New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG IOP Institute of Physics

PAPER • OPEN ACCESS

Simple method for asymmetric twin-field quantum key distribution

To cite this article: Wenyuan Wang and Hoi-Kwong Lo 2020 *New J. Phys.* **22** 013020

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

OPEN ACCESS

RECEIVED
19 July 2019

REVISED
4 December 2019

ACCEPTED FOR PUBLICATION
16 December 2019

PUBLISHED
20 January 2020

PAPER

Simple method for asymmetric twin-field quantum key distribution

Wenyuan Wang[1] **and Hoi-Kwong Lo**

Centre for Quantum Information and Quantum Control (CQIQC), Dept. of Electrical & Computer Engineering and Dept. of Physics, University of Toronto, Toronto, Ontario, M5S 3G4, Canada

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

E-mail: wenyuan.wang@mail.utoronto.ca **and** hklo@ece.utoronto.ca

Keywords: quantum key distribution, twin field quantum key distribution (TF-QKD), quantum cryptography, quantum network, asymmetric channels

Abstract

Twin-field quantum key distribution (TF-QKD) can beat the linear bound of repeaterless QKD systems. After the proposal of the original protocol, multiple papers have extended the protocol to prove its security. However, these works are limited to the case where the two channels have equal amount of loss (i.e. are symmetric). In a practical network setting, it is very likely that the channels are asymmetric due to e.g. geographical locations. In this paper we extend the 'simple TF-QKD' protocol to the scenario with asymmetric channels. We show that by simply adjusting the two signal states of the two users (and not the decoy states) they can effectively compensate for channel asymmetry and consistently obtain an order of magnitude higher key rate than previous symmetric protocol. It also can provide 2–3 times higher key rate than the strategy of deliberately adding fibre to the shorter channel until channels have equal loss (and is more convenient as users only need to optimize their laser intensities and do not need to physically modify the channels). We also perform simulation for a practical case with three decoy states and finite data size, and show that our method works well and has a clear advantage over prior art methods with realistic parameters.

1. Background

Quantum key distribution (QKD) is proven to provide information-theoretic security to two communicating parties. Without efficient quantum repeaters, however, QKD is limited in the maximum distance over which it can generate secure keys. The linear bound [1, 2] is a theoretical upper bound for maximum key rate-distance relation for repeaterless QKD. Interestingly, the twin-field (TF) QKD protocol proposed in 2018 [3] uses a clever technique to surpass the linear bound: it uses a setup where two parties, Alice and Bob, communicate with an untrusted third party, Charles. Instead of using two-photon interference like in measurement-device-independent (MDI) QKD [4], TF-QKD makes use of single-photon interference to generate keys, and on average only one photon passes through either Alice's or Bob's channel—which allows to key rate to scale with transmittance over only half the distance between Alice and Bob. Not only does TF-QKD surpass the repeaterless bound, it also provides security against attacks on measurement devices [5] similar to MDI-QKD. Because of these advantages, TF-QKD has attracted much attention worldwide since its proposal. Since a rigorous security proof is not provided in the original proposal, several papers have improved the protocol and provided security proof [6–10]. Also, recently there have been multiple reports of TF-QKD demonstrated experimentally [11–14].

However, all the above security proofs and experimental demonstrations only consider the symmetric case where Alice's and Bob's channels have the same amount of loss. In reality, though, in a network setting, due to e.g. geographical locations, or Alice and Bob being situated on moving free-space platforms (such as ships or satellites), it is very likely that Alice's and Bob's channels are not symmetric. In the future, if a quantum network is build around the protocol—e.g. a star-shaped network where numerous users (senders) are connected to one central node with measurement devices, asymmetry will be an even more severe problem since it is difficult to

maintain the same channel loss for all users (and users might join/leave a network at arbitrary locations). If channels are asymmetric, for prior art protocols, users would either have to suffer from much higher quantum-bit-error-rate (QBER) and hence lower key rate, or would have to deliberately add fibre to the shorter channel to compensate for channel asymmetry, which is inconvenient (since it requires physically modifying the channels) and also provides sub-optimal key rate.

Similar limitation to symmetric channels have been observed in MDI-QKD. In [15], we have proposed a method to overcome this limitation, by allowing Alice and Bob to adjust their intensities (and use different optimization strategies for two decoupled bases) to compensate for channel loss, without having to physically adjust the channels. The method has also been successfully experimentally verified for asymmetric MDI-QKD in [16].

In this work, we will apply our method to TF-QKD and show that it is possible to obtain good key rate through asymmetric channels by adjusting Alice's and Bob's intensities—in fact, we will show that, Alice and Bob only need to adjust their signal intensities to obtain optimal performance. We show that the security of the protocol is not affected, and that an order of magnitude higher (than symmetric protocol) or 2-3 times higher (than adding fibre) key rate can be achieved with the new method. Furthermore, we show with numerical simulation results that our method works well for both finite-decoy and finite-data case with practical parameters, making it a convenient and powerful method to improve the performance of TF-QKD through asymmetric channels in reality.

While we use the same main idea of allowing Alice and Bob to use asymmetric intensities to compensate for asymmetric channel losses as in [15], there are some key differences that need to be addressed for asymmetric TF-QKD. Firstly, the security proof need to be discussed, to show that the introduction of asymmetric channels and intensities do not affect security. Secondly, as we will later show in section 4, there is an interesting distinction between the MDI-QKD protocol in [15] and the TF-QKD protocol in [9] in how the two bases X and Z respectively react to asymmetric incoming intensities, which makes the optimal strategies for asymmetric-intensity MDI-QKD and TF-QKD different. We will discuss this in more detail in section 4.

The idea of TF-QKD protocol through asymmetric channels has also been discussed in a recent paper [17]. Our work is different from [17] in several aspects. First, [17] starts with a different protocol—'sending or not sending protocol'. Second, [17] is mostly numerical. In contrast, we start with the 'simple TF-QKD' protocol in [9] and consider its asymmetric-intensity version. We include both analytical and numerical reasoning. We also provide a detailed discussion about the physics behind the security of our asymmetric-intensity protocol.

The layout of the paper is as follows: in section 2, we define the setup and the protocol we use. In section 3 we will extend the security proof in [9] to the case with asymmetric intensities and channels. In section 4, we discuss the how the performance of TF-QKD is affected by channel asymmetry and asymmetric intensities (and for the latter, what are the best strategies for choosing the intensities). We show the effectiveness of our method with simulation results in section 5.

