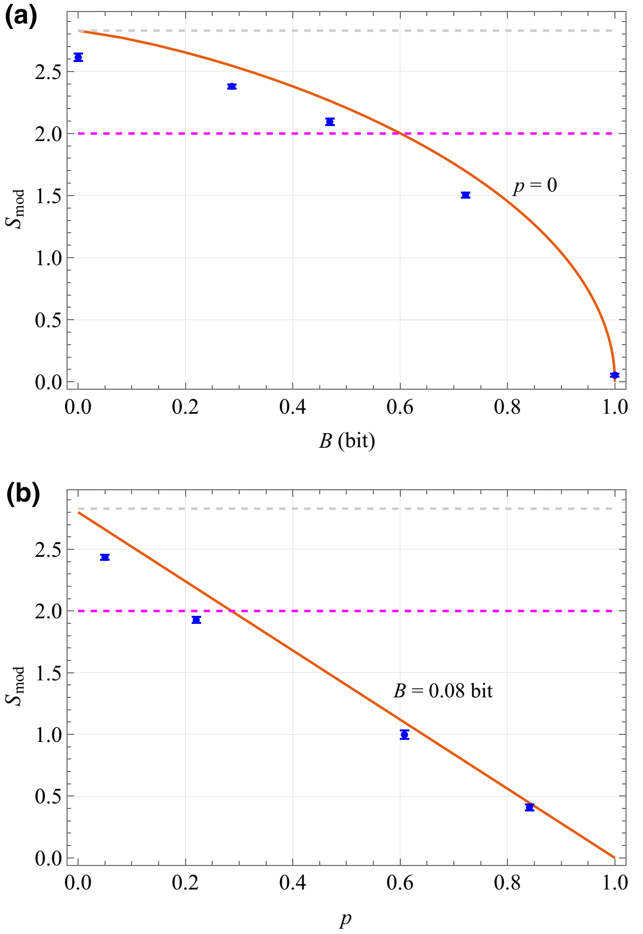

FIG. 4. Experimental results of CHSH parameter versus different controlling configurations. Red solid lines denote the theoretical prediction, and blue dots denote the experimental results. Magenta dashed lines denote the threshold for inequality violation.

entanglement states are realized through spontaneous four-wave mixing (SFWM) effect. Note that in our setup, the asymmetric interferometer which is traditionally deployed at the pump side to induce time-bin superposition state [34] is reduced, which implies that the delay of time bins of our source is reconfigurable. The resulting broadband signal-idler spectrum is then directed to a dense wavelength division multiplexer (DWDM) module thus being divided into multiple channels. Here channels C30 and C37 of the International Telecommunication Union (ITU) grid (full width at half maximum: 25 GHz) are selected for demonstration, and we note that more channels are directly supported in our system. The fiber spool at each quantum link is simulated with a 5-dB fixed attenuator in this proof-of-principle demonstration. Finally the end users receive the controlled entangled states to implement quantum cryptography. A detailed description of the generation of modulation signal and correlation test is provided in Appendix C.

The experimental results are as follows: the overall heralding efficiency of the experimental setup is 1.6 %, including losses from the photonic waveguide chip (−6.5 dB), transmission and coupling (−7 dB), spectral filtering (−4 dB), and photon detection (−0.5 dB). The obtained maximal coincidence rate exceeds 2 kHz, including the ones detected in time basis (the side peaks), with a coincidence to accidental ratio (CAR) of 50. In Figs. 4(a) and 4(b) we present the modulated CHSH parameter results, which are in good agreement with the theoretical model. The gap between data and theory arises mainly from the imperfect interference, and the observed entanglement visibility is 96.1(5) % (see Appendix D for more results), which per se well suffices the requirement of defending against collective attack in device-independent scenario [43]. Note that collective attack is independent of other attacks.

VI. CONCLUSION

Control of access to entanglement resource is shown to be critical in preventing quantum cryptography from unwanted usage and malicious attacks. Inspired by the quantum secret sharing protocol, we propose a protocol to endow conventional entanglement sources with access control, by introducing a twofold phase randomization. We show that by employing our protocol under onefold phase randomization, the entanglement distributor can effectively control users. Further, memory attack on measurement apparatuses can be defended against with the protocol under twofold phase randomization, and the cost is negligible as the measurement devices can be safely reused in our protocol.

