Measurement-device-independent quantum communication with an untrusted source

Feihu Xu

Phys. Rev. A **92**, 012333 — Published 29 July 2015

DOI: 10.1103/PhysRevA.92.012333

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

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.

I. INTRODUCTION

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 [1–3]. Commercial QKD systems have appeared on the market [4, 5], and QKD networks have been developed [6–8]. Unfortunately, due to real-life imperfections, a crucial problem in current QKD implementations is the discrepancy between its theory and practice [3]. An eavesdropper (Eve) could exploit such imperfections and hack a QKD system. Indeed, the recent demonstrations of various attacks [9–16] 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) [17] removes all detector side-channel attacks. This kind of attack is arguably the most important security loophole in conventional QKD implementations [12–16]. The assumption in MDI-QKD is that the state preparation can be trusted. Unlike security patches [18–20] and device-independent QKD [21], 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 [22–29] and experimental [30–35] studies. See [36] 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 [37], quantum fingerprinting [38, 39], blind quantum computing [40], and multiparty quantum communication [29]. This scheme is advantageous in comparison to the recent demonstrations of quantum access networks [6–8], 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' frequency-locked lasers are trusted. However, since frequency-locked lasers[1] used in MDI-QKD experiments [30, 33, 35] 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) It is well known that the major challenge in implementation of Fig. 1(a) is the performance of high-fidelity interference between photons from spatially separated lasers [17, 30]. (iii) In fiber communication, it is necessary to introduce additional time-synchronization system and to include complex feedback controls to compensate for the polarization rotations (e.g., an implementation in [34]). All these challenges render Fig. 1(a) difficult for practical implementations and applications.

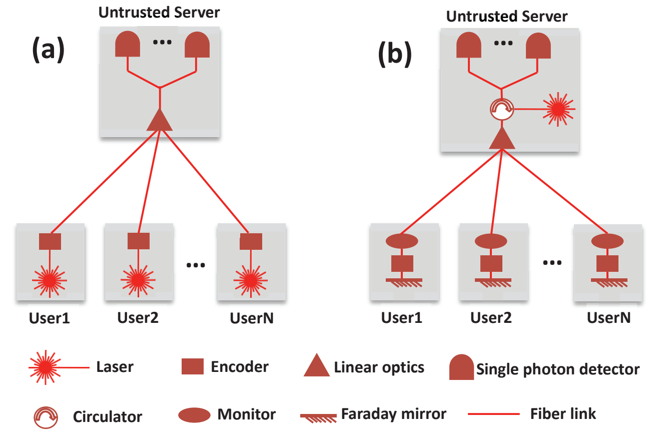

FIG. 1: (Color online) (a) A fiber-based quantum network with N trusted lasers. (b) A quantum network with a single *untrusted* laser source.

Recently, to mitigate the experimental complexity of the interference from two remote lasers, several groups have proposed a new protocol against untrusted detectors [41–44]. A slight drawback is that a rigorous security analysis for this

[1] See, for instance, http://dev.wavelengthreferences.com/clarity-precision-frequency-standard.

protocol is challenging, which makes the protocol vulnerable to attacks if certain assumptions cannot be satisfied [45]. Another elegant proposal to resolve the limitations in the implementation of MDI-QKD is the so-called plug&play MDI-QKD [46]. Despite the importance of this proposal, a crucial part to guarantee the security – source monitoring – is ignored, which makes plug&play MDI-QKD vulnerable to various source attacks [9–11]. Also, a complete security proof for plug&play MDI-QKD and the analysis of practical imperfections are missing.

In this paper, we overcome the challenges of Fig. 1(a) by proposing a MDI quantum network with a single untrusted source in Fig. 1(b). The untrusted server transmits strong 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 conventional plug&play QKD [47, 48], we show what measures by the users are necessary to ensure the 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. These results provide a complete security analysis for plug&play MDI-QKD, and more importantly, make plug&play MDI-QKD unconditionally secure, even with practical imperfections.

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 wavelength division multiplexing (WDM) [49].

The additional assumption, as compared to the initial MDI quantum network, is the trust of the monitoring devices. Note that the users need to monitor only classical laser pulses instead of single-photon signals. Such monitoring can be easily 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 in order to prevent the so-called Trojan-horse attack [9]. It is important that proof-of-concept experiments have been reported towards implementation of this monitoring [50–52] and that ID Quantique's commercial system (i.e., Clavis2) has already included a preliminary version of the monitor [4]. Recently, the security of the intensity detector has been studied comprehensively in [52]. 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 [53].

The rest of this paper is organized as follows. We introduce the protocol of MDI-QKD with an untrusted source in Sec. II. In Sec. III, we present the security analysis of our protocol by introducing an equivalently virtual model. In Sec. IV, we show the simulation results about the key rate comparison between MDI-QKD with an untrusted source and MDI-QKD with trusted sources, and study how device imperfections affect the protocol. Finally, we conclude this paper in Sec. V.

