PAPER • OPEN ACCESS

Practical aspects of measurement-device-independent quantum key distribution

New Journal of Physics
The open access journal for physics

Practical aspects of measurement-device-independent quantum key distribution

Feihu Xu[1,4], Marcos Curty[2], Bing Qi[1,3] and Hoi-Kwong Lo[1]

[1] Centre for Quantum Information and Quantum Control, Department of Physics and Department of Electrical & Computer Engineering, University of Toronto, Toronto, ON M5S 3G4, Canada

[2] Escuela de Ingeniería de Telecomunicación, Department of Signal Theory and Communications, University of Vigo, Vigo, Pontevedra, E-36310, Spain

E-mail: feihu.xu@utoronto.ca

New Journal of Physics **15** (2013) 113007 (28pp)
Received 31 May 2013
Published 7 November 2013
Online at http://www.njp.org/
doi:10.1088/1367-2630/15/11/113007

Abstract. A novel protocol, measurement-device-independent quantum key distribution (MDI-QKD), removes all attacks from the detection system, the most vulnerable part in QKD implementations. In this paper, we present an analysis for practical aspects of MDI-QKD. To evaluate its performance, we study various error sources by developing a general system model. We find that MDI-QKD is highly practical and thus can be easily implemented with standard optical devices. Moreover, we present a simple analytical method with only two (general) decoy states for the finite decoy-state analysis. This method can be used directly by experimentalists to demonstrate MDI-QKD. By combining the system model with the finite decoy-state method, we present a general framework for the optimal choice of the intensities of the signal and decoy states. Furthermore, we consider a common situation, namely *asymmetric*

[3] Present address: Quantum Information Science Group, Computational Sciences and Engineering Division, Oak Ridge National Laboratory, Oak Ridge, TN 37831-6418, USA.

[4] Author to whom any correspondence should be addressed.

MDI-QKD, in which the two quantum channels have different transmittances. We investigate its properties and discuss how to optimize its performance. Our work is of interest not only to experiments demonstrating MDI-QKD but also to other non-QKD experiments involving quantum interference.

Contents

1. Introduction

Quantum key distribution (QKD) [1–3] enables an unconditionally secure means of distributing secret keys between two spatially separated parties, Alice and Bob. The security of QKD has been rigorously proven based on the laws of quantum mechanics [4]. Nevertheless, owing to the imperfections in real-life implementations, a large gap between its theory and practice remains unfilled. In particular, an eavesdropper (Eve) may exploit these imperfections and launch specific attacks. This is commonly called quantum hacking. The first successful quantum hacking against a commercial QKD system was the time-shift attack [5] based on a proposal in [6]. More recently, the phase-remapping attack [7] and the detector-control attack [8] have been implemented against various practical QKD systems. Also, other attacks have appeared in the literature [9]. These results suggest that quantum hacking is a major problem for the real-life security of QKD.

To close the gap between theory and practice, a natural attempt was to characterize the specific loophole and find a countermeasure. For instance, Yuan, Dynes and Shields proposed an efficient countermeasure against the detector-control attack [10]. Once an attack is known, the prevention is usually uncomplicated. However, unanticipated attacks are most dangerous, as it is impossible to fully characterize real devices and account for *all* loopholes. Hence, researchers moved to the second approach—(full) device-independent QKD [11]. It requires

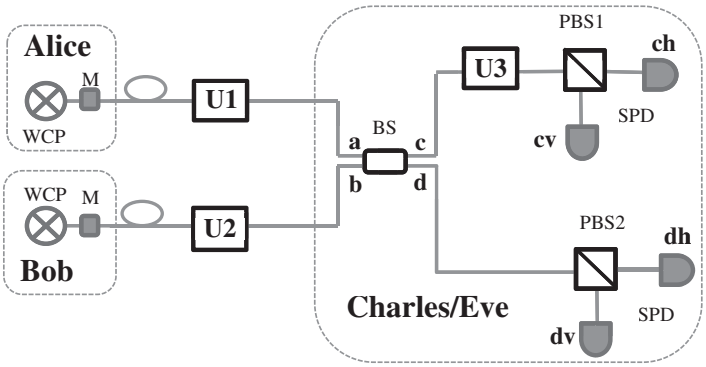

Figure 1. MDI-QKD system model. WCP, weak coherent pulse; M, polarization and intensity modulators; BS, beam splitter; PBS, polarization BS; SPD, single-photon detector. In MDI-QKD [14], each of Alice and Bob prepares BB84 states in combination with decoy states and sends them to an untrusted relay Charles (or Eve), who is supposed to perform a BSM. As an example, this figure considers a polarization-encoding scheme. Three unitary operators (U) are used to model the polarization misalignment (or rotation); PBS2 is defined as the fundamental measurement basis; U_1 (U_2) represents the polarization misalignment of Alice's (Bob's) channel transmission, while U_3 models the misalignment of the other measurement setting, PBS1. In the ideal case without any polarization misalignment, the rectilinear (Z) basis, used for key generation in equation (1), refers to the basis of PBS1 and PBS2.

no specification of the internal functionality of QKD devices and offers nearly perfect security. Its legitimate users (Alice and Bob) can be treated as a *quasi* black box by assuming no memory attacks [12]. Nevertheless, device-independent QKD is not really practical because it requires near-unity detection efficiency and generates an extremely low key rate [13]. Therefore, to our knowledge, there has been no experimental paper on device-independent QKD.

Fortunately, Lo *et al* [14] have recently proposed an innovative scheme—measurement-device-independent QKD (MDI-QKD)—that removes all detector side-channel attacks, the most important security loophole in conventional QKD implementations [5, 6, 8, 9]. As an example of a MDI-QKD scheme (see figure 1), each of Alice and Bob locally prepares phase-randomized signals (this phase randomization process can be realized using a quantum random number generator such as [15]) in the BB84 polarization states [1] and sends them to an *untrusted* quantum relay, Charles (or Eve). Charles is supposed to perform a Bell state measurement (BSM) and broadcast the measurement result. Since the measurement setting is only used to post-select entanglement (in an equivalent virtual protocol [14]) between Alice and Bob, it can be treated as a *true* black box. Hence, MDI-QKD is inherently immune to all attacks in the detection system. This is a major achievement as MDI-QKD allows legitimate users to not only perform secure quantum communications with untrusted relays[5] but also out-source the manufacturing of detectors to untrusted manufacturers.

[5] This also implies the feasibility of 'Pentagon using China satellite for US-Africa command'. See www.bloomberg.com/news/2013-04-29/pentagon-using-china-satellite-for-u-s-africa-command.html.

Conceptually, the key insight of MDI-QKD is *time reversal*. This is in the same spirit as one-way quantum computation [16]. More precisely, MDI-QKD built on the idea of a time-reversed Einstein–Podolsky–Rosen (EPR) protocol for QKD [17]. By combining the decoy-state method [18] with the time-reversed EPR protocol, MDI-QKD gives both good performance and good security.

MDI-QKD is highly practical and can be implemented with standard optical components. The source can be a non-perfect single-photon source (together with the decoy-state method), such as an attenuated laser diode emitting weak coherent pulses (WCPs), and the measurement setting can be a simple BSM realized by linear optics. Hence, MDI-QKD has attracted intensive interest in the QKD community. A number of follow-up theoretical works have already been reported in [19–25]. Meanwhile, experimental attempts on MDI-QKD have also been made by several groups [26–29]. Nonetheless, before it can be applied in real life, it is important to address a number of practical issues. These include:

(i) Modeling the errors: an implementation of MDI-QKD may involve various error sources such as the mode mismatch resulting in a non-perfect Hong–Ou–Mandel (HOM) interference [30]. Thus, the first question is: how will these errors affect the performance of MDI-QKD?[6] Or, what is the physical origin of the quantum bit error rate (QBER) in a practical implementation?

(ii) Finite decoy-state protocol and finite-key analysis: as mentioned before, owing to the lack of true single-photon sources [31], QKD implementations typically use laser diodes emitting WCPs [3] and single-photon contributions are estimated by the decoy-state protocol [18]. In addition, a real QKD experiment is completed in finite time, which means that the length of the output keys is finite. Thus, the estimation of relevant parameters suffers from statistical fluctuations. This is called the finite-key effect [32]. Hence, the second question is: how can one design a practical finite decoy-state protocol and perform a finite-key analysis in MDI-QKD?

(iii) Choice of intensities: an experimental implementation needs to know the optimal intensities for the signal and decoy states in order to optimize the system performance. Previously, [21, 22] have independently discussed the finite decoy-state protocol. However, the high computational cost of the numerical approach proposed in [21], together with the lack of a rigorous discussion of the finite-key effect in both [21, 22], makes the optimization of parameters difficult. Thus, the third question is: how can one obtain these optimal intensities?

(iv) Asymmetric MDI-QKD: as shown in figure 2, in real life, it is quite common that the two channels connecting Alice and Bob to Charles have different transmittances. We call this situation *asymmetric* MDI-QKD. Importantly, this asymmetric scenario appeared naturally in a recent proof-of-concept experiment [26], where a tailored length of fiber was intentionally added in the short arm to balance the two channel transmittances. Since an additional loss is introduced into the system, it is unclear whether this solution is optimal. Hence, the final question is: how can one optimize the performance of this asymmetric case?

[6] From the security aspect, one can in principle operate a MDI-QKD system without knowing the exact origin of the observed QBER. However, from the performance aspect, it is important to study the origin of the QBER in order to maximize the secure key rate.

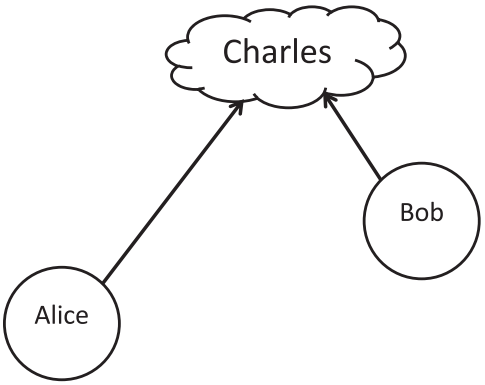

Figure 2. Asymmetric MDI-QKD. The two channels connecting Alice to Charles and Bob to Charles have *different* transmittances. In real-life MDI-QKD, asymmetry appeared naturally in a recent proof-of-concept experiment [26].

The second question has already been discussed in [21, 22, 24] and solved in [33]. In this paper, we offer additional discussions on this point and answer the other questions. Our contributions are summarized below.

(i) To better understand the physical origin of the QBER, we propose generic models for various error sources. In particular, we investigate two important error sources—polarization misalignment and mode mismatch. We find that in a polarization-encoding MDI-QKD system [14, 28, 29], polarization misalignment is the major source contributing to the QBER and mode mismatch (in the time or frequency domain), however, does not appear to be a major problem. These results are shown in section 3. Moreover, we provide a mathematical model to simulate a MDI-QKD system. This model is a useful tool for analyzing experimental results and performing the optimization of parameters. Although this model is proposed to study MDI-QKD, it is also useful for other non-QKD experiments involving quantum interference, such as entanglement swapping [34] and linear optics quantum computing [35]. This result is shown in appendix B.

(ii) A previous method to analyze MDI-QKD with a finite number of decoy states assumes that Alice and Bob can prepare a vacuum state [22]. Here, however, we present an analytical approach with two *general* decoy states, i.e. without the assumption of vacuum. This is particularly important for the practical implementations, as it is usually difficult to create a vacuum state in decoy-state QKD experiments [36, 37]. The different intensities are usually generated with an intensity modulator, which has a finite extinction ratio (e.g. around 30 dB). Additionally, we also simulate the expected key rates numerically and thus present an optimized method with two decoy states. Ignoring for the moment the finite-key effect, experimentalists can directly use this method to obtain a rough estimation of the system performance. Section 4 contains the main results for this point.

(iii) By combining the system model, the finite decoy-state protocol and the finite-key analysis of [33], we offer a general framework to determine the optimal intensities of the signal and decoy states. Notice that this framework has already been adopted and verified in the experimental demonstration reported in [29]. These results are shown in section 5.