2. Protocol

Here we consider a similar TF-QKD setup as in [9] 'Protocol 3'. Alice and Bob choose two bases X and Z randomly. When X basis is chosen, Alice (Bob) sends states $|\alpha\rangle_a$ ($|\alpha\rangle_b$) for bit $b_A = 0$ ($b_B = 0$) or states $|-\alpha\rangle_a$ ($|-\alpha\rangle_b$) for bit $b_A = 1$ ($b_B = 1$). When Z basis is chosen, Alice and Bob send phase-randomized coherent states ρ_{a,β_A} (ρ_{b,β_B}), where the decoy state intensities are $\{\beta_A, \beta_B\}$. Note that here Alice and Bob have a common phase reference for X basis signals. After the signals are sent to Charles, the detector events are denoted as k_c, k_d (0 denotes no click, and 1 denotes a click).

The papers [3, 9] consider only the case where the channels between Alice (Bob) and Charles have equal transmittances. In reality, it is possible that the channels might have different levels of loss, due to e.g. geographical locations or moving platforms Here we are interested in three questions for TF-QKD with asymmetric channels:

1. Does channel asymmetry affect security?
2. How does channel asymmetry affect the QBER and hence key rate?[2]
3. Can we improve the performance of the protocol under channel asymmetry?

[2] In the supplementary materials of [16], we and our collaborators presented a preliminary study on this point, and showed that asymmetry decreases single-photon interference visibility—which will in turn increase observable QBER for TF-QKD.

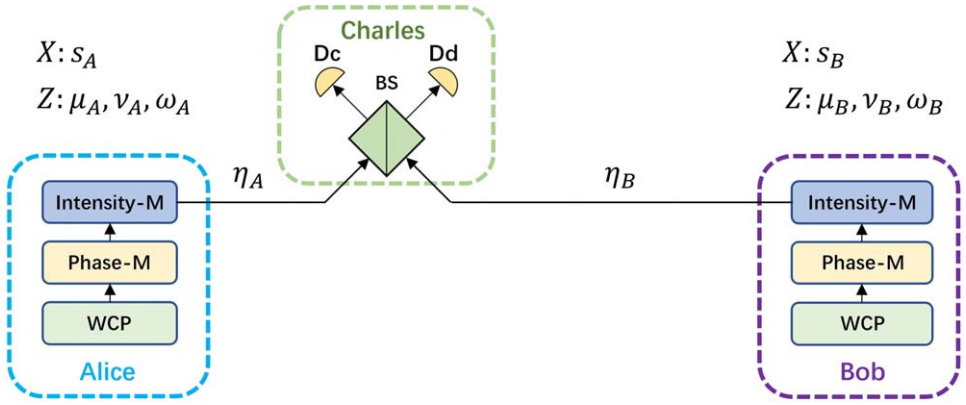

Figure 1. An example setup for a twin-field QKD system. Alice and Bob send signals in X and Z bases randomly. In X basis, Alice and Bob send coherent states with amplitudes α_A, α_B (with intensities $s_A = \alpha_A^2$, $s_B = \alpha_B^2$—in the asymmetric case, we allow s_A to be different from s_B), phase-modulated by $\{0, \pi\}$ depending on the encoded bit. In Z basis, Alice and Bob send signals in phase-randomized coherent states, with intensities chosen from $\{\mu_A, \nu_A, \omega_A\}$ and $\{\mu_A, \nu_A, \omega_A\}$, respectively. Charles performs a swap test on the incoming signals and reports the click events in his two detectors D_c, D_d (denoted by k_c, k_d). By choosing different intensities between Alice and Bob (and using the decoupled X and Z bases), the protocol can have high key rate even if Alice and Bob's channels have different transmittances, η_A, η_B.

We will use our method from [15] and apply it to Protocol 3 in [9], to make an '*asymmetric-intensity*' TF-QKD protocol that works well even when channels are highly asymmetric. Similar to MDI-QKD, the protocol in [9] has decoupled X and Z bases. Here we allow Alice and Bob to have different intensities in the X and the Z bases respectively, such that in X basis Alice (Bob) now send states $|\alpha_A\rangle_a$ ($|\alpha_B\rangle_b$) for bit $b_A = 0$ ($b_B = 0$) or states $|-\alpha_A\rangle_a$ ($|-\alpha_B\rangle_b$) for bit $b_A = 1$ ($b_B = 1$). We can denote the signal intensities as $s_A = \alpha_A^2$, $s_B = \alpha_B^2$. In the Z basis, the amplitudes for the phase-randomized coherent states, $\{\beta_A, \beta_B\}$, can be different for Alice and Bob too (we can denote the intensities as $\{\beta_A^2, \beta_B^2\}$, and for the three-decoy case, the sets of intensities can be specifically written as $\{\mu_A, \nu_A, \omega_A\}$ and $\{\mu_A, \nu_A, \omega_A\}$). An example setup can be found in figure 1.

We will answer the above three questions by showing in the following text three main pieces of results:

(1) neither asymmetric channels nor asymmetric intensities between Alice and Bob affect security;

(2) the X basis (signal state) QBER will increase with channel asymmetry, and greatly reduce the key rate of TF-QKD if no compensation is performed—on the other hand, the Z basis gain (as well as the upper bound to the yield and phase-error rate derived from the observable data in the Z basis) is little affected by channel asymmetry;

(3) we can use different intensities between Alice and Bob to compensate for channel asymmetry and get good key rate—in fact, using only different signal states between Alice and Bob (and keeping all decoy states and probabilities identical for Alice and Bob) can already effectively compensate for channel asymmetry and allow good key rate for asymmetric TF-QKD.

3. Security

In this section we will show that neither asymmetric channels nor asymmetric intensities between Alice and Bob affect security. Following the discussion in [9], the key is generated from events in the X basis, and the secure key rate is bounded using the bit-error rate and the phase-error rate. The X basis bit-error rate is directly obtained as an observable, hence the key part of the security proof lies in the estimation of X basis phase-error rate (equivalent to the Z basis bit-error rate) based on the Z basis observables—which, since Z basis signals are phase-randomized, is not directly obtainable.

In the security proof in [9], the phase-error rate is obtained by upper-bounding the phase-error rate using the estimated *yields* of given photon numbers $\{m, n\}$ (which can be upper-bounded by using decoy-state analysis, based on observed count rates, i.e. the gains, in the Z basis).

The key message we'd like to point out is that, this entire estimation process of the phase error rate *does not* rely on the fact that Alice and Bob use the same amplitude α for their signal states, or that the channels have the same transmittance. Therefore, here we will follow the proof in [9] step-by-step, but with asymmetric intensities and channel transmittances, to show that the security proof can be easily extended to the asymmetric case.

A small note is that, the formulation of the original security proof in [9] appears to assume a single Kraus operator for the channel (i.e. a pure state after the measurement, which could involve measurements from Charles and/or Eve), but the proof can, in fact, be extended to cover the general case where the state could be a mixed state after passing through the channel and potentially being disturbed by Eve[3]. We have discussed with the original authors of [9], and we thank Koji Azuma for pointing out this fact [18] and the details of incorporating multiple Kraus operators to represent a mixed state after the measurement (and applying Cauchy–Schwarz inequality to the mixed state to obtain the bounds on the phase error rate). In the following text we will use the formulation of multiple Kraus operators and density matrices as in Koji Azuma's clarification of the original proof.