We experimentally verify the feasibility of our protocol in a time-bin encoded system using off-the-shelf devices, in which the control to entanglement source is precisely demonstrated. In our setup, the interferometer at the pump side is reduced, which significantly improves the robustness and grants reconfigurability of the delay of time bins to the source. The observed entanglement visibility of our setup is over 96%, which indicates that the traditional collective attack is individually addressed. We believe an upgrade of current entanglement source bases on our protocol can significantly improve its performance and flexibility in quantum cryptography applications.

ACKNOWLEDGMENTS

The authors thank Professor Wei Zhang for providing Si waveguide chips in the early stage of the investigation. This work is supported by National Natural Science Foundation of China under Grants No. 62105034 (L.Z.), No. 12105010 (Q.Z.), and No. 62250710162 (Z.Y.).

APPENDIX A: CHEATING SCHEME FOR UNAUTHORIZED USERS

We first note that in the original three-party QSS protocol, only one of the participants is assumed to be dishonest and the dealer will share its information with the honest one. Notably, there is no point to QSS if both participants are dishonest. In a controlling scenario, the two unauthorized users both gain no information from the source, but it is possible for them to infer which state they are indeed sharing if they collaborate (as they definitely will), which is distinct from QSS but rather fits the third-man quantum cryptography scenario. Trivially, for state $|\phi^+\rangle$, they will with almost certainty (depending on the entanglement visibility) observe coincidence event at the port "++" or "−−" if they both measure σ_X. With the same measurement setting, if they are alternatively sharing state $|\phi^-\rangle$, they will very much likely observe a coincidence event at the output "+−" or "−+." Thus given sufficiently many events, they can finally find the pattern of the modulation string no matter how long (finite) it is.

The only limitation is that on revealing modulation string, they cannot simultaneously do the security certification, which requires switching nonorthogonal measurement bases; nor generate secret keys, where communicating measurement outcomes is prohibited. Hence, the source needs to distribute random bits throughout the session rather than repeating a fixed-length random string, to make sure the unauthorized users do not exploit a pattern to implement QKD protocol.

APPENDIX B: OPTIMAL U FOR UNAUTHORIZED USERS

Without ancillary information, the unauthorized users can only guess a $\mathbf{T}_D$. For simplicity, we assume that $\mathbf{T}_D$ comprises fully "0." If for example, $\mathbf{T}_D$ and $\mathbf{T}_U$ have only one bit difference (specific location of the different bit does not matter), then $U = (N-2)/N$ as there are two opposite bits and would cancel each other. Generally we derive that

$$U = \frac{1}{2^{N-1}N}\sum_{i=0}^{\lfloor N/2\rfloor}\binom{i}{N}(N-2i), \qquad \text{(B1)}$$

the expected value for unauthorized users. Note that the probability of "$\mathbf{T}_D$ and $\mathbf{T}_U$ have n bit difference" is $1/2^N\binom{n}{N}$, and we consider only positive U here. In Fig. 5 we present U as a function of N, in which one finds that $U = 1$ thus above the threshold $1/\sqrt{2}$ only for $N = 0, 1$. For a reasonably long modulation string, it is impossible for unauthorized users to reproduce $\mathbf{T}_D$ and demonstrate violation of Bell-type inequalities.

APPENDIX C: GENERATION OF MODULATION SIGNAL AND THE CORRELATION TEST

As the CES protocol requires three element states, we adopt the direct phase-modulation technique [40] to accurately introduce the desired phase shift or phase randomization to the time-bin entanglement states. A pair of gain-switched distributed feedback (DFB) lasers (Gooch & Housego, typical linewidth, 1 MHz; pulse duration, 80 ps) are modulated by 2.5-GHz signals and employed in optical injection-locking configuration. The remarkable advantage of this setup is that the phase randomization can be readily achieved by switching the master driving signal across the

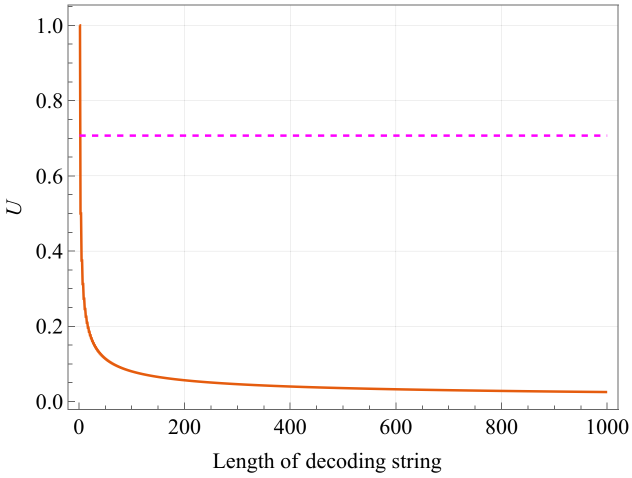

FIG. 5. The expected value of U for unauthorized users as a function of N. Magenta dashed line denotes the threshold for inequality violation.

