Fully Passive Quantum Key Distribution

Wenyuan Wang,[1,*] Rong Wang,[1] Chengqiu Hu,[1] Victor Zapatero,[2,3,4] Li Qian,[5,6] Bing Qi,[7] Marcos Curty,[2,3,4] and Hoi-Kwong Lo[1,5,8,6,9,†]

[1]*Department of Physics, University of Hong Kong, Pokfulam Road, Hong Kong*
[2]*Vigo Quantum Communication Center, University of Vigo, Vigo E-36310, Spain*
[3]*Escuela de Ingeniería de Telecomunicación, Department of Signal Theory and Communications, University of Vigo, Vigo E-36310, Spain*
[4]*AtlanTTic Research Center, University of Vigo, Vigo E-36310, Spain*
[5]*Department of Electrical and Computer Engineering, University of Toronto, Toronto, Ontario, M5S 3G4, Canada*
[6]*Centre for Quantum Information and Quantum Control (CQIQC), University of Toronto, Toronto, Ontario, M5S 1A7, Canada*
[7]*Cisco Systems, San Jose, California 95134, USA*
[8]*Department of Physics, University of Toronto, Toronto, Ontario, M5S 1A7, Canada*
[9]*Quantum Bridge Technologies, Inc., 100 College Street, Toronto, Ontario, M5G 1L5, Canada*

(Received 29 November 2022; accepted 19 April 2023; published 31 May 2023)

We propose a fully passive linear optical quantum key distribution (QKD) source that implements both random decoy-state and encoding choices with postselection only, thus eliminating all side channels in active modulators. Our source is general purpose and can be used in, e.g., BB84, the six-state protocol, and reference-frame-independent QKD. It can even potentially be combined with measurement-device-independent QKD to achieve robustness against side channels in both detectors and modulators. We also perform a proof-of-principle experimental source characterization to show its feasibility.

DOI: 10.1103/PhysRevLett.130.220801

Background.—Quantum key distribution (QKD) [1,2] offers, in principle, information-theoretic security for communication between two users, Alice and Bob. However, practical imperfections including side channels may lead to security loopholes [3–8]. While measurement-device-independent QKD [9] removes all side channels from the detectors, *source* imperfections remain a challenge to the practical security of QKD systems. For instance, modulators may introduce side channels [5,6] and are susceptible to Trojan horse attacks [3,4] from Eve.

Passive decoy-state setups [10,11] and a passive encoding scheme [12] have both been proposed for QKD, which respectively perform the decoy-state [13–15] intensity choice and the BB84 state choice by only performing postselection on measurement results, thus avoiding the use of source modulators [16]. An illustration of them can be found in Figs. 1(a) and 1(b).

Nonetheless, up to now, for more than 10 years, passive encoding has never been successfully combined with passive decoys with linear components and weak coherent pulse (WCP) sources. The main challenge is this: *the intensity and polarization of the prepared states are coupled in a passive QKD setup*. This makes passive-encoding QKD incompatible with the standard decoy-state analysis, thus severely limiting its practical use.

Our contribution.—In this Letter, we make two main contributions: (1) we design a *passive source* capable of creating a coherent state of arbitrary polarization and arbitrary intensity with only linear optics. (2) We propose a class of *passive QKD protocols* using our new source and design a set of postselection strategies to decouple the intensity and polarization distributions and enable decoy-state analysis.

This work allows *fully passive* QKD with both encoding and decoy setting choices implemented passively via local detection and postselection only, hence eliminating all side channels in the source modulators. Importantly, our source is *general purpose* and can be used in various protocols. Indeed, the class of passive protocols we propose in this work is only one example. Our approach can also potentially be combined with measurement-device-independent (MDI) protocols to further eliminate detector side channels and enable even higher implementation security. We believe that this work will open up a whole new direction of highly practical fully passive QKD systems.

Some alternative approaches worth noting include Refs. [24–26]. A brief discussion of the difference between our proposal and each of them is included in the Supplemental Material [27], Sec. A.