(iv) Finally, we model and evaluate the performance of an *asymmetric* MDI-QKD system. This allows us to study its properties and determine the experimental configuration that maximizes its secret key rate. These results are shown in section 6.

2. Preliminary

The secure key rate of MDI-QKD in the asymptotic case (i.e. assuming an infinite number of decoy states and signals) is given by [14]

$$R \geqslant P_Z^{1,1} Y_Z^{1,1} [1 - H_2(e_X^{1,1})] - Q_Z f_e(E_Z) H_2(E_Z), \tag{1}$$

where $Y_Z^{1,1}$ and $e_X^{1,1}$ are, respectively, the yield (i.e. the probability that Charles declares a successful event) in the rectilinear (Z) basis and the error rate in the diagonal (X) basis given that both Alice and Bob send single-photon states ($P_Z^{1,1}$ denotes this probability in the Z basis); H_2 is the binary entropy function given by $H_2(x) = -x \log_2(x) - (1-x)\log_2(1-x)$; Q_Z and E_Z denote, respectively, the gain and QBER in the Z basis and $f_e \geqslant 1$ is the error correction inefficiency function. Here we use the Z basis for key generation and the X basis for testing only [38]. In practice, Q_Z and E_Z are directly measured in the experiment, while $Y_Z^{1,1}$ and $e_X^{1,1}$ can be estimated using the finite decoy-state method.

Next, we introduce some additional notations. We consider one signal state and two weak decoy states for the finite decoy-state protocol. The parameter μ is the intensity (i.e. the mean photon number per optical pulse) of the signal state[7]. ν and ω are the intensities of the two decoy states, which satisfy $\mu > \nu > \omega \geqslant 0$. The sets $\{\mu_a, \nu_a, \omega_a\}$ and $\{\mu_b, \nu_b, \omega_b\}$ contain, respectively, Alice's and Bob's intensities. The sets $\{\mu_a^{opt}, \nu_a^{opt}, \omega_a^{opt}\}$ and $\{\mu_b^{opt}, \nu_b^{opt}, \omega_b^{opt}\}$ denote the optimal intensities that maximize the key rate. L_{ac} and t_a (L_{bc} and t_b) denote the channel distance and transmittance from Alice (Bob) to Charles. In the case of a fiber-based system, $t_a = 10^{-\alpha L_{ac}/10}$ with α denoting the channel loss coefficient ($\alpha \approx 0.2\,\mathrm{dB\,km^{-1}}$ for a standard telecom fiber). η_d is the detector efficiency and Y_0 is the background rate that includes detector dark counts and other background contributions. The parameters e_d, e_t and e_m denote, respectively, the errors associated with the polarization misalignment, the time-jitter and the total mode mismatch (see definitions below).

3. Practical error sources

In this section, we consider the original MDI-QKD setting [14], i.e. the symmetric case with $t_a = t_b$. The asymmetric case will be discussed in section 6. To model the practical error sources, we focus on the fiber-based polarization-encoding MDI-QKD system proposed in [14] and demonstrated in [28, 29]. Notice, however, that with some modifications, our analysis can also be applied to other implementations such as free-space transmission, the phase-encoding scheme and the time-bin-encoding scheme. See also [20, 25], respectively, for models of phase-encoding and time-bin-encoding schemes.

A comprehensive list of practical error sources is as follows[8].

(i) Polarization misalignment (or rotation).

(ii) Mode mismatch including time-jitter, spectral mismatch and pulse-shape mismatch.

(iii) Fluctuations of the intensities (modulated by Alice and Bob) at the source.

[7] We assume that the coherent state is phase-randomized. Thus, its photon number follows a Poisson distribution of mean μ.

[8] This list does not consider the state-preparation error [19, 22], because a strict discussion about this problem is related to the security proof of MDI-QKD, which will be considered in future publications.

(iv) Background rate.

(v) Asymmetry of the beam splitter (BS).

Here, we primarily analyze the first two error sources, i.e. polarization misalignment and mode mismatch. The other error sources present minor contributions to the QBER in practice, and are discussed in appendix A.

3.1. Polarization misalignment

Polarization misalignment (or rotation) is one of the most significant factors contributing to the QBER in not only the polarization-encoding BB84 system [1] but also the polarization-encoding MDI-QKD system. Since MDI-QKD requires two transmitting channels and one BSM (instead of one channel and a simple measurement as in the BB84 protocol), it is cumbersome to model its polarization misalignment. Here, we solve this problem by proposing a simple model in figure 1. One of the polarization BSs (PBSs) (PBS2 in figure 1) is defined as the fundamental measurement basis[9]. Three unitary operators, $\{U_1, U_2, U_3\}$, are considered to model the polarization misalignment of each channel [35]. The operator U_1 (U_2) represents the misalignment of Alice's (Bob's) channel transmission, while U_3 models the misalignment of the other measurement setting, PBS1.

For simplicity, we consider a simplified model with a two-dimensional unitary matrix[10] (see section I.A. of [35])

$$U_k = \begin{pmatrix} \cos\theta_k & -\sin\theta_k \\ \sin\theta_k & \cos\theta_k \end{pmatrix}, \tag{2}$$

where $k = 1, 2, 3$ and θ_k (polarization-rotation angle) is in the range of $[-\pi,\pi]$. For each value of k, we define the polarization misalignment error $e_k = \sin^2\theta_k$ and the total error $e_{\mathrm{d}} = \sum_{k=1}^{3} e_k$. Note that e_{d} is equivalent to the systematic QBER in a polarization-encoding BB84 system.

From the model of figure 1, we can analyze the effect of polarization misalignment by evaluating the secure key rate given by equation (1). See appendix B for details. By using the practical parameters listed in table 1, we perform a numerical simulation of the asymptotic key rates for different values of polarization misalignment, e_{d}. The result is shown in figure 3. In this simulation, we temporarily ignore mode mismatch (i.e., set $e_{\mathrm{m}} = 0$ in table 1) and make two practical assumptions for the polarization misalignment: (a) each polarization-rotation angle, θ_k, follows a *Gaussian* distribution with a standard deviation of $\theta_k^{\mathrm{std}} = \arcsin(\sqrt{e_k})$; and (b) the probability distribution of e_k is selected as $e_1 = e_2 = 0.475e_{\mathrm{d}}$ and $e_3 = 0.05e_{\mathrm{d}}$.[11] Figure 3 shows

[9] Although we use PBS2 as the reference basis, the method is also applicable to other reference bases such as PBS1.

[10] That is, if we denote the two incoming modes in the horizontal and vertical polarization by the creation operators $a_h^\dagger$ and $a_v^\dagger$, and the outgoing modes by $b_h^\dagger$ and $b_v^\dagger$, then the unitary operator yields an evolution of the form $b_h^\dagger = \cos\theta_k a_h^\dagger - \sin\theta_k a_v^\dagger$ and $b_v^\dagger = \sin\theta_k a_h^\dagger + \cos\theta_k a_v^\dagger$. This unitary matrix is a simple form rather than the general one (see section I.A in [35]). Nonetheless, we believe that the result for a more general unitary transformation will be similar to our simulation results.

[11] Two remarks for the distribution of the three unitary operators: (a) we assume that the two channel transmissions, i.e. U_1 and U_2, introduce much larger polarization misalignments than the other measurement basis, U_3 (PBS1 in figure 1), because PBS1 is located in Charles's local station and can be carefully aligned (in principle). Hence, we choose $e_1 = e_2 = 0.475e_{\mathrm{d}}$ and $e_3 = 0.05e_{\mathrm{d}}$. (b) Notice that the simulation result is more or less *independent* of the distribution of e_k.

Table 1. List of practical parameters for all numerical simulations. These experimental parameters, including the detection efficiency η_d, the total misalignment error e_d and the background rate Y_0, are from the 144 km QKD experiment reported in [39]. Since two SPDs are used in [39], the background rate of each SPD here is roughly half of the value there. We assume that the four SPDs in MDI-QKD (see figure 1) have identical η_d and Y_0. The parameter e_m is the total mode mismatch that is quantified from the experimental values of Tang *et al* [29].

η_d	e_d	Y_0	f_e	e_m
14.5%	1.5%	6.02×10^{-6}	1.16	2%

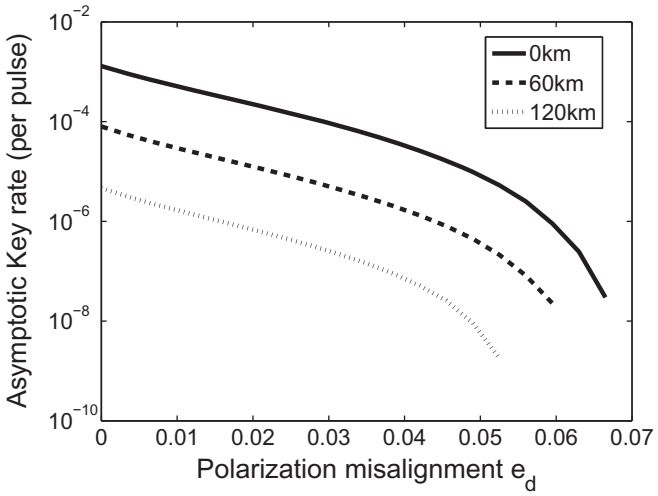

Figure 3. Polarization misalignment tolerance. Following the model illustrated in figure 1, we incorporate the polarization misalignment into the derivation of the asymptotic key rate given by equation (1). We find that MDI-QKD is robust against practical errors due to polarization misalignment.

that a polarization-encoding system can tolerate up to about 6.7% polarization misalignment at 0 km, while at 120 km it can only tolerate up to 5% misalignment. It also shows that MDI-QKD is moderately robust to errors due to polarization misalignment.

3.2. Mode mismatch

We primarily use the model of mode mismatch in time domain, called time-jitter[12] , to discuss our method. This model is shown in figure 4. We describe Alice's and Bob's quantum states in the time domain as

$$\begin{aligned} \text{Alice} &: |\phi_a\rangle = |T_a\rangle \\ \text{Bob} &: |\phi_b\rangle = \alpha|T_a\rangle + \beta|\overline{T_a}\rangle, \end{aligned} \tag{3}$$

[12] Time-jitter is the variance in arrival times of Alice's and Bob's packets at Charles's station.

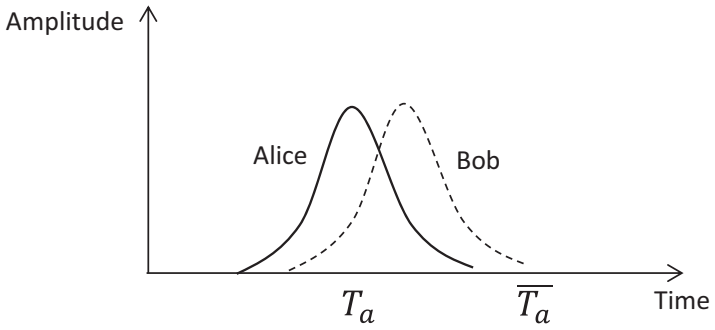

Figure 4. Model for mode mismatch in the time domain (time-jitter). Alice's state is defined as the reference basis, while Bob's state is a superposition of Alice's fundamental mode $|T_a\rangle$ and the orthogonal mode $|\overline{T_a}\rangle$ (see equation (3)).

where $|\overline{T_a}\rangle$ is the orthogonal time mode of $|T_a\rangle$, $\beta = \sqrt{e_t}$, $\alpha = \sqrt{1-e_t}$, and e_t is defined as the time-jitter that represents the probability of Alice's state not overlapping with that of Bob[13].

This model is a very general method that can be used to study the mode mismatch problem in other domains for a variety of quantum optics experiments involving quantum interference. For instance, a similar discussion can be applied to the spectral (wavelength) mismatch if we write equation (3) in the frequency domain. One can also refer to [40] for a general discussion about the spectral mismatch. Considering equation (3) in the form of Alice's and Bob's pulse shapes, we can also analyze the pulse-shape mismatch. Here we define the *total* mode mismatch in all domains as e_m.