master laser's lasing threshold. Operationally, as illustrated in the inset of Fig. 3 in the main text, state $|\phi^+\rangle$ corresponds to applying a regular driving voltage to the master laser (signal "0"); state $|\phi^-\rangle$ corresponds to applying a shallow driving voltage (signal "1"), while state $\hat{R}$ corresponds to a reversing voltage (signal "2"). The master laser centered at 1550.52 nm has optical power approximately 80 μW varying depending on the modulation signal. A 2.5-GHz square signal is applied to the slave laser for pulse preparation. The output power of EDFA is 10 mW.

For the detection part, two AMZIs are placed, respectively, at the two end users, which can control the phase thus setting desired measurement bases by varying the temperature. The AMZI is homemade, which comprises two polarization-maintained 50:50 fiber couplers and a set of temperature control modules, and is enclosed by a box to shield it from environmental temperature fluctuations. The time delay of the AMZI is 400 ps, which is in line with the pump-pulse repetition frequency. The phase of AMZI is actively stabilized based on temperature, and a cw reference light beam (not shown in the figure) centered at 1550.52 nm is used to provide the feedback control.

To simulate the cases where unauthorized users or malicious devices somehow gain partially the modulation information, we deliberately set several nontrivial modulation configurations, and then implement the CHSH test. That is to say, we prepare beforehand several nonuniformly distributed random strings such that there is a "bias" in the modulation, which can be regarded as the consequence of breaching. In the postprocessing procedure, we do not implement any operation to the outcome string, this is equivalent to setting a plain $\mathbf{T}_U$ (with full "0" or full "1"), and thus U is solely dependent on $\mathbf{T}_D$ in our experiment. Through the above settings, we essentially characterize how S_{mod} varies given designated values of B and p. Note that in the practical implementation, we first obtain the value of U, then we compute B. The generation of the modulation strings is accomplished by using a random number generator on a desktop computer. For this proof-of-principle demonstration, instead of a large continuous random string via using block cipher algorithm, we adopt a random string comprising 5000 random classical trits, and then load the sequences of string on an arbitrary wave generator (AWG, Tektronix, 70002B) and repeat it to produce the modulation signal. At the users' side, photon coincidence is registered using a time tagger (ID Quantique, ID900) for four pairs of output simultaneously with the time bin of width 100 ps. For each pair of outputs, there are three possible photon arrival times, which results in three equidistant coincidence peaks in the arrival-time histogram. The coincident events in the central peak yield detections in the phase basis, according to which we compute the correlation E and hence the modulated CHSH parameter S_{mod} by varying the measurement basis.

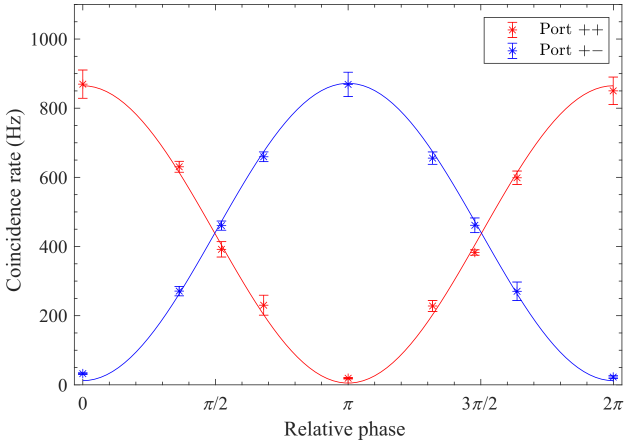

FIG. 6. Interference fringes of AMZI with respect to $|\phi^+\rangle$.

APPENDIX D: CHARACTERIZATION OF INTERFEROMETER

In Fig. 6 we present the experimental results of biphoton interference fringes of outputs "++" and "+−" of the one of the AMZIs, when the source is fixed with state $|\phi^+\rangle$. The red dots denote the rate of coincidence counts from output "++," and blue dots denote the rate of coincidence counts from output "+−." The solid curves are the fitted sinusoidal function of the photon coincident rates.