We can start by imagining a virtual scenario where Alice (Bob) prepares entangled states between a local qubit A (B) and a signal a (b) to be sent to Charles. After Charles performs a measurement on the signals, the X basis phase-error rate (or Z basis bit-error rate) can be obtained by Alice (Bob) measuring their local qubits in the Z basis. The initial states can be written as:

$$|\psi_X^A\rangle_{Aa} = \frac{1}{\sqrt{2}}(|+\rangle_A|\alpha_A\rangle_a + |-\rangle_A|-\alpha_A\rangle_a)$$
$$|\psi_X^B\rangle_{Bb} = \frac{1}{\sqrt{2}}(|+\rangle_B|\alpha_B\rangle_b + |-\rangle_B|-\alpha_B\rangle_b) \quad (1)$$

here $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ are the X basis states. Here in the asymmetric-intensity case, we allow $s_A = \alpha_A^2$ to be different from $s_B = \alpha_B^2$. For convenience, here let us write $|\psi_X\rangle_{AaBb} = |\psi_X^A\rangle_{Aa}|\psi_X^B\rangle_{Bb}$. We can then write the density matrix of the initial state as

$$\rho_{AaBb} = |\psi_X\rangle_{AaBb}\ {}_{AaBb}\langle\psi_X|. \quad (2)$$

Now, the process of signals a and b going through their respective channels and Charles making a measurement can be represented by a set of Kraus operators $\{\hat{M}^{ab}_{k_c k_d, e}\}$, where k_c, k_d are Charles' detector events, and e is the (implicit) measurement results of a potential eavesdropper Eve. The superscript ab represents that this operator only acts on the systems a, b (pulses sent to Charles) and not on A, B (local qubits in Alice's and Bob's labs). From the perspective of Alice and Bob, as e is not announced, the state they obtain is equivalent to Eve having discarded all measurement results e. After signals pass through the channels and Charles announces the measurement result k_c, k_d, the conditional state becomes:

$$\rho'_{AaBb} = \frac{\sum_e \hat{M}^{ab}_{k_c k_d, e}\rho_{AaBb}\hat{M}^{ab\dagger}_{k_c k_d, e}}{p_{XX}(k_c, k_d)} \quad (3)$$

here $p_{XX}(k_c, k_d)$ is the X basis Gain for detection events k_c, k_d (which can be 0,1 or 1,0 for a detection event to be considered successful). Note that, this set of operator $\{\hat{M}^{ab}_{k_c k_d, i}\}$ includes all information of the channels, detectors (and the eavesdropper) and is a general representation of their joint effects, and, importantly, it *does not* require that the channels are symmetric at all.

By measuring their local qubits in the Z basis, Alice and Bob can obtain the Z basis bit-error rate $e_{ZZ,k_c k_d}$ (i.e. the X basis phase-error rate):

$$e_{ZZ,k_c k_d} = \sum_{j=0,1} {}_{AB}\langle jj|\rho'_{AB}|jj\rangle_{AB}, \quad (4)$$

where ρ'_{AB}, the state of the local qubits A, B, can be obtained by performing a partial trace over the systems a, b

$$\rho'_{AB} = tr_{ab}(\rho'_{AaBb}). \quad (5)$$

Now, the key observation in the proof of [9] is that, Alice and Bob making a measurement on the local qubits A and B after sending signals a and b and Charles making a measurement should be equivalent to the time-reversed scenario where Alice and Bob first make local Z basis measurements on the initial pure states $|\psi_X^A\rangle_{Aa}$, $|\psi_X^B\rangle_{Bb}$, and then send the signal systems a and b to Charles. After Alice and Bob make the local measurements, the states become

[3] The explicit discussion about using a single Kraus operator for each announcement outcome was also previously made in [10] in a different security proof. So, this is a known result.

$$
\begin{aligned}
{}_A\langle 0||\psi_X\rangle_{Aa} &= |C_0^A\rangle_a \\
{}_A\langle 1||\psi_X\rangle_{Aa} &= |C_1^A\rangle_a \\
{}_B\langle 0||\psi_X\rangle_{Bb} &= |C_0^B\rangle_b \\
{}_B\langle 1||\psi_X\rangle_{Bb} &= |C_1^B\rangle_b
\end{aligned} \tag{6}
$$

which are cat states:

$$
\begin{aligned}
|C_0^A\rangle_a &= \mathrm{e}^{-\frac{\alpha_A^2}{2}}\sum_{n=0}^{\infty}\frac{\alpha_A^{2n}}{\sqrt{2n}}|2n\rangle_a = \sum_{n=0}^{\infty} c_n^{A,(0)}|n\rangle_a \\
|C_1^A\rangle_a &= \mathrm{e}^{-\frac{\alpha_A^2}{2}}\sum_{n=0}^{\infty}\frac{\alpha_A^{2n+1}}{\sqrt{2n+1}}|2n+1\rangle_a = \sum_{n=0}^{\infty} c_n^{A,(1)}|n\rangle_a \\
|C_0^B\rangle_b &= \mathrm{e}^{-\frac{\alpha_B^2}{2}}\sum_{n=0}^{\infty}\frac{\alpha_B^{2n}}{\sqrt{2n}}|2n\rangle_b = \sum_{n=0}^{\infty} c_n^{B,(0)}|n\rangle_b \\
|C_1^B\rangle_b &= \mathrm{e}^{-\frac{\alpha_B^2}{2}}\sum_{n=0}^{\infty}\frac{\alpha_B^{2n+1}}{\sqrt{2n+1}}|2n+1\rangle_b = \sum_{n=0}^{\infty} c_n^{B,(1)}|n\rangle_b
\end{aligned} \tag{7}
$$

here the even (odd) cat states only contain nonzero amplitudes for even (odd) photon numbers. Nonetheless we can still write the amplitudes as $c_n^{A,(0)}$, $c_n^{B,(0)}$ ($c_n^{A,(1)}$, $c_n^{B,(1)}$) for all photon number states, where the coefficients are zero for odd (even) photon number states in an even (odd) cat state.

Note that here in the asymmetric-intensity case, Alice and Bob's cat states are not the same, because they use different signal intensities (hence different amplitudes α_A, α_B), but as we will show below, the derivation of the upper bound for the phase error rate does not depend on the fact that Alice and Bob have the same cat states. Therefore, the security is not compromised by using asymmetric signal intensities[4].

