Measurement-device-independent quantum communication with an untrusted source

Feihu Xu*
Research Laboratory of Electronics, Massachusetts Institute of Technology,
77 Massachusetts Avenue, Cambridge, Massachusetts 02139, USA
(Dated: April 25, 2015)

Measurement-device-independent quantum key distribution (MDI-QKD) can provide enhanced security, as compared to traditional QKD, and it constitutes an important framework for a quantum network with an untrusted network server. Still, a key assumption in MDI-QKD is that the sources are trusted. We propose here a MDI quantum network with a single untrusted source. We have derived a complete proof of the unconditional security of MDI-QKD with an untrusted source. Using simulations, we have considered various real-life imperfections in its implementation, and the simulation results show that MDI-QKD with an untrusted source provides a key generation rate that is close to the rate of initial MDI-QKD in the asymptotic setting. Our work proves the feasibility of the realization of a quantum network. The network users need only low-cost modulation devices, and they can share both an expensive detector and a complicated laser provided by an untrusted network server.

Measurement-device-independent quantum key distribution (MDI-QKD) [1] removes all detector side-channel attacks. This kind of attack is arguably the most important security loophole in conventional QKD implementations [2]. The assumption in MDI-QKD is that the state preparation can be trusted. Unlike security patches and device-independent QKD, MDI-QKD can remove all detector loopholes and is also practical for current technology. Hence, MDI-QKD has attracted a lot of scientific attention in both theoretical and experimental studies [3–5].

An important feature of MDI-QKD is that it can be used to build a fiber-based MDI quantum network with a fully *untrusted* network server (see Fig. 1(a)). This framework can realize various quantum information-processing protocols, such as quantum repeater, quantum fingerprinting [6], blind quantum computing [7], and multiparty quantum communication [8]. This scheme is advantageous in comparison to the recent demonstrations of quantum access networks [9], since it completely removes the need for the trust of the central relay node. Nevertheless, the scheme faces several crucial challenges in practice: (i) A key assumption is that the users' lasers are trusted. However, since coherent lasers are complicated apparatuses, there is a great risk involved in each user's trust that a commercial compact laser does not have any security loopholes [10]. (ii) A major challenge in implementation is the performance of high-fidelity interference between photons from different, separated lasers [3, 4]. (iii) In fiber communication, it is necessary to include complex feedback controls to compensate for the polarization rotations and propagation delays (e.g., an implementation in [4]). An additional time-synchronization system is also required. (iv) Each user normally requires a frequency-locked laser at a specific wavelength [3, 4], which is not compatible with optical networks based on wavelength division multiplexing (WDM).

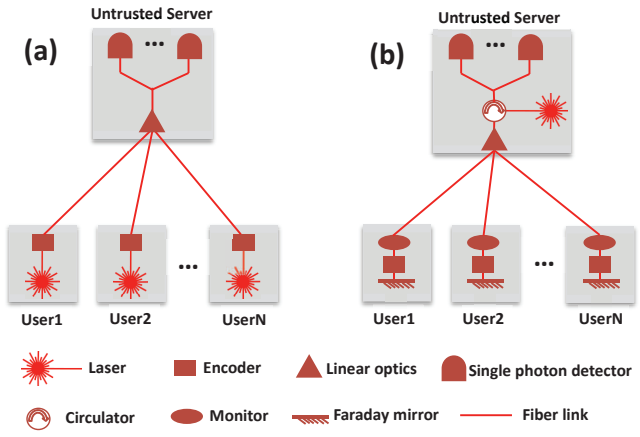

FIG. 1: (a) A fiber-based quantum network with N trusted lasers. (b) A quantum network with a single *untrusted* laser source.

In this paper, we overcome the above challenges by proposing a MDI quantum network with a single untrusted source in Fig. 1(b). The untrusted server transmits strong classical laser pulses to users, all of whom monitor the pulses, encode their bit information and send the attenuated pulses back to the server for measurement. We focus on the application of such a network to QKD. Crucially, we show that, even with an untrusted source, the communication security can be analyzed quantitatively and rigorously. Motivated by the security analysis for plug&play QKD [11], we show what measures by the users are necessary to ensure security, and to rigorously derive a lower bound of the secure key generation rate. Moreover, we propose a novel decoy state method for MDI-QKD with an untrusted source. Furthermore, using simulations, we study how different real-life imperfections affect the security, and our simulation results show that MDI-QKD with an untrusted source provides a key generation rate that is close to the rate with trusted sources in the asymptotic limit.

Our proposed MDI quantum network has the following advantages: (i) It completely removes the trust of the laser source. (ii) It can realize the MDI quantum network with a *single* laser, which enables a high-fidelity interference among photons from different users. (iii) Due to the bi-directional structure, the system can automatically compensate for any birefringence effects and polarization-dependent losses in optical fibers, a feature that makes the system highly stable. (iv) The users can utilize the strong pulses from the server to easily synchronize and share time references. (v) There is a prospect

of leveraging costly infrastructure for the quantum network, since the single laser source can be broadband, dynamically reconfigured and shared by several users via WDM.

The additional assumption, as compared to the initial MDI quantum network, is the trust of the monitoring devices. The users need to monitor only *classical* laser pulses instead of single-photon signals. Such monitoring can be realized by a standard optical filter and a classical intensity detector, and it is a necessary part of both BB84 and the initial MDI-QKD to prevent the Trojan-horse attack [12]. It is important that proof-of-concept experiments have been reported towards implementation of this monitoring [13, 14] and that ID Quantique's commercial system (i.e., Clavis2) has already included a preliminary version of the monitor [15]. Recently, the security of the intensity detector has been studied comprehensively in [14]. Our work may lead to future research on an efficient implementation of the single-mode filtering and monitoring. This monitoring is also a key ingredient in other quantum communication protocols such as quantum illumination [16].

To illustrate our proposal, in Fig. 2, we present a specific design for QKD with two users. With simple modifications, our scheme can be applied to multiple users [8]. We consider a time-bin encoding, and the procedures of the protocol is shown in the caption of Fig. 2. Since the source is entirely unknown and untrusted, we use three measures to enhance the security of our protocol [11, 12]: *(i)* We place a narrow bandpass filter (together with a single mode fiber) to allow a single mode in spectral and spatial domains to enter into the Encoder. The analysis in [17] shows that with standard optical devices, the single mode assumption can be guaranteed with a high rate of accuracy. *(ii)* We monitor the pulse energy and the arrival time to acquire certain information about the photon number distribution (PND) and the timing mode. By randomly sampling the pulses to test the photon numbers, we can estimate some bounds on the output PND. In Fig. 2, this estimation is accomplished by the beam-splitter (BS) and intensity detector (ID). *(iii)* Alice and Bob use phase modulators (PM1 and PM3) to apply the active phase randomization. The phase randomization is a general assumption made in most security proofs for laser-based QKD [18] and the randomization can disentangle the input pulse into a classical mixture of Fock states.

All the above three measures lead us to analyze the security of MDI-QKD with an untrusted source quantitatively and rigorously. In our analysis, we define the pulses with the photon number $m_a \in [(1-\delta_a)M_a, (1+\delta_a)M_a]$ as "*untagged pulses*" and pulses with the photon number $m_a < (1-\delta_a)M_a$ or $m_a > (1+\delta_a)M_a$ as "*tagged pulses*". From the random sampling theorem, we draw the follow proposition [11].

Proposition 1. Consider that $2k$ pulses are sent to Alice from an untrusted source, and, of these pulse, V_a pulses are untagged. Alice randomly assigns each pulse a status as either a sampling pulse or an encoding pulse with equal probabilities. In total, $V_a^{\rm s}$ sampling pulses and $V_a^{\rm e}$ encoding pulses are untagged. The probability that $V_a^{\rm e} \leq V_a^{\rm s} - 2\epsilon_a k$ satisfies

$$P(V_a^{\rm e} \leq V_a^{\rm s} - 2\epsilon_a k) \leq \exp(-k\epsilon_a^2) \qquad (1)$$

where ϵ_a is a small positive real number chosen by Alice (i.e. the error probability due to statistical fluctuations). That is, Alice can conclude that $V_a^{\rm e} > V_a^{\rm s} - \epsilon_a k$ with confidence level $\tau_a > 1 - \exp(-k\epsilon_a^2)$.

The proof is shown in the Supplementary Material. This proposition shows that Alice/Bob can estimate the number of untagged encoding pulses from the sampling pulses. In our analysis, Alice and Bob focus only on the untagged pulses for key generation and discard the other pulses. In practice, since Alice and Bob cannot perform quantum nondemolishing measurement with current technology, they do *not* know which pulses are tagged and which are untagged. Also, in MDI-QKD with an untrusted source, Eve is given significantly greater power, since she can control both the input

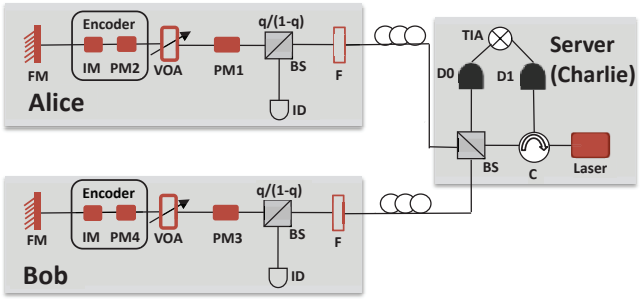

FIG. 2: Schematic diagram of a time-bin-encoding MDI-QKD with an untrusted source. The strong laser pulses are generated by Charlie and sent to Alice (Bob), who uses an optical filter (F) for filtering, a classical intensity detector (ID) for monitoring and a phase modulator PM1 (PM3) for phase randomization. The pulses are encoded by an Encoder and they are reflected by a Faraday mirror (FM). Finally, the pulses from Alice and Bob interfere at Charlie's BS and detected by two single photon detectors (D0 and D1), whose coincident counts are recorded by a time interval analyzer (TIA). A coincident event projects the photons into the singlet state $|\psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$. BS: beam splitter; IM: intensity modulator.