Fully passive source.—As shown in Fig. 1(c), we propose a setup where Alice uses four laser sources operating at the strong light level. Importantly, we assume all lasers are independently phase-randomized, the justification of which will be discussed in a later section. Two pairs of lasers respectively interfere in a setup similar to that of passive decoy-state generation, outputting signal pulses with arbitrary intensities μ_H and μ_V (between 0 and $\mu_{\max}$, the sum of intensities from one pair of lasers) and random phases ϕ_H

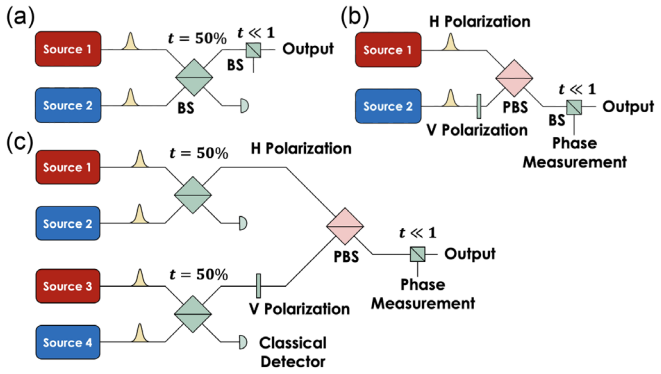

FIG. 1. (a) Passive decoy-state setup [10,11]. The output intensity is determined by the random phase difference between the two sources. Alice postselects the intensity with a classical detector to prepare decoy-state settings. (b) Passive encoding setup [12]. The output polarization is determined by the random phase difference between two sources. Alice postselects the polarization with a phase measurement to prepare BB84 states. (c) Our fully passive source. The output state is a phase-randomized coherent state with arbitrary polarization and arbitrary intensity. Alice can postselect based on observations from her two classical detectors and her phase measurement between the H and V modes. Here, the sources emit *strong* light, which is attenuated to the single-photon level before being sent out. The same setup is applicable to time-bin phase encoding if we replace the polarizer and the polarizing beam splitter with a delay line and a beam splitter.

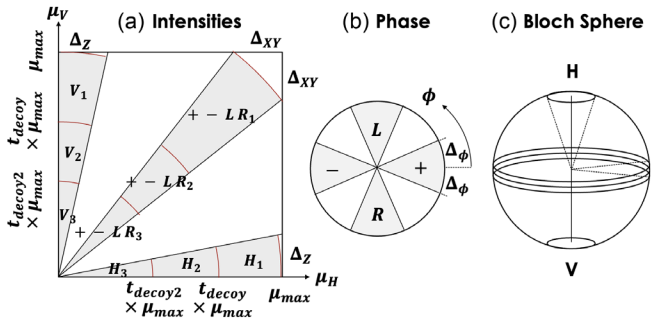

FIG. 2. (a) Postselection on intensities (μ_H, μ_V). The shaded regions correspond to the Z basis and X-Y plane on the Bloch sphere. The slope $x = \mu_V/\mu_H$ on this plot determines the latitude (polar angle) θ_{HV} of the state on the Bloch sphere. The postselected regions can further be divided into subregions to implement decoy states. (b) The phase postselection step that determines the longitude of the state, which helps Alice determine, e.g., the X basis and Y basis polarization states. (c) Corresponding states on the Bloch sphere based on the intensity postselection step.

and ϕ_V. The pulses are rotated into H and V polarizations and combined at a polarizing beam splitter. The output state is still a coherent state, with intensity $\mu = \mu_H + \mu_V$ and a global random phase (say ϕ_H [40]). The polarization mode can be described by the creation operator

$$a^\dagger_{\theta_{HV},\phi_{HV}} = \cos(\theta_{HV}/2)a^\dagger_H + e^{i\phi_{HV}} \sin(\theta_{HV}/2)a^\dagger_V, \quad (1)$$