For Alice and Bob's local Z basis measurement results $i, j \in \{0,1\}$ and for detection events k_c, k_d:

$$
\begin{aligned}
{}_{AB}\langle ij|\rho'_{AB}|ij\rangle_{AB} &= {}_{AB}\langle ij|\mathrm{tr}_{ab}(\rho'_{AaBb})|ij\rangle_{AB} \\
&= \mathrm{tr}_{ab}({}_{AB}\langle ij|\rho'_{AaBb}|ij\rangle_{AB}) \\
&= \frac{1}{p_{XX}(k_c,k_d)}\mathrm{tr}_{ab}({}_{AB}\langle ij|\sum_e \hat{M}^{ab}_{k_ck_d,e}\rho_{AaBb}\hat{M}^{ab\dagger}_{k_ck_d,e}|ij\rangle_{AB}) \\
&= \frac{1}{p_{XX}(k_c,k_d)}\sum_e \mathrm{tr}_{ab}(\hat{M}^{ab}_{k_ck_d,e}\,{}_{AB}\langle ij|\rho_{AaBb}|ij\rangle_{AB}\hat{M}^{ab\dagger}_{k_ck_d,e}) \\
&= \frac{1}{p_{XX}(k_c,k_d)}\sum_e \mathrm{tr}_{ab}(\hat{M}^{ab}_{k_ck_d,e}|C_i^A\rangle_a|C_j^B\rangle_b\,{}_a\langle C_i^A|\,{}_b\langle C_j^B|\hat{M}^{ab\dagger}_{k_ck_d,e}) \\
&= \frac{1}{p_{XX}(k_c,k_d)}\sum_e {}_a\langle C_i^A|\,{}_b\langle C_j^B|\hat{M}^{ab\dagger}_{k_ck_d,e}\hat{M}^{ab}_{k_ck_d,e}|C_i^A\rangle_a|C_j^B\rangle_b \\
&= \frac{1}{p_{XX}(k_c,k_d)}\,{}_a\langle C_i^A|\,{}_b\langle C_j^B|\sum_e \hat{M}^{ab\dagger}_{k_ck_d,e}\hat{M}^{ab}_{k_ck_d,e}|C_i^A\rangle_a|C_j^B\rangle_b
\end{aligned} \tag{8}
$$

which means that, the probabilities for local Z basis measurement results $i, j \in \{0, 1\}$ (which determine the phase-error rate) can be acquired by observing the gain if Alice and Bob sent cat states. However, Alice and Bob are not really sending cat states—when Z basis is chosen, they are sending phase-randomized coherent states. Using decoy-state analysis, what Alice and Bob acquire are the yields for phase-randomized photon number states, $p_{ZZ}(k_c, k_d|n_A, n_B) = {}_a\langle n_A|\,{}_b\langle n_B|\sum_e \hat{M}^{ab\dagger}_{k_ck_d,e}\hat{M}^{ab}_{k_ck_d,e}|n_A\rangle_a|n_B\rangle_b$. The yields for photon number states are linked to equation (8) using the Cauchy–Schwarz inequality that upper-bounds the gains for cat states (and subsequently the phase-error rate):

[4] The performance, however, does depend on signal intensities, as we will show in section 4. The protocol favors smaller α_A, α_B for lower phase error rate, which become one of the factors—but not the only factor—that affect the optimal choice of signal intensities.

$$
\begin{aligned}
&{}_a\langle C_i^A|\ {}_b\langle C_j^B|\sum_e \hat{M}^{ab\dagger}_{k_c k_d,e}\hat{M}^{ab}_{k_c k_d,e}|C_i^A\rangle_a|C_j^B\rangle_b \\
&= \sum_{m_A,m_B,n_A,n_B=0}^{\infty} c^{A,(i)}_{m_A}c^{B,(j)}_{m_B}c^{A,(i)}_{n_A}c^{B,(j)}_{n_B} \times \sum_e {}_a\langle m_A|\ {}_b\langle m_B|\hat{M}^{ab\dagger}_{k_c k_d,e}\hat{M}^{ab}_{k_c k_d,e}|n_A\rangle_a|n_B\rangle_b \\
&\leqslant \sum_{m_A,m_B,n_A,n_B=0}^{\infty} c^{A,(i)}_{m_A}c^{B,(j)}_{m_B}c^{A,(i)}_{n_A}c^{B,(j)}_{n_B} \\
&\quad \times \sum_e \sqrt{{}_a\langle n_A|\ {}_b\langle n_B|\hat{M}^{ab\dagger}_{k_c k_d,e}\hat{M}^{ab}_{k_c k_d,e}|n_A\rangle_a|n_B\rangle_b}\sqrt{{}_a\langle m_A|\ {}_b\langle m_B|\hat{M}^{ab\dagger}_{k_c k_d,e}\hat{M}^{ab}_{k_c k_d,e}|m_A\rangle_a|m_B\rangle_b}\,,
\end{aligned}
\tag{9}
$$

where we have applied Cauchy–Schwarz inequality to the two vectors $\hat{M}^{ab}_{k_c k_d,e}|n_A\rangle_a|n_B\rangle_b$ and $\hat{M}^{ab}_{k_c k_d,e}|m_A\rangle_a|m_B\rangle_b$. We can then write:

$$
\begin{aligned}
&\sum_{m_A,m_B,n_A,n_B=0}^{\infty} c^{A,(i)}_{m_A}c^{B,(j)}_{m_B}c^{A,(i)}_{n_A}c^{B,(j)}_{n_B} \\
&\quad \times \sum_e \sqrt{{}_a\langle n_A|\ {}_b\langle n_B|\hat{M}^{ab\dagger}_{k_c k_d,e}\hat{M}^{ab}_{k_c k_d,e}|n_A\rangle_a|n_B\rangle_b}\sqrt{{}_a\langle m_A|\ {}_b\langle m_B|\hat{M}^{ab\dagger}_{k_c k_d,e}\hat{M}^{ab}_{k_c k_d,e}|m_A\rangle_a|m_B\rangle_b} \\
&\leqslant \sum_{m_A,m_B,n_A,n_B=0}^{\infty} c^{A,(i)}_{m_A}c^{B,(j)}_{m_B}c^{A,(i)}_{n_A}c^{B,(j)}_{n_B} \\
&\quad \times \sqrt{{}_a\langle n_A|\ {}_b\langle n_B|\sum_e \hat{M}^{ab\dagger}_{k_c k_d,e}\hat{M}^{ab}_{k_c k_d,e}|n_A\rangle_a|n_B\rangle_b}\sqrt{{}_a\langle m_A|\ {}_b\langle m_B|\sum_e \hat{M}^{ab\dagger}_{k_c k_d,e}\hat{M}^{ab}_{k_c k_d,e}|m_A\rangle_a|m_B\rangle_b} \\
&= \left[\sum_{n_A,n_B=0}^{\infty} c^{A,(i)}_{n_A}c^{B,(j)}_{n_B}\sqrt{p_{ZZ}(k_c,\,k_d|n_A,\,n_B)}\right]^2,
\end{aligned}
\tag{10}
$$