Next, let us discuss how e_m affects the key rate given by equation (1). As illustrated in figure 1, the overlapping modes between Alice's and Bob's pulses experience a HOM interference at the BS, while the non-overlapping modes transmit through the BS without interference. Assuming that $\eta_d \gg Y_0$ and ignoring the polarization misalignment for the moment, we find that the mode mismatch *only* affects the gains and the error rates in the X basis rather than those in the Z basis[14]. Hence, in equation (1), e_m mainly affects $e_X^{1,1}$. In practice, $e_X^{1,1}$ can be estimated from the finite decoy-state protocol, i.e. from the gains (Q_X) and QBERs (E_X) in the X basis. Similar to the analysis of the polarization misalignment in section 3.1, we can incorporate e_m into the derivations of Q_X and E_X following the method of appendix B.[15]

Using the parameters of table 1, we simulate the asymptotic key rates for different values of e_m. The results are shown in figure 5. In this simulation, we temporarily ignore polarization misalignment (i.e. we set $e_d = 0$) and only focus on mode mismatch. At 0 km, we find that the system can tolerate up to 80% mode mismatch and at 120 km, the tolerable value is about 50%.

[13] In experiment, the value of e_t can be quantified from the fidelity between the two pulses in time domain. This fidelity can be obtained by measuring the pulse width and the time-jitter value between the two pulses. From the experimental values of [29], e_t is below 1.5%.

[14] Suppose both Alice and Bob encode their optical pulses in the same mode of horizontal polarization in the Z basis. Ignoring the polarization misalignment, the interference result will *only* generate a click on the horizontal detectors rather than create coincident detections. This holds both for the cases of perfect interference ($e_m = 0$) and non-interference ($e_m = 1$). Thus, $e_m = 1$ does not increase the QBER in the Z basis.

[15] In the derivation of Q_X and E_X with mode mismatch, the non-overlapping modes can be essentially treated as background counts increasing the background count rate of each detector. The final result is a summation over the overlapping and non-overlapping modes.

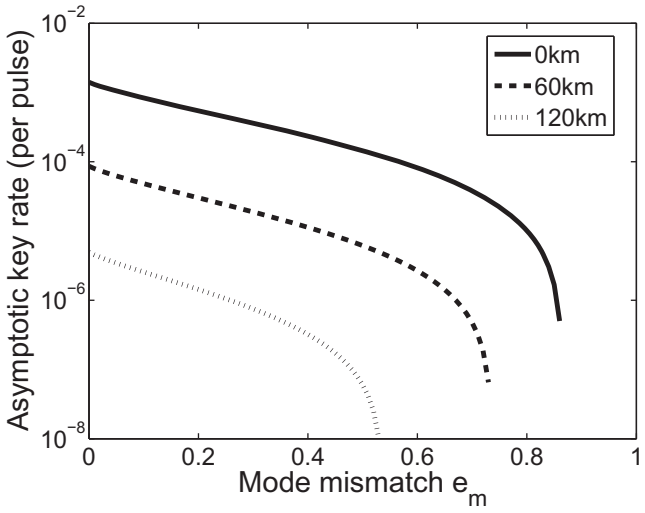

Figure 5. Mode mismatch tolerance. In the asymptotic case, a polarization-encoding MDI-QKD system can tolerate up to 80% mode mismatch at 0 km. Mode mismatch does not appear to be a major problem in a polarization-encoding implementation of MDI-QKD.

Hence, a polarization-encoding MDI-QKD system is *less* sensitive to mode mismatch than to polarization misalignment[16]. Notice also that we have quantified the value of e_{m} (see table 1) by using the experimental parameters from [29] and find that e_{m} is usually small in practice (e.g. below 5%). Therefore, mode mismatch does not appear to be a major problem in a MDI-QKD implementation.

4. Finite decoy-state protocol with two general decoy states

In a MDI-QKD implementation, by performing the measurements for the different intensities used by Alice and Bob, we can obtain [14]

$$Q_Z^{q_{\mathrm{a}}q_{\mathrm{b}}} = \sum_{n,m=0} \mathrm{e}^{-(q_{\mathrm{a}}+q_{\mathrm{b}})} \frac{q_{\mathrm{a}}^n}{n!} \frac{q_{\mathrm{b}}^m}{m!} Y_Z^{n,m}, \tag{4}$$

$$Q_X^{q_{\mathrm{a}}q_{\mathrm{b}}} E_X^{q_{\mathrm{a}}q_{\mathrm{b}}} = \sum_{n,m=0} \mathrm{e}^{-(q_{\mathrm{a}}+q_{\mathrm{b}})} \frac{q_{\mathrm{a}}^n}{n!} \frac{q_{\mathrm{b}}^m}{m!} Y_X^{n,m} e_X^{n,m}, \tag{5}$$

where q_{a} (q_{b}) denotes Alice's (Bob's) intensity setting, $Q_Z^{q_{\mathrm{a}}q_{\mathrm{b}}}$ ($E_X^{q_{\mathrm{a}},q_{\mathrm{b}}}$) denotes the gain (QBER) in the Z (X) basis with the intensity pair $\{q_{\mathrm{a}}, q_{\mathrm{b}}\}$, and $Y_Z^{n,m}$ ($e_X^{n,m}$) denotes the yield (error rate) given that Alice and Bob send respectively an n-photon and m-photon pulse. Here the goal of the finite decoy-state protocol is to estimate $Y_Z^{1,1}$ and $e_X^{1,1}$ (used to generate a secure key) from

[16] Note however that in a time-bin-encoding system [26, 27], the mode mismatch such as time-jitter might be more important than the polarization misalignment.

Table 2. Analytical equations for the two decoy-state protocol. See the main text for details. Here, for the estimation of $Y_{Z,L}^{1,1}$, we only consider one case and refer to equation (7) for the other case. Ignoring the finite-key effect, these results can be directly used by experimentalists to obtain an estimation of the expected system performance.

$Y_{Z,L}^{1,1} \geqslant \frac{1}{(\mu_a-\omega_a)(\mu_b-\omega_b)(\nu_a-\omega_a)(\nu_b-\omega_b)(\mu_a-\nu_a)} \times$ $[(\mu_a^2-\omega_a^2)(\mu_b-\omega_b)(Q_Z^{\nu_a\nu_b}e^{(\nu_a+\nu_b)}+Q_Z^{\omega_a\omega_b}e^{(\omega_a+\omega_b)}-Q_Z^{\nu_a\omega_b}e^{(\nu_a+\omega_b)}-Q_Z^{\omega_a\nu_b}e^{(\omega_a+\nu_b)})-$ $(\nu_a^2-\omega_a^2)(\nu_b-\omega_b)(Q_Z^{\mu_a\mu_b}e^{\mu_a+\mu_b}+Q_Z^{\omega_a\omega_b}e^{(\omega_a+\omega_b)}-Q_Z^{\mu_a\omega_b}e^{(\mu_a+\omega_b)}-Q_Z^{\omega_a\mu_b}e^{(\omega_a+\mu_b)}]$
$e_{X,U}^{1,1} \geqslant \frac{1}{(\nu_a-\omega_a)(\nu_b-\omega_b)Y_{X,L}^{1,1}} \times$ $[e^{(\nu_a+\nu_b)}Q_X^{\nu_a\nu_b}E_X^{\nu_a\nu_b}+e^{(\omega_a+\omega_b)}Q_X^{\omega_a\omega_b}E_X^{\omega_a\omega_b}-e^{(\nu_a+\omega_b)}Q_X^{\nu_a\omega_b}E_X^{\nu_a\omega_b}-e^{(\omega_a+\nu_b)}Q_X^{\omega_a\nu_b}E^{\omega_a\nu_b}]$

the set of linear equations given by equations (4) and (5) using different intensity settings[17]. More specifically, we estimate a lower bound for $Y_Z^{1,1}$ and an upper bound for $e_X^{1,1}$. We denote these two bounds, respectively, as $Y_{Z,L}^{1,1}$ and $e_{X,U}^{1,1}$.

The general approach for the finite decoy-state protocol has been discussed in [33]. In this section, however, we present a much simpler analytical method with only two decoy states. The final results are summarized in table 2. They can be directly used by experimentalists (without knowing the details of Curty *et al* [33]) to obtain a rough estimation of the expected system performance. Notice that our notations are different from [33] in that we primarily estimate the probabilities in the case of an infinite number of signals, while [33] focuses on the estimation of counts by incorporating the finite-key effect.

Now, let us start to discuss this two decoy-state protocol. As mentioned before, the intensities of the signal and decoy states satisfy $\mu > \nu > \omega$ and our protocol is applicable to either $\omega = 0$ or $\omega \neq 0$. The key method to estimate $Y_{Z,L}^{1,1}$ from equation (4) can be divided into two steps:

(i) Cancel out the terms Y_Z^{0m} and Y_Z^{n0} using Gaussian elimination.
(ii) Cancel out either the term Y_Z^{12} or Y_Z^{21} depending on the intensity values selected in the first step.

For the first step, we choose intensity pairs from $\{\mu_a, \omega_a, \mu_b, \omega_b\}$ and $\{\nu_a, \omega_a, \nu_b, \omega_b\}$,[18] and generate two quantities Q_Z^{M1} and Q_Z^{M2} given by

$$Q_Z^{M1} = Q_Z^{\nu_a\nu_b}e^{(\nu_a+\nu_b)} + Q_Z^{\omega_a\omega_b}e^{(\omega_a+\omega_b)} - Q_Z^{\nu_a\omega_b}e^{(\nu_a+\omega_b)} - Q_Z^{\omega_a\nu_b}e^{(\omega_a+\nu_b)},$$

$$Q_Z^{M2} = Q_Z^{\mu_a\mu_b}e^{(\mu_a+\mu_b)} + Q_Z^{\omega_a\omega_b}e^{(\omega_a+\omega_b)} - Q_Z^{\mu_a\omega_b}e^{(\mu_a+\omega_b)} - Q_Z^{\omega_a\mu_b}e^{(\omega_a+\mu_b)}.$$

[17] For one signal state and two decoy states ($q_a \in \{\mu_a, \nu_a, \omega_a\}$ and $q_b \in \{\mu_b, \nu_b, \omega_b\}$), $Y_Z^{1,1}$ and $e_X^{1,1}$ can be estimated from the linear equations for nine intensity pairs.

[18] According to Curty *et al* [33], it is also possible for other two combinations of intensities: (i) choosing intensity pairs from $\{\mu_a, \nu_a, \mu_b, \nu_b\}$ and $\{\nu_a, \omega_a, \nu_b, \omega_b\}$, substituting ω with ν for Q_Z^{M2} in equation (6) and then performing similar calculations; (ii) choosing intensity pairs from $\{\mu_a, \nu_a, \mu_b, \nu_b\}$ and $\{\mu_a, \omega_a, \mu_b, \omega_b\}$, substituting ω with ν for Q_Z^{M2} and substituting ν with μ for Q_Z^{M1} in equation (6) and performing similar calculations. Here we numerically found that the optimal intensity choice is to choose from $\{\mu_a, \omega_a, \mu_b, \omega_b\}$ and $\{\nu_a, \omega_a, \nu_b, \omega_b\}$.

To cancel out Y_Z^{12} or Y_Z^{21}, we consider two cases.