II. MDI-QKD WITH AN UNTRUSTED SOURCE

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 [29]. We consider a time-bin encoding [30], and the protocol runs as follows.

a. Preliminaries Alice and Bob use a pre-shared key for authentication, and they negotiate parameters needed during the protocol run. Alice and Bob perform a calibration measurement of their devices.

b. Preparation and distribution Charlie generates a strong laser pulse, which creates two time-bin pulses (early pulse and late pulse) after an interferometer. Charlie uses a beam splitter (BS) to split the two time-bin pulses into two parts and send them to Alice and Bob via two quantum channels (e.g., optical fibers).

c. Monitoring and Encoding phase Once the pulses arrive at Alice (Bob), they pass through an optical filter, a monitoring unit, which consists of a BS and an intensity detector (ID). The pulses are phase-randomized by a phase modulator, PM1 (PM3), and then encoded by an Encoder that consists of an intensity modulator (IM) and a PM. Alice and Bob also use the IM to generate signal/decoy states. Finally, the pulses are reflected by a Faraday mirror (FM) and attenuated by a variable optical attenuator (VOA) to single-photon level.

c. Measurement phase The time-bin-encoded weak coherent pulses from Alice and Bob travel back through the two channels, interfere at the BS of Charlie and finally they are detected by two single photon detectors. A coincident event projects the photons into the so-called singlet state $|\psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$ [30].

d. Basis and signal/decoy reconciliation Alice and Bob announce their encoding bases and signal/decoy intensity levels over the authenticated public channel and keep the samples measured in the same bases for signal/decoy states.

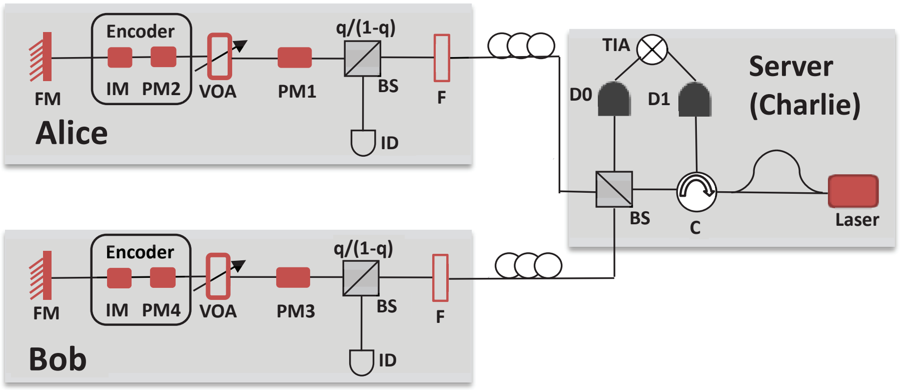

FIG. 2: (Color online) Schematic diagram of a time-bin-encoding MDI-QKD with an untrusted laser source. The strong time-bin laser pulses are generated by a pulsed laser and an interferometer in Charlie and they are split into two groups by a beam splitter (BS). Once these pulses arrived at Alice (Bob), they pass through an optical filter (F), a monitoring unit with a BS and a classical intensity detector (ID), a phase modulator (PM1 and PM3) for phase randomization and a variable optical attenuator (VOA). Then, the pulses are encoded by an Encoder that consists of an intensity modulator (IM) and a PM, 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). The coincident counts are recorded by a time interval analyzer (TIA).

e. Parameter estimation Alice and Bob perform the security analysis and the decoy state analysis based on their monitoring results and Charlie's public announcements.

g. Error reconciliation and privacy amplification Alice and Bob perform the error correction. To ensure that they share a pair of identical keys, they perform an error-verification step using two-universal hash functions. Finally, Alice and Bob apply the privacy amplification to produce the final secret key.

Since the source is entirely unknown and untrusted, we use three measures to enhance the security of our protocol [9, 47].

1. We place a narrow bandpass filter (together with a single mode fiber), i.e., F in Fig. 2, to allow only a single mode in spectral and spatial domains to enter into the Encoder. Note that a wavelength-bandpass filter has already been implemented in commercial QKD systems (i.e., Clavis2) [4]. Moreover, the analysis in [54] shows that with standard optical devices, the single mode assumption can be guaranteed with a high rate of accuracy.

2. We monitor the pulse energy and the arrival time to acquire certain information about the photon number distribution (PND) and the timing mode. Such monitoring can also defend the Trojan house attack [9] and it has been included in commercial QKD systems [4]. 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 Alice's and Bob's BS and ID. In practice, besides the ID, a spectrum analyzer can also be introduced to monitor the spectral information.

3. Alice and Bob use PM1 and PM3 to apply the active phase randomization [50]. The phase randomization is a general assumption made in most security proofs for laser-based QKD [55–57] 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.

III. SECURITY ANALYSIS

A. System model

To analyze the security of Fig. 2, we model Alice's (Bob's) system in Fig. 3(a). We model all the losses as a $\lambda/(1-\lambda)$ beam splitter, i.e., the internal transmittance of Alice's (Bob's) local lab is λ_a (λ_b), which can be set accurately via VOA in Fig. 2. Each input pulse after the filter (F) 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 corresponding sampling pulse by using the random sampling theorem [58, 59]. 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) [48]. For the imperfect ID in Fig. 3(a), assuming that its efficiency is $\eta_{\mathrm{ID}} \leq 1$, we model the $q/(1-q)$ BS and the imperfect ID as a $q'/(1-q')$ BS and a perfect ID with $q' = (1-q)\eta_{\mathrm{ID}}$. To ensure that an identical attenuation is applied to the encoding pulses in both models, we redefine the internal transmittance in the virtual model as: $\lambda' = q\lambda/q' \leq 1$. Moreover, 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 of the encoding pulses and the sampling pulses. 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 [48].