where we again use Cauchy–Schwarz inequality by considering two vectors $\vec{u}$, $\vec{v}$ whose eth components are

$$
\begin{aligned}
u_e &= \sqrt{{}_a\langle n_A|_b\langle n_B|\hat{M}^{ab\dagger}_{k_c k_d,e}\hat{M}^{ab}_{k_c k_d,e}|n_A\rangle_a|n_B\rangle_b} \\
v_e &= \sqrt{{}_a\langle m_A|_b\langle m_B|\hat{M}^{ab\dagger}_{k_c k_d,e}\hat{M}^{ab}_{k_c k_d,e}|m_A\rangle_a|m_B\rangle_b}
\end{aligned}
\tag{11}
$$

respectively, and apply $\vec{u}\cdot\vec{v} \leqslant \sqrt{\vec{u}\cdot\vec{u}}\sqrt{\vec{v}\cdot\vec{v}}$.

This means that, the phase-error rate can be upper-bounded by the yields for photon number states $p_{ZZ}(k_c,\,k_d|n_A,\,n_B)$:

$$
\begin{aligned}
p_{XX}(k_c,\,k_d)e_{ZZ}(k_c,\,k_d) &= p_{XX}(k_c,\,k_d)\sum_{j=0,1} {}_{AB}\langle jj|\rho'_{AB}|jj\rangle_{AB} \\
&\leqslant \sum_{j=0,1}\left[\sum_{n_A,n_B=0}^{\infty} c^{A,(j)}_{n_A}c^{B,(j)}_{n_B}\sqrt{p_{ZZ}(k_c,\,k_d|n_A,\,n_B)}\right]^2
\end{aligned}
\tag{12}
$$

this phase error rate, combined with the bit error rate in the X basis, can be used to perform privacy amplification on the error-corrected raw keys and obtain the secure key.

The key point is that, the above proof that upper bounds the phase error rate does not require the fact that $\alpha_A = \alpha_B$ at all. The different signal intensities will cause Alice and Bob to have different cat states, but these states are independently used to obtain inner product with ${}_A\langle i|$ and ${}_B\langle j|$ respectively. With the Cauchy–Schwarz inequality, the joint cat states are reduced to a mixture of photon number states, and there are no cross-terms between the two cat states.

This means that, using asymmetric intensities between Alice and Bob will not affect the estimation of phase error rate. Moreover, as we described in equation (3), $\{\hat{M}^{ab}_{k_c k_d,e}\}$ is a general representation of the channels and detection, and does not require that $\eta_A = \eta_B$ either, i.e. asymmetric channels do not affect the security proof either.

Additionally, the decoy intensities $\{\beta_A^2,\,\beta_B^2\}$ might be different for Alice and Bob too, but these states are only used to estimate the yields of photon number states $p_{ZZ}(k_c,\,k_d|n_A,\,n_B)$ using decoy-state analysis, which is exactly the same process as in MDI-QKD. As long as Eve cannot distinguish pulses from different intensity settings, this decoy-state analysis is secure, even in the asymmetric setting—since the sending of a given photon number n given the Poisson distribution $P(n|\mu) = \mathrm{e}^{-\mu}\frac{\mu^n}{n!}$ is a Markov process, i.e. memoryless process, Eve has no way of telling which intensity setting the photon number state came from, therefore using asymmetric intensities does not affect the estimation of yields for photon number states $p_{ZZ}(k_c,\,k_d|n_A,\,n_B)$.

Therefore, overall, we conclude that neither asymmetric channel losses, nor asymmetric intensities Alice and Bob use (for signal states or decoy states), will affect the security of the protocol. Asymmetry will only affect the performance of the protocol (which will be the subject of discussion in the next section)—asymmetric channels

will result in higher QBER and subsequently lower key rate, and asymmetric intensities can compensate for channel asymmetry and enable high key rate for the protocol even when channels are highly asymmetric.

4. Performance

In this section we will discuss how channel asymmetry, and asymmetric intensities, can affect the performance of TF-QKD.

4.1. Channel model

We will first discuss the channel model in the asymmetric case. Again, we extend the expressions in the appendix of [9], and consider asymmetric intensities and channel transmittances.

To obtain the secure key rate, three sets of observables are needed: the X basis gain $p_{XX}(k_c, k_d)$, the X basis bit-error rate $e_{XX}(k_c, k_d)$, and the Z basis gain $p_{ZZ}(k_c, k_d|\beta_A, \beta_B)$ (for all combinations of $\{\beta_A, \beta_B\}$).

Now, let us suppose Alice and Bob send signals with intensities s_A, s_B, and channels between Alice/Bob and Charles have transmittances η_A, η_B. For simplicity we can write:

$$\begin{aligned}\gamma_A &= s_A\eta_A\\ \gamma_B &= s_B\eta_B\end{aligned} \tag{13}$$

for signal states, and

$$\begin{aligned}\gamma'_A &= \mu^i_A\eta_A\\ \gamma'_B &= \mu^j_B\eta_B\end{aligned} \tag{14}$$

for decoy states, where μ^i_A and μ^j_B are selected from the set of decoy intensities.

The other imperfections in the channel include the dark count rate p_d, the polarization misalignment between Alice and Bob θ, and the phase mismatch ϕ between Alice and Bob. If we first do not consider dark counts and phase mismatch, the intensities arriving at the detectors C and D at Charles can be written as (similar to the discussions in [19]):

$$\begin{aligned}D_c &= \frac{1}{2}(\gamma_A + \gamma_B - 2\sqrt{\gamma_A\gamma_B}\cos\theta)\\ D_d &= \frac{1}{2}(\gamma_A + \gamma_B + 2\sqrt{\gamma_A\gamma_B}\cos\theta)\end{aligned} \tag{15}$$

the probability that one detector clicks and the other does not (e.g. C clicks and D does not) can be written as

$$(1 - \mathrm{e}^{-D_c})\mathrm{e}^{-D_d} = \mathrm{e}^{-D_d} - \mathrm{e}^{-(D_c+D_d)} = \mathrm{e}^{-\frac{1}{2}[\gamma_A+\gamma_B+2\sqrt{\gamma_A\gamma_B}\cos\theta]} - \mathrm{e}^{-(\gamma_A+\gamma_B)}. \tag{16}$$

