Fully passive quantum conference key agreement

Jinjie Li,[1] Wenyuan Wang,[1,2,*,†] and H. F. Chau[1,2,‡]

[1]*Department of Physics, University of Hong Kong, Pokfulam Road, Hong Kong*

[2]*HK Institute of Quantum Science & Technology, University of Hong Kong, Pokfulam Road, Hong Kong*

(Received 10 September 2024; revised 27 April 2026; accepted 4 November 2026; published 18 November 2026)

Quantum conference key agreement (CKA) provides a secure method for multiparty communication. A recently developed interference-based prepare-and-measure quantum CKA possesses the advantages of measurement-device-independence, namely, being immune to side channels from the detector side. Besides, it achieves good key- rate performance, especially for high-loss channels, due to the use of single-photon interference. Meanwhile, several fully passive QKD schemes have been proposed, which eliminate all side channels from the source modulation side. We extend the fully passive idea to an interference-based CKA, which has a high level of implementation security for many-user communication.

DOI: 10.1103/6bq6-s1tw

I. INTRODUCTION

Quantum key distribution (QKD) enables secure communication between two parties by leveraging the principles of quantum mechanics, resulting in information-theoretic security [1,2]. QKD has been extensively developed both theoretically and experimentally over the past few decades. One major challenge in implementing QKD arises from the side channels that are inherently embedded in imperfect experimental equipment [3–7]. A novel protocol, called MDI-QKD [8], ensures immunity from all loopholes on the detector side. Later, TF-QKD [9,10] was proposed, which possesses the same detector-side immunity and overcomes the fundamental rate-distance limit of QKD by using single-photon interference. While QKD is typically applied between two parties, efforts have been made to explore information-theoretically secure communication among many users through quantum networks or quantum conference key agreement (CKA) [11–22]. In this paper, all CKA use quantum particles and channels. Notably, among the CKA protocols, several recently proposed ones are inspired by TF-QKD and are based on single-photon interference. They can achieve good key-rate performance, especially under high-loss scenarios [23–25].

The side channels from source modulators can be eliminated by applying a recently proposed idea called fully passive QKD [26–30]. Such side channels may leak information to an eavesdropper or be attacked using a Trojan-horse attack [3,6]. Passive decoy [31,32] and passive encoding [32], respectively, remove the active modulators that generate the desired intensity or polarization of signals, replacing them with local detection and postselection. On the other hand, fully passive QKD simultaneously postselects both intensity and polarization, removing all modulators from the sources. This idea was first applied to BB84 [26–28] and later to MDI-QKD [33,34]. Using a different source design, two fully passive schemes for TF-QKD [35] and CV-QKD [36] have also been proposed. Recently, there have also been reports of successful experimental demonstrations of fully passive QKD [29,30]. Those works demonstrated that while enjoying the benefit of better security at the sources, not much key-rate performance needs to be sacrificed.

In this work, we combine the idea of fully passive QKD with CKA, named fully passive CKA, that could possess advantages from both ideas. Our main contributions and the challenges we met in this work are as follows:

(i) We apply the fully passive scheme to a multiuser scenario, along with a phase- mismatching strategy, to achieve a high sifting efficiency and reasonable performance. Fully passive protocols often suffer from heavy sifting, especially in the multiuser scenario. We show that the sifting efficiency is significantly improved using the phase-mismatching method.

(ii) Numerical simulation of fully passive CKA is challenging due to the large number of high-dimensional integration calculations required. However, we show that efficient computation can be

*Contact author: wenyuan.wang@naist.ac.jp

†Present address: Nara Institute of Science and Technology, Japan.

‡Contact author: hfchau@hku.hk

Published by the American Physical Society under the terms of the Creative Commons Attribution 4.0 International license. Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

achieved through the use of a high-performance integration library [37] and an optimized computer program. We also introduce a "branch cutting" method that significantly increases computation efficiency without sacrificing key-rate performance. Details of this method can be found in the Methods section.

(iii) We studied several practical imperfections of the protocol, such as phase-measurement fluctuations, intensity fluctuations, and nonuniform phase distribution. Details can be found in Secs. IV and V.

In this paper, we first briefly recapitulate both passive TF-QKD and active CKA in Sec. II, the details of the fully passive CKA protocol are explained in Sec. III, including the setup preparation, how to perform the protocol, the security proof, and the calculation of key rate. In Sec. IV, we explicitly show simulated results for four-party fully passive CKA. In Sec. V, we provide some discussions on the protocol, as well as potential future development.

II. PREVIOUS WORKS

A. Passive TF QKD

Passive sources remove side channels from the source modulator, and TF-QKD has the MDI property, which removes side channels from the detectors. Fully passive TF-QKD has both advantages.

Reference [35] mainly considers a particular type of TF-QKD protocol, CAL-TF QKD [10] (although the method is potentially extendable to other TF-QKD protocols too). In this passive TF QKD protocol, processes including encoding, decoy-state setting choices, and basis choices are all done by postselection. The key is to use degrees of freedom coming from the randomness of passive sources.

Each party's source setup is just like the one shown in Fig. 1(a), which will be described in the following section. Alice and Bob each make two-phase measurements in their local lab. In a signal round, Alice and Bob both divide their phase domain $[0, 2\pi\}$ into M slices and only postselect those rounds when their two local measurements land in the same slice and their slices are the top slice or the bottom (representing 0 and π phase in TF QKD). In a testing round, they postselect based on the difference of their two local measurements, representing their output intensities.

The process works under very heavy sifting, resulting in poor key-rate performance. However, in Ref. [35], a phase slice-matching strategy was introduced so that all signals could be used and contribute to the key rate. Alice and Bob send the signals to the central node, Charlie, and Charlie announces the measurement results of his two detectors, d1 and d2. The key rate is contributed by two detection patterns, for certain slice combinations, $R(k_{A1}, k_{A2}, k_{B1}, k_{B2}) = R = R_{1,0} + R_{0,1}$, where