In Fig. 3(b), we define m_a (n_a) as the photon number of the pulses that input (output) Alice. We also define the pulses that input Alice as

- Untagged pulses: $m_a \in [(1-\delta_a)M_a, (1+\delta_a)M_a]$;
- Tagged pulses: $m_a < (1-\delta_a)M_a$ or $m_a > (1+\delta_a)M_a$.

Here δ_a is a small positive real number, and M_a is a large positive integer (which can be the average of the input photon numbers of the pulses received by Alice). The same definitions apply to Bob's pulses with parameters $\{m_b, n_b, \delta_b, M_b\}$. Note that $\{\delta_a, \delta_b, M_a, M_b\}$ are chosen by Alice and Bob.

From the random sampling theorem, we draw the follow proposition [47].

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^{s} sampling pulses and V_a^{e} encoding pulses are untagged. The probability that $V_a^{\mathrm{e}} \leq V_a^{\mathrm{s}} - 2\epsilon_a k$ satisfies*

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

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 $V_a^{\mathrm{e}} > V_a^{\mathrm{s}} - \epsilon_a k$ with confidence level $\tau_a > 1 - \exp(-k\epsilon_a^2)$.

The proof is shown in Appendix A. This proposition shows that Alice can estimate V_a^{e} from V_a^{s}. Bob's untagged pulses have the same property. Furthermore, if we define Δ_a (Δ_b) as the average probability that a sampling pulse belongs to a tagged sampling pulse in the asymptotic case, then Alice (Bob) can conclude that there are no fewer than $(1-\Delta_a-\epsilon_a)k$ ($(1-\Delta_b-\epsilon_b)k$) untagged encoding pulses with high fidelity.

B. Untagged 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 (QND) measurement on the photon number of the input pulses with current technology, they do not know which pulses are tagged and which are untagged. Consequently, the gain and the quantum bit error rate (QBER) of the untagged pulses can *not* be measured directly. Alice and Bob can measure only the overall gain and the QBER. 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 QBER of the untagged pulses. Furthermore, in the case that an untagged pulse inputs Alice/Bob in Fig. 3(a), then the conditional probability that n_a (n_b) photons are emitted by Alice obeys a binomial distribution, which can be controlled by Alice's (Bob's) internal transmittance. Alice (Bob) can also estimate the bounds of such a binomial distribution. The specific bounds for the gain, QBER and the PND of the untagged pulses are shown in Appendix B. Using these bounds, we can prove the security of MDI-QKD with an untrusted source quantitatively.

C. Key rate

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

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

where $\underline{Q_{11}^{\mathrm{Z}}}$ and $\overline{e_{11}^{\mathrm{X}}}$ 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 given by $H_2(x)$=$-x\log_2(x) - (1-x)\log_2(1-x)$; $Q_{e,\mu\mu}^{\mathrm{Z}}$ and $E_{e,\mu\mu}^{\mathrm{Z}}$ 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 simulations, we consider $f_e = 1.16$). Here we use the Z basis for key generation and the X basis for testing only. In practice, $Q_{e,\mu\mu}^{\mathrm{Z}}$ and $E_{e,\mu\mu}^{Z}$ are directly measured in the experiment, while $\underline{Q_{11}^{\mathrm{Z}}}$ and $\overline{e_{11}^{\mathrm{X}}}$ are estimated from the decoy states.

D. Decoy states

In the previous decoy-state protocols for MDI-QKD [22, 24–26, 28], the key assumption is that the yield, $Y_{n_a n_b}$[2], remains the same for signal or decoy states. 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). In this case, the parameter that is the *same* for any signal and decoy

[2] $Y_{n_a n_b}$ 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.

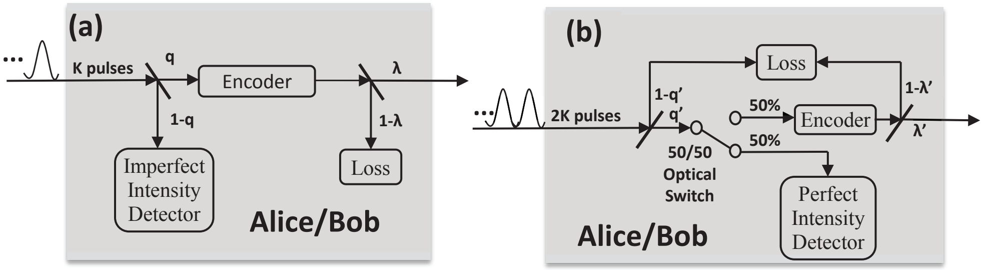

FIG. 3: (a) The actual model for Fig. 2. All the internal loss of Alice/Bob is modeled as a $\lambda/(1-\lambda)$ beam splitter. (b) An equivalent virtual model. The loss is modeled as a $\lambda'/(1-\lambda')$ beam splitter. $q' = \eta_{\rm ID}(1-q)$, where $\eta_{\rm ID} \leq 1$ is the efficiency of the imperfect intensity detector. $\lambda' = q\lambda/q'$. The virtual model, which has features from (a), is used to analyze the security of (a).

state is $Y_{m_a m_b n_a n_b}$[3]. Similarly, the conditional QBERs are also different if Eve controls the source.