Including the phase mismatch and dark counts, we can write the X basis gain and QBER in a similar form as [9]:

$$\begin{aligned}p_{XX}(k_c, k_d) = \frac{1}{2}(1 - p_d)(\mathrm{e}^{-\sqrt{\gamma_A\gamma_B}\cos\phi\cos\theta} + \mathrm{e}^{\sqrt{\gamma_A\gamma_B}\cos\phi\cos\theta})\\ \times \mathrm{e}^{-\frac{1}{2}(\gamma_A+\gamma_B)} - (1 - p_d)^2\mathrm{e}^{-(\gamma_A+\gamma_B)}\end{aligned} \tag{17}$$

$$e_{XX}(k_c, k_d) = \frac{\mathrm{e}^{-\sqrt{\gamma_A\gamma_B}\cos\phi\cos\theta} - (1-p_d)\mathrm{e}^{-\frac{1}{2}(\gamma_A+\gamma_B)}}{\mathrm{e}^{-\sqrt{\gamma_A\gamma_B}\cos\phi\cos\theta} + \mathrm{e}^{\sqrt{\gamma_A\gamma_B}\cos\phi\cos\theta} - 2(1-p_d)\mathrm{e}^{-\frac{1}{2}(\gamma_A+\gamma_B)}} \tag{18}$$

and the Z basis gain is the integral over all possible (random) relative phases:

$$p_{ZZ}(k_c, k_d|\beta_A, \beta_B) = (1 - p_d)[\mathrm{e}^{-\frac{1}{2}(\gamma'_A+\gamma'_B)}I_0(\sqrt{\gamma'_A\gamma'_B}\cos\theta) - \mathrm{e}^{-(\gamma'_A+\gamma'_B)}] + p_d(1 - p_d)\mathrm{e}^{-(\gamma'_A+\gamma'_B)}, \tag{19}$$

where $I_0(x)$ is a modified Bessel function of the first kind.

The Z basis gain can be used in decoy-state analysis to obtain m, n photon yields $p_{ZZ}(k_c, k_d|n_A, n_B)$. Here for simplicity we first consider the infinite-decoy case, where $p_{ZZ}(k_c, k_d|n_A, n_B)$ can be assumed to be perfectly known (similar to supplementary information equations (18), (19) in [9] but with asymmetric channel transmittances):

$$p_{ZZ}(k_c, k_d|n_A, n_B) = (1 - p_d)q_{ZZ}(k_c, k_d|n_A, n_B) + (1 - p_d)p_d(1 - \eta_A)^{n_A}(1 - \eta_B)^{n_B}, \tag{20}$$

where

$$q_{ZZ}(k_c,\,k_d|n_A,\,n_B)=\sum_{k=0}^{n_A}\binom{n_A}{k}\sum_{l=0}^{n_B}\binom{n_B}{l}\frac{\eta_A^k\eta_B^l(1-\eta_A)^{n_A-k}(1-\eta_B)^{n_B-l}}{2^{k+l}k!l!}\sum_{m=0}^{k}\binom{k}{m}\sum_{p=0}^{l}\binom{l}{p}\sum_{q=\max(0,m+p-l)}^{\min(k,m+p)}\binom{k}{q}\binom{l}{m+p-q}(m+p)!(k+l-m-p)!\cos^{m+q}(\theta_A)\cos^{m+p-q}(\theta_B)\sin^{2k-m-q}(\theta_A)\sin^{2l-m-2p+q}(\theta_B)-(1-\eta_A)^{n_A}(1-\eta_B)^{n_B}. \tag{21}$$

In the case with finite decoys (e.g. 3 decoy states for each of Alice and Bob), we can use linear programming to upper-bound the yields, which is described in more detail in appendix.

Afterwards, the phase-error rate can be upper-bounded using these yields:

$$p_{XX}(k_c,\,k_d)e_{ZZ}(k_c,\,k_d)\leqslant\sum_{i=0,1}\left[\sum_{n_A,n_B=0}^{\infty}c_{n_A}^{A,(i)}c_{n_B}^{B,(i)}\sqrt{p_{ZZ}(k_c,\,k_d|n_A,\,n_B)}\right]^2. \tag{22}$$

With the the X basis gain $p_{XX}(k_c, k_d)$, the X basis bit-error rate $e_{XX}(k_c, k_d)$, and the phase-error rate $e_{ZZ}(k_c, k_d)$, we can obtain the final secure key rate:

$$R_{k_ck_d}=p_{XX}(k_c,\,k_d)\times[1-h_2(e_{XX}(k_c,\,k_d))-h_2(e_{ZZ}(k_c,\,k_d))], \tag{23}$$

where $h_2(x)=-x\log_2(x)-(1-x)\log_2(1-x)$ is the binary entropy function.

4.2. Effect of channel and intensity asymmetry on gain and QBER

In the estimation of key rate, only three sets of observables are used: the X basis gain $p_{XX}(k_c, k_d)$, the X basis bit-error rate $e_{XX}(k_c, k_d)$, and the set of Z basis gain for each combination of decoy intensities $p_{ZZ}(k_c,\,k_d|\beta_A,\,\beta_B)$. Here we note that, the X basis gain and Z basis gain do not explicitly depend on the symmetry of incoming signal strengths γ_A/γ_B, and only the X basis QBER is affected by γ_A/γ_B.

For simplicity, here let us consider the second-order approximation for the Bessel function and exponential function, and for now ignore the phase mismatch and dark count rate:

$$I_0(x)=1+\frac{1}{4}x^2+O(x^4)$$
$$e^x=1+x+\frac{1}{2}x^2+O(x^3). \tag{24}$$

We can then rewrite the X basis gain as:

$$p_{XX}(k_c,\,k_d)=\frac{1}{2}(\mathrm{e}^{-\sqrt{\gamma_A\gamma_B}\cos\theta}+\mathrm{e}^{\sqrt{\gamma_A\gamma_B}\cos\phi\cos\theta})\times\mathrm{e}^{-\frac{1}{2}(\gamma_A+\gamma_B)}-\mathrm{e}^{-(\gamma_A+\gamma_B)}$$
$$\approx\frac{1}{2}(\gamma_A+\gamma_B)-\frac{1}{8}[3\gamma_A^2+3\gamma_B^2+(2+4e_d)\gamma_A\gamma_B] \tag{25}$$

and the Z basis gain as:

$$p_{ZZ}(k_c,\,k_d|\beta_A,\,\beta_B)=\mathrm{e}^{-\frac{1}{2}(\gamma'_A+\gamma'_B)}I_0(\sqrt{\gamma'_A\gamma'_B}\,\cos\theta)-\mathrm{e}^{-(\gamma'_A+\gamma'_B)}$$
$$\approx\frac{1}{2}(\gamma'_A+\gamma'_B)-\frac{1}{8}[3\gamma'^2_A+3\gamma'^2_B+(4+2e_d)\gamma'_A\gamma'_B], \tag{26}$$