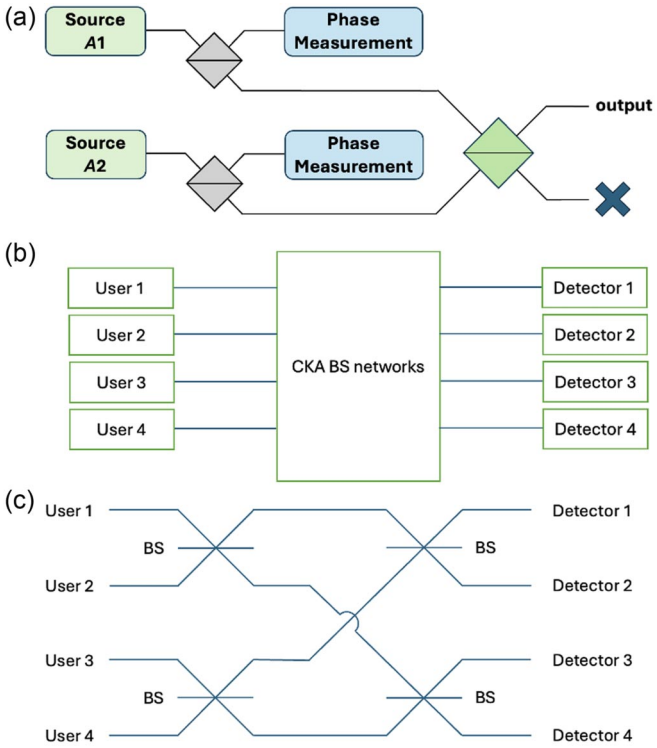


FIG. 1. (a) Fully passive source setup for a single user involves the preparation of two sources by the user. The phases of these two sources are measured. The two legs are combined at a BS, and one output leg is designated as the final output of the fully passive source, based on Ref. [35]. (b) Schematic setup of a four-user CKA, based on Ref. [23]. (c) An example of a four-user BS network, based on Ref. [23]

$R_{d_1,d_2} = p(d_1, d_2)[1 - fh(e_{X,d_1,d_2}) - h(e_{Z,d_1,d_2})]$, where $p(d_1, d_2)$ is the probability of obtaining the click pattern (d_1, d_2), f is the error-correction efficiency, $h(x) = -x \log_2 x - (1-x)\log_2(1-x)$ is the binary entropy function, and e_{X,d_1,d_2} and e_{Z,d_1,d_2} are the quantum bit error rate (QBER) and phase-error rate, respectively.

Because of the phase slice-matching strategy, the total key rate is the sum of all signals:

$$R = \frac{1}{M^4} \sum_{k_{A1},k_{A2},k_{B1},k_{B2}=1}^{M} R(k_{A1}, k_{A2}, k_{B1}, k_{B2}), \qquad (1)$$

where k represents the indices of slices into which the random phase falls, which goes from 1 to M.

B. Conference key agreement

The CKA protocol allows multiple parties to conduct secure communication, and our work is based on a recently proposed CKA protocol based on single-photon interference, which is a generalization of TF-QKD. The protocol enables measurement-device-independence and can tolerate high loss [23].

Each party prepares a WCP source and sends signals to the central node, Charlie, through a network of BSs, as shown in Fig. 1. The parties send many rounds of signals: each round can be either a parameter estimation round, where parties send phase-randomized coherent lights with intensities determined by the decoy-state setting, or a key-generation round, where parties send coherent states. Charlie announces his detection pattern across his multiple detectors. A round is considered successful only if exactly one detector clicks, we denote this single-click event as Ω_j, where j indexes the specific detector that clicked. All other detection patterns are discarded. The parties then perform parameter estimation to calculate the phase-error rate and QBER. The key rate is calculated by

$$R = \sum_{j}^{M} Pr(\Omega_j|PE)\left[1 - h(Q_Z^j) - \max_{i>0} h(Q^j_{X_0,X_i})\right], \quad (2)$$

where the index j represents the detector, and the index i represents the party. Q_Z^j is the phase-error rate, and $Q^j_{X_0,X_i}$ is the QBER between party 0 and party i. In this work, our key rate follows the same structural format; a detailed discussion can be found in Sec. III D and Appendix B.

III. METHOD

We describe our fully passive CKA protocol, which combines the single-photon-interference-based CKA protocol proposed in Ref. [23] with the fully passive TF-QKD source and the source security analysis proposed in Ref. [35].

The fully passive CKA protocol differs from the active CKA in several key aspects:

(i) The application of fully passive sources introduces additional complexity to the channel model, specifically in the yield estimation from decoy-state analysis, which requires certain adjustments.

(ii) Unlike in the active case, where parties must decide whether to perform a key-generation (KG) round or a parameter estimation (PE) round, in the fully passive CKA, all rounds of experiments are performed in the same manner, without the need for basis choosing. This lack of a sifting problem is an advantage for the fully passive case, particularly when the number of users is larger.

(iii) The fully passive CKA is less affected by misalignment in signal preparation, which is another significant advantage.

A. Setup

For a four-user fully passive CKA, each user has a fully passive source. A fully passive source, as shown in Fig. 1(a), consists of two laser sources that are completely random and independent of each other [35]. Each user measures the phases of the two pulses. The random pulses sent from the two sources interfere and the transmitted signal is the final signal sent by the user. For simplicity, throughout the paper, we assume that all users have the same intensity, $u_{\max}/2$, from both laser sources. The final signal from a fully passive source can have any phase between 0 and 2π and any intensity between 0 and $u_{\max}$. One could divide the whole 2π range into an even number, M, of sectors of the same angle, and label the top sector as sector 1, and in ascending order clockwise.

The prepared fully passive sources then go into a CKA beam splitter (BS) network. The CKA network consists of a combination of 50:50 BSs, as shown in Figs. 1(b) and 1(c) [23]. Specifically, the BSs are arranged in s layers, each layer, represented by $r = 0, 1, \ldots, s-1$, contains 2^{s-1} BSs. A four-user example is shown in Fig. 1. Therefore, each layer can accept 2^s input signals, labeled a_i^r, where $i = 0, 1, \ldots 2^s - 1$ represents the position of the input site. In rth layer, the signals a_i^r and $a_{i+2^r}^r$ interfere at the same BS.