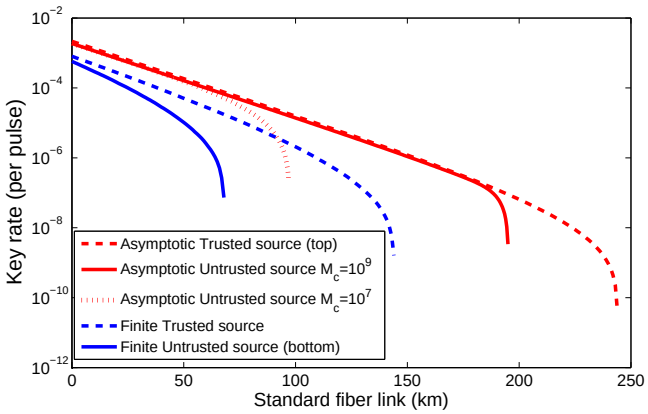

FIG. 3: Simulation results. Red curves are for an infinite number of signals. With $M_c = 10^9$ and practical imperfections, MDI-QKD with an untrsuted source can tolerate about 195 km distance. At the distances below 180 km, the key rates for the two cases (with trusted and untrusted source) are almost overlapping. Blue curves are for a finite number of signals with 20% detector efficiency.

and the output of the source. Hence, the decoy state analysis is more challenging. However, rather surprisingly, we find that it is still possible to achieve the unconditional security quantitatively. From proposition 1, they know the probability that a certain pulse is tagged or untagged. Hence, the key insight is that Alice and Bob can estimate the upper and lower *bounds* of the gain and the quantum bit error rate (QBER) of the untagged pulses. Moreover, they can also estimate the bounds of the PND of the untagged pulses. Using these bounds, we can prove the security and perform the decoy state analysis for MDI-QKD with an untrusted source. The details of our unconditional security analysis and the novel decoy state estimation are shown in the Supplementary Material.

η_d	Y_0	e_d	f	α
20%	3×10^{-6}	0.1%	75 MHz	0.21 dB/km
η_{ID}	σ_{ID}	q	ϵ	k
0.7	6.55×10^{4}	0.01	10^{-10}	3.5×10^{13}

TABLE I: List of practical parameters for simulation. The detection efficiency η_d and the dark count rate Y_0 are from commercial ID-220 detectors [15]. The channel misalignment error e_d, the system repetition rate f, the total number of pulses k and the fiber loss coefficient α are from the 200 km MDI-QKD experiment [4]. The efficiency of the ID η_{ID}, the noise of the ID σ_{ID}, and the BS ratio q are from [11]. ϵ is the security bound considered in our finite-key analysis.

In our numerical simulation, we consider various imperfections, including additional channel loss due to the bidirectional structure, the noise of ID, and the finite-data statistics. We use the experimental parameters, listed in Table I for simulation. We assume that the source in Charlie is Poissonian centered at M_c photons per optical pulse. The simulation results are shown in Fig. 3. The simulation results show that MDI-QKD with an untrusted source provides a key generation rate that is close to the rate with trusted sources in the asymptotic limit. Finite data size reduces the efficiencies. In the finite data setting, our protocol can tolerate about 70 km fiber with standard commercial detectors of 20% efficiency. With state-of-the-art detectors [19], the protocol can easily generate keys over 200 km fiber.

In summary, we for the first time propose a MDI quantum network with an untrusted source. In this network, the complicated and expensive detectors, together with the laser source, can be provided by an untrusted network server that can be shared by all users; that is, a star-type MDI quantum access network can be readily realized on the basis of our proposal for several quantum information processing protocols [6–8]. Our work proves the feasibility of such a realization. Moreover, we present a complete security analysis for MDI-QKD with an untrusted source. Our analysis and simulation consider various practical imperfections, and our protocol is practically secure and ready for implementation.

More details of our work are shown in the attached Supplementary Material.

* Electronic address: fhxu@mit.edu

[1] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).

[2] L. Lydersen *et al.*, Nat. Photon. **4**, 686 (2010); I. Gerhardt *et al.*, Nat. Commun. **2**, 349 (2011).

[3] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Phys. Rev. Lett. **111**, 130501 (2013); Y. Liu *et al.*, Phys. Rev. Lett. **111**, 130502 (2013). T. Ferreira da Silva *et al.*, Phys. Rev. A **88**, 052303 (2013); Z. Tang, *et al.*, Phys. Rev. Lett. **112**, 190503 (2014).

[4] Y.-L. Tang *et al.*, Phys. Rev. Lett. **113**, 190501 (2014)

[5] F. Xu, M. Curty, B. Qi, and H. Lo, IEEE J. Select. Topics Quantum Electron. **21**, 6601111 (2015).

[6] H. Buhrman, R. Cleve, J. Watrous, R. De Wolf, Phys. Rev. Lett. **87**, 167902 (2001); J. M. Arrazola and N. Lütkenhaus, Phys. Rev. A **89**, 062305 (2014); F. Xu, J. M. Arrazola *et al.*, arXiv:1503.05499 (2015).

[7] S Barz et al., Science **335**, 303 (2012); A. Broadbent, J. Fitzsimons, E. Kashefi, in Proc. of the 50th Annual Symposium on Foundations of Computer Science, pp. 517526 (2009); V. Dunjko, E. Kashefi, and A. Leverrier, Phys. Rev. Lett. **108**, 200502 (2012).

[8] Y. Fu, H.-L. Yin, T.-Y. Chen, and Z.-B. Chen, Phys. Rev. Lett. **114**, 090501 (2015).

[9] M. Sasaki *et al.*, Opt. Express **19**, 10387 (2011); B. Fröhlich *et al.*, Nature **501**, 69 (2013); R. J. Hughes *et al.*, arXiv:1305.0305 (2013).

[10] Y. Tang et al., Phys. Rev. A 88, 022308 (2013).

[11] Y. Zhao, B. Qi, and H.-K. Lo, Phys. Rev. A **77**, 052327 (2008); Y. Zhao, B. Qi, H.-K. Lo, and L. Qian, New J. Phys. **12**, 023024 (2010).

[12] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Phys. Rev. A **73**, 022320 (2006).

[13] Y. Zhao, B. Qi, and H.-K. Lo, Appl. Phys. Lett. **90**, 044106 (2007); X. Peng *et al.*, Optics letters **33**, 2077 (2008); S. Sun and L. Liang, Appl. Phys. Lett. **101**, 071107 (2012); T Kobayashi, A Tomita, A Okamoto, Phys. Rev. A 90, 032320 (2014).

[14] S. Sajeed *et al.*, Phys. Rev. A **91**, 032326 (2015)

[15] http://www.idquantique.com

[16] Z. Zhang,M. Tengner, T. Zhong, F.N.C. Wong, and J. H. Shapiro, Phys. Rev. Lett. **111**, 010501 (2013).

[17] F. Xu *et al.*, arXiv:1408.3667 (2014).

[18] D. Gottesman, H.-K. Lo, N. Lütkenhaus and J. Preskill, Quant. Inf. Comput. **4**, 325 (2004); H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).

[19] F. Marsili *et al.*, Nat. Photon. **7**, 210 (2013).

Measurement-device-independent quantum communication with an untrusted source

Feihu Xu*
Research Laboratory of Electronics, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, Massachusetts 02139, USA
(Dated: April 3, 2015)

Measurement-device-independent quantum key distribution (MDI-QKD) can provide enhanced security, as compared to traditional QKD, and it constitutes an important framework for a quantum network with an untrusted network server. Still, a key assumption in MDI-QKD is that the sources are trusted. We propose here a MDI quantum network with a single untrusted source. We have derived a complete proof of the unconditional security of MDI-QKD with an untrusted source. Using simulations, we have considered various real-life imperfections in its implementation, and the simulation results show that MDI-QKD with an untrusted source provides a key generation rate that is close to the rate of initial MDI-QKD in the asymptotic setting. Our work proves the feasibility of the realization of a quantum network. The network users need only low-cost modulation devices, and they can share both an expensive detector and a complicated laser provided by an untrusted network server.

The global quantum network is believed to be the next-generation information-processing platform for speedup computation and a secure means of communication. Among the applications of the quantum network, quantum key distribution (QKD) is one of the first technology in quantum information science to produce practical applications [1, 2]. Unfortunately, due to real-life imperfections, a crucial problem in current QKD implementations is the discrepancy between its theory and practice [2]. An eavesdropper (Eve) could exploit such imperfections and hack a QKD system. Indeed, the recent demonstrations of various attacks [3, 4] on practical QKD systems highlight that the theory-practice discrepancy is a major problem for practical QKD.

Measurement-device-independent quantum key distribution (MDI-QKD) [5] removes all detector side-channel attacks. This kind of attack is arguably the most important security loophole in conventional QKD implementations [4]. The assumption in MDI-QKD is that the state preparation can be trusted. Unlike security patches [6] and device-independent QKD [7], MDI-QKD can remove all detector loopholes and is also practical for current technology. Hence, MDI-QKD has attracted a lot of scientific attention in both theoretical [8, 9] and experimental [10–12] studies. See [13] for a review of its recent development.