where we have defined $\theta_{HV} = 2\cos^{-1}[\sqrt{\mu_H/(\mu_H+\mu_V)}]$ and $\phi_{HV} = \phi_V - \phi_H$ (the polar and azimuthal angles that uniquely determine a state on the Bloch sphere). This means that, given a set of input parameters $(\mu_H, \mu_V, \phi_H, \phi_V)$, we can always map it to some phase-randomized coherent state with some polarization on the Bloch sphere. In fact, even the inverse holds true (a proof can be found in the Supplemental Material, Sec. B), i.e., any desired intensity within $(0, \mu_{\max})$ [41] and any polarization on the Bloch sphere can be created by some parameters $(\mu_H, \mu_V, \phi_H, \phi_V)$. This means that our source is general purpose and is capable of creating a coherent state with arbitrary intensity and polarization on the Bloch sphere while also maintaining global phase randomization.

Passive protocol.—To use the source, Alice needs to use the observations from her classical measurements to decide on a set of postselection strategies to determine the states she intends to prepare. Here, as an example, we show how she can prepare six polarization states $\{H, V, +, -, L, R\}$ in three bases and perform the decoy-state analysis. Note that this is not her only possible choice, but we select this set of states as they can be used in a wide class of symmetric [42] protocols such as BB84, reference-frame-independent (RFI) QKD, and the six-state protocol. A pair of such sources can even in principle be used for MDI-QKD or RFI-MDI-QKD. Alice can perform two types of postselection: (1) Alice observes $(\mu_H, \mu_V, \phi_{HV})$ from her measurements and defines postselection regions $\{S_i\}$ on these variables. Signals that fall within a region are considered to be prepared in the given state. An example set of $\{S_i\}$ can be found in Fig. 2, which allows us to prepare states in six polarizations $\{H, V, +, -, L, R\}$, and also prepare various decoy settings using the subdivided regions. (2) Importantly, Alice can perform an *additional postselection* on the signals to either keep or discard signals based on an arbitrary distribution $q_\mu(\mu_H, \mu_V)$. This is equivalent to a coin flip whose bias depends on the values (μ_H, μ_V) that Alice measures. This allows Alice to shape the natural intensity probability distribution resulting from the passive decoy interferometers $p_\mu(\mu_H, \mu_V) = 1/[\pi^2\sqrt{\mu_H(\mu_{\max}-\mu_H)\mu_V(\mu_{\max}-\mu_V)}]$ into an arbitrary distribution $p'_\mu = p_\mu \times q_\mu$ she desires. For this, Alice requires some local random bits, which could be obtained from a quantum random number generator. This strategy can be used in our decoy-state analysis to decouple the distribution of polarization from intensities. An illustration can be found in Fig. 3.

A main difference between a passive QKD protocol and an active one is that, in the former, all states Alice prepares are postselected over finite regions $\{S_i\}$. This results in two problems: (1) each of the decoy settings represents a collection of WCP states with a continuous range of (i.e., mixed) polarizations and intensities. We need to use these collections of states to estimate the single-photon statistics. (2) The single-photon component in the signal

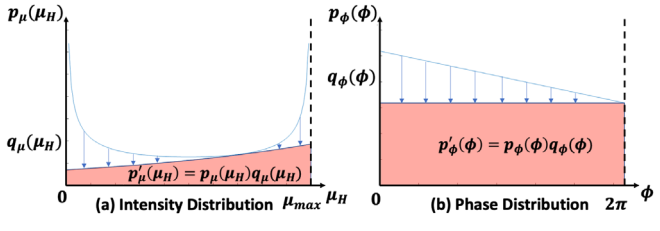

FIG. 3. Examples of additional postselection on intensity or phase distribution by Alice. We can use this technique to, e.g., modify the intensity distributions of μ_H or μ_V, or to shape a nonuniform but known phase distribution into a uniform one.