Case 1. $\left(\frac{\mu_a+\omega_a}{\nu_a+\omega_a}\right) \leqslant \frac{\mu_b+\omega_b}{\nu_b+\omega_b}$ we use $(\mu_b^2-\omega_b^2)(\mu_a-\omega_a)\times Q_Z^{M1}-(\nu_b^2-\omega_b^2)(\nu_a-\omega_a)\times Q_Z^{M2}$ to cancel out Y_Z^{12}. Thus, $Y_{Z,L}^{1,1}$ is given by

$$\frac{(\mu_a^2-\omega_a^2)(\mu_b-\omega_b)Q_Z^{M1}-(\nu_a^2-\omega_a^2)(\nu_b-\omega_b)Q_Z^{M2}}{(\mu_a-\omega_a)(\mu_b-\omega_b)(\nu_a-\omega_a)(\nu_b-\omega_b)(\mu_a-\nu_a)}. \tag{6}$$

Case 2. $(\frac{\mu_a+\omega_a}{\nu_a+\omega_a} > \frac{\mu_b+\omega_b}{\nu_b+\omega_b})$ we cancel out Y_Z^{21} using the same method as in case 1 and derive $Y_{Z,L}^{1,1}$ as

$$\frac{(\mu_b^2-\omega_b^2)(\mu_a-\omega_a)Q_Z^{M1}-(\nu_b^2-\omega_b^2)(\nu_a-\omega_a)Q_Z^{M2}}{(\mu_a-\omega_a)(\mu_b-\omega_b)(\nu_a-\omega_a)(\nu_b-\omega_b)(\mu_b-\nu_b)}. \tag{7}$$

Similarly, the strategy to estimate $e_{X,U}^{1,1}$ from equation (5) requires to cancel out $Y_X^{0,m}e_X^{0,m}$ and $Y_X^{n,0}e_X^{n,0}$. Thus, we choose intensity pairs from $\{\nu_a, \omega_a, \nu_b, \omega_b\}$ [19] and derive $e_{X,U}^{1,1}$ as

$$\frac{1}{(\nu_a-\omega_a)(\nu_b-\omega_b)Y_{X,L}^{1,1}}[e^{(\nu_a+\nu_b)}Q_X^{\nu_a\nu_b}E_X^{\nu_a\nu_b}+e^{(\omega_a+\omega_b)}Q_X^{\omega_a\omega_b}E_X^{\omega_a\omega_b}$$

$$-e^{(\nu_a+\omega_b)}Q_X^{\nu_a\omega_b}E_X^{\nu_a\omega_b}e^{(\omega_a+\nu_b)}Q_X^{\omega_a\nu_b}E^{\omega_a\nu_b}],$$

where $Y_{X,L}^{1,1}$ can be estimated using a similar method to that for $Y_{Z,L}^{1,1}$.[20] The final equations are summarized in table 2.

5. Optimal choice of intensities

In this section, we develop a general framework to choose the optimal intensity values for the signal and decoy states. This framework is shown in figure 6, and is composed of four steps.

(i) Quantify the parameters and errors of the system. For simulation purposes, we will consider the parameters shown in table 1.

(ii) Model the system using the techniques presented in section 3. A complete model for a polarization-encoding MDI-QKD can be found in appendix B.

(iii) Implement the finite decoy-state protocol. For this, we will consider the analytical method with two decoy states introduced in section 4. In the simulation, for the weakest decoy state ω, we set its minimum value at 5×10^{-4} (per pulse)[21].

(iv) Apply the finite-key analysis. Here, we employ the rigorous finite-key analysis of [33] and consider a total number of signals $N=10^{14}$ [22] together with a security bound of $\epsilon=10^{-10}$.

[19] Similar to the estimation of Y_{ZL}^{11} according to Curty *et al* [33], it is also possible for other two combinations, i.e. $\{\mu_a, \nu_a, \mu_b, \nu_b\}$ or $\{\mu_a, \omega_a, \mu_b, \omega_b\}$. We numerically found that the optimal choice is to choose from $\{\nu_a, \omega_a, \nu_b, \omega_b\}$.

[20] In theory $Y_X^{11}=Y_Z^{11}$. Thus we can decide to implement the standard decoy-state method only in the Z basis and estimate Y_X^{11} from Y_Z^{11} while in the X basis we only implement the decoy states instead of the signal state. The advantage of such an implementation is to increase the key rate. See also [22] for a similar discussion.

[21] We assume that the intensity of the signal state is about 0.5 and the maximum extinction ratio of a practical intensity modulator is around 30 dB [36, 37]. Thus, the lowest intensity that can be modulated is 5×10^{-4}.

[22] The number of signals in the X (or Z) basis and the distribution of the signals over the signal and decoy states are both optimized numerically to maximize the key rate.

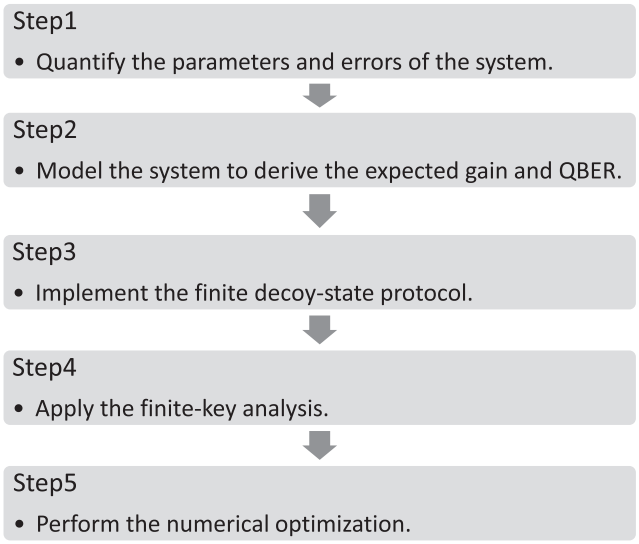

Figure 6. Framework to choose the optimal intensities. Step 1 is to quantify the parameters and errors of the system (see table 1 for some representative values). Step 2 is to model the system, i.e. derive the gain and QBER by incorporating the practical error sources (see appendix B for the case of a polarization based system). Step 3 is to implement the finite decoy-state protocol (see section 4). Step 4 is to apply the finite-key analysis [33]. Step 5 is to perform the numerical optimization to get the optimal intensities as well as other parameters such as the optimal selection for the probabilities of different intensity settings.

(v) Perform the numerical optimization. In our simulation, we use a MATLAB program to maximize the secure key rate and thus obtain the optimal parameters under different channel transmittances.

Based on this framework, the optimal intensities that maximize the key rate at different transmission distances are shown in figure 7. Notice also that our approach has already been applied to the experimental demonstration reported in [29], where the polarization misalignment is around 0.7% and the total mode mismatch is below 2%. Owing to the low operation rate there, the value of ω is set to 0.01. The optimal intensities in this scenario are $\mu_a^{opt} = \mu_b^{opt} \approx 0.3$ and $\nu_a^{opt} = \nu_b^{opt} \approx 0.1$.

6. Asymmetric measurement-device-independent quantum key distribution (MDI-QKD)

A schematic diagram of the asymmetric MDI-QKD is shown in figure 2. Note that this asymmetric scenario appeared naturally in a recent field-test experiment performed in Calgary [26]. Another concrete illustration can be found at the Tokyo QKD network [41], in which the asymmetric case occurs if Koganei-1 (Alice) and Koganei-3 (Bob) use Koganei-2 (Charles) as the quantum relay to perform MDI-QKD, where the two fiber links are, respectively, 90 and 1 km. Here we define a parameter x to quantify the ratio of the two channel transmittances, i.e. $x = t_a/t_b$. In the Calgary's system, $x = 0.752$, while in the Tokyo QKD network $x = 0.017$.

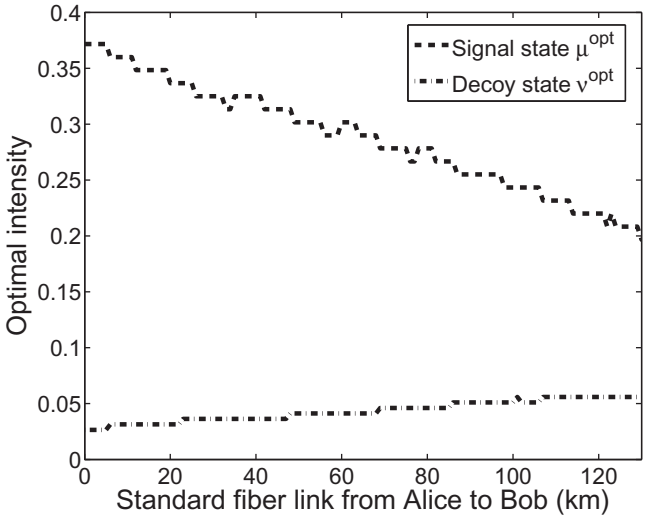

Figure 7. Optimal intensities. These intensity values are obtained by numerically maximizing the key rate in the finite-key case. They correspond to the situation where $\mu_a^{opt} = \mu_b^{opt} = \mu^{opt}$ and $\nu_a^{opt} = \nu_b^{opt} = \nu^{opt}$. The other decoy state ω is optimized at its minimum value, i.e. $\omega_a^{opt} = \omega_b^{opt} = 5 \times 10^{-4}$. Here we use the method described in section 4 for the finite decoy-state protocol and that of Curty *et al* [33] for the finite-key analysis. For this, we consider a total number of signals $N = 10^{14}$ together with a security bound of $\epsilon = 10^{-10}$. The non-smooth behaviors in the figure are mainly due to the lack of numerical accuracy.

6.1. Problem identification

The main question here is how to choose the optimal intensities in this asymmetric situation. In the asymptotic case, these optimal intensities refer to the two signal states μ_a^{opt} and μ_b^{opt}. Let us discuss two possible options.

The first option is to choose $\mu_a^{opt} = \mu_b^{opt}$ with both in $O(1)$. If we ignore the system imperfections such as background counts and other practical errors, the error rates ($e_X^{1,1}$ and E_Z in equation (1)) will be zero, while $P_Z^{1,1} Y_Z^{1,1}$ can be maximized with $\mu_a^{opt} = \mu_b^{opt} = 1$ (see appendix B.1 for the details). However, in practice, it is inevitable to have some practical errors such as the polarization misalignment discussed above. A relatively large intensity in the short channel will significantly increase the QBER due to the misalignment. Moreover, owing to the intensity mismatch on Charles's side ($\mu_a^{opt} t_a \neq \mu_b^{opt} t_b$), the quantum interference known as the HOM dip, will be imperfect. As a consequence, this option leads to a relatively large QBER, which decreases the key rate due to the cost of error correction.

To minimize the QBER, a second option is to choose $\mu_a^{opt} t_a = \mu_b^{opt} t_b$ regardless of x. We denote this situation as the *symmetric choice* (indicated by symmetry in figure 8 and table 3). An equivalent implementation scheme for this option is to add a tailored length of fiber in the local station of the sender with the short channel transmission (i.e. Bob in figure 2) in order to balance the two channel transmittances. In fact, such a scheme was recently implemented in a proof-of-principle MDI-QKD experiment [26]. However, when x is far from 1, to satisfy $\mu_a t_a = \mu_b t_b$, either μ_a or μ_b needs to be relatively small. Hence, we cannot derive good bounds for $P_Z^{1,1} Y_Z^{1,1}$ and $e_X^{1,1}$. In particular, the increase of $e_X^{1,1}$ results in the decrease of the key rate due to the cost of privacy amplification.

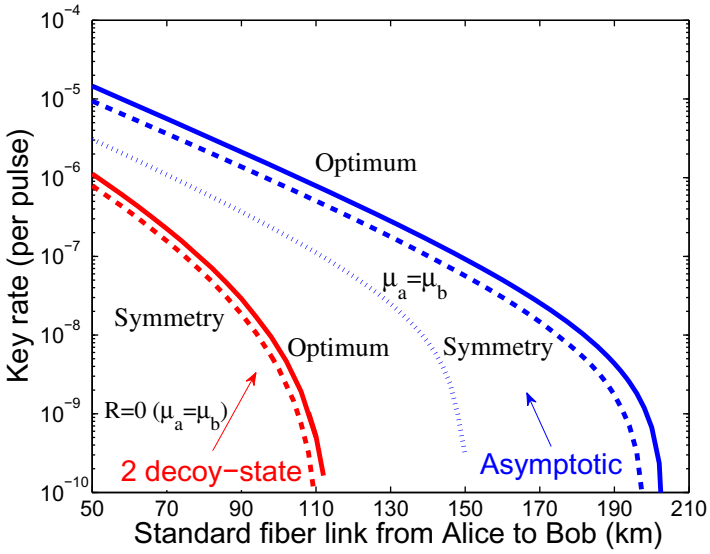

Figure 8. Key rate comparison with 50 km channel mismatch. We assume a fixed channel mismatch, $x = 0.1$ (L_{ac}–$L_{bc} = 50$ km). In the symmetric choice (symmetry in figure), we set $\mu_a t_a = \mu_b t_b$, while in the optimal choice (optimum in figure), we non-trivially determine the optimal intensities by numerical simulation. The red curves are evaluated by the two decoy-state protocol (section 4) combined with the finite-key analysis of Curty *et al* [33]. Note that in each curve, all the intensities of the signal and decoy states are optimized by maximizing the key rate. On average, the key rate with the optimal choice is around 80% larger than that with the symmetric choice in both asymptotic and two decoy-state cases.