To describe the evolution of signals within the BS network, we divide the input signals at each layer into two sets, we define the set

$$F_r := \bigcup_{k=0}^{2^{s-r-1}-1} \left\{\hat{a}_{k2^{r+1}}, \hat{a}_{k2^{r+1}+1} \cdots, \hat{a}_{k2^{r+1}+2^r-1}\right\}, \quad (3)$$

and the remaining signals in the complementary set $\overline{F_r}$. The evolution of signals in rth layer obeys

$$(\hat{a}_i^{(r)})^\dagger \to \frac{1}{\sqrt{2}}\left[(\hat{a}_i^{(r+1)})^\dagger + (\hat{a}_{i+2^r}^{(r+1)})^\dagger\right] \ \forall\ i \in F_r, \quad (4)$$

$$(\hat{a}_j^{(r)})^\dagger \to \frac{1}{\sqrt{2}}\left[(\hat{a}_{j-2^r}^{(r+1)})^\dagger - (\hat{a}_j^{(r+1)})^\dagger\right] \ \forall\ j \in \bar{F}_r. \quad (5)$$

Therefore, the overall evolution of the whole BS network from the input to the final $(s-1)$th layer satisfies

$$\hat{a}_i^\dagger \to \frac{1}{\sqrt{N_D}} \sum_{j=0}^{N_D-1} (-1)^{\vec{j}\cdot\vec{i}} \hat{d}_j^\dagger, \quad (6)$$

where $d_j^\dagger$ represents the output signals, $\vec{j}$ is the binary representation of the detector's position, $j = 0, 1, \ldots, N_D - 1$, where $N_D = 2^s$ is the number of detectors. The vectors $\vec{i}$ is the vector form of binary representation of the user's index, $0, 1, 2, \ldots, N_U - 1$, where $N_U \le 2^s$ is the number of users [23].

B. Protocol

(1) State preparation and measurement: Each party, A_i, prepares the state based on the fully passive source setup and sends out the signals to the untrusted party that possesses the BS network, as shown in Fig. 1(c). Each

party locally measures the two phases, denoted ϕ_{i1} and ϕ_{i2}. Charlie, the untrusted party at the detection side, publicly announces the detection results. A successful event occurs when there is exactly one click (single-click event), and all other unsuccessful events are discarded. The single-click events are labeled as Ω_j, where j denotes which the detector that clicks [23].

(2) Postprocessing: A round of experiment is done when all parties send the fully passive signals and receive Charlie's detection announcement. After a large number of rounds are performed, the first party, A_0, publicly announce a random binary sequence that decides if the corresponding round is a key-generation (KG) round or a parameter estimation (PE) round, with probabilities p_X and $1-p_X$, respectively. One key advantage of our fully passive CKA protocol is that there is no basis sifting across multiple users, as each other user simply chooses the same publicly announced basis as Alice after the transmission. This is because, for our protocol, both the KG and PE round use the same physical signal, and the difference lies only in postprocessing, which can be done after the transmission. This is especially advantageous when the number of users is large. For N_U users, the advantage of sifting efficiency over an active CKA scheme is $p_X^{N_U-1}$.

(2a) KG round: Each party, A_i, divides the whole 2π range into M slices where M must be an even number, and each of their local phase measurements should land into one of the slices indexed k_{i1} and k_{i2}. A KG round is successful only when the slice indices obey $k_{i1}=k_{i2}=1$ for all i, or $k_{i1}=k_{i2}=M/2+1$ for all i. The top slice corresponds to the plus state in X-basis, and hence corresponds to a classical bit 0, and the bottom slice corresponds to the minus state in X-basis, and hence corresponds to a classical bit 1. The unsuccessful events are discarded. This postselection method discards the majority of the signals, resulting in very low sifting. However, we will show in the following sections that the discarded signals can contribute to the key rate. For now, to introduce the protocol clearly, we do not yet consider other signals.

(2b) PE round: Each party, A_i, calculates their local phase differences, $|\phi_{i1}-\phi_{i2}|$, this is equivalent to finding their output signal intensity in the range between 0 and $u_{\max}$. For example, in a three-decoy protocol, each party divides their intensity range into three parts. Each party announces which part their signal falls into based on $|\phi_{i1}-\phi_{i2}|$. In this way, all n parties essentially divide an n-dimensional square into small squares, each square, labeled S_{ijkl}, corresponds to a decoy-state choice by all parties. They perform decoy-state analysis to estimate the yield, $Y_{n_1n_2n_3n_4}$, and subsequently calculate the phase-error rate [35]. Appendix A provides details on how to perform decoy-state analysis for a two-decoy example.

(3) All parties perform many rounds described in step 2. Their raw key is from many succesful KG rounds, each party record(s) a classical 0 or 1 from one successful KG round. All parties perform error correction and privacy amplification to obtain the final key, the same as what would be done in active CKA protocols [23].

C. Security

The security analysis for fully passive CKA should be the same as that of active CKA, except for the imperfections in the source preparation from the fully passive sources. (See Appendix B for a brief summary of the secure key rate of the active CKA.) Instead of having a perfectly prepared signal, the phases can have any value between $[-\Delta,\Delta]$, where $\Delta=\pi/M$. This naturally causes fluctuations in the phases and intensities of the final output signals from the fully passive sources that go into the BS network.

To address this issue, we can apply the analysis from Ref. [35]. One can consider an equivalent local setup that takes in two perfectly prepared signals of intensities $u_{\max}/2$. These signals are split from one perfectly prepared signal, as shown in Fig. 2. Each signal goes through a random phase modulation within the range $[-\Delta,\Delta]$. Then, the two modulated signals combine at a BS, where one of the BS output signals becomes the final output signal. Essentially, this equivalent setup replaces the two randomly generated phases inside the slice $k_{i1}=k_{i2}=1$ with two random phase modulations, ϕ_{A1} and ϕ_{A2}. We name the local channel at each user's lab $\mathcal{E}_{A_i}$, which includes the two-phase modulation and the BSs.

The most pessimistic scenario is that the entire channel is untrusted—we could yield the channel to the eavesdropper, Eve. This would have two effects: (1) In the KG basis, QBER would be higher, and (2) in the PE basis while estimating the yields, there are additional local

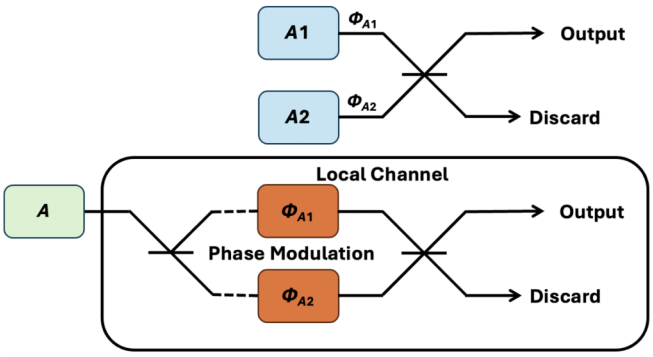


FIG. 2. Two equivalent setups that the top subfigure is a simplified fully passive source for one user, A. A prepares two random sources, A_1, A_2 with phases ϕ_{A1}, ϕ_{A2}, respectively. Two signals join at a BS. Bottom is an equivalent setup to the fully passive source. Alice prepares one (perfectly prepared) source signal split evenly into two signals. Then each signal goes through a random phase modulation, ϕ_{A1}, ϕ_{A2}. Two signals then join at a BS. The local phase modulations and the two BSs are denoted channel $\mathcal{E}_A$.

losses caused by the local channels $\mathcal{E}_{A_i}$ because originally, our estimation of yields from performing decoy-state analysis only represents the external channels, here, one needs to adjust them to include the effects of local channels $\mathcal{E}_{A_i}$. After the adjustments, the "corrected yields" could be used to estimate the phase-error rate. (The details of the corrected yields and the phase-error rate calculation can be found in Appendix C.)