Therefore, in MDI-QKD with an untrusted source, Eve is given significantly greater power, since she can control both the input and the output of Alice's and Bob's lab. The decoy state analysis is more challenging. However, rather surprisingly, it is still possible to achieve the unconditional security quantitatively, even if the source is given to Eve [47]. This is so mainly because we are focusing only on the untagged pulses, whose PND, gain and QBER can be *bounded*. Therefore, we are still able to estimate $\underline{Q}_{11}^{Z}$ and $\overline{e}_{11}^{X}$. Such an estimation can be completed by using either the numerical method based on linear programming or the analytical method. The details of this estimation are shown in Appendix C.

IV. NUMERICAL SIMULATION

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 single photon detectors [4]. 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 [34]. The efficiency of the intensity detector (ID) η_{ID}, the noise of the ID σ_{ID}, and the beam splitter ratio q are from [48]. ϵ is the security bound considered in our finite-key analysis.

The details of the simulation techniques, including the model for the imperfect intensity detector, the tagged ratio Δ and the finite-data statistics, are shown in the Appendix D. We use the experimental parameters, listed in Table I for 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 [48]. We find numerically that $\delta = 0.01$ is a near an optimal value. In addition, we assume that the source in Charlie is Poissonian centered at M_c photons per optical pulse. In this bi-directional structure, Alice's and Bob's average input photon numbers (M_a and M_b) depend on the channel loss and M_c. The gain and the QBER are derived using the channel model presented in [25].

The simulation results with an infinite number of signals are shown by the red curves in Fig. 4. We consider two decoy states: we fix the vacuum state at $\omega = 0$, the weak decoy state at $\nu = 0.01$, and optimize the signal state μ for different distances. With $M_c = 10^7$ (Charlie's mean photon number per pulse), the case with an untrusted source (red dotted curve) is similar to that with trusted sources (red dashed curve) 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 Eq. (B1)). This is so especially 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 $M_c = 10^9$ (red solid curve). The two cases (with trusted sources and with an untrusted source) have similar results. 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 $\sim$ 9.6 mW. This laser power can be provided by many commercial pulsed laser diodes.

The simulation results with a finite number of signals are shown by the blue curves in Fig. 4. We choose the confidence level τ for the statistical fluctuations of the estimation of the number of untagged pulses (see Eq. (1)) as $\tau_a = \tau_b =$

[3] $Y_{m_a m_b n_a n_b}$ is defined as 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.

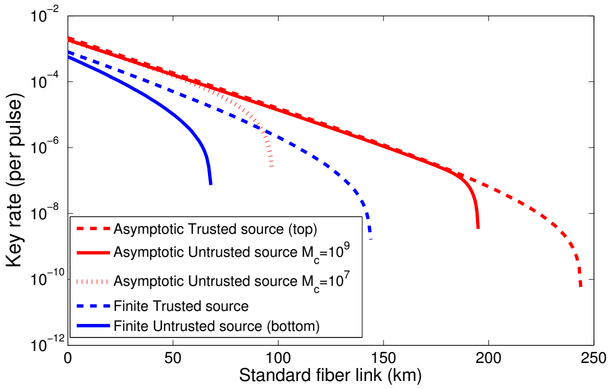

FIG. 4: (Color online) Simulation results. Red curves are for an infinite number of signals. M_c denotes the mean of the photon number (per pulse) of Charlie's laser pulses. With $M_c = 10^9$ and practical imperfections, MDI-QKD with an untrsuted source can tolerate about 195 km distance. At the distances 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. Finite data size reduces the efficiencies for both cases. MDI-QKD with an untrusted source can still tolerate over 70 km fiber with detectors of 20% efficiency.

$\tau \geq 1 - 10^{-7}$, which suggests that $\epsilon_a = \epsilon_b = 3.03 \times 10^{-7}$. We set $M_c = 10^9$. 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 are non-zero in this finite data case, and thus the estimate of the gain of the untagged pulses becomes not tight (see Appendix D)[4]. 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 [60], however, the protocol can easily generate keys over 200 km fiber.

V. DISCUSSION

In summary, we 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 [36–40]. 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, including additional loss introduced by the bi-directional structure, the inefficiency and noise of the intensity monitor, and the finite data-size effect. Furthermore, our protocol is practically secure and ready for implementation. An experimental demonstration is in progress.

It is worthy to mention that one practical issue associated with Fig. 2 is the temporal matching. For instance, the two channels – Alice-Charlie and Bob-Charlie – may be different in practice, then the arrival times are mismatch when the pulses return back to Charlie. One solution, as demonstrated already in [30], is to introduce addition fibers inside either Alice or Bob to match the channel length. Note that, similar to the conventional plug&play system [4], in our proposal, each of Alice and Bob should hold certain length of fiber spool as the optical buffer. Consequently, Alice/Bob can control the length of this fiber buffer to match the channel difference. Furthermore, the feedback control techniques, demonstrated in [34] could also be used to ameliorate temporal-matching issues.

There are still several imperfections that are not analyzed in our paper, such as the source flaws in the state preparation [54], the non-ideality in the optical filter, and the imperfections in the electronics of the classical intensity detector [52]. These questions lead to an interesting future project, that is, deriving a refined analysis that includes all possible (small) imperfections and side channels in users. For instance, Ref. [61] has reported comprehensive analysis against the Trojan horse attack. We expect that this research direction will move an important step towards unconditionally secure communication networks that are also practical.