where the terms higher than second order are omitted, and θ is the total polarization misalignment angle between Alice and Bob satisfying $\theta=2\sin^{-1}(\sqrt{e_d})$ (suppose Alice–Charles and Bob–Charles each has misalignment error e_d, but with misalignment angles in different directions). We can see that, the gain in both X and Z basis is dominated by the term $\frac{1}{2}(\gamma_A+\gamma_B)=\frac{1}{2}(s_A\eta_A+s_B\eta_B)$ or $\frac{1}{2}(\gamma'_A+\gamma'_B)=\frac{1}{2}(\mu_A^i\eta_A+\mu_B^j\eta_B)$, i.e. taking first-order approximation:

$$p_{XX}(k_c,\,k_d)\approx\frac{1}{2}(\gamma_A+\gamma_B)$$
$$p_{ZZ}(k_c,\,k_d|\beta_A,\,\beta_B)\approx\frac{1}{2}(\gamma'_A+\gamma'_B) \tag{27}$$

which means that the gain scales with the *average* of arriving intensities through Alice's and Bob's channels—this is different from MDI-QKD, where the gain only contains the second-order terms γ_A^2, γ_B^2, $\gamma_A\gamma_B$. We can also see that the gain does not depend on the asymmetry of arriving intensities, e.g. γ_A/γ_B.

On the other hand, the QBER in X basis depends on the balance of arriving intensities:

$$e_{XX}(k_c, k_d) = \frac{e^{-\sqrt{\gamma_A\gamma_B}\cos\phi\cos\theta} - (1-p_d)e^{-\frac{1}{2}(\gamma_A+\gamma_B)}}{e^{-\sqrt{\gamma_A\gamma_B}\cos\phi\cos\theta} + e^{\sqrt{\gamma_A\gamma_B}\cos\phi\cos\theta} - 2(1-p_d)e^{-\frac{1}{2}(\gamma_A+\gamma_B)}} \approx \frac{\frac{1}{2}(\gamma_A+\gamma_B) - \sqrt{\gamma_A\gamma_B}\cos\theta + \frac{1}{2}\gamma_A\gamma_B\cos^2\theta - \frac{1}{8}(\gamma_A+\gamma_B)^2}{(\gamma_A+\gamma_B) + \gamma_A\gamma_B\cos^2\theta - \frac{1}{4}(\gamma_A+\gamma_B)^2} \tag{28}$$

which, in the first-order approximation[5], can be simplified as:

$$e_{XX}(k_c, k_d) \approx \frac{\frac{1}{2}(\gamma_A+\gamma_B) - \sqrt{\gamma_A\gamma_B}\cos\theta}{\gamma_A+\gamma_B} = \frac{\frac{1}{2}(\frac{\gamma_A}{\gamma_B}+1) - \sqrt{\frac{\gamma_A}{\gamma_B}}\cos\theta}{\frac{\gamma_A}{\gamma_B}+1}. \tag{29}$$

We can see that here the X basis QBER does depend on asymmetry—more precisely, it depends on how much the arriving intensities at Charles, $\gamma_A = \eta_A s_A$ and $\gamma_B = \eta_B s_B$ are balanced. This is understandable physically, since the X basis key generation depends on single-photon interference and relies on the indistinguishability of incoming signals. This means that, in the case that channels are not symmetric, compensating for the channel asymmetry with different signal intensities for Alice and Bob and aiming for $\eta_A s_A = \eta_B s_B$ can help minimize the X basis QBER.

On the other hand, in the Z basis, the bit-error rate (i.e. the X basis phase-error rate) cannot be directly measured, but is instead upper-bounded using the observable gain data from the decoy states. As we mentioned above, the Z basis gain (in the first-order approximation) scales with $\frac{1}{2}(\gamma'_A + \gamma'_B) = \frac{1}{2}(\mu_A^i\eta_A + \mu_B^i\eta_B)$ and does not depend on the symmetry between incoming intensities. Moreover, the yields $p_{ZZ}(k_c, k_d|n_A, n_B)$ are estimated using linear programming. For instance, for three decoys where Alice and Bob respectively use $\{\mu_A, \nu_A, \omega_A\}$, $\{\mu_B, \nu_B, \omega_B\}$ as their decoy states, there are nine sets of observable gains, $\{Q_{\mu\mu}, Q_{\mu\nu}, Q_{\mu\omega}, Q_{\nu\mu}, Q_{\nu\nu}, Q_{\nu\omega}, Q_{\omega\mu}, Q_{\omega\nu}, Q_{\omega\omega}\}$, each of which constitutes a constraint for the linear program that helps bound the yields $p_{ZZ}(k_c, k_d|n_A, n_B)$. Such a structure makes the linear program relatively robust against asymmetry in the decoy states, and the linear program can fairly accurately upper-bound the yields as long as the intensities are of reasonable values (i.e. $\mu_A \neq \nu_A$, $\mu_B \neq \nu_B$, and none of the intensities are too large e.g. > 1).

The phase error rate, as shown in equation (17), is based on a linear combination of the square root of the yields. It is therefore also very little affected by asymmetry, and almost always reaches a good value (at least in the infinite-data case) so long as the intensities are within reasonable range, regardless of the asymmetries in channel transmittances or decoy intensities.

We plot the QBER in the X and the Z bases versus asymmetry in arriving intensities (e.g. $s_A\eta_A/s_B\eta_B$ or $\mu_A\eta_A/\mu_B\eta_B$) in figure 2. As can be seen, the X basis QBER depends heavily on asymmetry and is minimal when $s_A\eta_A/s_B\eta_B = 1$, while the upper-bounded Z basis QBER (i.e. phase-error rate) is hardly affected by asymmetry.

Therefore, a viable strategy for TF-QKD in asymmetric channels is to compensate for the channel asymmetry with signal intensities $\{s_A, s_B\}$ only, while the decoy intensities $\{\mu_A, \nu_A, \omega_A\}$, $\{\mu_B, \nu_B, \omega_B\}$ can be still kept symmetric. However, note that the signal intensities not only determines (1) X basis QBER, it also affects (2) X basis gain (which determines the raw key generation rate, and favors large s_A, s_B), as well as (3) upper-bound of phase error rate (since the cat states are determined by signal intensities, and the estimation favors small s_A, s_B—typically < 0.1—for a tighter upper bound on phase error rate). Criteria (1)–(3) cannot be simultaneously satisfied, therefore an optimization for $\{s_A, s_B\}$ is required for highest key rate.

Interestingly, we can compare this with the case of MDI-QKD. As described in [15], the 4-intensity protocol (and 7-intensity protocol in the extended asymmetric case) has decoupled X and Z bases, where Z basis is used for key generation and X basis uses decoy states to estimation phase-error rate. In MDI-QKD, the X basis data depends on two-photon interference and requires balanced arriving intensities (or else the X basis QBER will increase dramatically), while the Z basis does not require indistinguishability of the signals, and is therefore insensitive to channel asymmetry. In MDI-QKD, all the X basis decoy states should satisfy e.g. $\mu_A\eta_A = \mu_B\eta_B$, while the signal states s_A, s_B can be chosen to simply optimize key generation rate. (Due to misalignment, there is a slight dependence of Z basis QBER to asymmetry too, hence optimal s_A, s_B are still not equal, but this is a much weaker dependence on symmetry than in the X basis, and optimal s_A/s_B is much closer to 1 than η_B/η_A in MDI-QKD.)