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

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

[3] A. K. Ekert, Quantum Cryptography Based on Bell's Theorem, Phys. Rev. Lett. **67**, 661 (1991).

[4] H.-K. Lo, X. Ma, and K. Chen, Decoy State Quantum Key Distribution, Phys. Rev. Lett. **94**, 230504 (2005).

[5] X.-B. Wang, Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography, Phys. Rev. Lett. **94**, 230503 (2005).

[6] H.-K. Lo, M. Curty, and B. Qi, Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **108**, 130503 (2012).

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

[8] R. Renner, N. Gisin, and B. Kraus, Information-theoretic security proof for quantum-key-distribution protocols, Phys. Rev. A **72**, 012332 (2005).

[9] C. H. Bennett, G. Brassard, and N. D. Mermin, Quantum Cryptography Without Bell's Theorem, Phys. Rev. Lett. **68**, 557 (1992).

[10] G.-J. Fan-Yuan, F.-Y. Lu, S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, Z. Zhou, Z.-H. Wang, J. Teng, G.-C. Guo, and

Z.-F. Han, Robust and adaptable quantum key distribution network without trusted nodes, Optica **9**, 812 (2022).

[11] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, W. Chen, Y.-G. Zhu, P. V. Morozov, A. V. Divochiy, Z. Zhou, G.-C. Guo, and Z.-F. Han, Twin-field quantum key distribution over 830-km fibre, Nat. Photon. **16**, 154 (2022).

[12] L. Zhou, J. Lin, Y. Jing, and Z. Yuan, Twin-field quantum key distribution without optical frequency dissemination, Nat. Commun. **14**, 928 (2023).

[13] E. Fitzke, L. Bialowons, T. Dolejsky, M. Tippmann, O. Nikiforov, T. Walther, F. Wissel, and M. Gunkel, Scalable Network for Simultaneous Pairwise Quantum Key Distribution via Entanglement-Based Time-Bin Coding, PRX Quantum **3**, 020341 (2022).

[14] J.-H. Kim, J.-W. Chae, Y.-C. Jeong, and Y.-H. Kim, Quantum communication with time-bin entanglement over a wavelength-multiplexed fiber network, APL Photonics **7**, 016106 (2022).

[15] S. P. Neumann, A. Buchner, L. Bulla, M. Bohmann, and R. Ursin, Continuous entanglement distribution over a transnational 248 km fiber link, Nat. Commun. **13**, 6134 (2022).

[16] S. K. Joshi, D. Aktas, S. Wengerowsky, M. Lončarić, S. P. Neumann, B. Liu, T. Scheidl, G. C. Lorenzo, Ž. Samec, L. Kling, A. Qiu, M. Razavi, M. Stipčević, J. G. Rarity, and R. Ursin, A trusted node–free eight-user metropolitan quantum communication network, Sci. Adv. **6**, eaba0959 (2020).

[17] S. Wengerowsky, S. K. Joshi, F. Steinlechner, H. Hübel, and R. Ursin, An entanglement-based wavelength-multiplexed quantum communication network, Nature **564**, 225 (2018).

[18] W. Zhang, T. van Leent, K. Redeker, R. Garthoff, R. Schwonnek, F. Fertig, S. Eppelt, W. Rosenfeld, V. Scarani, C. C.-W. Lim, and H. Weinfurter, A device-independent quantum key distribution system for distant users, Nature **607**, 687 (2022).

[19] D. Mayers and A. Yao, in *Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No.98CB36280)* (IEEE Comput. Soc, Palo Alto, CA, USA, 1998), p. 503.

[20] J. Barrett, L. Hardy, and A. Kent, No Signaling and Quantum Key Distribution, Phys. Rev. Lett. **95**, 010503 (2005).

[21] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, Rev. Mod. Phys. **86**, 419 (2014).

[22] A. Acín, N. Gisin, and L. Masanes, From Bell's Theorem to Secure Quantum Key Distribution, Phys. Rev. Lett. **97**, 120405 (2006).

[23] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Device-Independent Security of Quantum Cryptography Against Collective Attacks, Phys. Rev. Lett. **98**, 230501 (2007).

[24] N. Gisin and B. Gisin, A local hidden variable model of quantum correlation exploiting the detection loophole, Phys. Lett. A **260**, 323 (1999).

[25] M. Ho, P. Sekatski, E. Y.-Z. Tan, R. Renner, J.-D. Bancal, and N. Sangouard, Noisy Preprocessing Facilitates a Photonic Realization of Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **124**, 230502 (2020).