D. Key rate

For an N-user fully passive CKA protocol, the key rate is [23]

$$R = \frac{1}{M^{2N_U}} \sum_{j=0}^{N_D-1} \Pr(\Omega_j|\mathrm{KG}) \left[1 - h(\bar{Q}_Z^j) - \max_{i\geq 1} h(Q_{X_0X_i}^j)\right] \tag{7}$$

The sifting factor $1/M^{2N_U}$ arises from the probability that all parties' slice choices comply with the KG round procedure, as explained in Sec. II A, given that the total number of slices is M. $\Pr(\Omega_j|\mathrm{KG})$ is the probability for a single-click event to happen in a KG round. $\bar{Q}_Z^j$ is the phase-error rate, described above, and $Q_{X_0X_i}^j$ is the QBER for a pair of users, A_0 and A_i [23],

$$Q_{X_0,X_i}^j = \Pr\left(X_0 \neq (-1)^{\vec{j}\cdot\vec{i}} X_i | \Omega_j, \mathrm{KG}\right). \tag{8}$$

The sifting factor, $1/M^{2N}$, may result in a low key rate, but Ref. [35] demonstrates that all other combinations can be utilized, eliminating the heavy sifting problem. First, the factor can be reduced to M^{2N-1} by rotating the global phase reference point freely over 0 to 2π, however, to utilize all other combinations, we need further explanation. We use a two-user case to explain the strategy and one could generalized to multiusers easily.

For two users, slice mismatching falls into four categories, none of which introduce additional loopholes. Therefore, no additional security proof is required. These categories can be mathematically represented by the 4 d.o.f.: $x_1 = (k_{A1} + k_{A2})/2$, $x_2 = k_{A2} - k_{A1}$, $x_3 = (k_{A1} + k_{A2})/2 - (k_{B1} + k_{B2})/2$, and $x_4 = (k_{B2} - k_{B1}) - (k_{A2} - k_{A1})$. The two-user case can be generalized for N users, where the degree of freedom is $2N$, and a similar set of $\{x_1, x_2, \ldots x_{2N}\}$ can represent all possible slice choices. Therefore, the key rates for all combinations can be added up [35], for instance, in the case of a four-user CKA,

$$R = \frac{1}{M^8} \sum_{k_{A1}=1}^{M} \sum_{k_{A2}=1}^{M} \cdots \sum_{k_{D2}=1}^{M} \max\left[0, R(k_{A1}, k_{A2}, \ldots k_{D2})\right], \tag{9}$$

where $R(k_{A1}, k_{A2}, \ldots k_{D2})$ is the key rate for individual slice combinations.

While all slice-choice combinations can contribute to the key rate, most of them do not provide a meaningful contribution. In particular, a combination does not contribute significantly if it satisfies one or a combination of the following conditions:

(i) The input phases mismatch for each party is large.
(ii) The final fully passive signal phases mismatch is large for each pair of parties.

In the simulation results presented in the following section, we have discarded the combinations that satisfy the above conditions. This approach partially resolves the heavy computational burden involved in calculating fully passive CKA key rates. We name the method a "branch cutting" method. (See Appendix D for details.)

IV. SIMULATED RESULTS

Our simulation of asymptotic fully passive CKA with four users involve calculating phase-error rates using both theoretical yields and linear programming to obtain upper bounds with a two-decoy setting. All users have the same intensity for their fully passive sources. Additionally, we compare these results with those of active four-user CKA. We plot key rates against the channel losses between one party and the central node, as shown in Fig. 3. The results show that implementing fully passive sources reduces the

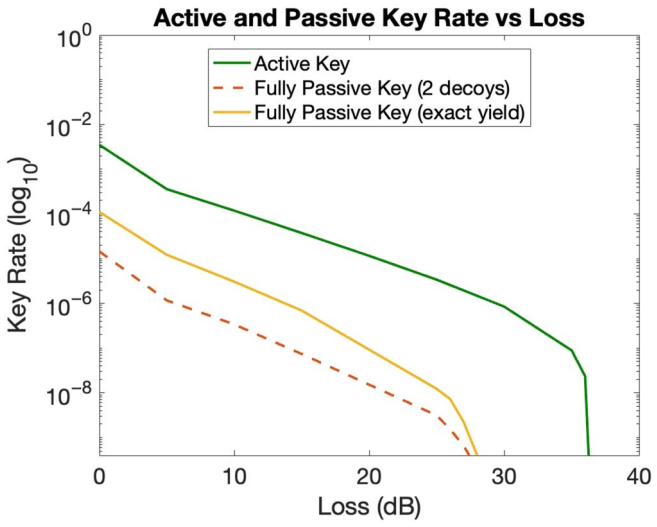


FIG. 3. Key-rate plot against channel losses between one party with the central node, for both four-user fully passive CKA and active CKA. For all cases, the input intensities for all users are the same. The input intensities used in the active CKA plot are optimized. The fully passive CKA intensities used were the same as the active ones for direct comparison. The number of slices used in the fully passive case is $M = 8$, and we have applied the "branch cutting" method (see Sec. III D). The phase-measurement fluctuation is also included (see Appendix E). The dark count used is 10^{-8}.

key rate by around 2 orders of magnitude by using the theoretical yields, and a further reduction of around an order of magnitude by using two-decoy linear programming to calculate yields' upper bounds. In the simulation's two-decoy setting, each party divided their intensity range evenly, as described in Sec III B. The disparity in the two fully passive CKA key-rate simulations could potentially be attributed to the utilization of a reduced number of decoys, which results in a looser bound on the photon number state yields in the two-decoy case. This aspect is discussed in Sec. V as a prospective area for future study. We have, for simplicity, included a phase misalignment of 0.02 rad for one user in our simulation. Moreover, as we tested, applying a phase misalignment of ± 0.02 rad across the users affects the key rate rather little, resulting in only an approximately 2% decrease in the key rate (see Sec. V). Meanwhile, we also included a phase-measurement fluctuation with standard deviation of 5°, see Appendix E for details. The four-user fully passive CKA could reach a communication loss of about 28 dB. While some communication performance is sacrificed, a much better implementation security, by applying fully passive sources, is obtained. In our fully passive CKA simulation, we used a "branch cutting" method to alleviate the heavy computational burden, see Appendix D for details.