Table 3. Optimal intensities of an asymmetric MDI-QKD system. The channel mismatch is fixed at $x = 0.1$ and thus $L_{ac} = \{50, 60, 70\,\text{km}\}$. In the asymptotic case, the ratio μ_a^{opt}/μ_b^{opt} for the optimal choice is around 4. In the symmetric choice, this ratio is 10. The parameters μ_a^{opt} and μ_b^{opt} are fixed regardless of t_a and t_b (see theorem 1 in appendix C.1). In the two decoy-state case (with different L_{bc}), the optimal intensities for the decoy state ν are about $\{\nu_a = 0.10, \nu_b = 0.01\}$ for the symmetric choice and $\{\nu_a^{opt} = 0.07, \nu_b^{opt} = 0.01\}$ for the optimal choice. The optimal value for the weakest decoy state is $\omega_a^{opt} = \omega_b^{opt} = 5 \times 10^{-4}$ for both choices. From the intensity values in this table, we find that the optimal choice for μ_a and μ_b does not always satisfy $\mu_a^{opt} t_a = \mu_b^{opt} t_b$, but the ratio $\mu_a^{opt} t_a / \mu_b^{opt} t_b$ is near 1. Also, in the asymptotic case, μ_a^{opt} and μ_b^{opt} are *only* determined by x instead of t_a or t_b.

	Asymptotic case				Two decoy-state case			
Parameters	Symmetry		Optimum		Symmetry		Optimum	
$x = 0.1$	μ_a	μ_b	μ_a^{opt}	μ_b^{opt}	μ_a	μ_b	μ_a^{opt}	μ_b^{opt}
$L_{bc} = 0$ km	0.75	0.08	0.60	0.15	0.49	0.05	0.46	0.08
$L_{bc} = 10$ km	0.75	0.08	0.60	0.15	0.46	0.05	0.41	0.07
$L_{bc} = 20$ km	0.75	0.08	0.60	0.15	0.41	0.03	0.38	0.06

In summary, we find that both of the above two options are sub-optimal. We present the optimal choice below.

6.2. *Summary of results*

The *optimal choice* (indicated by optimum in figure 8 and table 3) that maximizes the key rate can be determined from numerical optimizations. Here we perform such optimizations and also analyze the properties of asymmetric MDI-QKD. Our main results are:

(i) In the asymptotic case, the optimal choice for μ_a and μ_b does not always satisfy $\mu_a^{opt} t_a = \mu_b^{opt} t_b$, but the ratio $\mu_a^{opt} t_a / \mu_b^{opt} t_b$ is near 1. For $x < 1$, $\mu_a^{opt} t_a / \mu_b^{opt} t_b \in [0.3, 1)$; for $x \geqslant 1$, $\mu_a^{opt} t_a / \mu_b^{opt} t_b \in [1, 3.5]$; this result can be seen from figure C.2). In the practical case with the two decoy-state protocol and finite-key analysis, $\{\mu_a^{opt}, \mu_b^{opt}\}$ and $\{\nu_a^{opt}, \nu_b^{opt}\}$ satisfy a similar condition with the ratio $\mu_a^{opt} t_a / \mu_b^{opt} t_b$ (or $\nu_a^{opt} t_a / \nu_b^{opt} t_b$) near 1, while $\{\omega_a^{opt}, \omega_b^{opt}\}$ are optimized at their smallest value. See table 3 for further details.

(ii) In an asymmetric system with $x = 0.1$ (50 km length difference for two standard fiber links), the advantage of the optimal choice is shown in figure 8, where the key rate with the optimal choice is around 80% larger than that with the symmetric choice in both asymptotic and practical cases[23]. We remark that when x is far from 1, this advantage is more significant. For instance, with $x = 0.01$ (100 km length difference), the key rate with the optimal choice is about 150% larger than that with the symmetric choice.

(iii) In the asymptotic case, at a short distance where background counts can be ignored: μ_a^{opt} and μ_b^{opt} are *only* determined by x instead of t_a or t_b (see the optimal intensities in table 3 and theorem 1 in appendix C); assuming a fixed x, μ_a^{opt} and μ_b^{opt} can be analytically derived and the optimal key rate is quadratically proportional to t_b (see appendix C).

Finally, notice that the channel transmittance ratio in Calgary's asymmetric system is near 1 ($x = 0.752$), hence the optimal choice can slightly improve the key rate compared to the symmetric choice (around 2% improvement). However, in Tokyo's asymmetric system ($x = 0.017$), the optimal choice can significantly improve the key rate by over 130%.

7. Discussion and conclusion

A key assumption in MDI-QKD [14] is that Alice and Bob trust their devices for the state preparation, i.e. they can generate ideal quantum states in the BB84 protocol. One approach to remove this assumption is to quantify the imperfections in the state preparation part and thus include them into the security proofs [19]. We believe that this assumption is practical because Alice's and Bob's quantum states are prepared by themselves and thus can be experimentally verified in a fully protected laboratory environment outside of Eve's interference. For instance, based on an earlier proposal [42], Lim *et al* [43] have introduced another interesting scheme in which each of Alice and Bob uses an entangled photon source (instead of WCPs) and quantifies the state-preparation imperfections via random sampling. That is, Alice and Bob randomly

[23] In more general cases with different numbers of signals N, we also find that the optimal choice is around 80% larger than the symmetric choice.

sample parts of their prepared states and perform a local Bell test on these samples. Such a scheme is very promising, as it is in principle a fully device-independent approach. It can be applied in short-distance communications.

In conclusion, we have presented an analysis for practical aspects of MDI-QKD. To understand the physical origin of the QBER, we have investigated various practical error sources by developing a general system model. In a polarization-encoding MDI-QKD system, polarization misalignment is the major source contributing to the QBER. Hence, in practice, an efficient polarization management scheme such as polarization feedback control [28, 44] can significantly improve the polarization stabilization and thus generate a higher key rate. We have also discussed a simple analytical method for the finite decoy-state analysis, which can be directly used by experimentalists to demonstrate MDI-QKD. In addition, by combining the system model with the finite decoy-state method, we have presented a general framework for the optimal intensities of the signal and decoy states. Furthermore, we have studied the properties of the asymmetric MDI-QKD protocol and discussed how to optimize its performance. Our work is relevant to both QKD and general experiments on quantum interference.

Acknowledgments

We thank W Cui, S Gao, L Qian for enlightening discussions and V Burenkov, Z Liao, P Roztocki for comments on the presentation of the paper. Support from funding agencies NSERC, the CRC program, European Regional Development Fund (ERDF), and the Galician Regional Government (projects CN2012/279 and CN 2012/260, 'Consolidation of Research Units: AtlantTIC') is gratefully acknowledged. FX would like to thank the Paul Biringer Graduate Scholarship for financial support.

Appendix A. Other practical errors

Here, we discuss other practical error sources and show that their contribution to the QBER is not very significant in a practical MDI-QKD system. For this reason, they are ignored in our simulations.

A.1. Intensity fluctuations at the source

The intensity fluctuations of the signal and decoy states at the source are relatively small (∼0.1 dB) [37]. Additionally, Alice and Bob can in principle locally and precisely quantify their own intensities. Therefore, this error source can be mostly ignored in the theoretical model that analyzes the performance of practical MDI-QKD (but one could easily include it in the analysis).

A.2. Threshold detector with background counts

The threshold single photon detector (SPD) can be modeled by a BS with η_d transmission and (1-η_d) reflection. The transmission part is followed by a unity efficiency detector, while the reflection part is discarded. η_d is defined as the detector efficiency. Background counts can be treated to be independent of the incoming signals. For simplicity, the system model discussed in appendix B assumes that the four SPDs (see figure 1) are identical and have a detection

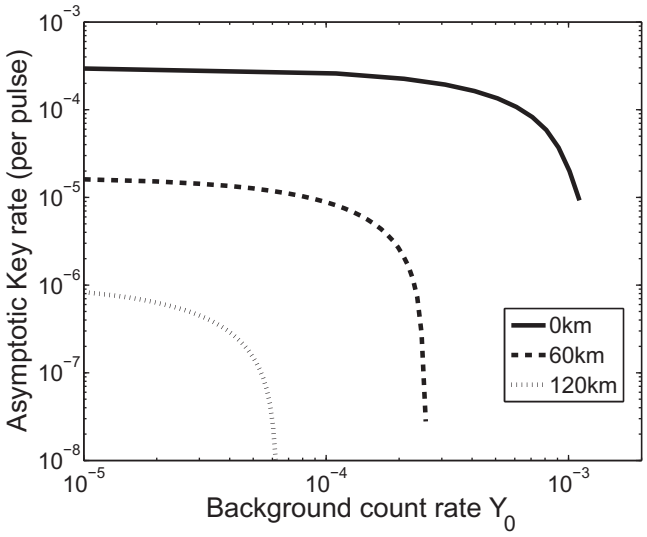

Figure A.1. Background counts tolerance. Following the model discussed in appendix B, we simulate the asymptotic key rates at different background count rates. MDI-QKD is robust to background counts.

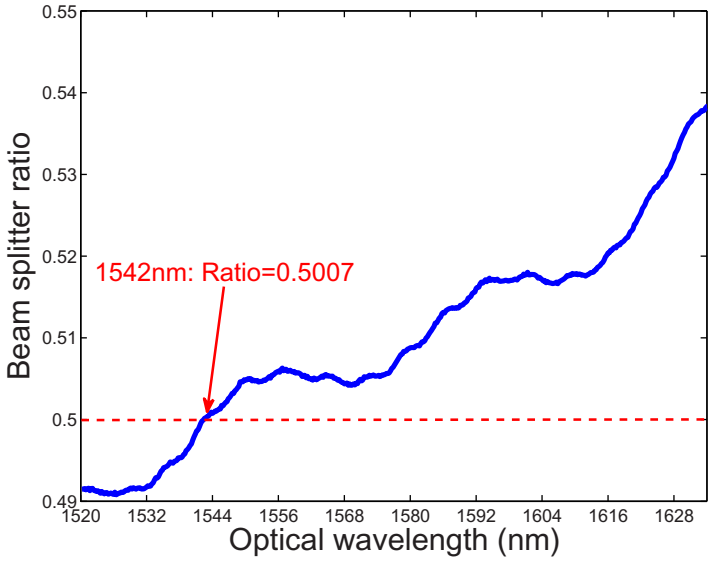

Figure A.2. Wavelength dependence of a fiber-based beam splitter. If the laser wavelength is 1542 nm [29], the BS ratio is 0.5007, which introduces negligible QBER (below 0.01%) in a typical MDI-QKD system.

efficiency η_d and a background rate Y_0. Note, however, that if this condition is not satisfied (i.e. there is some detection efficiency mismatch) our system model can be adapted to take care also of this case.

All the simulations reported in the main text already consider a background rate of $Y_0 = 6.02 \times 10^{-6}$ (see table 1). Figure A.1 simulates more general cases of the asymptotic key rates at different background count rates. At 0 km, the MDI-QKD system can tolerate up to 10^{-3} (per pulse) background counts.

A.3. Beam splitter ratio

In practice, for telecom wavelengths, the asymmetry of the BS (i.e. not 50:50) is usually small. For instance, the wavelength dependence of the fiber-based BS in our laboratory (Newport-13101550-5050 fiber coupler) is experimentally quantified in figure A.2. If the laser wavelength is 1542 nm [29], the BS ratio is 0.5007, which introduces negligible QBER (below 0.01%) in a MDI-QKD system. Hence, this error source can also be ignored in the theoretical model of MDI-QKD.