VI. ACKNOWLEDGEMENT

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

Appendix A: Proof of Proposition 1

We follow [48] to prove Proposition 1. Among all the V untagged pulses, each pulse has probability 1/2 to be assigned as an untagged encoding pulse. Therefore, the probability that $V_a^{\mathrm{e}} = v$ obeys a binomial distribution. Cumulative probability is given by [59]

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

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

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

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

$$P(V_a^{\mathrm{e}} \leq \frac{V - 2\epsilon k}{2}) \leq \exp(-k\epsilon^2). \tag{A1}$$

[4] That is, due to statistical fluctuations, the proportion of tagged pulses is increased. Our analysis is conservative in that Eve can fully control the tagged pulses, which makes the security bound worse than MDI-QKD with trusted sources.

By definition, we have

$$V = V_a^{\mathrm{e}} + V_a^{\mathrm{s}}. \tag{A2}$$

Substituting Equation (A2) into Equation (A1), we have

$$P(V_a^{\mathrm{e}} \leq V_a^{\mathrm{s}} - \epsilon k) \leq \exp(-k\epsilon^2). \quad \square \tag{A3}$$

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 an encoding 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

$$P[V_a^{\mathrm{e}} \leq \frac{\beta}{1-\beta}(V_a^{\mathrm{s}} - 2\epsilon k)] \leq \exp(-4k\epsilon^2\beta^2). \tag{A4}$$

Appendix B: Properties of untagged pulses

The main concept to analyze the properties of the untagged pulses follows the analysis for plug&play QKD presented in [47]. 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:

$$\begin{aligned} Q &\leq \overline{Q} = \frac{Q_e}{(1-\Delta_a-\epsilon_a)(1-\Delta_b-\epsilon_b)}, \\ Q &\geq \underline{Q} = \max(0, \frac{Q_e - 1 + (1-\Delta_a-\epsilon_a)(1-\Delta_b-\epsilon_b)}{(1-\Delta_a-\epsilon_a)(1-\Delta_b-\epsilon_b)}). \end{aligned} \tag{B1}$$

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

$$\begin{aligned} \overline{E \cdot Q} &= \frac{Q_e E_e}{(1-\Delta_a-\epsilon_a)(1-\Delta_b-\epsilon_b)}, \\ \underline{E \cdot Q} &= \max(0, \frac{Q_e E_e - 1 + (1-\Delta_a-\epsilon_a)(1-\Delta_b-\epsilon_b)}{(1-\Delta_a-\epsilon_a)(1-\Delta_b-\epsilon_b)}). \end{aligned} \tag{B2}$$

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:

$$P(n_a|m_a) = \binom{m_a}{n_a}(\lambda_a q)^{n_a}(1-\lambda_a q)^{m_a-n_a} \quad (0 \leq \lambda_a \leq 1) \tag{B3}$$

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

$$\begin{aligned} \overline{P(n_a|m_a)} &= \begin{cases} (1-\lambda_a q)^{(1-\delta_a)M_a}, & \text{if } n_a = 0; \\ \binom{(1+\delta_a)M_a}{n_a}(\lambda_a q)^{n_a}(1-\lambda_a q)^{(1+\delta_a)M_a-n_a}, & \text{if } 1 \leq n \leq (1+\delta_a)M_a; \\ 0, & \text{if } n_a > (1+\delta_a)M_a; \end{cases} \\ \underline{P(n_a|m_a)} &= \begin{cases} (1-\lambda_a q)^{(1+\delta_a)M_a}, & \text{if } n_a = 0; \\ \binom{(1-\delta_a)M_a}{n_a}(\lambda_a q)^{n_a}(1-\lambda_a q)^{(1-\delta_a)M_a-n_a}, & \text{if } 1 \leq n \leq (1-\delta_a)M_a; \\ 0, & \text{if } n_a > (1-\delta_a)M_a; \end{cases} \end{aligned} \tag{B4}$$

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

Appendix C: Decoy state analysis

Various decoy-state methods have been proposed for MDI-QKD [22, 24, 28]. Among all these decoy state protocols, the two decoy state protocol has been shown to be the optimal one [28], it has already been used in all experimental MDI-QKD implementations reported so far [30–35]. 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 [28]. 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 [22, 24, 28], 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. $Y_{n_a n_b}^{\mu\mu} = Y_{n_a n_b}^{\nu\nu}$. Here $Y_{n_a n_b}^{\mu\mu}$ 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: $e_{n_a n_b}^{\mu\mu} \neq e_{n_a n_b}^{\nu\nu}$ 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:

$$\begin{aligned} Y_{n_a n_b}^{\mu\mu} &= Y_{n_a n_b}^{\nu\nu} \\ e_{n_a n_b}^{\mu\mu} &= e_{n_a n_b}^{\nu\nu}. \end{aligned}$$

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

$$\begin{aligned} Y_{m_a m_b n_a n_b}^{\mu\mu} &= Y_{m_a m_b n_a n_b}^{\nu\nu} \\ e_{m_a m_b n_a n_b}^{\mu\mu} &= e_{m_a m_b n_a n_b}^{\nu\nu}. \end{aligned}$$