V. DISCUSSIONS

In this work, we propose a fully passive CKA scheme that can simultaneously remove side channels from both the detector and source modulation sides. Furthermore, it possesses the benefit of high key rate under highly lossy channels, thanks to the application of single-photon interference. Notably, this work is the first protocol proposed that possesses such a high level of implementation security for multiparty communication.

Our simulation shows that the key rate compared to an active CKA is about 2 to 3 orders of magnitude lower due to the nature of heavy sifting in fully passive schemes. (3 to 4 orders of magnitude lower while using linear programs to perform decoy-state analysis.) However, better implementation security at the source side is achieved, and therefore a reasonable amount of key-rate sacrifice is acceptable. Just like fully passive TF-QKD [35], our fully passive CKA scheme has some additional advantages over the active case, including:

(i) There is no need to choose a basis, as there is no sifting required. This is because the procedure for performing a KG round and a PE round is identical.

(ii) Our protocol possesses an inherent resistance to large phase misalignments, similar to that of fully passive TF-QKD [35]. This arises from the symmetry in the *local* phase-slice reference point for each user. Because the protocol sums the key-rate contributions from all phase positions over 0 to 2π, a misalignment that shifts a user away from their optimal "zero-position" phase slice simply maps them onto another valid phase slice on the circumference.

(iii) We highlight two nuances regarding this symmetric behavior. First, because the phase space is divided into discrete segments (a slice size of $\pi/4$ when $M = 8$), a substantial channel misalignment of $\pi/4 + \delta$ simplifies to a minor misalignment of just δ. Conversely, small misalignments of δ occurring strictly within a slice boundary cannot be fully canceled and will introduce a slight increase in the QBER. Second, to reduce computational overhead in our simulations, we utilized a branch-cutting technique (detailed in Appendix D) that restricts the evaluated phase slices to those near the zero position. Although this approach reliably models realistic, small-scale errors (such as a test with misalignments of 0, $+0.02$, -0.02, and -0.02 rad, which caused around a 2% drop in the key rate at both 5 and 10 dB, applying $[x = y = 3]$ branch-cut setting), it computationally breaks the full rotational symmetry, meaning very large misalignments would not cancel in this specific simulation setup. To handle large misalignments, in principle, one can turn off the branch-cutting setup and include all the phase slices in the calculation.

These advantages are particularly useful in the case of CKA, since a larger number of users would normally induce heavier sifting and more difficulties in aligning.

Several implementation imperfections may need some brief comments here: For the phase distribution, gain-switched lasers were proven to be feasible in experiments for both high-speed MDI-QKD [38] and fully passive BB84 QKD [29,30]. Intensity distributions (which represent phase distributions in passive protocols) and random tests have shown that gain-switched lasers follow the uniform and independent assumptions well. Even if nonuniform phase distributions arise, as long as we can characterize the phase distribution of the source, even if it is nonuniform, and if we can accurately measure the phase of each pulse, we can perform an additional round of postselection to selectively discard signals with different probabilities depending on the measured phase. This strategy, proposed in Ref. [26], aims to "shape" it into a uniform distribution. However, accurately measuring the phase presents another challenge, which we will discuss below.

On the other hand, if phase correlations are present, a recent work [39] has studied the potential higher-order correlations in gain-switched lasers and proposed a security analysis to address this, which is, in principle, also applicable to our scheme. The intensity distributions have demonstrated close adherence to theoretical predictions, suggesting a near-uniform phase distribution [29,30]. Moreover, randomness tests have revealed minimal self-correlation among

intensities, indicating a similar lack of correlation among phases; the robust performance of gain-switched lasers for such randomness generation is well established in both QKD and quantum random number generation [40,41].

In Appendix E, we investigate how phase-measurement fluctuations may impact performance. Our analysis shows that when the phase measurement follows a Gaussian distribution with a standard deviation of 5°, the key rate decreases by approximately 10%.

Furthermore, it is necessary to consider the impact of practical receiver-side and channel imperfections, such as detector-efficiency mismatches and out-of-mode misalignments (e.g., polarization, time, and spatial misalignments). Because our fully passive CKA protocol employs an MDI-type architecture with a completely untrusted central node, receiver-side imperfections cannot open side channels and therefore do not compromise the security proof. They enter solely through the channel model, affecting only the protocol's performance. To evaluate this degradation in a realistic, asymmetric setting, we simulated the four-user protocol with detector efficiency mismatches of 1, 0.94, 0.97, and 0.92, alongside slightly varying dark count rates of 1×10^{-8}, 1.2×10^{-8}, 0.9×10^{-8}, and 1.1×10^{-8}. We also incorporated out-of-mode misalignments of 0, 0.05, −0.03, and 0.04 rad, respectively. Using the $[x=3, y=3]$ branch-cut setting, the key rate decreased by only approximately 1% at both 5 and 10 dB channel losses. This demonstrates that the performance degradation in a realistic setting with receiver-side imperfections is highly negligible.

This work is a proof-of-concept that a fully passive scheme can be applied to a multiuser communication scheme without losing much key-rate performance. However, there is room for further improvement in key-rate performance when higher performance computers are available. These improvements include the optimization of the slice number M, and the input intensity, as well as performing a full calculation of all slice choices without using the "branch cutting" method.

A next step, with higher computational power, is to calculate the performance for more users. Specifically, the scaling law between the number of users and the sifting caused by the application of fully passive sources is planned for future study. Additionally, an experimental realization of the protocol is a subsequent step, and it will be the first fully passive many-user experiment. Incorporating a three-decoy-state analysis may result in tighter yield upper bounds and increase key-rate performance and therefore remains to be implemented in future work.