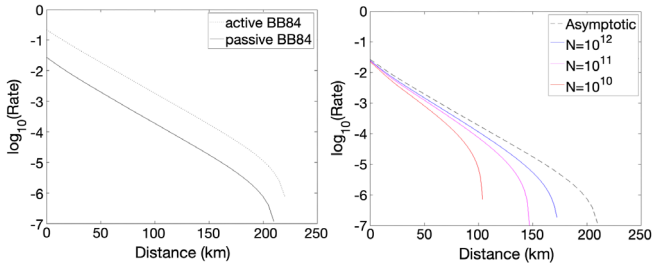

FIG. 4. Left: key rate comparison between active and fully passive decoy-state BB84 assuming infinite data size, using the strategy in Fig. 2. The size of the Z basis postselection regions and the maximum intensities are optimized. Right: key rate simulation for fully passive decoy-state BB84 under finite-size effects (considering collective attacks) with different data sizes. A full optimization on all postselection parameters is performed.

state, say in the Z basis, has mixed polarizations too. This is an encoding imperfection and requires additional security analysis. (Ref. [44] studied a similar imperfection, although its analysis is only applicable to MDI-QKD.)

We address the problem in two steps: (1) we design specific postselection regions that allow us to perform standard decoy-state analysis and obtain the upper and lower bounds on the statistics for *perfectly prepared* single photons, $\{Y_1^{\text{perfect}}, e_1 Y_1^{\text{perfect}}\}$. (2) We show that the mixed polarization in the single-photon state preparation does not increase the privacy amplification amount needed, i.e., we can simply use the statistics from perfectly encoded photons to calculate the key rate.

First, let us look at the decoy states. Because of the finite postselection regions, in order to estimate the yields (a similar argument applies to the error yields), the linear constraints take the form of

$$\langle Q\rangle_{S_i} = \sum_{n=0}^{\infty} \langle P_n Y_n\rangle_{S_i}, \tag{2}$$

where the brackets represent integrating over S_i and calculating the expected value, while Q, P_n, and Y_n are respectively the gain, the Poissonian distribution, and the n-photon yield.

The biggest challenge is that the decoy states have *mixed* and *correlated* polarizations and intensities, resulting in P_n and Y_n being *coupled*, as both P_n and Y_n depend on the polarization of the signal (which takes a range of values in S_i). This prevents us from constructing a linear program for the decoy analysis. To solve this problem, we prove that, if we use the particular "sector-shaped" regions in Fig. 2(a), and use postselection to shape the intensity distribution into $p_\mu \propto \exp(\mu_H + \mu_V)$, we can decouple the polarization distribution from the average photon number distribution and rewrite Eq. (2) as

$$\langle Q\rangle_{S_i} = \sum_{n} \langle P_n\rangle_{S_i} \times Y_n^{\text{mixed}}, \tag{3}$$

where Y_n^{mixed} is the yield Y_n integrated over all possible polarization angles (θ_{HV}, ϕ_{HV}) in S_i following an angular probability distribution. Importantly, Y_n^{mixed} is in general different for each S_i (meaning that a linear program cannot be constructed), but our specific postselection strategy allows Y_n^{mixed} to be the same for all decoy settings S_i. A rigorous proof can be found in the Supplemental Material, Sec. C. Equation (3) can be solved as a linear program to obtain the lower bound $Y_1^{\text{mixed},L}$ (and similarly the upper bound $e_1 Y_1^{\text{mixed},U}$ for the error yield). We also prove that, specifically for single photons, $Y_1^{\text{mixed},L}$ and $e_1 Y_1^{\text{mixed},U}$ happen to respectively also be lower and upper bounds on the yield and error yield Y_1^{perfect} and $e_1 Y_1^{\text{perfect}}$ of single-photon states prepared with perfect polarizations.

We further show that the mixed polarizations in the single-photon components of the signal state do not increase the amount of privacy amplification needed. In simple words, if we consider the equivalent entanglement distribution picture, the imperfect single-photon state preparation is equivalent to noisy positive operator-valued measures (i.e., classical postprocessing noise) in Alice's system. This means that Eve cannot gain additional information. A detailed proof can be found in the Supplemental Material, Sec. D. We can then simply use the aforementioned perfect statistics to estimate the privacy amplification amount when calculating the key rate, i.e., $Y_1^{\text{perfect},Z}[1 - h_2(e_1^{\text{perfect},X})]$.