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. (B4), (B1), (B2) 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:

$$\begin{aligned} Q_{\gamma_a\gamma_b}^{\chi} &= \sum_{m_a=(1-\delta_a)M_a}^{m_a=(1+\delta_a)M_a} \sum_{m_b=(1-\delta_b)M_b}^{m_b=(1+\delta_b)M_b} \sum_{n_a=0}^{\infty} \sum_{n_b=0}^{\infty} P_{in}(m_a) P_{in}(m_b) P^{\gamma_a}(n_a|m_a) P^{\gamma_b}(n_b|m_b) Y_{m_a m_b n_a n_b} \\ E_{\gamma_a\gamma_b}^{\chi} Q_{\gamma_a\gamma_b}^{\chi} &= \sum_{m_a=(1-\delta_a)M_a}^{m_a=(1+\delta_a)M_a} \sum_{m_b=(1-\delta_b)M_b}^{m_b=(1+\delta_b)M_b} \sum_{n_a=0}^{\infty} \sum_{n_b=0}^{\infty} P_{in}(m_a) P_{in}(m_b) P^{\gamma_a}(n_a|m_a) P^{\gamma_b}(n_b|m_b) Y_{m_a m_b n_a n_b} e_{m_a m_b n_a n_b} \end{aligned} \tag{C1}$$

where $\chi \in \{\mathrm{X}, \mathrm{Z}\}$ denotes the basis choice, γ_a (γ_b) denotes Alice's (Bob's) intensity setting, $Q_{\gamma_a\gamma_b}^{\chi}$ ($E_{\gamma_a\gamma_b}^{\chi}$) 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. (B3).

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

$$
\begin{aligned}
Q_{11}^{\mathrm{Z}} &= \sum_{m_a=(1-\delta_a)M_a}^{m_a=(1+\delta_a)M_a} \sum_{m_b=(1-\delta_b)M_b}^{m_b=(1+\delta_b)M_b} P_{in}(m_a)P_{in}(m_b)P^{\mu}(1|m_a)P^{\mu}(1|m_b)Y_{m_a m_b 11} \\
&\geq \underline{P_{1|m_a}^{\mu} P_{1|m_b}^{\mu}} \sum_{m_a=(1-\delta_a)M_a}^{m_a=(1+\delta_a)M_a} \sum_{m_b=(1-\delta_b)M_b}^{m_b=(1+\delta_b)M_b} P_{in}(m_a)P_{in}(m_b)Y_{m_a m_b 11} \equiv \underline{P_{1|m_a}^{\mu} P_{1|m_b}^{\mu}} S_{11}^{\mathrm{Z}},
\end{aligned}
\tag{C2}
$$

where the bounds of the probabilities are from Eqs. (B4). Thus, the estimation on $\underline{Q_{11}^{\mathrm{Z}}}$ is equivalent to the estimation of $\underline{S_{11}^{\mathrm{Z}}}$, and Eq. (C1) can be written as

$$
\begin{aligned}
Q_{\gamma_a\gamma_b}^{\mathcal{X}} &= \sum_{n_a,n_b=0}^{\infty} P^{\gamma_a}(n_a|m_a)P^{\gamma_b}(n_b|m_b)S_{n_a n_b}^{\mathcal{X}} \\
E_{\gamma_a\gamma_b}^{\mathcal{X}} Q_{\gamma_a\gamma_b}^{\mathcal{X}} &= \sum_{n_a,n_b=0}^{\infty} P^{\gamma_a}(n_a|m_a)P^{\gamma_b}(n_b|m_b)S_{n_a n_b}^{\mathcal{X}} e_{n_a n_b}^{\mathcal{X}}
\end{aligned}
\tag{C3}
$$

1. Numerical approaches

Ignoring statistical fluctuations temporally, the estimations on $\underline{S_{11}^{\mathrm{Z}}}$ and $\overline{e_{11}^{\mathrm{X}}}$, from Eq. (C3) 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:

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

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

where $\mathcal{S}_{\mathrm{cut}}$ denotes a finite set of indexes n_a and n_b, with $\mathcal{S}_{\mathrm{cut}} = \{n_a, n_b \in \mathbb{N} \text{ with } n_a \leq A_{\mathrm{cut}} \text{ and } n_b \leq B_{\mathrm{cut}}\}$, for prefixed values of $A_{\mathrm{cut}} \geq 2$ and $NB_{\mathrm{cut}} \geq 2$. In our simulations, we choose $A_{\text{cut}} = 7$ and $B_{\text{cut}} = 7$, as larger A_{cut} and B_{cut} have negligible effect on decoy-state estimation. More discussions can be seen in [22]. 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 $Q^X_{\gamma_a\gamma_b}$ and $E^X_{\gamma_a\gamma_b}$. These additional constraints can be analyzed by using statistical estimation methods, such as standard error analysis [22] or Chernoff bound [26]. A rigorous finite-key analysis can also be implemented by following the technique presented in [26].

2. Analytical approaches

A rigorous estimation is to solve the equation set of Eq. (C3) by using the constrains on the binomial probability distributions given by Eq. (B4). 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 [58]:

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

$$\binom{m}{n}(\lambda q)^n(1-\lambda q)^{m-n} \to \exp(-\mu)\frac{\mu^n}{n!} \tag{C4}$$

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 [9]. From the approximation, Eq. (C3) can be estimated using the similar methods presented in [28].