For finite-size analysis, we cite the results from Ref. [42] (which proposed a finite-size analysis for active CAL TF-QKD) and [35] (which extended it to passive CAL TF-QKD). Notably, Ref. [35] demonstrated that practical performance can be achieved for passive TF-QKD with reasonable data sizes (e.g., $N=10^{13}$). In its analysis, the Z-basis decoy-state estimation remains minimally affected as it only needs to be performed once and is shared across all key-generation sets, while smaller X-basis signal data (due to postselecting phase slices) is a more unique challenge for passive TF-QKD. However, Ref. [35] showed that, using concentration inequalities [42], one can still obtain an acceptable bound on the phase-error rate. This approach is, in principle, applicable to passive CKA, too (which has a structure similar to CAL TF-QKD, and it also allows the sharing of decoy statistics across all key-generation patterns), though a rigorous study will be a subject for future work.

ACKNOWLEDGMENTS

We thank H.-K. Lo. for insightful comments. H. F. C. is supported by the RGC Grant No. 17303323 of the HKSAR Government. W. W. acknowledges support from the University of Hong Kong Seed Fund for Basic Research for New Staff, the Hong Kong RGC General Research Fund (No. 17312922), and the NSFC Young Scientist Fund (No. 12204391).

DATA AVAILABILITY

The data and code that support the findings of this article are openly available [43].

CONFLICTS OF INTEREST

Authors declare no conflict of interest.

APPENDIX A: DECOY-STATE ANALYSIS—TWO-DECOY

Decoy-state analysis is utilized to determine the upper bounds of the yields, denoted as $Y^{Z,j}_{m_A m_B m_C m_D}$, by applying linear programs to the set of equations, in the four-user case [23,35]:

$$G^{j}_{S_{ijkl}} = \sum_{m_A,\cdots,m_D=0}^{\infty} Y^{j}_{m_A,\cdots,m_D} \langle P(m_A, m_B, m_C, m_D)\rangle_{S_{ijkl}} \tag{A1}$$

where $G^{j}_{S_{ijkl}}$ is a direct observable from the channel model, representing the conditional probability of a single-click event in a PE round, given the decoy-state setting S_{ijkl}, $G^{j}_{S_{ijkl}} = \Pr(\Omega_j|S_{ijkl})$ [23].

The average photon number distribution is given by

$$\langle P^{Z}(m_A,\cdots,m_D)\rangle_{S_{ijkl}} = \frac{1}{P_{S_{ijjk}}} \int_{S_{ijkl}} P_{\text{Poisson}}(\mu_A, m_A)\cdots P_{\text{Poisson}}(\mu_D, m_D) P_{\text{int}}(\mu_A,\cdots,\mu_D) d\mu_A \cdots d\mu_D, \tag{A2}$$

where P_{Poisson} is the Poissonian distribution, and

$$P_{S_{ijjk}} = \int_{S_{ijkl}} P_{\text{int}}(\mu_A, \ldots, \mu_D) d\mu_A \cdots d\mu_D, \tag{A3}$$

$$P_{\text{int}}(\mu_A, \cdots, \mu_D) = \frac{1}{\pi^4 \sqrt{\mu_A(\mu_{\max} - \mu_A)} \sqrt{\mu_B(\mu_{\max} - \mu_B)} \sqrt{\mu_C(\mu_{\max} - \mu_C)} \sqrt{\mu_D(\mu_{\max} - \mu_D)}} \tag{A4}$$

is the intensity probability distribution [35]. The bounds obtained from the linear program can then be applied to Eq. (B1) for local loss correction and subsequently to calculate the phase-error rate.

APPENDIX B: ACTIVE CKA KEY RATE [23]

The lower bound of the asymptotic key rate of active CKA with one-way reconciliation, under collective attacks can be written as

$$r \geq \sum_{j=0}^{M-1} \Pr(\Omega_j|\text{KG}) \times [H(X_0|E)_{\Omega_j} - \max_{i \geq 1} H(X_0|X_i)_{\Omega_j}] \tag{B1}$$

where each postselected successful events, Ω_j, corresponds to a separate key, and we add them up to form the final key. Here, M is the number of detectors. The term $H(X_0|E)$ is the entropy of the outcome of a KG round of the first party A_0 given the information held by the eavesdropper. The term $H(X_0|X_i)$ is the entropy of the outcome of a KG round of the first party A_0 given another party A_i's outcome.

APPENDIX C: SECURITY

The imperfect preparation from the two inputs of the fully passive sources can be regarded as two-phase modulation $[-\Delta, \Delta]$, as shown in Fig. 2. As mentioned in the main text, we pessimistically yield the entire channel $\mathcal{E}_{A_i}$, which includes the phase modulations and the two BSs, to Eve. Under this assumption, one obvious effect is the KG basis QBER will be larger. Another effect is that we need to consider the effects of the local channels on PE, specifically, the estimation of yields.

Taking a four-user fully passive CKA as an example, estimates of yields, denoted as $Y^{Z,j}_{m_A m_B m_C m_D}$, can be obtained by performing decoy state analysis. The output photon numbers are represented by m_A, m_B, m_C, and m_D (see Appendix D), while j indicates the single-photon event Ω_j. Here, we explicitly use the superscript Z to indicate that it is in the Z basis for clarity. However, it will be omitted in subsequent equations. While considering the local channel losses, one corrects the yield in the following way:

$$\begin{aligned} Y^j_{n_A n_B n_C n_D} = \int_{-\Delta_\phi}^{\Delta_\phi} \int_{-\Delta_\phi}^{\Delta_\phi} \cdots \int_{-\Delta_\phi}^{\Delta_\phi} \sum_{m_A=0}^{n_A} \sum_{m_B=0}^{n_B} \sum_{m_C=0}^{n_C} \sum_{m_D=0}^{n_D} P_{\phi_{A1},\phi_{A2}}(m_A|n_A) P_{\phi_{B1},\phi_{B2}}(m_B|n_B) \\ P_{\phi_{C1},\phi_{C2}}(m_C|n_C) P_{\phi_{D1},\phi_{D2}}(m_D|n_D)\, Y^j_{m_A m_B m_C m_D} d\phi_{A1} d\phi_{A2} \ldots d\phi_{D2} \end{aligned} \tag{C1}$$

where the local photon loss from m_A, m_B, m_C, m_D to n_A, n_B, n_C, n_D that is represented by a conditional probability $P_{\phi_{A1},\phi_{A2}}(m_A|n_A)$, using party A as an instance [35].