An important feature of MDI-QKD is that it can be used to build a fiber-based MDI quantum network with a fully *untrusted* network server (see Fig. 1(a)). This framework can realize various quantum information-processing protocols, such as quantum repeater [14], quantum fingerprinting [15], blind quantum computing [16], and multiparty quantum communication [9]. This scheme is advantageous in comparison to the recent demonstrations of quantum access networks [17], since it completely removes the need for the trust of the central relay node. Nevertheless, the scheme faces several crucial challenges in practice: (i) A key assumption is that the users' lasers are trusted. However, since coherent lasers are complicated apparatuses, there is a great risk involved in each user's trust that a commercial compact laser does not have any security loopholes. (ii) A major challenge in implementation is the performance of high-fidelity interference between photons from different, separated lasers [18]. (iii) In fiber communication, it is necessary to include complex feedback controls to compensate for the polarization rotations and propagation delays (e.g., an implementation in [11]). An additional time-synchronization system is also required. (iv) Each user normally requires a frequency-locked laser at a specific wavelength [10, 11], which is not compatible with optical networks based on wavelength division multiplexing (WDM) [19].

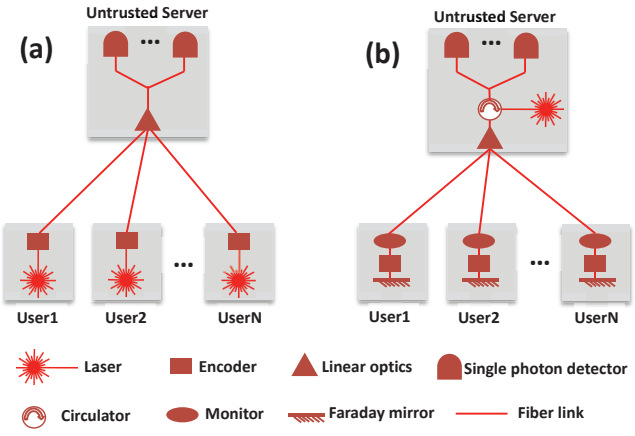

FIG. 1: (a) A fiber-based quantum network with N trusted lasers. (b) A quantum network with a single *untrusted* laser source.

In this paper, we overcome the above challenges by proposing a MDI quantum network with a single untrusted source in Fig. 1(b). The untrusted server transmits strong classical laser pulses to users, all of whom monitor the pulses, encode their bit information and send the attenuated pulses back to the server for measurement. We focus on the application of such a network to QKD. Crucially, we show that, even with an untrusted source, the communication security can be analyzed quantitatively and rigorously. Motivated by the security analysis for plug&play QKD [20], we show what measures by the users are necessary to ensure security, and to rigorously derive a lower bound of the secure key generation rate. Moreover, we propose a novel decoy state method for MDI-QKD with an untrusted source. Furthermore, using simulations, we

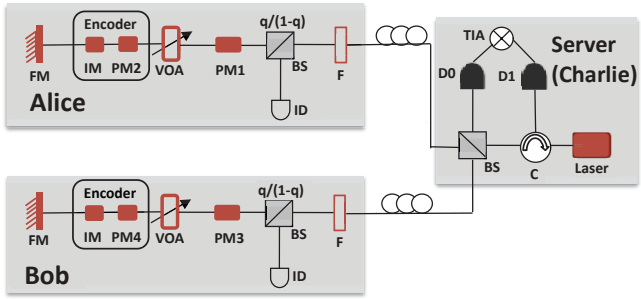

FIG. 2: Schematic diagram of a time-bin-encoding MDI-QKD with an untrusted source. The strong laser pulses are generated by Charlie and sent to Alice (Bob), who uses an optical filter (F) for filtering, a classical intensity detector (ID) for monitoring and a phase modulator PM1 (PM3) for phase randomization. The pulses are encoded by an Encoder and they are reflected by a Faraday mirror (FM). Finally, the pulses from Alice and Bob interfere at Charlie's BS and detected by two single photon detectors (D0 and D1), whose coincident counts are recorded by a time interval analyzer (TIA). BS: beam splitter; IM: intensity modulator.

study how different real-life imperfections affect the security, and our simulation results show that MDI-QKD with an untrusted source provides a key generation rate that is close to the rate with trusted sources in the asymptotic limit.

Our proposed MDI quantum network has the following advantages: (i) It completely removes the trust of the laser source. (ii) It can realize the MDI quantum network with a *single* laser, which enables a high-fidelity interference among photons from different users. (iii) Due to the bi-directional structure, the system can automatically compensate for any birefringence effects and polarization-dependent losses in optical fibers, a feature that makes the system highly stable. (iv) The users can utilize the strong pulses from the server to easily synchronize and share time references. (v) There is a prospect of leveraging costly infrastructure for the quantum network, since the single laser source can be broadband, dynamically reconfigured and shared by several users via WDM.

The additional assumption, as compared to the initial MDI quantum network, is the trust of the monitoring devices. The users need to monitor only *classical* laser pulses instead of single-photon signals. Such monitoring can be realized by a standard optical filter and a classical intensity detector, and it is a necessary part of both BB84 and the initial MDI-QKD to prevent the Trojan-horse attack [3]. It is important that proof-of-concept experiments have been reported towards implementation of this monitoring [21, 22] and that ID Quantique's commercial system (i.e., Clavis2) has already included a preliminary version of the monitor [23]. Recently, the security of the intensity detector has been studied comprehensively in [22]. Our work may lead to future research on an efficient implementation of the single-mode filtering and monitoring. This monitoring is also a key ingredient in other quantum communication protocols such as quantum illumination [24].

To illustrate our proposal, in Fig. 2, we present a specific design for QKD with two users. With simple modifications, our scheme can be applied to multiple users [9]. We consider a time-bin encoding, and the protocol runs as follows: Charlie generates a strong laser pulse. Once the pulse arrives at Alice (Bob), it passes through an optical filter, a monitoring unit with a beam splitter (BS) and an intensity detector (ID), and a variable optical attenuator (VOA). The pulse is encoded by an Encoder that consists of an intensity modulator and a phase modulator (PM), and then it is reflected by a Faraday mirror (FM). Finally, the two pulses from Alice and Bob interfere at the BS of Charlie and are detected by two single photon detectors. A coincident event projects the photons into the singlet state $|\psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$.

Since the source is entirely unknown and untrusted, we use three measures to enhance the security of our protocol [3, 20]: *(i)* We place a narrow bandpass filter (together with a single mode fiber) to allow a single mode in spectral and spatial domains to enter into the Encoder. The analysis in [25] shows that with standard optical devices, the single mode assumption can be guaranteed with a high rate of accuracy. *(ii)* We monitor the pulse energy and the arrival time to acquire certain information about the photon number distribution (PND) and the timing mode. By randomly sampling the pulses to test the photon numbers, we can estimate some bounds on the output PND. In Fig. 2, this estimation is accomplished by the BS and ID. *(iii)* Alice and Bob use PM1 and PM3 to apply the active phase randomization. The phase randomization is a general assumption made in most security proofs for laser-based QKD [26] and the randomization can disentangle the input pulse into a classical mixture of Fock states. All the above three measures lead us to analyze the security of MDI-QKD with an untrusted source quantitatively and rigorously.

To analyze the security of Fig. 2, we model Alice's (Bob's) system in Fig. 3(a). Each input pulse is split into two via a BS: One (defined as the *encoding pulse*) is sent to the encoder for encoding, and the other (defined as the *sampling pulse*) is sent to the ID for sampling. One might suppose that the PND of the encoding pulse could be easily estimated from the measurement result of the sampling pulse from the random sampling theorem [27]. However, this supposition is *not* true. Any input pulse, after the phase randomization, is in a Fock state. Therefore, in the case of a pair of encoding and sampling pulses originating from the same input pulse, the PNDs of the two pulses are *correlated*. This restriction suggests that the random sampling theorem cannot be directly applied.

We resolve the above restriction and analyze the security by introducing a virtual model in Fig. 3(b). In the virtual model, we introduce a 50:50 optical switch to realize the active sampling. The optical switch, which is different from a BS, is solely a sampling device, without any restriction on the correlation of the PNDs. The random sampling theorem can be applied. A crucial fact is that the internal losses in the actual model and the virtual model are identical. The upper and lower bounds of output PND estimated from the virtual model are therefore also valid for those of the actual model, i.e., these two models are equivalent in the security analysis, an equivalence that has been proved in [20].

In Fig. 3(b), define the pulses with the photon number $m_a \in [(1-\delta_a)M_a, (1+\delta_a)M_a]$ as "*untagged pulses*" and

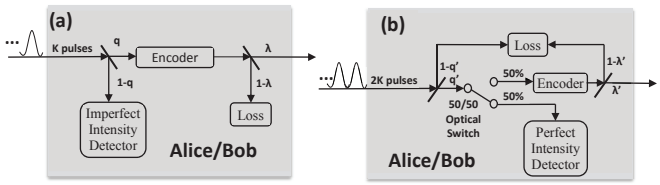

FIG. 3: (a) The actual model for Fig. 2. All the internal loss of Alice/Bob is modeled as a $\lambda/1-\lambda$ BS. (b) An equivalent virtual model for security analysis. The loss is modeled as a $\lambda'/1-\lambda'$ BS with $\lambda' = q\lambda/q'$. $q' = \eta_{\rm ID}(1-q)$, where $\eta_{\rm ID} \leq 1$ is the efficiency of the ID.

pulses with the photon number $m_a < (1-\delta_a)M_a$ or $m_a > (1+\delta_a)M_a$ as "*tagged pulses*". From the random sampling theorem, we draw the follow proposition [20].