The lower bound of S^Z_{11} is given by

$$\underline{S^Z_{11}} = \frac{1}{(\mu-\omega)^2(\nu-\omega)^2(\mu-\nu)} \times [(\mu^2-\omega^2)(\mu-\omega)(\underline{Q^Z_{\nu\nu}}e^{2\nu} + \underline{Q^Z_{\omega\omega}}e^{2\omega} - \overline{Q^Z_{\nu\omega}}e^{\nu+\omega} - \overline{Q^Z_{\omega\nu}}e^{\omega+\nu}) - \\ (\nu^2-\omega^2)(\nu-\omega)(\overline{Q^Z_{\mu\mu}}e^{2\mu} + \overline{Q^Z_{\omega\omega}}e^{2\omega} - \underline{Q^Z_{\mu\omega}}e^{\mu+\omega} - \underline{Q^Z_{\omega\mu}}e^{\omega+\mu})].$$

The upper bound of $S^X_{11}e^X_{11}$ is given by

$$\overline{S^X_{11}e^X_{11}} = \frac{1}{(\nu-\omega)^2} \times [e^{2\nu}\overline{Q^X_{\nu\nu}E^X_{\nu\nu}} + e^{2\omega}\overline{Q^X_{\omega\omega}E^X_{\omega\omega}} - e^{\nu+\omega}\underline{Q^X_{\nu\omega}E^X_{\nu\omega}} - e^{\omega+\nu}\underline{Q^X_{\omega\nu}E^X_{\omega\nu}}].$$

By combining the bounds of the probabilities in Eqs. (B4) and Eq. (C2), we can obtain Proposition 2 and 3.

Appendix D: Simulation techniques

In simulation, the gain and the QBER are derived using the channel model presented in [25]. We consider two decoy states: $\nu = 0.01$ and $\omega = 0$, and we optimize the signal state μ for different distances. We choose $f_e = 1.16$

1. 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 [48], we introduce a term, called conservative interval ς. We then define $\underline{V}^{\text{s}}$ 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 $\tau_{\text{c}} = 1 - c(\varsigma)$, the number of untagged sampling pulses $V^{\text{s}} \geq \underline{V}^{\text{s}}$. 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 $\sigma_{\rm ID}^2$ 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

$$P(m'|m) = \frac{1}{\sigma_{\rm IM}\sqrt{2\pi}}\exp[-\frac{(m-m')^2}{2\sigma_{\rm ID}^2}]. \quad \text{(D1)}$$

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 $\sigma^2+\sigma_{\rm ID}^2$.

2. 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

$$\Delta = 1-[\Phi(M'+\delta M'+\varsigma)-\Phi(M'-\delta M'-\varsigma))], \quad \text{(D2)}$$

where Φ is the cumulative distribution function of the photon number for the measured pulses [58]. 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 $M+\sigma_{\rm ID}^2$. The Gaussian cumulative distribution function is given by [58]

$$\Phi_g(x) = \frac{1}{2}[1+\text{erf}(\frac{x-M'}{\sqrt{2(M+\sigma_{\rm ID}^2)}})], \quad \text{(D3)}$$

where $\text{erf}(x) = \frac{2}{\sqrt{\pi}}\int_0^x e^{-t^2}dt$ is the error function. Notice that $\text{erf}(x)$ is an odd function, from Eqs. (D2) and (D3), we have

$$\Delta = 1-\text{erf}(\frac{\delta M'+\varsigma}{\sqrt{2M+2\sigma_{\rm ID}^2}}). \quad \text{(D4)}$$

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 [48]. We find numerically that $\delta = 0.01$ is a near an optimal value.

3. 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 $\epsilon_a = \epsilon_b = 3.03\times10^{-7}$. 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 [22] or Chernoff bound [26]. In this paper, we analyze the statistical fluctuations by using the standard error analysis method presented in [22]. In simulation, we choose $\epsilon = 10^{-10}$ as the overall security bound.

[*] Electronic address: fhxu@mit.edu

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Reviews of Modern Physics **74**, 145 (2002).

[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Reviews of Modern Physics **81**, 1301 (2009).

[3] H.-K. Lo, M. Curty, and K. Tamaki, Nature Photonics **8**, 595 (2014).

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

[5] QuantumCTek: http://www.quantum-info.com/en.php; QaSky: http://www.qasky.com/EN/Default.aspx; QuintessenceLabs Pty. Ltd: http://www.quintessencelabs.com .

[6] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, *et al.*, Optics Express **19**, 10387 (2011).

[7] B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, Nature **501**, 69 (2013).

[8] R. J. Hughes, J. E. Nordholt, K. P. McCabe, R. T. Newell, C. G. Peterson, and R. D. Somma, arXiv preprint arXiv:1305.0305 (2013).