$$P_{\phi_{A1},\phi_{A2}}(m_A|n_A) = \left| \frac{1}{2!} \sqrt{\frac{n_A!}{m_A!(n_A - m_A)!}} [1 + e^{i\pi/2 + (\phi_{A2} - \phi_{A1})}]^{m_A} [1 + e^{i\pi/2 + (\phi_{A2} - \phi_{A1})}]^{(n_A - m_A)} \right|^2, \tag{C2}$$

the yield then can be used to calculate the phase-error rate just as active CKA [23]:

$$\bar{Q}^j_Z = \frac{1}{\Pr(\Omega_j|\text{KG})} \sum_{v \in \mathcal{V}} \left(\sum_{n_0 + \cdots + n_{N-1} \leq \bar{n}} \prod_{i=0}^{N-1} c^{(v_i)}_{i,n_i} \sqrt{\bar{Y}^j_{n_0,\cdots,n_{N-1}}} + \Delta_{v,\bar{n}} \right)^2, \tag{C3}$$

where $\Pr(\Omega_j|\text{KG})$ is the conditional probability that a single-click event happens, given that the round is a KG round, N is the number of users, and $\bar{n}$ is the cutoff photon number used to perform decoy-state analysis, and

$$\mathcal{V} = \{v \in \{0, 2^N - 1\} : |\vec{v}| \bmod 2 = 0\}, \tag{C4}$$

$$c_{i,n}^{(l)} = \begin{cases} e^{-\alpha_i^2/2}\frac{\alpha_i^n}{\sqrt{n!}} & \text{if } n+l \text{ is even,} \\ 0 & \text{if } n+l \text{ is odd,} \end{cases} \tag{C5}$$

$$\Delta_{v,\bar{n}} = \sum_{n_0+\cdots+n_{N-1}\geq \bar{n}+2} \prod_{i=0}^{N-1} c_{i,n_i}^{(v_i)}. \tag{C6}$$

APPENDIX D: BRANCH-CUTTING METHOD

In fully passive CKA, in order to speed up the calculation, we introduce this method to not calculate some slice-choice combinations because those do not contribute meaningful key rate or have zero key rate. These discarded combinations satisfy at least one of the following criteria:

(i) The input phases mismatch for each party is large. Specifically, for party i, let k_{i1} and k_{i2} be her two slice choices, we require $|k_{i1} - k_{i2}| \leq x$ for all i.

(ii) The final fully passive signal phases mismatch is large for each pair of parties. Specifically, for a pair of parties i and j, we demand

$$\frac{k_{i1}+k_{i2}}{2} - \frac{k_{j1}+k_{j2}}{2} \leq y, \tag{D1}$$

for all pairs.

Here, x and y must be a positive integer that is less than the total slice number M. In this paper, $M = 8$ and $x = y = 3$ were used in the simulation shown.

Here, we present in Table I some tests we carried out to observe the trade-off between computational time and key rate by choosing different values of x and y:

APPENDIX E: PHASE-MEASUREMENT FLUCTUATIONS

We also conducted a simulation to investigate how phase-measurement fluctuations affect key rate performance. In this simulation, we incorporated a Gaussian measurement distribution with a standard deviation of 5°. By applying a significance level of three standard deviations on each side, we observed an approximate 10% reduction in key-rate performance.

TABLE I. Trade-off between computational time and key rate for different branch- cutting choices.

Branch cutting choice	Key rate	Computational time
$x = y = 2$	1	1
$x = 2, y = 3$	4	5
$x = 3, y = 2$	6	8
$x = 2, y = 4$	10	23
$x = y = 3$	15	35

During the simulation, we convolved the phase probability distribution with the Gaussian measurement distribution for each slice. Specifically, we first truncated the overall phase distribution $f(\phi)$, originally defined over $[0, 2\pi]$, to create a modified distribution $\tilde{f}(\phi)$ [see Fig. 4(a)]. The truncated phase distribution $\tilde{f}(\phi)$ is explicitly defined as

$$\tilde{f}(\phi) = \begin{cases} f(\phi), & \text{if } \phi \in [\phi_{\text{slice}}^-, \phi_{\text{slice}}^+], \\ 0, & \text{otherwise,} \end{cases}$$

where $[\phi_{\text{slice}}^-, \phi_{\text{slice}}^+]$ denotes the angular range of the slice of interest, and $f(\phi)$ is the original phase probability distribution. We then convolved $\tilde{f}(\phi)$ with the Gaussian distribution $G(\phi)$:

$$(\tilde{f} * G)(\phi) = \int_{-\infty}^{\infty} \tilde{f}(\phi')G(\phi - \phi')d\phi'.$$

The resulting distribution was integrated using extended limits, widened by three standard deviations (3σ) on each side compared to the original integration range [see Fig. 4(b)].

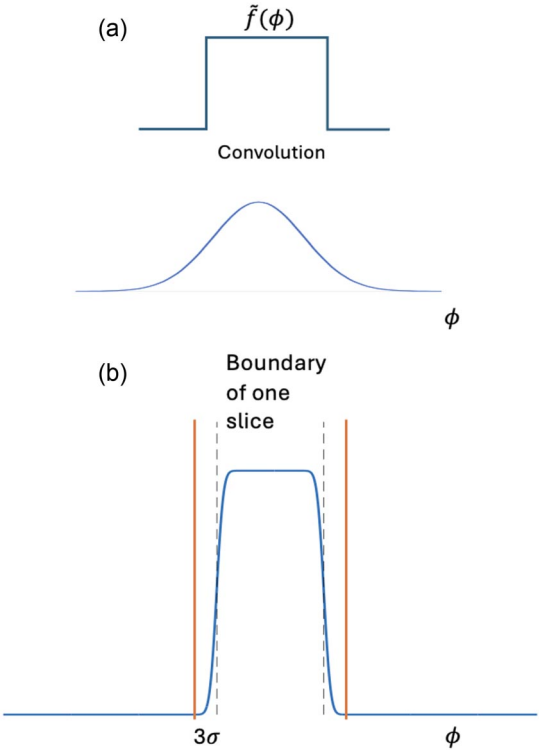


FIG. 4. (a) Truncated distribution $\tilde{f}(\phi)$ and a Gaussian distribution. (b) Resulting distribution after convolution. Dashed lines denote the original slice boundaries, while orange lines indicate the integration limits extended by 3σ.

Including phase-measurement fluctuations and applying finite integration limits led to two effects: (1) a small loss of signal in the distribution tails, and (2) a slight increase in quantum bit error rate (QBER). These factors collectively resulted in a minor reduction in the achievable key rate.

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

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

[3] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Trojan-horse attacks on quantum-key-distribution systems, Phys. Rev. A **73**, 022320 (2006).

[4] K. Tamaki, M. Curty, and M. Lucamarini, Decoy-state quantum key distribution with a leaky source, New J. Phys. **18**, 065008 (2016).