Proposition 1. Consider that $2k$ pulses are sent to Alice from an untrusted source, and, of these pulse, V_a pulses are untagged. Alice randomly assigns each pulse a status as either a sampling pulse or an encoding pulse with equal probabilities. In total, $V_a^{\rm s}$ sampling pulses and $V_a^{\rm e}$ encoding pulses are untagged. The probability that $V_a^{\rm e} \leq V_a^{\rm s} - 2\epsilon_a k$ satisfies

$$P(V_a^{\rm e} \leq V_a^{\rm s} - 2\epsilon_a k) \leq \exp(-k\epsilon_a^2) \tag{1}$$

where ϵ_a is a small positive real number chosen by Alice (i.e. the error probability due to statistical fluctuations). That is, Alice can conclude that $V_a^{\rm e} > V_a^{\rm s} - \epsilon_a k$ with confidence level $\tau_a > 1-\exp(-k\epsilon_a^2)$.

The proof is shown in the Supplementary Material. This proposition shows that Alice/Bob can estimate the number of untagged encoding pulses from the sampling pulses. If we define Δ_a as the average probability that a sampling pulse belongs to a tagged sampling pulse in the asymptotic case, then Alice can conclude that there are no fewer than $(1-\Delta_a-\epsilon_a)k$ untagged encoding pulses with high fidelity. Bobs untagged pulses have the same property.

In our analysis, Alice and Bob focus only on the untagged pulses for key generation and discard the other pulses. In practice, since Alice and Bob cannot perform quantum nondemolishing measurement with current technology, they do *not* know which pulses are tagged and which are untagged. However, from proposition 1, they know the probability that a certain pulse is tagged or untagged. Hence, they can estimate the upper and lower bounds of the gain and the quantum bit error rate (QBER) of the untagged pulses. Moreover, Alice (Bob) can also estimate the bounds of the PND of the untagged pulses. The specific bounds for the gain, QBER and the PND of the untagged pulses are shown in Supplementary Material. Using these bounds, we can prove the security of MDI-QKD with an untrusted source.

The secure key rate of MDI-QKD with an untrusted source in the asymptotic limit is given by

$$\begin{aligned} R \geq (1-\Delta_a-\epsilon_a)(1-\Delta_b-\epsilon_b)\underline{Q_{11}^{\rm Z}}[1-H_2(\overline{e_{11}^{\rm X}})] \\ -Q_{e,\mu\mu}^{\rm Z} f_e(E_{e,\mu\mu}^{\rm Z}) H_2(E_{e,\mu\mu}^{\rm Z}), \end{aligned} \tag{2}$$

where $\underline{Q_{11}^{\rm Z}}$ and $\overline{e_{11}^{\rm X}}$ are, respectively, the lower bound of the gain in the rectilinear (Z) basis and the upper bound of the error rate in the diagonal (X) basis, given that both Alice and Bob send single-photon states in *untagged* pulses; H_2 is the binary entropy function; $Q_{e,\mu\mu}^{\rm Z}$ and $E_{e,\mu\mu}^{\rm Z}$ denote, respectively, the overall gain and QBER in the Z basis when Alice and Bob use signal states; $f_e \geq 1$ is the error correction inefficiency function. In practice, $Q_{e,\mu\mu}^{\rm Z}$ and $E_{e,\mu\mu}^{\rm Z}$ are directly measured in the experiment, while $\underline{Q_{11}^{\rm Z}}$ and $\overline{e_{11}^{\rm X}}$ are estimated from the decoy states.

In MDI-QKD with an untrusted source, Eve is given significantly greater power, since she can control both the input and the output of the source. Hence, the decoy state analysis is more challenging. However, rather surprisingly, we find that it is still possible to achieve the unconditional security quantitatively. This is so mainly because we focus only on the untagged pulses, whose PND, gain and QBER can be *bounded*. Therefore, we are still able to estimate $\underline{Q_{11}^{\rm Z}}$ and $\overline{e_{11}^{\rm X}}$. The details of the decoy state estimation are shown in the Supplementary Material.

η_d	Y_0	e_d	f	α
20%	3×10^{-6}	0.1%	75 MHz	0.21 dB/km
η_{ID}	σ_{ID}	q	ϵ	k
0.7	6.55×10^{4}	0.01	10^{-10}	3.5×10^{13}

TABLE I: List of practical parameters for simulation. The detection efficiency η_d and the dark count rate Y_0 are from commercial ID-220 detectors [23]. The channel misalignment error e_d, the system repetition rate f, the total number of pulses k and the fiber loss coefficient α are from the 200 km MDI-QKD experiment [11]. The efficiency of the ID η_{ID}, the noise of the ID σ_{ID}, and the BS ratio q are from [20]. ϵ is the security bound considered in our finite-key analysis.

In our simulation, we consider various imperfections, including additional channel loss due to the bi-directional structure, the noise of ID, the tagged ratio Δ and the finite-data statistics. The detailed model for these imperfections is shown in the Supplementary Material. We use the experimental parameters, listed in Table I for simulation. We assume that the source in Charlie is Poissonian centered at $M_{\rm c}$ photons per optical pulse.

The simulation results with an infinite number of signals are shown by the red curves in Fig. 4. With $M_{\rm c} = 10^7$, the case with an untrusted source (dotted curve) is similar to that with trusted sources at short distances. The condition changes at long distances. This occurs because at long distances, due to the channel loss, the photon numbers arrived at by Alice and Bob will be much smaller than M_c. The lower input photon number increases Δ and the estimate of the gain of the untagged pulses is sensitive to the value of Δ (see Supplementary Material), when the measured overall gain is small over long distances. In contrast, over short distances, the gain is significantly greater than Δ; therefore, the key rates for the two cases are almost overlapping. A natural scheme for the improvement of the performance of MDI-QKD with an untrusted source is the use of a brighter laser. Indeed, the performance is improved substantially by setting $M_{\rm c} = 10^9$ [28].

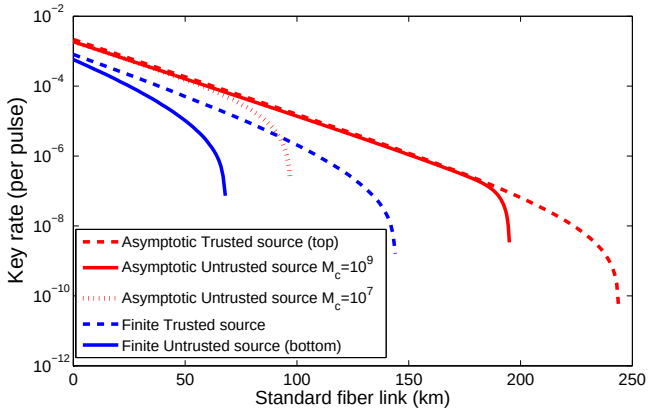

FIG. 4: Simulation results. Red curves are for an infinite number of signals. With $M_{\rm c} = 10^9$ and practical imperfections, MDI-QKD with an untrsuted source can tolerate about 195 km distance. At the distances below 180 km, the key rates for the two cases (with trusted and untrusted source) are almost overlapping. Blue curves are for a finite number of signals with 20% detector efficiency.

The two cases (with trusted sources and with an untrusted source) have similar results.

With $M_{\rm c} = 10^9$, the simulation results with a finite number of signals are shown by the blue curves in Fig. 4. We can see that finite data size clearly reduces the efficiencies: first, the statistical fluctuation for decoy-state MDI-QKD becomes important, and this factor reduces the performance of both the trusted source and the untrusted source. Second, ϵ_a and ϵ_b (see Proposition 1) are non-zero in this finite data case, and thus the estimate of the gain of the untagged pulses becomes not tight at long distances (see Supplementary Material). In the finite data setting, our protocol can tolerate about 70 km fiber with standard commercial detectors of 20% efficiency. With state-of-the-art detectors [29], the protocol can easily generate keys over 200 km fiber.

In summary, we for the first time propose a MDI quantum network with an untrusted source. In this network, the complicated and expensive detectors, together with the laser source, can be provided by an untrusted network server that can be shared by all users; that is, a star-type MDI quantum access network can be readily realized on the basis of our proposal for several quantum information processing protocols [2, 14–16]. Our work proves the feasibility of such a realization. Moreover, we present a complete security analysis for MDI-QKD with an untrusted source. Our analysis and simulation consider various practical imperfections, and our protocol is practically secure and ready for implementation. An experimental demonstration is in progress.

We thank H.-K. Lo, B. Qi, S. Sun and H. Zbinden for valuable discussions. Support from the Office of Naval Research (ONR) and the Air Force Office of Scientific Research (AFOSR) is acknowledged.

Notes added: After completing the early version of our work, we notice a proof-of-principle test of the plug&play MDI-QKD [30]. However, a crucial part to guarantee the security – source filtering and monitoring – is ignored. Also, a complete security proof and the analysis of imperfections are missing. Our work overcomes these limitations and makes plug&play MDI-QKD unconditionally secure, even with practical imperfections.