[9] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Physical Review A **73** (2006).
[10] F. Xu, B. Qi, and H.-K. Lo, New Journal of Physics **12**, 113026 (2010).
[11] S. Sun, M. Jiang, and L. Liang, Physical Review A **83**, 062331 (2011).
[12] Y. Zhao, C. Fung, B. Qi, C. Chen, and H.-K. Lo, Physical Review A **78**, 042333 (2008).
[13] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nature Photonics **4**, 686 (2010).
[14] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Nature Communications **2**, 349 (2011).
[15] H. Weier, H. Krauss, M. Rau, M. Fuerst, S. Nauerth, and H. Weinfurter, New Journal of Physics **13**, 073024 (2011).
[16] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, Physical Review Letters **107**, 110501 (2011).
[17] H.-K. Lo, M. Curty, and B. Qi, Physical Review Letters **108**, 130503 (2012).
[18] Z. Yuan, J. Dynes, and A. Shields, Applied Physics Letters **98**, 231104 (2011).
[19] T. Ferreira da Silva, G. B. Xavier, G. P. Temporão, and J. P. von der Weid, Optics Express **20**, 18911 (2012).
[20] C. Lim, N. Walenta, M. Legre, N. Gisin, and H. Zbinden, IEEE Journal of Selected Topics in Quantum Electronics **21**, 6601305 (2015).
[21] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Physical Review Letters **98**, 230501 (2007).
[22] X. Ma, C.-H. F. Fung, and M. Razavi, Physical Review A **86**, 052305 (2012).
[23] X. Ma and M. Razavi, Physical Review A **86**, 062319 (2012).
[24] X.-B. Wang, Physical Review A **87**, 012320 (2013).
[25] F. Xu, M. Curty, B. Qi, and H.-K. Lo, New Journal of Physics **15**, 113007 (2013).
[26] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Nature Communications **5**, 3732 (2014).
[27] F. Xu, B. Qi, Z. Liao, and H.-K. Lo, Applied Physics Letters **103**, 061101 (2013).
[28] F. Xu, H. Xu, and H.-K. Lo, Physical Review A **89**, 052333 (2014).
[29] Y. Fu, H.-L. Yin, T.-Y. Chen, and Z.-B. Chen, Physics Review Letters **114**, 090501 (2015).
[30] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Physical Review Letters **111**, 130501 (2013).
[31] 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, Physical Review Letters **111**, 130502 (2013).
[32] T. Ferreira da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporão, and J. P. von der Weid, Physical Review A **88**, 052303 (2013).
[33] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, Physics Review Letters **112**, 190503 (2014).
[34] 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).
[35] 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).
[36] F. Xu, M. Curty, B. Qi, and H. Lo, IEEE Journal of Selected Topics in Quantum Electronics **21**, 6601111 (2015).
[37] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Physical Review Letters **81**, 5932 (1998).
[38] J. M. Arrazola and N. Lütkenhaus, Physical Review A **89**, 062305 (2014).
[39] F. Xu, J. M. Arrazola, *et al.*, arXiv preprint arXiv:1503.05499 (2015).
[40] V. Dunjko, E. Kashefi, and A. Leverrier, Physical Review Letters **108**, 200502 (2012).
[41] P. Gonzalez, L. Rebon, T. F. da Silva, M. Figueroa, C. Saavedra, M. Curty, G. Lima, G. Xavier, and W. Nogueira, arXiv preprint arXiv:1410.1422 (2014).
[42] C. C. W. Lim, B. Korzh, A. Martin, F. Bussieres, R. Thew, and H. Zbinden, Applied Physics Letters **105**, 221112 (2014).
[43] W.-F. Cao, Y.-Z. Zhen, Y.-L. Zheng, Z.-B. Chen, N.-L. Liu, K. Chen, and J.-W. Pan, arXiv preprint arXiv:1410.2928 (2014).
[44] W.-Y. Liang, M. Li, Z.-Q. Yin, W. Chen, S. Wang, X.-B. An, G.-C. Guo, and Z.-F. Han, arXiv preprint arXiv:1505.00897 (2015).
[45] B. Qi, Physical Review A **91**, 020303 (2015).
[46] Y.-S. Kim, Y. Choi, O. Kwon, S.-W. Han, and S. Moon, arXiv preprint arXiv:1501.03344 (2015).
[47] Y. Zhao, B. Qi, and H.-K. Lo, Physical Review A **77**, 052327 (2008).
[48] Y. Zhao, B. Qi, H.-K. Lo, and L. Qian, New Journal of Physics **12**, 023024 (2010).
[49] T. Chapuran, P. Toliver, N. Peters, J. Jackel, M. Goodman, R. Runser, S. McNown, N. Dallmann, R. Hughes, K. McCabe, *et al.*, New Journal of Physics **11**, 105001 (2009).
[50] Y. Zhao, B. Qi, and H.-K. Lo, Applied Physics Letters **90**, 044106 (2007).
[51] X. Peng, H. Jiang, B. Xu, X. Ma, and H. Guo, Optics Letters **33**, 2077 (2008).
[52] S. Sajeed, I. Radchenko, S. Kaiser, J.-P. Bourgoin, A. Pappa, L. Monat, M. Legré, and V. Makarov, Physical Review A **91**, 032326 (2015).
[53] Z. Zhang, M. Tengner, T. Zhong, F. N. Wong, and J. H. Shapiro, Physical Review Letters **111**, 010501 (2013).
[54] F. Xu, S. Sajeed, S. Kaiser, Z. Tang, L. Qian, V. Makarov, and H.-K. Lo, arXiv preprint arXiv:1408.3667 (2014).
[55] W. Hwang, Physical Review Letters **91**, 57901 (2003).
[56] H.-K. Lo, X. Ma, and K. Chen, Physical Review Letters **94**, 230504 (2005).
[57] X. Wang, Physical Review Letters **94**, 230503 (2005).
[58] A. Papoulis and S. U. Pillai, *Probability, random variables, and stochastic processes* (Tata McGraw-Hill Education, 2002).
[59] W. Hoeffding, Journal of the American statistical association **58**, 13 (1963).
[60] F. Marsili, V. Verma, J. Stern, S. Harrington, A. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. Shaw, R. Mirin, *et al.*, Nature Photonics **7**, 210 (2013).
[61] M. Lucamarini, I. Choi, M. B. Ward, J. F. Dynes, Z. Yuan, and A. J. Shields, arXiv preprint arXiv:1506.01989 (2015).