Simulation results.—We include numerical simulation results for the fully passive decoy-state BB84 protocol in Fig. 4. A simulation for passive RFI-QKD can also be found in the Supplemental Material, Sec. H. We set a misalignment of $e_d = 2\%$ on the X-Z plane, per-detector dark count $p_d = 10^{-6}$, detection efficiency of 1 (merged into channel loss), error-correction efficiency of $f_e = 1.16$, and a failure probability of $\epsilon = 10^{-7}$ for the finite-size scenario. We see that, asymptotically, the fully passive protocol has reasonable performance, albeit having about a 1 order of magnitude lower key rate compared to its active counterpart, mainly due to the sifting factor resulting from postselection and the inherent quantum bit error rate due to using finite postselection regions. We can also see that, despite extensive postselection, the protocol has quite good

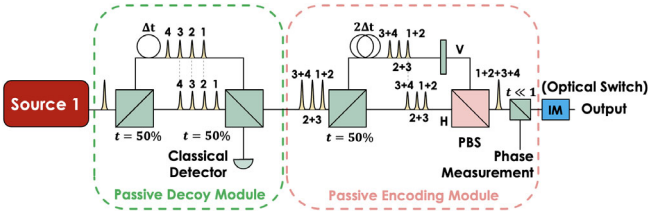

FIG. 5. An equivalent setup for a fully passive source using only one single laser. This setup makes use of two delay lines of Δt and $2\Delta t$ to interfere four independent pulses from different time bins. Here, we need to use a fixed-intensity modulator (or an optical switch) to suppress every three out of four output pulses. Note that this does not leak additional information as a fixed pattern of signals is selected and no random number is used [56].

performance in the finite-size scenario, even with a relatively small data size like $N = 10^{10}$ sent by Alice.

Experimental considerations.—Our proposed scheme depends on three key assumptions: (1) the phase distributions from the sources are random, uniform, and independent. (2) Alice can accurately measure the intensities and the phase of each pulse. (3) The four laser pulses can be maintained at the same intensities, polarizations, and frequencies for high interference visibility. Assumption 1 is in fact a prerequisite for active QKD, too, and there have been successful implementations of QKD systems [45] relying only on the phase randomness of the source without active phase randomization, as well as usage of such randomness in quantum random number generators [46–50]. Assumption 2 imposes requirements on Alice's measurement devices, where inaccuracies resulting in imperfect characterization of $\langle P_n \rangle_{S_i}$ in the decoy-state analysis would have similar effects as intensity fluctuations in active QKD. Assumption 3

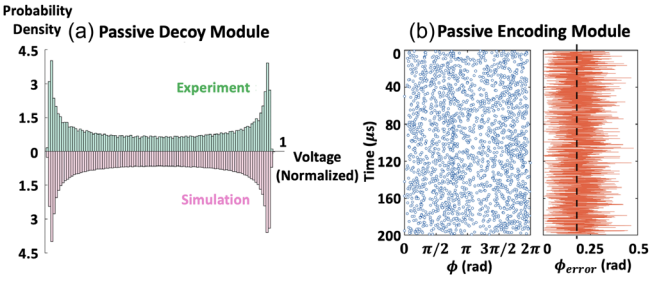

FIG. 6. (a) Histogram of experimentally observed intensities for the passive decoy module. It follows the theoretical prediction well, implying uniform phase distribution, good measurement accuracy, and good interference visibility. Additionally, the intensity data passed an autocorrelation test, implying randomness of phase distribution. (b) Measured phase ϕ and characterized error ϕ_{error}, showing we can perform accurate phase measurement. Phase measurements are performed by measuring in the X or Y bases (detailed setup included in the Supplemental Material, Sec. J). For simplicity, the passive encoding module is separately tested from the passive decoy module, meaning that here we only create and measure states randomly on the equator of the Bloch sphere.

may pose a bigger challenge for experimentalists. While interference from off-the-shelf WCP sources has been reported [52–55], frequency mismatch in our setup will result in phase drift, so one would need to choose narrow laser bandwidths and short pulse widths. We also propose an alternative setup in Fig. 5, where we use a single laser, delay lines, and an optical switch to implement the source and avoid frequency mismatch.