* Electronic address: fhxu@mit.edu

[1] C. H. Bennett and G. Brassard, Pro. of IEEE Int. Con. on Comp., Syst. Sig. Processing, Bangalore, India, IEEE Press (New York), 1984, pp. 175-179; A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991)
[2] H.-K. Lo, M. Curty, and K. Tamaki, Nat. Photon. **8**, 595 (2014)
[3] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Phys. Rev. A **73**, 022320 (2006).
[4] Y. Zhao, C. Fung, B. Qi, C. Chen, and H.-K. Lo, Phys. Rev. A **78**, 042333 (2008); F. Xu, B. Qi, and H.-K. Lo, New J. Phys. **12**, 113026 (2010); L. Lydersen *et al.*, Nat. Photon. **4**, 686 (2010); I. Gerhardt *et al.*, Nat. Commun. **2**, 349 (2011); H. Weier *et al.*, New J. Phys. **13**, 073024 (2011); N. Jain *et al.*, Phys. Rev. Lett. **107**, 110501 (2011).
[5] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
[6] Z. Yuan, J. Dynes, and A. Shields, Appl. Phys. Lett. **98**, 231104 (2011); T. Ferreira da Silva *et al.*, Opt. Express 20, 18911 (2012); C. Lim, N.Walenta,M. Legre, N. Gisin, and H. Zbinden, IEEE J. Select. Topics Quantum Electron. **21**, 6601305 (2015).
[7] A. Acín *et al.* Phys. Rev. Lett. **98**, 230501 (2007);
[8] X. Ma, C.-H. F. Fung, and M. Razavi, Phys. Rev. A **86**, 052305 (2012); X.-B.Wang, Phys. Rev. A **87**, 012320 (2013); F. Xu, M. Curty, B. Qi, and H.-K. Lo, New J. Phys. **15**, 113007 (2013); M. Curty *et al.*, Nat. Commun. **5**, 3732 (2014); F. Xu, H. Xu, and H.-K. Lo, Phys. Rev. A **89**, 052333 (2014);
[9] Y. Fu, H.-L. Yin, T.-Y. Chen, and Z.-B. Chen, Phys. Rev. Lett. **114**, 090501 (2015).
[10] A. Rubenok *et al.*, Phys. Rev. Lett. **111**, 130501 (2013); Y. Liu *et al.*, Phys. Rev. Lett. **111**, 130502 (2013). T. Ferreira da Silva *et al.*, Phys. Rev. A **88**, 052303 (2013); Z. Tang, *et al.*, Phys. Rev. Lett. **112**, 190503 (2014).
[11] Y.-L. Tang *et al.*, Phys. Rev. Lett. **113**, 190501 (2014)
[12] R. Valivarthi, *et al.*, arXiv:1501.07307 (2015); Z. Yuan *et al.*, Phys. Rev. Appl. **2**, 064006 (2014)
[13] F. Xu, M. Curty, B. Qi, and H. Lo, IEEE J. Select. Topics Quantum Electron. **21**, 6601111 (2015).
[14] H.-J. Briegel,W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998);
[15] J. M. Arrazola and N. Lütkenhaus, Phys. Rev. A **89**, 062305 (2014). F. Xu, J. M. Arrazola *et al.*, arXiv:1503.05499 (2015).
[16] V. Dunjko, E. Kashefi, and A. Leverrier, Phys. Rev. Lett. **108**, 200502 (2012).
[17] M. Sasaki *et al.*, Opt. Express **19**, 10387 (2011); B. Fröhlich *et al.*, Nature **501**, 69 (2013); R. J. Hughes *et al.*, arXiv:1305.0305 (2013).
[18] To mitigate the experimental complexity of the interference from different lasers, several groups have proposed a new protocol against untrusted detectors [P. Gonzalez, et al. arXiv:1410.1422 (2014); C. C. W. Lim et al, Applied Physics

Letters 105, 221112 (2014);W.-F. Cao et al., arXiv:1410.2928 (2014)]. A slight drawback is that a rigorous security analysis for this protocol is challenging, which makes the protocol vulnerable to attacks if certain assumptions cannot be satisfied [B. Qi, Phys. Rev. A 91, 020303 (2015)].

[19] T. Chapuran *et al.*, New J. Phys. **11**, 105001 (2009).

[20] Y. Zhao, B. Qi, and H.-K. Lo, Phys. Rev. A **77**, 052327 (2008); Y. Zhao, B. Qi, H.-K. Lo, and L. Qian, New J. Phys. **12**, 023024 (2010).

[21] Y. Zhao, B. Qi, and H.-K. Lo, Appl. Phys. Lett. **90**, 044106 (2007); X. Peng *et al.*, Optics letters **33**, 2077 (2008); S. Sun and L. Liang, Appl. Phys. Lett. **101**, 071107 (2012)

[22] S. Sajeed *et al.*, Phys. Rev. A **91**, 032326 (2015)

[23] http://www.idquantique.com

[24] Z. Zhang *et al.*, Phys. Rev. Lett. **111**, 010501 (2013).

[25] F. Xu *et al.*, arXiv:1408.3667 (2014).

[26] D. Gottesman, H.-K. Lo, N. Lütkenhaus and J. Preskill, Quant. Inf. Comput. **4**, 325 (2004); W. Hwang, Phys. Rev. Lett. **91**, 57901 (2003); H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005); X. Wang, Phys. Rev. Lett. **94**, 230503 (2005).

[27] A. Papoulis and S. U. Pillai, "Probability, random variables, and stochastic processes" (Tata McGraw-Hill Education, 2002).

[28] Note that sub-nanosecond pulses with $\sim 10^9$ photons per pulse can be easily generated with directly modulated laser diodes. For instance, if the wavelength is 1550 nm and the pulse repetition rate is 75 MHz, the average laser power of Charlie's source is ~ 9.6 mW. This laser power can be provided by many commercial pulsed laser diodes.

[29] F. Marsili *et al.*, Nat. Photon. **7**, 210 (2013).

[30] Y.-S. Kim *et al.*, arXiv:1501.03344 (2015).

Supplementary Material for Measurement-device-independent quantum communication with an untrusted source

Feihu Xu*
Research Laboratory of Electronics, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, Massachusetts 02139, USA

I. PROOF OF PROPOSITION 1

We follow [1] to prove Proposition 1. Among all the V untagged pulses, each pulse has probability 1/2 to be assigned as an untagged coding pulse. Therefore, the probability that $V_a^{\rm e}=v$ obeys a binomial distribution. Cumulative probability is given by [2]

$$P(V_a^{\rm e}\leq\frac{V-2\epsilon k}{2}|V=v)\leq\exp(-\frac{4\epsilon^2k^2}{v})$$

For any $v\in[0,2k]$, $2k/v\geq 1$. Therefore, we have

$$P(V_a^{\rm e}\leq\frac{V-2\epsilon k}{2}|V\in[0,2k])\leq\exp(-k\epsilon^2).$$

Since $V\in[0,2k]$ is always true, the above inequality reduces to

$$P(V_a^{\rm e}\leq\frac{V-2\epsilon k}{2})\leq\exp(-k\epsilon^2). \quad (1)$$

By definition, we have

$$V=V_a^{\rm e}+V_a^{\rm s}. \quad (2)$$

Substituting Equation (2) into Equation (1), we have

$$P(V_a^{\rm e}\leq V_a^{\rm s}-\epsilon k)\leq\exp(-k\epsilon^2). \quad \square \quad (3)$$

The above proof can be easily generalized to the case where for each pulse sent from the untrusted source to Alice/Bob, Alice/Bob randomly assigns it as either a coding pulse with probability β, or a sampling pulse with probability $1-\beta$. Here $\beta\in(0,1)$ is chosen by Alice/Bob. It is then straightforward to show that

$$P[V_a^{\rm e}\leq\frac{\beta}{1-\beta}(V_a^{\rm s}-2\epsilon k)]\leq\exp(-4k\epsilon^2\beta^2). \quad (4)$$

II. PROPERTIES OF UNTAGGED PULSES

The main concept to analyze the properties of the untagged pulses follows the analysis for plug&play QKD presented in [3]. Both Alice and Bob will focus on the $(1-\Delta_a-\epsilon_a)k$ and $(1-\Delta_b-\epsilon_b)k$ untagged pulses for key generation and discard the other pulses. This provides a conservative way to analyze the security, and also, owing to the input photon numbers of the untagged pulses concentrated within a narrow range, this makes it much easier to analyze the security.

In practice, since Alice and Bob cannot perform quantum non-demolishing measurement on the photon number of the input pulses with current technology, they do not know which pulses are tagged and which are untagged. As a result, the gain Q and the quantum bit error rate (QBER) E of the untagged pules cannot be measured experimentally. Here Q is defined as the *conditional* probability that Charlie has a coincident event given that both Alice and Bob send out an untagged pulse and Alice and Bob use the same basis; E is defined as error rates inside Q.