[26] J. Barrett, R. Colbeck, and A. Kent, Memory Attacks on Device-Independent Quantum Cryptography, Phys. Rev. Lett. **110**, 010503 (2013).

[27] W.-Z. Liu, Y.-Z. Zhang, Y.-Z. Zhen, M.-H. Li, Y. Liu, J. Fan, F. Xu, Q. Zhang, and J.-W. Pan, Toward a Photonic Demonstration of Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **129**, 050502 (2022).

[28] D. P. Nadlinger, P. Drmota, B. C. Nichol, G. Araneda, D. Main, R. Srinivas, D. M. Lucas, C. J. Ballance, K. Ivanov, E. Y.-Z. Tan, P. Sekatski, R. L. Urbanke, R. Renner, N. Sangouard, and J.-D. Bancal, Experimental quantum key distribution certified by Bell's theorem, Nature **607**, 682 (2022).

[29] M. Curty and H.-K. Lo, Foiling covert channels and malicious classical post-processing units in quantum key distribution, Npj Quantum Inf. **5**, 1 (2019).

[30] M. Żukowski, A. Zeilinger, M. Horne, and H. Weinfurter, Quest for GHZ states, Acta Phys. Pol. A **93**, 187 (1998).

[31] R. Cleve, D. Gottesman, and H.-K. Lo, How to Share a Quantum Secret, Phys. Rev. Lett. **83**, 648 (1999).

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

[33] Y.-A. Chen, A.-N. Zhang, Z. Zhao, X.-Q. Zhou, C.-Y. Lu, C.-Z. Peng, T. Yang, and J.-W. Pan, Experimental Quantum Secret Sharing and Third-Man Quantum Cryptography, Phys. Rev. Lett. **95**, 200502 (2005).

[34] W. Tittel, H. Zbinden, and N. Gisin, Experimental demonstration of quantum secret sharing, Phys. Rev. A **63**, 042301 (2001).

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

[36] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Proposed Experiment to Test Local Hidden-Variable Theories, Phys. Rev. Lett. **23**, 880 (1969).

[37] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson, Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres, Nature **526**, 682 (2015); M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-Å. Larsson, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin, B. Wittmann, and A. Zeilinger, Significant-Loophole-Free Test of Bell's Theorem with Entangled Photons, Phys. Rev. Lett. **115**, 250401 (2015) ; L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman, K. J. Coakley, S. D. Dyer, C. Hodge, A. E. Lita, V. B. Verma, C. Lambrocco, E. Tortorici, A. L. Migdall, Y. Zhang, D. R. Kumor, W. H. Farr, F. Marsili, M. D. Shaw, J. A. Stern, C. Abellán, W. Amaya, V. Pruneri, T. Jennewein, M. W. Mitchell, P. G. Kwiat, J. C. Bienfang, R. P. Mirin, E. Knill, and S. W. Nam, Strong Loophole-Free Test of Local Realism, Phys. Rev. Lett. **115**, 250402 (2015).

[38] J. Daemen and V. Rijmen, *The Design of Rijndael: AES — the Advanced Encryption Standard* (Springer-Verlag,

Gaithersburg, MD, 2002), p. 238, Specification for the Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197 (2001).

[39] N. Walenta *et al.*, A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing, New J. Phys. **16**, 013047 (2014).

[40] Z. L. Yuan, B. Fröhlich, M. Lucamarini, G. L. Roberts, J. F. Dynes, and A. J. Shields, Directly Phase-Modulated Light Source, Phys. Rev. X **6**, 031044 (2016).

[41] D. Llewellyn, Y. Ding, I. I. Faruque, S. Paesani, D. Bacco, R. Santagati, Y.-J. Qian, Y. Li, Y.-F. Xiao, M. Huber, M. Malik, G. F. Sinclair, X. Zhou, K. Rottwitt, J. L. O'Brien, J. G. Rarity, Q. Gong, L. K. Oxenlowe, J. Wang, and M. G. Thompson, Chip-to-chip quantum teleportation and multi-photon entanglement in silicon, Nat. Phys. **16**, 148 (2020).

[42] X. Chen, Z. Fu, Q. Gong, and J. Wang, Quantum entanglement on photonic chips: A review, Adv. Photon. **3**, 064002 (2021).

[43] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, Device-independent quantum key distribution secure against collective attacks, New J. Phys. **11**, 045021 (2009).