Appendix B. System model—analytical key rate

In this section, we discuss an analytical method to model a polarization-encoding MDI-QKD system. That is, we calculate $Y_Z^{1,1}$, $e_X^{1,1}$, Q_Z and E_Z and thus estimate the expected key rate from equation (1).

To simplify our calculation, we make two assumptions about the practical error sources: (i) since most practical error sources do not contribute significantly to the system performance, we only consider the polarization misalignment e_{d}, the background count rate Y_0 and the detector efficiency η_{d}; (ii) for the model of the polarization misalignment, we consider only two unitary operators, U_1 and U_2, to represent, respectively, the polarization misalignment of Alice's and Bob's channel transmission, i.e. set $U_3 = I$ in the generic model of section 3.1. For simplicity, a more rigorous derivation with $U_3 \neq I$ is not shown here, but it can be easily completed following our procedures discussed below.

B.1. $Y_Z^{1,1}$ and $e_X^{1,1}$

In the asymptotic case, we assume that $Y_Z^{1,1}$ and $e_X^{1,1}$ in equation (1) can be perfectly estimated with an infinite number of signals and decoy states. Thus, they are given by

$$e_X^{1,1} = \frac{1}{2} - \frac{t_{\mathrm{a}} t_{\mathrm{b}} \eta_{\mathrm{d}}^2 (1-e_{\mathrm{d}})^2 (1-Y_0)^2}{4 Y_X^{1,1}},$$

$$Y_Z^{1,1} = (1-Y_0)^2 \left[4Y_0^2 (1-t_{\mathrm{a}}\eta_{\mathrm{d}})(1-t_{\mathrm{b}}\eta_{\mathrm{d}}) + 2Y_0 \left(t_{\mathrm{a}}\eta_{\mathrm{d}} + t_{\mathrm{b}}\eta_{\mathrm{d}} - \frac{3 t_{\mathrm{a}} t_{\mathrm{b}} \eta_{\mathrm{d}}^2}{2} \right) + \frac{t_{\mathrm{a}} t_{\mathrm{b}} \eta_{\mathrm{d}}^2}{2} \right], \tag{B.1}$$

where $Y_X^{1,1} = Y_Z^{1,1}$. Importantly, we can see that ignoring the imperfections of polarization misalignment and background counts (i.e. $e_{\mathrm{d}} = 0$, $Y_0 = 0$), $e_X^{1,1}$ is zero, while $P_Z^{1,1} Y_Z^{1,1}$ ($P_Z^{1,1} = \mu_{\mathrm{a}} \mu_{\mathrm{b}} \mathrm{e}^{-(\mu_{\mathrm{a}}+\mu_{\mathrm{b}})}$) can be maximized with $\mu_{\mathrm{a}} = \mu_{\mathrm{b}}$. Thus, the optimal choice of intensities is $\mu_{\mathrm{a}} = \mu_{\mathrm{b}} = 1$. However, in practice, it is inevitable to have certain practical errors, which result in this optimal choice being a *function* of the values of practical errors.

B.2. Q_Z and E_Z

Now, let us calculate Q_Z and E_Z, which are eventually given by equation (B.12). To further simplify our discussion, we use {horizonal, vertical, 45°, 135°} to represent the BB84 polarization states. Also, $\{HH, HV, ++, +-\}$ will denote Alice's and Bob's encoding modes.

We define the following notations:

$$\begin{aligned}
&\gamma_a = \sqrt{\mu_a t_a \eta_d}, \quad \gamma_b = \sqrt{\mu_b t_b \eta_d},\\
&\beta = \gamma_a\gamma_b, \quad \gamma = \gamma_a^2 + \gamma_b^2,\\
&\lambda = \gamma_a\gamma_b\sqrt{e_{d1}(1-e_{d1})}, \quad \omega = \gamma_a^2 + e_{d1}(\gamma_b^2 - \gamma_a^2).
\end{aligned}$$

B.2.1. Derivation of Q_Z^{HH}. First, both Alice and Bob encode their states in the H mode (symmetric to V mode). We assume that U_1 and U_2 (see equation (2)) rotate the polarization in the *same* direction, i.e. $\theta_1\theta_2 > 0$. The discussion regarding rotation in the opposite direction (i.e. $\theta_1\theta_2 < 0$) is in B.2.4.

In Charles's laboratory, after the BS and PBS (see figure 1), the optical intensities received by each SPD are given by

$$\begin{aligned}
D_{ch} : |A|^2 &= \frac{(1-e_{d1})(\gamma_a^2+\gamma_b^2) - 2\gamma_a\gamma_b\cos(\phi)(1-e_{d1})}{2},\\
D_{dh} : |C|^2 &= \frac{(1-e_{d1})(\gamma_a^2+\gamma_b^2) + 2\gamma_a\gamma_b\cos(\phi)(1-e_{d1})}{2},\\
D_{cv} : |B|^2 &= \frac{e_{d1}(\gamma_a^2+\gamma_b^2) - 2\gamma_a\gamma_b\cos(\phi)e_{d1}}{2},\\
D_{dv} : |D|^2 &= \frac{e_{d1}(\gamma_a^2+\gamma_b^2) + 2\gamma_a\gamma_b\cos(\phi)e_{d1}}{2},
\end{aligned} \tag{B.2}$$

where ϕ denotes the relative phase between Alice's and Bob's weak coherent states. Thus, the detection probability of each threshold SPD is

$$P_V = 1 - (1-Y_0)\,e^{-|V|^2}, \tag{B.3}$$

where $V = A, B, C, D$. Then, the coincident counts are

$$\begin{aligned}
Q_Z^{HH,\psi^+} &= 2P_AP_B(1-P_C)(1-P_D),\\
Q_Z^{HH,\psi^-} &= 2P_AP_D(1-P_B)(1-P_C),
\end{aligned}$$

where Q_Z^{HH,ψ^+} and Q_Z^{HH,ψ^-} denote, respectively, the probability of the projection on the Triplet $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|H,V\rangle + |V,H\rangle)$ and the Singlet $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|H,V\rangle - |V,H\rangle)$. Here from figure 1, Triplet means the coincident detections of {ch & cv} or {dh & dv}; Singlet means the coincident detections of {ch & dv} or {cv & dh}. After averaging over the relative phase ϕ (integration over $[0, 2\pi]$), we have

$$\begin{aligned}
Q_Z^{HH,\psi^+} &= 2\,e^{-\frac{\gamma}{2}}(1-Y_0)^2[I_0(\beta) + (1-Y_0)^2\,e^{-\frac{\gamma}{2}}\\
&\quad -(1-Y_0)\,e^{-\frac{\gamma(1-e_{d1})}{2}}I_0(e_{d1}\beta) - (1-Y_0)\,e^{-\frac{\gamma e_{d1}}{2}}I_0(\beta - e_{d1}\beta)],\\
Q_Z^{HH,\psi^-} &= 2\,e^{-\frac{\gamma}{2}}(1-Y_0)^2[I_0(\beta - 2\beta e_{d1}) + (1-Y_0)^2\,e^{-\frac{\gamma}{2}}\\
&\quad -(1-Y_0)\,e^{-\frac{\gamma(1-e_{d1})}{2}}I_0(e_{d1}\beta) - (1-Y_0)\,e^{-\frac{\gamma e_{d1}}{2}}I_0(\beta - e_{d1}\beta)],
\end{aligned} \tag{B.4}$$

where $I_0(\cdot)$ is the modified Bessel function. Therefore, Q_Z^{HH} is given by

$$Q_Z^{HH} = Q_Z^{HH,\psi^+} + Q_Z^{HH,\psi^-}. \tag{B.5}$$

Here, to simplify equation (B.2.1), we ignore background counts, i.e. $Y_0 = 0$, and use a second order approximation (as both β and γ are typically on the order of 0.01) such that

$$I_0(\beta) = 1 + \frac{\beta^2}{4} + O(\beta^4),$$
$$e^{\gamma} = 1 + \gamma + \frac{\gamma^2}{2} + O(\gamma^3),$$

then, equation (B.2.1) can be estimated as

$$\begin{aligned} Q_Z^{HH,\psi^+} &= \frac{\gamma^2 e_{\mathrm{d1}}(1-e_{\mathrm{d1}})}{2} + \beta^2 e_{\mathrm{d1}}(1-e_{\mathrm{d1}}), \\ Q_Z^{HH,\psi^-} &= \frac{\gamma^2 e_{\mathrm{d1}}(1-e_{\mathrm{d1}})}{2} - \beta^2 e_{\mathrm{d1}}(1-e_{\mathrm{d1}}), \end{aligned} \tag{B.6}$$

and Q_Z^{HH} is given by

$$Q_Z^{HH} = \gamma^2 e_{\mathrm{d1}}(1-e_{\mathrm{d1}}). \tag{B.7}$$

B.2.2. Derivation of Q_Z^{HV}. Alice (Bob) encodes her (his) state in the H (V) mode (symmetric to V (H)). We also assume $\theta_1\theta_2 > 0$. At Charles's side, the optical intensities received by each SPD are given by

$$|A'|^2 = \frac{(1-e_{\mathrm{d1}})\gamma_{\mathrm{a}}^2 + e_{\mathrm{d1}}\gamma_{\mathrm{b}}^2 - 2\lambda\cos(\phi)}{2},$$

$$|B'|^2 = \frac{e_{\mathrm{d1}}\gamma_{\mathrm{a}}^2 + (1-e_{\mathrm{d1}})\gamma_{\mathrm{b}}^2 - 2\lambda\cos(\phi)}{2},$$

$$|C'|^2 = \frac{(1-e_{\mathrm{d1}})\gamma_{\mathrm{a}}^2 + e_{\mathrm{d1}}\gamma_{\mathrm{b}}^2 + 2\lambda\cos(\phi)}{2},$$

$$|D'|^2 = \frac{e_{\mathrm{d1}}\gamma_{\mathrm{a}}^2 + (1-e_{\mathrm{d1}})\gamma_{\mathrm{b}}^2 + 2\lambda\cos(\phi)}{2}.$$

The detection probability of each SPD is described by equation (B.3). Q_Z^{HV,ψ^+} and Q_Z^{HV,ψ^-} can be calculated similarly to equation (B.4). After averaging over ϕ, the results are

$$\begin{aligned} Q_Z^{HV,\psi^+} &= 2\,\mathrm{e}^{-\frac{\gamma}{2}}(1-Y_0)^2[I_0(2\lambda) + (1-Y_0)^2\,\mathrm{e}^{-\frac{\gamma}{2}} \\ &\quad -(1-Y_0)\,\mathrm{e}^{-\frac{\omega}{2}} I_0(\lambda) - (1-Y_0)\,\mathrm{e}^{-\frac{\gamma-\omega}{2}} I_0(\lambda)], \\ Q_Z^{HV,\psi^-} &= 2\,\mathrm{e}^{-\frac{\gamma}{2}}(1-Y_0)^2[1 + (1-Y_0)^2\,\mathrm{e}^{-\frac{\gamma}{2}} \\ &\quad -(1-Y_0)\,\mathrm{e}^{-\frac{\omega}{2}} I_0(\lambda) - (1-Y_0)\,\mathrm{e}^{-\frac{\gamma-\omega}{2}} I_0(\lambda)]. \end{aligned} \tag{B.8}$$

Therefore, Q_Z^{HV} is given by

$$Q_Z^{HV} = Q_Z^{HV,\psi^+} + Q_Z^{HV,\psi^-}. \tag{B.9}$$

To simplify equation (B.8) we once again ignore the background counts and take a second order approximation. Equation (B.8) can be estimated as

$$\begin{aligned} Q_Z^{HV,\psi^+} &= \frac{\omega(\gamma-\omega)}{2}+\lambda^2, \\ Q_Z^{HV,\psi^-} &= \frac{\omega(\gamma-\omega)}{2}-\lambda^2, \end{aligned} \tag{B.10}$$

and Q_Z^{HV} is given by

$$Q_Z^{HV} = \omega(\gamma-\omega). \tag{B.11}$$

B.2.3. Derivation of Q_Z and E_Z. Finally, Q_Z and E_Z can be expressed as

$$\begin{aligned} Q_Z &= \frac{Q_Z^{HH}+Q_Z^{HV}}{2}, \\ E_Z &= \frac{Q_Z^{HH}}{Q_Z^{HH}+Q_Z^{HV}}, \end{aligned} \tag{B.12}$$

where the different terms on the rhs of this equation are given by equations (B.2.1), (B.5), (B.8) and (B.9). Therefore, together with equation (B.1), we could derive the analytical key rate of equation (1).