In experiment, Alice and Bob can measure the overall gain Q_e and the overall QBER E_e. The subscript e denotes the experimentally measurable overall properties. Moreover, they know the probability that certain pulse to be tagged or untagged from the above analysis. Although they cannot measure the gain Q and the QBER E of the untagged pulses directly, they can estimate the upper bounds and lower bounds of them. The upper bound and lower bound of Q are:

$$\begin{aligned}Q\leq\overline{Q}&=\frac{Q_e}{(1-\Delta_a-\epsilon_a)(1-\Delta_b-\epsilon_b)},\\ Q\geq\underline{Q}&=\max(0,\frac{Q_e-1+(1-\Delta_a-\epsilon_a)(1-\Delta_b-\epsilon_b)}{(1-\Delta_a-\epsilon_a)(1-\Delta_b-\epsilon_b)}).\end{aligned} \quad (5)$$

The upper bound and lower bound of $E\cdot Q$ can be estimated as

$$\begin{aligned}\overline{E\cdot Q}&=\frac{Q_eE_e}{(1-\Delta_a-\epsilon_a)(1-\Delta_b-\epsilon_b)},\\ \underline{E\cdot Q}&=\max(0,\frac{Q_eE_e-1+(1-\Delta_a-\epsilon_a)(1-\Delta_b-\epsilon_b)}{(1-\Delta_a-\epsilon_a)(1-\Delta_b-\epsilon_b)}).\end{aligned} \quad (6)$$

Moreover, suppose that an untagged pulse with input photon number $m_a\in[(1-\delta_a)M_a,(1+\delta_a)M_a]$ inputs Fig.3(a) of main-text, the conditional probability that n_a photons are emitted by Alice given that m_a photons enter Alice obeys binomial distribution as:

$$P(n_a|m_a)=\binom{m_a}{n_a}(\lambda_a q)^{n_a}(1-\lambda_a q)^{m_a-n_a}\quad(0\leq\lambda_a\leq 1) \quad (7)$$

For Alice's untagged bits, we can show that the upper bound and lower bound of $P(n_a|m_a)$ are:

$$\overline{P(n_a|m_a)} = \begin{cases} (1-\lambda_a q)^{(1-\delta_a)M_a}, & \text{if } n_a = 0; \\ \binom{(1+\delta_a)M_a}{n_a}(\lambda_a q)^{n_a}(1-\lambda_a q)^{(1+\delta_a)M_a - n_a}, & \text{if } 1 \le n \le (1+\delta_a)M_a; \\ 0, & \text{if } n_a > (1+\delta_a)M_a; \end{cases}$$
$$\underline{P(n_a|m_a)} = \begin{cases} (1-\lambda_a q)^{(1+\delta_a)M_a}, & \text{if } n_a = 0; \\ \binom{(1-\delta_a)M_a}{n_a}(\lambda_a q)^{n_a}(1-\lambda_a q)^{(1-\delta_a)M_a - n_a}, & \text{if } 1 \le n \le (1-\delta_a)M_a; \\ 0, & \text{if } n_a > (1-\delta_a)M_a; \end{cases} \quad (8)$$

under the condition: $(1+\delta_a)M_a\lambda_a q < 1$. This condition suggests that the expected output photon number of any untagged pulse should be lower than 1. This is normally a basic condition in decoy-state BB84 and MDI-QKD based on weak coherent pulses. For example, for $M_a = 10^7$ and $q = 0.01$, Alice can simply set $\lambda_a = 10^{-6}$ so that the expected output photon number is

III. DECOY STATE ANALYSIS

Various decoy-state methods have been proposed for MDI-QKD [4–6]. Among all these decoy state protocols, the two decoy state protocol has been shown to be the optimal one [6], it has already been used in all experimental MDI-QKD implementations reported so far [7–12]. In this protocol, there are three states: Alice's signal state μ_a (for which the internal transmittance is λ_a^μ), Alice's two weak decoy states ν_a and ω_a (for which the internal transmittance is $\lambda_a^\omega < \lambda_a^\nu < \lambda_a^\mu$). In this work, we focus on the *symmetric* case where the two channel transmissions from Alice to Charlie and from Bob to Charlie are equal. In symmetric case, the optimal intensities for Alice and Bob are equal [6]. Hence, to simplify our discussion, we assume that equal intensities are used by Alice and Bob, i.e., γ_a=γ_b=γ with $\gamma \in \{\mu, \nu, \omega\}$. Also, we consider that only the signal state is used to generate the final key, while the decoy states are solely used to test the channel properties.

In previous decoy-state protocols for MDI-QKD [4–6], the key assumption is that the yield of n_a and n_b photon state $Y_{n_a n_b}$ remains the same, whatever signal states or decoy states are chosen by Alice and Bob, e.g. $Y^{\mu\mu}_{n_a n_b} = Y^{\nu\nu}_{n_a n_b}$. Here $Y^{\mu\mu}_{n_a n_b}$ is defined as the conditional probability that Charlie has a coincident event given that Alice (Bob) sends out an n_a (n_b) photon signal and they both chose signal state by setting internal transmittances λ_a^μ and λ_b^μ. This is true because in previous analysis, Eve knows only the output photon numbers n_a and n_b of each pulse. However, this assumption is *no* longer valid in the case that the source is controlled by Eve. Because Eve knows both the input photon number m_a (m_b) and the output photon number n_a (n_b) when she controls the source. Therefore she can perform an attack that depends on the values of both m and n. In this case, the parameter that is the *same* for any signal and decoy states is $Y_{m_a m_b n_a n_b}$, the conditional probability that Charlie has a coincident event given that the two pulses enter Alice's and Bob's lab with photon number m_a and m_b, and they emitted from Alice's and Bob's lab with photon number n_a and n_b. Similarly, the conditional QBERs are also different: $e^{\mu\mu}_{n_a n_b} \neq e^{\nu\nu}_{n_a n_b}$ if Eve controls the source. The parameter that is the same for the signal state and the decoy states is $e_{m_a m_b n_a n_b}$.

In summary, in MDI-QKD, if the source is assumed to be trusted, we have:

$$Y^{\mu\mu}_{n_a n_b} = Y^{\nu\nu}_{n_a n_b}$$
$$e^{\mu\mu}_{n_a n_b} = e^{\nu\nu}_{n_a n_b}.$$

If the source is accessible to Eve (i.e., the source is untrusted), we have:

$$Y^{\mu\mu}_{m_a m_b n_a n_b} = Y^{\nu\nu}_{m_a m_b n_a n_b}$$
$$e^{\mu\mu}_{m_a m_b n_a n_b} = e^{\nu\nu}_{m_a m_b n_a n_b}.$$

The dependence of $Y_{n_a n_b}$ and $e_{n_a n_b}$ on different states is a fundamental difference between MDI-QKD with an untrusted source and MDI-QKD with trusted source. Therefore, in MDI-QKD with an untrusted source, Eve is given significantly greater power, and the decoy state analysis is much more *challenging*. However, rather surprisingly, it is still possible to achieve the unconditional security quantitatively even if the source is given to Eve. This is mainly because we are only focusing on the untagged pulses, whose photon number distribution, the gain and the QBER can be *bounded* via Eqs. (8), (5), (6) respectively. Therefore we are still able to estimate $\underline{Q_{11}^{\mathrm{Z}}}$ and $\overline{e_{11}^{\mathrm{X}}}$. Such estimation can be completed by using either numerical method based on linear programming or analytical method.

In a MDI-QKD implementation with an untrusted source, by performing the measurements for different intensity settings, we can obtain:

$$
\begin{aligned}
Q^{\chi}_{\gamma_a\gamma_b} &= \sum_{m_a=(1-\delta_a)M_a}^{m_a=(1+\delta_a)M_a}\sum_{m_b=(1-\delta_b)M_b}^{m_b=(1+\delta_b)M_b}\sum_{n_a=0}^{\infty}\sum_{n_b=0}^{\infty} P_{in}(m_a)P_{in}(m_b)P^{\gamma_a}(n_a|m_a)P^{\gamma_b}(n_b|m_b)Y_{m_a m_b n_a n_b} \\
E^{\chi}_{\gamma_a\gamma_b}Q^{\chi}_{\gamma_a\gamma_b} &= \sum_{m_a=(1-\delta_a)M_a}^{m_a=(1+\delta_a)M_a}\sum_{m_b=(1-\delta_b)M_b}^{m_b=(1+\delta_b)M_b}\sum_{n_a=0}^{\infty}\sum_{n_b=0}^{\infty} P_{in}(m_a)P_{in}(m_b)P^{\gamma_a}(n_a|m_a)P^{\gamma_b}(n_b|m_b)Y_{m_a m_b n_a n_b}e_{m_a m_b n_a n_b}
\end{aligned}
\tag{9}
$$

where $\chi \in \{\mathrm{X}, \mathrm{Z}\}$ denotes the basis choice, γ_a (γ_b) denotes Alice's (Bob's) intensity setting, $Q^{\chi}_{\gamma_a\gamma_b}$ ($E^{\chi}_{\gamma_a\gamma_b}$) denotes the gain (QBER); where $P_{\text{in}}(m_a)$ is the probability that the input signal contains m_a photons (i.e., the ratio of the number of signals with m input photons over k), $P^{\gamma_a}(n_a|m_a)$ is the conditional probability that the output signal contains n_a photons given the input signal contains m_a photons, for state γ_a and is given by Eq. (7).