We have performed a proof-of-principle experimental characterization of our source to show its feasibility. We build our system based on Fig. 5, which sequentially consists of a single gain-switched laser, a passive decoy module, and a passive encoding module. In Fig. 6 we show that the source has random and uniform phase distribution and that we can perform accurate intensity and phase measurements.

Discussion.—In this Letter, we have presented a simple yet effective scheme to implement a fully passive QKD protocol and applied it to passive decoy-state BB84 (and to RFI-QKD in the Supplemental Material). Our source is in principle also compatible with MDI-QKD, and a similar postselection idea can even be applied to twin-field QKD sources.

We thank Yue Jiang, Kai Sum Chan, Chenyang Li, Yujia Zhou, and Xiaohao Chen for helpful discussions. This project is financially supported by the University of Hong Kong start-up grant and NSERC. H.-K. L. also acknowledges support from MITACS, CFI, ORF, Huawei Technologies, Inc., the Royal Bank of Canada, and Innovative Solutions Canada. W. W. acknowledges support from the Hong Kong RGC General Research Fund (GRF) and the University of Hong Kong Seed Fund for Basic Research for New Staff. M. C. and V. Z. acknowledge support from the Galician Regional Government (consolidation of Research Units: AtlantTIC), the Spanish Ministry of Economy and Competitiveness (MINECO), the Fondo Europeo de Desarrollo Regional (FEDER) through Grant No. PID2020-118178RB-C21, MICIN with funding from the European Union NextGenerationEU (PRTR-C17.I1) and the Galician Regional Government with own funding through the "Planes Complementarios de I+D+I con las Comunidades Autonomas" in Quantum Communication, and the European Union's Horizon Europe research and innovation programme under the project QSNP (Quantum encryption and future quantum network technologies).

Note added.—Recently, an alternative approach to passive QKD has been proposed [60].