If we ignore background counts and take the second order approximation from equations (B.6), (B.10), Q_Z and E_Z can be written as

$$\begin{aligned} Q_Z &= \frac{\beta^2+e_{\mathrm{d}}(1-\frac{e_{\mathrm{d}}}{2})(\gamma^2-2\beta^2)}{2}, \\ E_Z &= \frac{\gamma^2 e_{\mathrm{d}}(1-\frac{e_{\mathrm{d}}}{2})}{4Q_Z}. \end{aligned} \tag{B.13}$$

B.2.4. Q_Z and E_Z with opposite rotation angle. When U_1 and U_2 rotate the polarization in the *opposite* direction, i.e. $\theta_1\theta_2 < 0$, equation (B.2) changes to

$$|A|^2 = \frac{(1-e_{\mathrm{d}1})(\gamma_{\mathrm{a}}^2+\gamma_{\mathrm{b}}^2)-2\gamma_{\mathrm{a}}\gamma_{\mathrm{b}}\cos(\phi)(1-e_{\mathrm{d}1})}{2},$$

$$|C|^2 = \frac{(1-e_{\mathrm{d}1})(\gamma_{\mathrm{a}}^2+\gamma_{\mathrm{b}}^2)+2\gamma_{\mathrm{a}}\gamma_{\mathrm{b}}\cos(\phi)(1-e_{\mathrm{d}1})}{2},$$

$$|B|^2 = \frac{e_{\mathrm{d}1}(\gamma_{\mathrm{a}}^2+\gamma_{\mathrm{b}}^2)+2\gamma_{\mathrm{a}}\gamma_{\mathrm{b}}\cos(\phi)e_{\mathrm{d}1}}{2},$$

$$|D|^2 = \frac{e_{\mathrm{d}1}(\gamma_{\mathrm{a}}^2+\gamma_{\mathrm{b}}^2)-2\gamma_{\mathrm{a}}\gamma_{\mathrm{b}}\cos(\phi)e_{\mathrm{d}1}}{2}.$$

After performing similar procedures to those of section B.2.1, equation (B.6) is altered to

$$\begin{aligned} Q_Z^{HH,\psi^+} &= \tfrac{\gamma^2 e_{\mathrm{d1}}(1-e_{\mathrm{d1}})}{2} - \beta^2 e_{\mathrm{d1}}(1-e_{\mathrm{d1}}), \\ Q_Z^{HH,\psi^-} &= \tfrac{\gamma^2 e_{\mathrm{d1}}(1-e_{\mathrm{d1}})}{2} + \beta^2 e_{\mathrm{d1}}(1-e_{\mathrm{d1}}). \end{aligned} \tag{B.14}$$

Since the QBER is mainly determined by Q_Z^{HH}, by comparing equation (B.6) to (B.13), we conclude that

$\theta_1\theta_2 > 0$ Projection on $|\psi^+\rangle$ results in a larger QBER than that on $|\psi^-\rangle$
$\theta_1\theta_2 < 0$ Projection on $|\psi^+\rangle$ results in a smaller QBER than that on $|\psi^-\rangle$

An equivalent analysis can also be applied to Q_Z^{HV} following section B.2.2, and thus equation (B.10) is altered to

$$\begin{aligned} Q_Z^{HV,\psi^+} &= \tfrac{\omega(\gamma-\omega)}{2} - \lambda^2, \\ Q_Z^{HV,\psi^-} &= \tfrac{\omega(\gamma-\omega)}{2} + \lambda^2. \end{aligned} \tag{B.15}$$

Therefore, the key rates of R^{ψ^-} (projections on the triplet) and R^{ψ^+} (projections on the singlet) are *correlated* with the relative direction of the rotation angles, while the overall key rate R ($R = R^{\psi^-} + R^{\psi^+}$) is *independent* of the relative direction of the rotation angles.

We finally remark that in a practical polarization-encoding MDI-QKD system, the polarization rotation angle of each quantum channel (θ_1 or θ_2) can be modeled by a Gaussian distribution with a standard deviation of $\theta_k^{\mathrm{std}} = \arcsin(\sqrt{e_k})$ ($k = 1, 2$), which means that both θ_1 and θ_2 (mostly) distribute in the range of $[-3\theta_k^{\mathrm{std}}, 3\theta_k^{\mathrm{std}}]$ and the relative direction between them also randomly distributes between $\theta_1\theta_2 > 0$ and $\theta_1\theta_2 < 0$. Hence, the effect of the polarization misalignment is the same for R^{ψ^-} and R^{ψ^+}, i.e. both R^{ψ^-} and R^{ψ^+} are independent of the total polarization misalignment. We can experimentally choose to measure either the singlet or the triplet by using only two detectors (but sacrificing half of the total key rate), such as in the experiments of [26, 29].

Appendix C. Asymmetric MDI-QKD

Here we discuss the properties of a practical asymmetric MDI-QKD system. For this, we derive an analytical expression for the estimated key rate and we optimize the system performance numerically.

C.1. Estimated key rate

The estimated key rate R_{est} is defined under the condition that background counts can be ignored. Note that this is a reasonable assumption for a short distance transmission.

Theorem 1. *$\mu_{\mathrm{a}}^{\mathrm{opt}}$ and $\mu_{\mathrm{b}}^{\mathrm{opt}}$ only depend on x rather than on t_{a} or t_{b}; Under a fixed x, R_{est} is quadratically proportional to t_{b}.*

Proof. when Y_0 is ignored, $e_X^{1,1}$ and $P^{1,1}Y_Z^{1,1}$ are given by (see equation (B.1))

$$e_X^{1,1} = e_\mathrm{d} - \frac{e_\mathrm{d}^2}{2},$$
$$P_Z^{1,1}Y_Z^{1,1} = \frac{\mu_\mathrm{a} t_\mathrm{a} \mu_\mathrm{b} t_\mathrm{b}\, \mathrm{e}^{-(\mu_\mathrm{a}+\mu_\mathrm{b})}\eta_\mathrm{d}^2}{2}.$$

□

If we take the second order approximation, Q_Z and E_Z are estimated as (see equation (B.13))

$$Q_Z = \frac{t_\mathrm{b}^2\eta_\mathrm{d}^2[2x\mu_\mathrm{a}\mu_\mathrm{b} + (\mu_\mathrm{b}^2 + x^2\mu_\mathrm{a}^2)(2e_\mathrm{d} - e_\mathrm{d}^2)]}{4},$$
$$E_Z = \frac{(\mu_\mathrm{b} + x\mu_\mathrm{a})^2(2e_\mathrm{d} - e_\mathrm{d}^2)}{2[2x\mu_\mathrm{a}\mu_\mathrm{b} + (\mu_\mathrm{b}^2 + x^2\mu_\mathrm{a}^2)(2e_\mathrm{d} - e_\mathrm{d}^2)]}. \tag{C.1}$$

By combining the above two equations with equation (1), the overall key rate can be written as

$$R_\mathrm{est} = \frac{t_\mathrm{b}^2\eta_\mathrm{d}^2}{2} G(x, \mu_\mathrm{a}, \mu_\mathrm{b}), \tag{C.2}$$

where $G(x, \mu_\mathrm{a}, \mu_\mathrm{b})$ has the form

$$G(x, \mu_\mathrm{a}, \mu_\mathrm{b}) = x\mu_\mathrm{a}\mu_\mathrm{b}\, \mathrm{e}^{-(\mu_\mathrm{a}+\mu_\mathrm{b})}\left[1 - H_2\left(e_\mathrm{d} - \frac{e_\mathrm{d}^2}{2}\right)\right]$$
$$- \frac{2x\mu_\mathrm{a}\mu_\mathrm{b} + (\mu_\mathrm{b}^2 + x^2\mu_\mathrm{a}^2)(2e_\mathrm{d} - e_\mathrm{d}^2)}{2} \times f_\mathrm{e} H_2(E_Z), \tag{C.3}$$

where E_Z is given by equation (C.1) and is also a function of $(x, \mu_\mathrm{a}, \mu_\mathrm{b})$. Therefore, optimizing R_est is equivalent to maximizing $G(x, \mu_\mathrm{a}, \mu_\mathrm{b})$ and the optimal values, $\mu_\mathrm{a}^\mathrm{opt}$ and $\mu_\mathrm{b}^\mathrm{opt}$, are *only* determined by x. Under a fixed x, the optimal key rate is quadratically proportional to t_b. For a given x, the maximization of $G(x, \mu_\mathrm{a}, \mu_\mathrm{b})$ can be done by calculating the derivatives over μ_a and μ_b and verified using the Jacobian matrix.

C.2. Properties of asymmetric MDI-QKD

We numerically study the properties of an asymmetric MDI-QKD system. In our simulations below, the asymptotic key rate, denoted by R_rig, is rigorously calculated from the key rate formula given by equation (1) in which each term is shown in appendix B. R_est denotes the estimated key rate from equation (C.2). The practical parameters are listed in table 1. We used the method of Curty *et al* [33] for the finite-key analysis.

Firstly, figure C.1 simulates the key rates of R_rig and R_est at different channel lengths. For short distances (i.e. total length $L_\mathrm{ac} + L_\mathrm{bc} < 100$ km), the overlap between R_est and R_rig demonstrates the accuracy of our estimation model of equation (C.2). Therefore, in the short distance range, we could focus on R_est to understand the behaviors of the key rate. Moreover, from the curve of $L_\mathrm{bc} = 1$ m, we have that this asymmetric system can tolerate up to $x = 0.004$ (120 km length difference for standard fiber links).

Secondly, figure C.2 shows $\mu_\mathrm{a}^\mathrm{opt}$ and $\mu_\mathrm{b}^\mathrm{opt}$, when both L_bc and L_ac are scanned from 1 m to 100 km. These parameters numerically verify theorem 1 at short distances ($x \geqslant 0.5$), $\mu_\mathrm{a}^\mathrm{opt}$

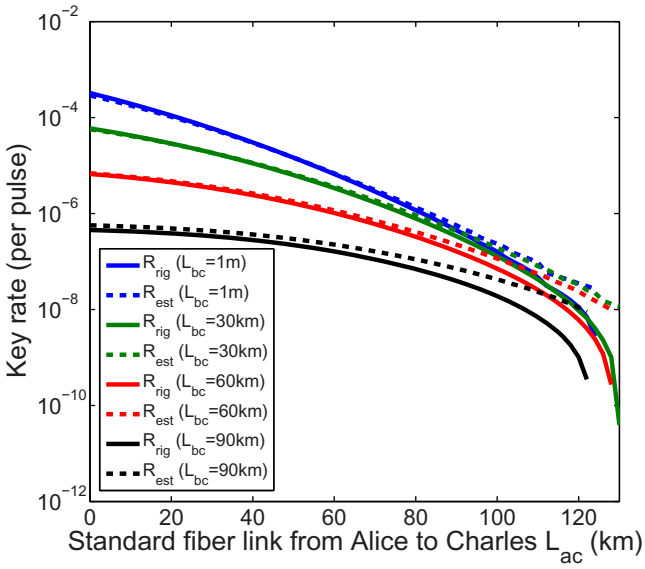

Figure C.1. Asymptotic key rates of R_{rig} and R_{est}. R_{rig} and R_{est} denote, respectively, the rigorous key rate (equation (1)) and the estimated key rate (equation (C.2)). At short distances, the overlap between R_{rig} and R_{est} demonstrates the accuracy of our estimation model, while at long distances, background counts affect its accuracy. An asymmetric system can tolerate a maximal channel mismatch of $x = 0.004$ (120 km length difference for two standard fiber links).