Q^{Z}_{11} for $\gamma_a = \mu$ and $\gamma_b = \mu$ can be written as

$$
\begin{aligned}
Q^{\mathrm{Z}}_{11} &= \sum_{m_a=(1-\delta_a)M_a}^{m_a=(1+\delta_a)M_a}\sum_{m_b=(1-\delta_b)M_b}^{m_b=(1+\delta_b)M_b} P_{in}(m_a)P_{in}(m_b)P^{\mu}(1|m_a)P^{\mu}(1|m_b)Y_{m_a m_b 11} \\
&\geq \underline{P^{\mu}_{1|m_a}P^{\mu}_{1|m_b}} \sum_{m_a=(1-\delta_a)M_a}^{m_a=(1+\delta_a)M_a}\sum_{m_b=(1-\delta_b)M_b}^{m_b=(1+\delta_b)M_b} P_{in}(m_a)P_{in}(m_b)Y_{m_a m_b 11} \equiv \underline{P^{\mu}_{1|m_a}P^{\mu}_{1|m_b}} S^{\mathrm{Z}}_{11},
\end{aligned}
\tag{10}
$$

where the bounds of the probabilities are from Eqs. (8). Thus, the estimation on $\underline{Q^{\mathrm{Z}}_{11}}$ is equivalent to the estimation of $\underline{S^{\mathrm{Z}}_{11}}$, and Eq. (9) can be written as

$$
\begin{aligned}
Q^{\chi}_{\gamma_a\gamma_b} &= \sum_{n_a,n_b=0}^{\infty} P^{\gamma_a}(n_a|m_a)P^{\gamma_b}(n_b|m_b)S^{\chi}_{n_a n_b} \\
E^{\chi}_{\gamma_a\gamma_b}Q^{\chi}_{\gamma_a\gamma_b} &= \sum_{n_a,n_b=0}^{\infty} P^{\gamma_a}(n_a|m_a)P^{\gamma_b}(n_b|m_b)S^{\chi}_{n_a n_b}e^{\chi}_{n_a n_b}
\end{aligned}
\tag{11}
$$

A. Numerical approaches

Ignoring statistical fluctuations temporally, the estimations on $\underline{S^{\mathrm{Z}}_{11}}$ and $\overline{e^{\mathrm{X}}_{11}}$, from Eq. (11) are constrained optimisation problems, which is linear and can be efficiently solved by linear programming (LP). The numerical routine to solve these problems can be written as:

$$
\begin{aligned}
&min: S_{11}^{\mathrm{Z}},\\
&s.t.: 0 \le S_{n_a n_b}^{\mathrm{Z}} \le 1, with\ n_a, n_b \in \mathcal{S}_{\mathrm{cut}};\\
&\overline{P(n_a|m_a)} = \begin{cases} (1-\lambda_a)^{(1-\delta_a)M_a}, & \text{if } n_a = 0;\\ \binom{(1+\delta_a)M_a}{n_a}\lambda^{n_a}(1-\lambda_a)^{(1+\delta_a)M_a-n_a}, & \text{if } 1 \le n \le (1+\delta_a)M_a;\\ 0, & \text{if } n_a > (1+\delta_a)M_a; \end{cases}\\
&\underline{P(n_a|m_a)} = \begin{cases} (1-\lambda_a)^{(1+\delta_a)M_a}, & \text{if } n_a = 0;\\ \binom{(1-\delta_a)M_a}{n_a}\lambda^{n_a}(1-\lambda_a)^{(1-\delta_a)M_a-n_a}, & \text{if } 1 \le n \le (1-\delta_a)M_a;\\ 0, & \text{if } n_a > (1-\delta_a)M_a; \end{cases}\\
&\underline{Q_{\gamma_a\gamma_b}^{\mathrm{Z}}} - 1 + \sum_{n_a,n_b\in S_{cut}} \underline{P^{\gamma_a}(n_a|m_a)P^{\gamma_b}(n_b|m_b)} \le \sum_{n,m\in\mathcal{S}_{\mathrm{cut}}} P^{\gamma_a}(n_a|m_a)P^{\gamma_b}(n_b|m_b)S_{n_a n_b}^{\mathrm{Z}} \le \overline{Q_{\gamma_a\gamma_b}^{\mathrm{Z}}}
\end{aligned}
$$

$$
\begin{aligned}
&Max: e_{11}^{\mathrm{X}},\\
&s.t.: 0 \le S_{n_a n_b}^{\mathrm{X}} \le 1, 0 \le S_{n_a n_b}^{\mathrm{X}} e_{n_a n_b}^{\mathrm{X}} \le 1, with\ n_a, n_b \in \mathcal{S}_{\mathrm{cut}}\\
&\overline{P(n_a|m_a)} = \begin{cases} (1-\lambda_a q)^{(1-\delta_a)M_a}, & \text{if } n_a = 0;\\ \binom{(1+\delta_a)M_a}{n_a}(\lambda_a q)^{n_a}(1-\lambda_a q)^{(1+\delta_a)M_a-n_a}, & \text{if } 1 \le n \le (1+\delta_a)M_a;\\ 0, & \text{if } n_a > (1+\delta_a)M_a; \end{cases}\\
&\underline{P(n_a|m_a)} = \begin{cases} (1-\lambda_a q)^{(1+\delta_a)M_a}, & \text{if } n_a = 0;\\ \binom{(1-\delta_a)M_a}{n_a}(\lambda_a q)^{n_a}(1-\lambda_a q)^{(1-\delta_a)M_a-n_a}, & \text{if } 1 \le n \le (1-\delta_a)M_a;\\ 0, & \text{if } n_a > (1-\delta_a)M_a; \end{cases}\\
&\underline{Q_{\gamma_a\gamma_b}^{\mathrm{X}}} - 1 + \sum_{n_a,n_b\in S_{cut}} \underline{P^{\gamma_a}(n_a|m_a)P^{\gamma_b}(n_b|m_b)} \le \sum_{n,m\in\mathcal{S}_{\mathrm{cut}}} P^{\gamma_a}(n_a|m_a)P^{\gamma_b}(n_b|m_b)S_{n_a n_b}^{\mathrm{X}} \le \overline{Q_{\gamma_a\gamma_b}^{\mathrm{X}}}\\
&\underline{Q_{\gamma_a\gamma_b}^{\mathrm{X}}E_{\gamma_a\gamma_b}^{\mathrm{X}}} - 1 + \sum_{n_a,n_b\in S_{cut}} \underline{P^{\gamma_a}(n_a|m_a)P^{\gamma_b}(n_b|m_b)} \le \sum_{n,m\in\mathcal{S}_{\mathrm{cut}}} P^{\gamma_a}(n_a|m_a)P^{\gamma_b}(n_b|m_b)S_{n_a n_b}^{\mathrm{X}}e_{n_a n_b}^{\mathrm{X}} \le \overline{Q_{\gamma_a\gamma_b}^{\mathrm{X}}E_{\gamma_a\gamma_b}^{\mathrm{X}}},
\end{aligned}
$$

where $\mathcal{S}_{\mathrm{cut}}$ denotes a finite set of indexes n_a and n_b, with $\mathcal{S}_{\mathrm{cut}} = \{n_a, n_b \in \mathbb{N}$ with $n_a \le A_{\mathrm{cut}}$ and $n_b \le B_{\mathrm{cut}}\}$, for prefixed values of $A_{\mathrm{cut}} \ge 2$ and $NB_{\mathrm{cut}} \ge 2$. In our simulations, we choose $A_{\mathrm{cut}} = 7$ and $B_{\mathrm{cut}} = 7$, as larger A_{cut} and B_{cut} have negligible effect on decoy-state estimation. More discussions can be seen in [4]. Here, $\gamma \in \{\mu, \nu, \omega\}$ for two decoy-state estimation. Notice that statistical fluctuations can be easily conducted by adding constraints on the experimental measurements of $Q_{\gamma_a\gamma_b}^{\chi}$ and $E_{\gamma_a\gamma_b}^{\chi}$. These additional constraints can be analyzed by using statistical estimation methods, such as standard error analysis [4] or Chernoff bound [13]. A rigorous finite-key analysis can also be implemented by following the technique presented in [13].

B. Analytical approaches

A rigorous estimation is to solve the equation set of Eq. (11) by using the constrains on the binomial probability distributions given by Eq. (8). The analytical expression for such an estimation is highly complicated. So, we only use numerical method presented in last section to study this precise estimation. Here, for the analytical expression, we present a relatively simple analytical method by using the Poisson limit theorem [14]:

Claim: Under the condition that $m \to \infty$ and $\lambda q \to 0$, such that $\mu = m\lambda q$, then

$$
\binom{m}{n}(\lambda q)^n(1-\lambda q)^{m-n} \to \exp(-\mu)\frac{\mu^n}{n!} \tag{12}
$$

The condition in this claim is easy to meet in an actual experiment as m can be larger than 10^6 and λq is normally lower that 10^{-7} in a practical setup. The intuition behind this approximation is that we applied heavy attenuation on the input pulses in Alice and bob. The input pulse has more than $\sim 10^6$ photons, while the output pulse has less than one photon on average. The internal attenuation of Alice's local lab is greater than -60dB. We know that heavy attenuation will transform arbitrary photon number distribution into a Poisson-like distribution. A qualitative argument on this argument for the plug-and-play structure has been provided in [15]. From the approximation, Eq. (11) can be estimated using the similar methods presented in [6].