*Corresponding author.
wenyuanw@hku.hk
†Corresponding author.
hoikwong@hku.hk

[1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of*

the International Conference on Computer System and Signal Processing (IEEE, New York, 1984).
[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. Ganapandithan, 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. Yoshino *et al.*, Quantum key distribution with an efficient countermeasure against correlated intensity fluctuations in optical pulses, npj Quantum Inf. **4**, 8 (2018).
[7] B. Qi, C. H. F. Fung, H. K. Lo, and X. Ma, Time-shift attack in practical quantum cryptosystems, Quantum Inf. Comput. **7**, 73 (2007).
[8] 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).
[9] H. K. Lo, M. Curty, and B. Qi, Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **108**, 130503 (2012).
[10] 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).
[11] 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).
[12] M. Curty, X. Ma, H. K. Lo, and N. Lütkenhaus, Passive sources for the Bennett-Brassard 1984 quantum-key-distribution protocol with practical signals, Phys. Rev. A **82**, 052325 (2010).
[13] W. Y. Hwang, Quantum Key Distribution with High Loss: Toward Global Secure Communication, Phys. Rev. Lett. **91**, 057901 (2003).
[14] H. K. Lo, X. F. Ma, and K. Chen, Decoy State Quantum Key Distribution, Phys. Rev. Lett. **94**, 230504 (2005).
[15] X. B. Wang, Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography, Phys. Rev. Lett. **94**, 230503 (2005).
[16] Another method called device-independent (DI) QKD [17–20], which can eliminate side channels from all devices, has been recently experimentally implemented [21–23]. Nonetheless, the current experiments are rather limited in distance and key rate.
[17] D. Mayers and A. Yao, Quantum cryptography with imperfect apparatus, in *Proceedings of the 39th Annual Symposium on Foundations of Computer Science* (IEEE, New York, 1998).
[18] 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).
[19] 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).
[20] J. Barrett, L. Hardy, and A. Kent, No Signaling and Quantum Key Distribution, Phys. Rev. Lett. **95**, 010503 (2005).
[21] D. P. Nadlinger *et al.*, Device-independent quantum key distribution, Nature (London) **607**, 682 (2022).
[22] W. Zhang *et al.*, A device-independent quantum key distribution system for distant users, Nature (London) **607**, 687 (2022).
[23] 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).
[24] M. Curty, M. Jofre, V. Pruneri, and M. W. Mitchell, Passive decoy-state quantum key distribution with coherent light, Entropy **17**, 4064 (2015).
[25] N. De La Cruz *et al.*, Decoy-state quantum key distribution with direct modulated commercial off-the-shelf VCSEL lasers, in *Proceedings of the IEEE International Conference on Quantum Computing and Engineering* (IEEE, New York, 2020).
[26] B. Qi, P. G. Evans, and W. P. Grice, Passive state preparation in the Gaussian-modulated coherent-states quantum key distribution, Phys. Rev. A **97**, 012317 (2018).
[27] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.130.220801 for additional explanations and proofs, additional simulation results, descriptions of the channel model, and the finite-size analysis used in the simulations, as well as details of the experimental setup and data. The Supplemental Material includes Refs. [28–39].
[28] I. Devetak and A. Winter, Distillation of secret key and entanglement from quantum states, Proc. R. Soc. A **461**, 207 (2005).
[29] Y. H. Zhou, Z. W. Yu, and X. B. Wang, Making the decoy-state measurement-device-independent quantum key distribution practically useful, Phys. Rev. A **93**, 042324 (2016).
[30] A. Laing, V. Scarani, J. G. Rarity, and J. L. O'Brien, Reference-frame-independent quantum key distribution, Phys. Rev. A **82**, 012304 (2010).
[31] R. Renner, N. Gisin, and B. Kraus, Information-theoretic security proof for quantum-key-distribution protocols, Phys. Rev. A **72**, 012332 (2005).
[32] O. Rodrigues, Des lois géométriques qui régissent les déplacements d'un système solide dans l'espace, et de la variation des coordonnées provenant de ces déplacements considérés indépendamment des causes qui peuvent les produire, J. Math. Pures Appl. **5**, 380 (1840).
[33] J. Wabnig, D. Bitauld, H. W. Li, A. Laing, J. L. O'Brien, and A. O. Niskanen, Demonstration of free-space reference frame independent quantum key distribution, New J. Phys. **15**, 073001 (2013).
[34] W. Y. Liang *et al.*, Proof-of-principle experiment of reference-frame-independent quantum key distribution with phase coding, Sci. Rep. **4**, 3617 (2014).
[35] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, Concise security bounds for practical decoy-state quantum key distribution, Phys. Rev. A **89**, 022307 (2014).

[36] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H. K. Lo, Finite-key analysis for measurement-device-independent quantum key distribution, Nat. Commun. **5**, 3732 (2014).

[37] F. Xu, H. Xu, and H. K. Lo, Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution, Phys. Rev. A **89**, 052333 (2014).

[38] W. Wang, F. Xu, and H. K. Lo, Asymmetric Protocols for Scalable High-Rate Measurement-Device-Independent Quantum Key Distribution Networks, Phys. Rev. X **9**, 041012 (2019).

[39] X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H. K. Lo, Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction, Phys. Rev. A **87**, 062327 (2013).

[40] The global phase here in fact can be an arbitrary value depending on the phase reference we choose (and here we chose ϕ_H as an example). The key point is that there is one degree of freedom for the global phase ϕ_G and an additional degree of freedom for the relative phase ϕ_{HV}. This ensures that we can generate arbitrary states on the Bloch sphere, and that the states are also globally phase-randomized.

[41] In fact, the intensity can exceed $\mu_{\max}$ (up to $2\mu_{\max}$ when θ_{HV} is exactly $\pi/2$), at the expense of a more limited range of polarizations.

[42] Note that, here in our protocol definition and decoy-state analysis we focus on a set of symmetric protocols, which prepare symmetric pairs of states for each basis and for, e.g., the X and Z bases the single-photon states satisfy $\rho_1^Z = \rho_1^X$ (i.e., they have basis independence). For asymmetric protocols, such as the three-state loss-tolerant protocol [43], our source would still be able to generate the desired states, but the decoy-state analysis would require a case-by-case revision. Nonetheless, for, e.g., loss tolerance, one can consider as well other symmetric protocols, such as those using the approach in Ref. [44], to avoid the asymmetry in the protocol.