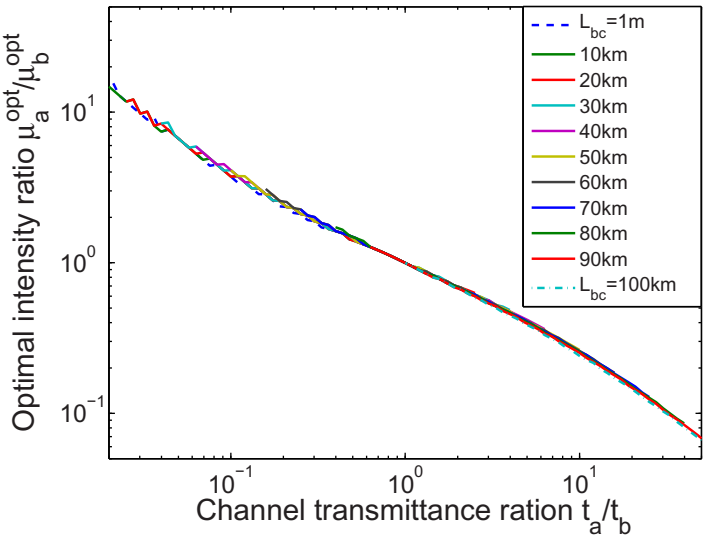

Figure C.2. Optimal μ_{a} and μ_{b}. At short distances (i.e. x is around 1 or bigger), $\mu_{\mathrm{a}}^{\mathrm{opt}}$ and $\mu_{\mathrm{b}}^{\mathrm{opt}}$ depend *only* on x, while at long distances (i.e. $x < 0.5$), background counts contribute significantly. The non-smooth behaviors here are mainly due to background counts and numerical errors.

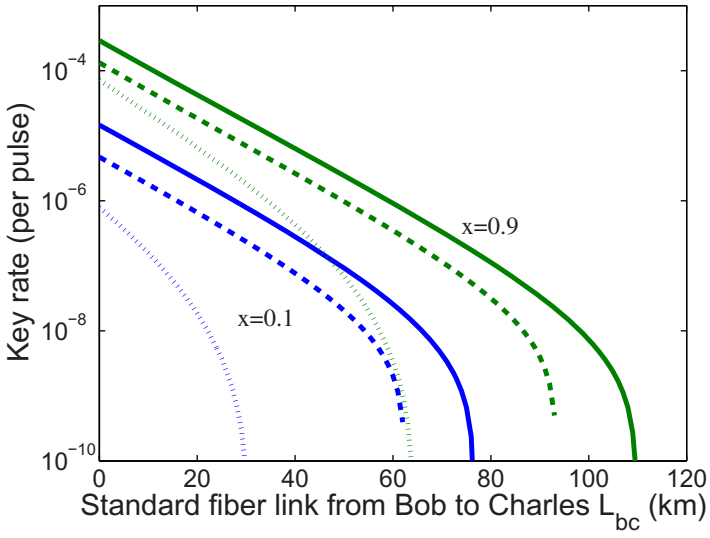

Figure C.3. Key rate with fixed x. Solid curves are the asymptotic key rates: as shown in equation (C.4), $\log_{10} R_{\text{est}}$ is linearly proportional to L_{bc}. Dashed curves are the two decoy-state key rates without the finite-key effect, i.e. with an infinite number of signals. Dotted curves are the two decoy-state key rates with the finite-key effect: with $x = 0.9$, the optimal intensities are $\mu_{\text{a}}^{\text{opt}} \approx \mu_{\text{b}}^{\text{opt}}$ and $\nu_{\text{a}}^{\text{opt}} \approx \nu_{\text{b}}^{\text{opt}}$; with $x = 0.1$, the optimal intensities satisfy $\mu_{\text{a}}^{\text{opt}}/\mu_{\text{b}}^{\text{opt}} = \nu_{\text{a}}^{\text{opt}}/\nu_{\text{b}}^{\text{opt}} \approx 7$ (see table 3 for some representative values). The weakest decoy state ω is set to 5×10^{-4}.

and $\mu_{\text{b}}^{\text{opt}}$ depend *only* on x, while at long distances ($x < 0.5$), background counts contribute significantly and result in non-smooth behaviors. $\mu_{\text{a}}^{\text{opt}}$ and $\mu_{\text{b}}^{\text{opt}}$ are both in $O(1)$.

Finally, we simulate the optimal key rates under two *fixed* x in figure C.3.

(i) Solid curves are the asymptotic keys: at short distances (L_{bc}+$L_{\text{ac}} < 120$ km), the maximal $G(x, \mu_{\text{a}}, \mu_{\text{b}})$ is fixed with a fixed x (see equation (C.3)). Taking the logarithm with base 10 of R_{est} and writing $t_{\text{b}} = 10^{-\alpha L_{\text{bc}}}$, equation (C.2) can be expressed as

$$\log_{10} R_{\text{est}} = -2\alpha L_{\text{bc}} + \log_{10} \frac{\eta_{\text{d}}^2 G(x, \mu_{\text{a}}, \mu_{\text{b}})}{2}. \tag{C.4}$$

Hence, the scaling behavior between the logarithm (base 10) of the key rate and the channel distance is linear, which can be seen in the figure. Here, $\alpha = 0.2$ dB km^{-1} (standard fiber link) results in a slope of -0.4.

(ii) Dotted curves are the two decoy-state key rates with the finite-key analysis: we consider a total number of signals $N = 10^{14}$ and a security bound of $\epsilon = 10^{-10}$; for the dotted curve with $x = 0.1$, the optimal intensities satisfy $\mu_{\text{a}}/\mu_{\text{b}} \approx \nu_{\text{a}}/\nu_{\text{b}} \approx 7$, which means that the ratios for the optimal μ and ν are roughly the same and this ratio is mainly determined by x. Even taking the finite-key effect into account, the system can still tolerate a total fiber link of 110 km.

References

[1] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. Computers, Systems and Signal Processing* (New York: IEEE) pp 175–9
[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[3] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[4] Mayers D 2001 *J. ACM* **48** 351
Lo H-K and Chau H F 1999 *Science* **283** 2050
Shor P and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301
[5] Zhao Y, Fung C-H F, Qi B, Chen C and Lo H-K 2008 *Phys. Rev.* A **78** 42333
[6] Qi B, Fung C-H F, Lo H-K and Ma X 2007 *Quantum Inf. Comput.* **7** 73
[7] Fung C-H F, Qi B, Tamaki K and Lo H-K 2007 *Phys. Rev.* A **75** 32314
Xu F, Qi B and Lo H-K 2010 *New J. Phys.* **12** 113026
[8] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 *Nature Photon.* **4** 686
Gerhardt I, Liu Q, Lamas-Linares A, Skaar J, Kurtsiefer C and Makarov V 2011 *Nature Commun.* **2** 349
[9] Weier H, Krauss H, Rau M, Fuerst M, Nauerth S and Weinfurter H 2011 *New J. Phys.* **13** 073024
Jain N, Wittmann C, Lydersen L, Wiechers C, Elser D, Marquardt C, Makarov V and Leuchs G 2011 *Phys. Rev. Lett.* **107** 110501
Li H-W *et al* 2011 *Phys. Rev.* A **84** 062308
Sun S, Jiang M and Liang L 2011 *Phys. Rev.* A **83** 062331
[10] Yuan Z, Dynes J and Shields A 2010 *Nature Photon.* **4** 800
Yuan Z, Dynes J and Shields A 2011 *Appl. Phys. Lett.* **98** 231104
[11] Mayers D and Yao A 2004 *Quantum Inf. Comput.* **4** 273
Acín A, Brunner N, Gisin N, Massar S, Pironio S and Scarani V 2007 *Phys. Rev. Lett.* **98** 230501
[12] Barrett J, Colbeck R and Kent A 2013 *Phys. Rev. Lett.* **110** 010503
[13] Gisin N, Pironio S and Sangouard N 2010 *Phys. Rev. Lett.* **105** 70501
Curty M and Moroder T 2011 *Phys. Rev.* A **84** 010304
[14] Lo H-K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[15] Xu F, Qi B, Ma X, Xu H, Zheng H and Lo H-K 2013 *Opt. Express* **20** 12366
[16] Raussendorf R and Briegel H J 2001 *Phys. Rev. Lett.* **86** 5188
Raussendorf R, Browne D E and Briegel H J 2003 *Phys. Rev.* A **68** 022312
[17] Biham E, Huttner B and Mor T 1996 *Phys. Rev.* A **54** 2651
Inamori H 2002 *Algorithmica* **34** 340
[18] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
Lo H-K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
Wang X-B 2005 *Phys. Rev. Lett.* **94** 230503
Ma X, Qi B, Zhao Y and Lo H-K 2005 *Phys. Rev.* A **72** 012326
[19] Tamaki K, Lo H-K, Fung C-H F and Qi B 2012 *Phys. Rev.* A **85** 042307
[20] Ma X and Razavi M 2012 *Phys. Rev.* A **86** 062319
[21] Ma X, Fung C-H F and Razavi M 2012 *Phys. Rev.* A **86** 052305
[22] Wang X-B 2013 *Phys. Rev.* A **87** 012320
[23] Xu F, Qi B, Liao Z and Lo H-K 2013 *Appl. Phys. Lett.* **103** 061101
[24] Song T-T, Wen Q-Y, Guo F-Z and Tan X-Q 2012 *Phys. Rev.* A **86** 022332
[25] Chan P, Slater J-A, Rubenok A, Lucio-Martinez I and Tittel W 2013 arXiv:1204.0738
[26] Rubenok A, Slater J-A, Chan P, Lucio-Martinez I and Tittel W 2013 *Phys. Rev. Lett.* **111** 130501
[27] Liu Y *et al* 2013 *Phys. Rev. Lett.* **111** 130502
[28] Silva T F, da Vitoreti D, Xavier G B, Temporão G P and Von der Weid J P 2012 arXiv:1207.6345
[29] Tang Z, Liao Z, Xu F, Qi B, Qian L and Lo H-K 2013 arXiv:1306.6134

[30] Hong C, Ou Z and Mandel L 1987 *Phys. Rev. Lett.* **59** 2044
[31] Grangier P, Sanders B and Vuckovic J 2004 *New J. Phys.* **6** doi:10.1088/1367-2630/6/1/E04
[32] Renner R 2005 arXiv:quant-ph/0512258
Scarani V and Renner R 2008 *Phys. Rev. Lett.* **100** 200501
[33] Curty M, Xu F, Cui W, Lim C C W, Tamaki K and Lo H-K 2013 arXiv:1307.1081
[34] Sangouard N, Simon C, Riedmatten H D and Gisin N 2011 *Rev. Mod. Phys.* **83** 33
[35] Kok P, Munro W J, Nemoto K, Ralph T C, Dowling J P and Milburn G 2007 *Rev. Mod. Phys.* **79** 135
[36] Rosenberg D, Harrington J W, Rice P R, Hiskett P A, Peterson C G, Hughes R J, Lita A E, Nam S W and Nordholt J E 2007 *Phys. Rev. Lett.* **98** 010503
Dixon A, Yuan Z, Dynes J, Sharpe A and Shields A 2008 *Opt. Express* **16** 18790
[37] Rosenberg D *et al* 2009 *New J. Phys.* **11** 045009
[38] Lo H-K, Chau H-F and Ardehali M 2005 *J. Cryptol.* **18** 133
[39] Ursin R *et al* 2007 *Nature Phys.* **3** 481
[40] Rohde P P, Mauerer W and Silberhorn C 2007 *New J. Phys.* **9** 91
[41] Sasaki M *et al* 2011 *Opt. Express* **19** 10387
[42] Braunstein S L and Pirandola S 2012 *Phys. Rev. Lett.* **108** 130502
[43] Lim C C W, Portmann C, Tomamichel M, Renner R and Gisin N 2013 *Phys. Rev. X* **3** 031006
[44] Xavier G B, Walenta N, de Faria G V, Temporão G P, Gisin N, Zbinden H and Von der Weid J P 2009 *New J. Phys.* **11** 045015