The lower bound of S_{11}^{Z} is given by

$$\underline{S_{11}^{\mathrm{Z}}} = \frac{1}{(\mu-\omega)^2(\nu-\omega)^2(\mu-\nu)} \times [(\mu^2-\omega^2)(\mu-\omega)(\underline{Q_{\nu\nu}^{\mathrm{Z}}}e^{2\nu} + \underline{Q_{\omega\omega}^{\mathrm{Z}}}e^{2\omega} - \overline{Q_{\nu\omega}^{\mathrm{Z}}}e^{\nu+\omega} - \overline{Q_{\omega\nu}^{\mathrm{Z}}}e^{\omega+\nu}) -$$
$$(\nu^2-\omega^2)(\nu-\omega)(\overline{Q_{\mu\mu}^{\mathrm{Z}}}e^{2\mu} + \overline{Q_{\omega\omega}^{\mathrm{Z}}}e^{2\omega} - \underline{Q_{\mu\omega}^{\mathrm{Z}}}e^{\mu+\omega} - \underline{Q_{\omega\mu}^{\mathrm{Z}}}e^{\omega+\mu})].$$

The upper bound of $S_{11}^{\mathrm{X}}e_{11}^{\mathrm{X}}$ is given by

$$\overline{S_{11}^{\mathrm{X}}e_{11}^{\mathrm{X}}} = \frac{1}{(\nu-\omega)^2} \times [e^{2\nu}\overline{Q_{\nu\nu}^{\mathrm{X}}E_{\nu\nu}^{\mathrm{X}}} + e^{2\omega}\overline{Q_{\omega\omega}^{\mathrm{X}}E_{\omega\omega}^{\mathrm{X}}} - e^{\nu+\omega}\underline{Q_{\nu\omega}^{\mathrm{X}}E_{\nu\omega}^{\mathrm{X}}} - e^{\omega+\nu}\underline{Q_{\omega\nu}^{\mathrm{X}}E_{\omega\nu}^{\mathrm{X}}}].$$

By combining the bounds of the probabilities in Eqs. (8) and Eq. (10), we can obtain Proposition 2 and 3.

IV. SIMULATION TECHNIQUES

In simulation, the gain and the QBER are derived using the channel model presented in [16]. We consider two decoy states: $\nu = 0.01$ and $\omega = 0$, and we optimize the signal state μ for different distances. We choose $f_e = 1.16$

A. Imperfect intensity detector

There are two major imperfections of the intensity detector (ID): inefficiency and noise. The inefficiency η_{ID} can be easily modeled as additional loss by using a beam splitter. The noise of the ID is another important imperfection. In a real experiment, the ID may indicate a certain pulse contains m' photons. Here we refer to m' as the *measured* photon number in contrast to the actual photon number m. However, due to the noise and the inaccuracy of the intensity monitor, this pulse may not contain exactly m' photons. To quantify this imperfection, following[1], we introduce a term, called conservative interval ς. We then define $\underline{V^{\mathrm{s}}}$ as the number of sampling pulses with measured photon number $m' \in [(1-\delta)M' + \varsigma, (1+\delta)M' - \varsigma]$, where $M' = M\eta_{ID}(1-q)$. One can conclude that, with confidence level $\tau_{\mathrm{c}} = 1 - c(\varsigma)$, the number of untagged sampling pulses $V^{\mathrm{s}} \geq \underline{V^{\mathrm{s}}}$. One can make $c(\varsigma)$ arbitrarily close to 0 by choosing a large enough ς. That is, for one individual pulse, the probability that $|m - m'| > \varsigma$ can be negligible.

In practice, various noise sources, including thermal noise, shot-noise, etc, may exist. Here, in simulation, we consider a simple noise model where a constant Gaussian noise with variance σ_{ID}^2 is assumed. That is, if m photons enter an efficient but noisy ID, the probability that the measured photon number is m' obeys a Gaussian distribution

$$P(m'|m) = \frac{1}{\sigma_{\mathrm{IM}}\sqrt{2\pi}} \exp[-\frac{(m-m')^2}{2\sigma_{\mathrm{ID}}^2}]. \quad (13)$$

Hence, the measured photon number distribution $P(m')$ has a larger variation than the actual photon number distribution $P(m)$ due to the noise. More concretely, if the input photon numbers obeys a Gaussian distribution centered at M with variance σ^2, the measured photon numbers also obeys a Gaussian distribution centered at M', but with a variance $\sigma^2 + \sigma_{\mathrm{ID}}^2$.

B. The tagged ratio Δ

For any $\delta \in [0,1]$ and the imperfect ID discussed above, we can calculate Δ from the measured photon number m' by

$$\Delta = 1 - [\Phi(M' + \delta M' + \varsigma) - \Phi(M' - \delta M' - \varsigma))], \quad (14)$$

where Φ is the cumulative distribution function of the photon number for the measured pulses [14]. Assuming that the system is based on a coherent source by Charlie, which means that the input photon number m obeys Poisson distribution. It is natural to set M to be the average input photon number. In numerical simulation, for ease of calculation, we approximate the Poisson distribution of the input photon number M as a Gaussian distribution centered at M with variance $\sigma^2 = M$. This is an excellent approximation because M is very large (10^7 or larger) in all the simulations presented below. Then, the measured photon number m' follows a Gaussian distribution centered at $M' = M\eta_{ID}(1-q)$ with a variance $M + \sigma_{\mathrm{ID}}^2$. The Gaussian cumulative distribution function is given by [14]

$$\Phi_g(x) = \frac{1}{2}[1 + \mathrm{erf}(\frac{x - M'}{\sqrt{2(M + \sigma_{\mathrm{ID}}^2)}})], \quad (15)$$

where $\mathrm{erf}(x) = \frac{2}{\sqrt{\pi}}\int_0^x e^{-t^2}dt$ is the error function. Notice that $\mathrm{erf}(x)$ is an odd function, from Eqs. (14) and (15), we have

$$\Delta = 1 - \mathrm{erf}(\frac{\delta M' + \varsigma}{\sqrt{2M + 2\sigma_{\mathrm{ID}}^2}}). \quad (16)$$

In simulation, for $\delta = \delta_a = \delta_b$, a choice for it that is too large or too small will make the security analysis less optimal [1]. We find numerically that $\delta = 0.01$ is a near an optimal value.

C. Finite-data statistics

A real-life QKD experiment is always completed in finite time, which means that the length of the output secret key is obviously finite. Thus, the parameter estimation procedure in QKD needs to take the statistical fluctuations of the different parameters into account. We assume that Charlie's source generates $2k$ pulses in an experiment. The finite data effect has two main consequences: First, the finite data size will introduce statistical fluctuations for the estimation of the number of untagged pulses. If the confidence level τ_a for Proposition 1 is expected to be close to 1, ϵ_a has to be positive. More concretely, for a fixed $2k$, if the estimate on the untrusted source is expected to have confidence level no less than τ_a, one has to choose ϵ_a as $\epsilon_{\rm a} = \sqrt{-\frac{\ln(1-\tau_a)}{k}}$. In simulation, we choose the confidence level τ (see Proposition 1) as $\tau_a = \tau_b = \tau \geq 1 - 10^{-7}$, which suggests that $\epsilon_a = \epsilon_b = 3.03 \times 10^{-7}$. Since ϵ_a and ϵ_b are non-zero in this finite data case, the estimate of the gain of the untagged pulses becomes not tight at long distances. That is, due to statistical fluctuations, the proportion of tagged pulses is increased at long distance. Our analysis is *conservative* in that Eve can fully control the tagged pulses, which makes the security bounds worse than MDI-QKD with trusted sources. This is the reason why MDI-QKD with an untrusted source is not as good as MDI-QKD with trusted sources in the finite-data case, which has been shown in the Fig.4 of main text.

Second, in decoy state MDI-QKD, the statistical fluctuations of experimental outputs have to be considered. The technique to analyze the statistical fluctuations can be analyzed by using statistical estimation methods, such as standard error analysis [4] or Chernoff bound [13]. In this paper, we analysis the statistical fluctuations by using the standard error analysis method presented in [4]. In simulation, we choose $\epsilon = 10^{-10}$ as the overall security bound considered in our finite-key analysis.

* Electronic address: fhxu@mit.edu

[1] Y. Zhao, B. Qi, H.-K. Lo, and L. Qian, New Journal of Physics **12**, 023024 (2010).

[2] W. Hoeffding, Journal of the American statistical association **58**, 13 (1963).

[3] Y. Zhao, B. Qi, and H.-K. Lo, Physical Review A **77**, 052327 (2008).

[4] X. Ma, C.-H. F. Fung, and M. Razavi, Physical Review A **86**, 052305 (2012).

[5] X.-B. Wang, Physical Review A **87**, 012320 (2013).

[6] F. Xu, H. Xu, and H.-K. Lo, Physical Review A **89**, 052333 (2014).

[7] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Phys. Rev. Lett. **111**, 130501 (2013).

[8] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, X. Ma, J. S. Pelc, M. M. Fejer, C.-Z. Peng, Q. Zhang, and J.-W. Pan, Phys. Rev. Lett. **111**, 130502 (2013).

[9] T. Ferreira da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporão, and J. P. von der Weid, Phys. Rev. A **88**, 052303 (2013).

[10] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, Physics Review Letters] **112**, 190503 (2014).

[11] Y.-L. Tang, H.-L. Yin, S.-J. Chen, Y. Liu, W.-J. Zhang, X. Jiang, L. Zhang, J. Wang, L.-X. You, J.-Y. Guan, *et al.*, Physical review letters **113**, 190501 (2014).

[12] R. Valivarthi, I. Lucio-Martinez, P. Chan, A. Rubenok, C. John, D. Korchinski, C. Duffin, F. Marsili, V. Verma, M. D. Shaw, *et al.*, arXiv preprint arXiv:1501.07307 (2015).

[13] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Nature Communications **5**, 3732 (2014).

[14] A. Papoulis and S. U. Pillai, *Probability, random variables, and stochastic processes* (Tata McGraw-Hill Education, 2002).

[15] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Physical Review A **73** (2006).

[16] F. Xu, M. Curty, B. Qi, and H.-K. Lo, New Journal of Physics **15**, 113007 (2013).