[43] K. Tamaki, M. Curty, G. Kato, H. K. Lo, and K. Azuma, Loss-tolerant quantum cryptography with imperfect sources, Phys. Rev. A **90**, 052314 (2014).

[44] J. E. Bourassa, I. W. Primaatmaja, C. C. W. Lim, and H. K. Lo, Loss-tolerant quantum key distribution with mixed signal states, Phys. Rev. A **102**, 062607 (2020).

[45] 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).

[46] B. Qi, Y. M. Chi, H. K. Lo, and L. Qian, High-speed quantum random number generation by measuring phase noise of a single-mode laser, Opt. Lett. **35**, 312 (2010).

[47] M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. P. Torres, M. W. Mitchell, and V. Pruneri, True random numbers from amplified quantum vacuum, Opt. Express **19**, 20665 (2011).

[48] 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).

[49] Z. L. Yuan, M. Lucamarini, J. F. Dynes, B. Fröhlich, A. Plews, and A. J. Shields, Robust random number generation using steady-state emission of gain-switched laser diodes, Appl. Phys. Lett. **104**, 261112 (2014).

[50] See also [51] for recent results that relax this assumption.

[51] G. Currás-Lorenzo, K. Tamaki, and M. Curty, Security of decoy-state quantum key distribution with imperfect phase randomization, arXiv:2210.08183.

[52] E. Moschandreou, J. I. Garcia, B. J. Rollick, B. Qi, R. Pooser, and G. Siopsis, Experimental study of Hong-Ou–Mandel interference using independent phase randomized weak coherent states, J. Lightwave Technol. **36**, 3752 (2018).

[53] Z. L. Yuan, M. Lucamarini, J. F. Dynes, B. Fröhlich, M. B. Ward, and A. J. Shields, Interference of Short Optical Pulses from Independent Gain-Switched Laser Diodes for Quantum Secure Communications, Phys. Rev. Appl. **2**, 064006 (2014).

[54] H. L. Yin *et al.*, Measurement-Device-Independent Quantum Key Distribution Over a 404 km Optical Fiber, Phys. Rev. Lett. **117**, 190501 (2016).

[55] 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).

[56] The active modulation here itself will not introduce any side channel, since it simply uses a fixed pattern and does not contain any encoding information. However, in practice, if the intensity modulator or optical switch in such a one-laser setup has a finite extinction ratio, this may be considered a side channel since neighboring pulses may leak part of the encoding information (which comes from the random phases of the four pulses $\{\phi_1, \phi_2, \phi_3, \phi_4\}$, so a neighboring pulse containing say $\{\phi_2, \phi_3, \phi_4, \phi_5\}$ may leak part of the information). In the most pessimistic case (neighboring pulse leaks all the information) this is similar to a Trojan horse attack [3]. What makes it different from a Trojan horse attack, though, is that the maximum intensity and timing of the leaked signals are both known to Alice and Bob. One can in principle apply the analysis from, e.g., Refs. [57–59] to lower bound the key rate given the extinction ratio. Based on these references, e.g., suppressing the unwanted pulses to an intensity 10^{-6} to 10^{-8} can prevent a significant reduction to the key rate, which is certainly achievable if one say concatenates more than one intensity modulator (each of which can typically provide about 30 dB of extinction ratio).

[57] M. Lucamarini, I. Choi, M. B. Ward, J. F. Dynes, Z. L. Yuan, and A. J. Shields, Practical Security Bounds Against the Trojan-Horse Attack in Quantum Key Distribution, Phys. Rev. X **5**, 031030 (2015).

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

[59] Á. Navarrete and M. Curty, Improved finite-key security analysis of quantum key distribution against Trojan-horse attacks, Quantum Sci. Technol. **7**, 035021 (2022).

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