[5] J. E. Bourassa, A. Gnanapandithan, L. Qian, and H.-K. Lo, Measurement-device-independent quantum key distribution with passive time-dependent source side channels, Phys. Rev. A **106**, 062618 (2022).

[6] K.-I. Yoshino, M. Fujiwara, K. Nakata, T. Sumiya, T. Sasaki, M. Takeoka, M. Sasaki, A. Tajima, M. Koashi, and A. Tomita, Quantum key distribution with an efficient countermeasure against correlated intensity fluctuations in optical pulses, npj Quantum Inf. **4**, 8 (2018).

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

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

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

[10] M. Curty, K. Azuma, and H.-K. Lo, Simple security proof of twin-field type quantum key distribution protocol, npj Quantum Inf. **5**, 64 (2019).

[11] K. Chen and H.-K. Lo, Multi-partite quantum cryptographic protocols with noisy GHZ states (2004).

[12] W. Huffman and V. Pless, Fundamentals of error-correcting codes.

[13] G. Murta, F. Grasselli, H. Kampermann, and D. Bruß, Quantum conference key agreement: A review, Adv. Quantum Technol. **3**, 2000025 (2020).

[14] Z. Zhang, R. Shi, and Y. Guo, Multipartite continuous variable quantum conferencing network with entanglement in the middle, Appl. Sci. **8**, 1312 (2018).

[15] C. Ottaviani, C. Lupo, R. Laurenza, and S. Pirandola, Modular network for high-rate quantum conferencing, Commun. Phys. **2**, 118 (2019).

[16] F. Grasselli, H. Kampermann, and D. Bruß, Finite-key effects in multipartite quantum key distribution protocols, New J. Phys. **20**, 113014 (2018).

[17] M. Epping, H. Kampermann, C. macchiavello, and D. Bruß, Multi-partite entanglement can speed up quantum key distribution in networks, New J. Phys. **19**, 093012 (2017).

[18] K. Horodecki, M. Winczewski, and S. Das, Fundamental limitations on the device-independent quantum conference key agreement, Phys. Rev. A **105**, 022604 (2022).

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

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

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

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

[23] G. Carrara, G. Murta, and F. Grasselli, Overcoming fundamental bounds on quantum conference key agreement, Phys. Rev. Appl. **19**, 064017 (2023).

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

[25] F. Grasselli, H. Kampermann, and D. Bruß, Conference key agreement with single-photon interference, New J. Phys. **21**, 123002 (2019).

[26] W. Wang, R. Wang, C. Hu, V. Zapatero, L. Qian, B. Qi, M. Curty, and H.-K. Lo, Fully passive quantum key distribution, Phys. Rev. Lett. **130**, 220801 (2023).

[27] V. Zapatero, W. Wang, and M. Curty, A fully passive transmitter for decoy-state quantum key distribution, Quantum Sci. Technol. **8**, 025014 (2023).

[28] V. Zapatero and M. Curty, Finite-key security of passive quantum key distribution, Phys. Rev. Appl. **21**, 014018 (2024).

[29] F.-Y. Lu, Z.-H. Wang, V. Zapatero, J.-L. Chen, S. Wang, Z.-Q. Yin, M. Curty, D.-Y. He, R. Wang, W. Chen, G.-J. Fan-Yuan, G.-C. Guo, and Z.-F. Han, Experimental demonstration of fully passive quantum key distribution, Phys. Rev. Lett. **131**, 110802 (2023).

[30] C. Hu, W. Wang, K.-S. Chan, Z. Yuan, and H.-K. Lo, Proof-of-principle demonstration of fully passive quantum key distribution, Phys. Rev. Lett. **131**, 110801 (2023).

[31] M. Curty, T. Moroder, X. Ma, and N. Lütkenhaus, Non-Poissonian statistics from Poissonian light sources with application to passive decoy state quantum key distribution, Opt. Lett. **34**, 3238 (2009).

[32] M. Curty, X. Ma, B. Qi, and T. Moroder, Passive decoy-state quantum key distribution with practical light sources, Phys. Rev. A **81**, 022310 (2010).

[33] J. Li, W. Wang, and H.-K. Lo, Fully passive measurement-device-independent quantum key distribution, Phys. Rev. Appl. **21**, 064056 (2024).

[34] X. Wang, F.-Y. Lu, Z.-H. Wang, Z.-Q. Yin, S. Wang, J.-Q. Geng, W. Chen, D.-Y. He, G.-C. Guo, and Z.-F. Han, Fully

passive measurement-device-independent quantum key distribution, Phys. Rev. Appl. **21**, 064067 (2024).
[35] W. Wang, R. Wang, H. F. Chau, and H.-K. Lo, Fully-passive twin-field quantum key distribution, arXiv:2304.12062.
[36] C. Li, C. Hu, W. Wang, R. Wang, and H.-K. Lo, Passive continuous variable quantum key distribution, arXiv:2212.01876.
[37] T. Hahn, Cuba—a library for multidimensional numerical integration, Comput. Phys. Commun. **168**, 78 (2005).
[38] R. I. Woodward, Y. S. Lo, M. Pittaluga, M. Minder, T. K. Paraïso, M. Lucamarini, Z. L. Yuan, and A. J. Shields, Gigahertz measurement-device-independent quantum key distribution using directly modulated lasers, npj Quantum Inf. **7**, 58 (2021).
[39] A. Marcomini, G. Currás-Lorenzo, D. Rusca, A. Valle, K. Tamaki, and M. Curty, Characterising higher-order phase correlations in gain-switched laser sources with application to quantum key distribution (2024).
[40] L. C. Comandar, M. Lucamarini, B. Fröhlich, J. F. Dynes, A. W. Sharpe, S. W.-B. Tam, Z. L. Yuan, R. V. Penty, and A. J. Shields, Quantum key distribution without detector vulnerabilities using optically seeded lasers, Nat. Photonics **10**, 312 (2016).
[41] C. Abellán, W. Amaya, M. Jofre, M. Curty, A. Acín, J. Capmany, V. Pruneri, and M. W. Mitchell, Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode, Opt. Express **22**, 1645 (2014).
[42] G. Currás-Lorenzo, Á. Navarrete, K. Azuma, G. Kato, M. Curty, and M. Razavi, Tight finite-key security for twin-field quantum key distribution, npj Quantum Inf. **7**, 22 (2021).
[43] J. Li, C++ simulation code for fully passive quantum conference key agreement (CKA), Zenodo (2025), 10.5281/zenodo.17803836.