[5] The first order approximation for $e_{XX}(k_d, k_d)$ assumes that γ_A, γ_B are much smaller than 1—which is reasonable, since to get a good phase-error rate estimation, usually s_A, s_B are smaller or equal to 0.1, and for positions of interest where TF-QKD beats PLOB bound, the loss in each channel is usually larger than 10 dB, which means that η_A and η_B are much smaller than 1 too—for instance 10 dB channel loss corresponds to 0.1 transmittance.

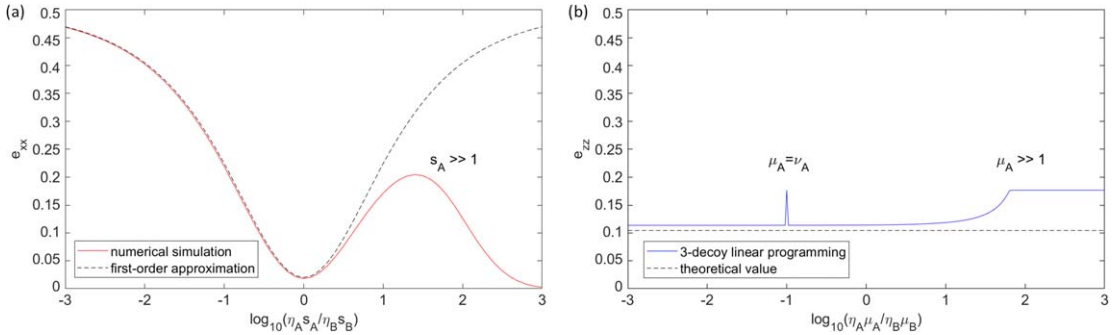

Figure 2. QBER versus asymmetry in arriving intensities at Charles, in the X and Z bases. Here we consider $k_c,\ k_d = 0,\ 1$, while the other case of $k_c, k_d = 1,0$ has exactly the same values. Both plots use parameters $\eta_A = \eta_B = 1$ (as well as detector efficiency 100%) and assume misalignment of 2% from Alice and Bob each, and no dark counts or phase mismatch. (a) We plot the X basis QBER (acquired from full expression in equation (14)) as well as its first-order approximation (acquired from equation (24)). Here we vary s_A while keeping $s_B = 0.1$ to test different levels of asymmetry. As can be seen, the X basis QBER heavily depends on the symmetry between arriving intensities $s_A\eta_A$ and $s_B\eta_B$. Physically, this is because key generation depends on single-photon interference and therefore requires indistinguishability of incoming signals. When $\eta_B/\eta_A \neq 1$, X basis QBER will increase drastically if intensities are symmetric, while one can adjust s_A/s_B such that $s_A/s_B = \eta_B/\eta_A$ to obtain minimal X basis QBER (Note that first-order deviation no longer works for $s_A \gg 1$—in this case, the majority of the detection events are double counts and are discarded, despite that the actual e_{xx} is lower among the single detections (approaching zero as s_A increases)—but generally the phase error rate estimation requires low signal intensities, and such high s_A will not return positive key rate anyway, so this region will not be of interest to us.). (b) We plot the Z basis bit-error rate (i.e. X basis phase-error rate) obtained from linear programming using data from 3 decoy states. Here we set $\nu_A = \nu_B = 0.01$, $\omega_A = \omega_B = 0$, and signal states $s_A = s_B = 0.1$. We fix $\mu_B = 0.1$ and vary s_A to test asymmetry. As can be seen, the upper-bounded phase error rate depends very little on the asymmetry between $\mu_A\eta_A$ and $\mu_B\eta_B$, and the linear program can effectively bound the error rate—in fact rather close to the theoretical value obtained with infinite-decoys—as long as μ_A, μ_B are of reasonable values (With two exceptions: when $\mu_A = \nu_A$, or $\mu_A \gg 1$, the constraints from observable data containing μ_A cannot provide any useful information, and the linear program has to use the data from one less decoy state, which is why the e_{zz} is higher for these two extreme cases.). The physical intuition is clear too: the yields are estimated by linear programming, which usually has redundant information (in the 9 cross terms $Q_{\mu_i\mu_j}$ where Alice and Bob each uses one of their three decoys) and is insensitive to asymmetry, and the phase-error rate (equation (17)) is a linear combination of the yields, which makes it insensitive to asymmetry just like the yields.

While our approach works both for MDI-QKD and TF-QKD, a key difference is that states that compensate for channel asymmetry are the signal states in TF-QKD (while this responsibility lies on decoy states in MDI-QKD), which are also involved in key generation and phase error estimation. This means that in TF-QKD, it is more difficult to simultaneously keep a low X basis QBER and a good key generation rate and low phase error rate. Perhaps due to this reason, the advantage of asymmetric-intensity protocols is somewhat less pronounced in TF-QKD—nonetheless, it still provides about an order of magnitude higher key rate than completely symmetric protocols and still 2–3 times higher key rate than adding fibre—which means that it still is the strategy that provides highest key rate when channels are asymmetric.

5. Numerical results

In this section we use the technique described above—to compensate for channel asymmetry simply with different s_A, s_B for Alice and Bob. We first compare our method with prior art techniques and study the numerically optimized intensities for the asymptotic (infinite-decoy, infinite-data) case. Then, we also show that our method works with finite decoys and also finite data size.

We plot the simulation results for asymptotic TF-QKD in figure 3. As can be seen, for the two cases where channel mismatch $x = \eta_A/\eta_B = 0.1$ and $\eta_A/\eta_B = 0.01$, our method consistently have much higher key rate than TF-QKD with symmetric intensities. Interestingly, we show that adding fibre can help users obtain higher key rate, but it comes with the additional inconvenience of having to physically modify the channel, and also it still has lower key rate than our method of simply adjusting signal intensities.

We also plot the ratio of optimal signal intensities in figure 4. As we have predicted, the optimal signal intensities are rather close to the relation of $s_A\eta_A = s_B\eta_B$, in order to maintain a lower X basis QBER. However, as we discussed, since signal states are also involved in key generation and phase error rate estimation (based on the imaginary cat states), they prevent the signal states from taking the values that minimize QBER (but rather, makes it choose the value that maximizes the overall key rate).

Additionally, we also plot our results for the practical case with finite number of decoys (here we use three decoys each for Alice and Bob: $\{\mu_A, \nu_A, \omega_A\}$, $\{\mu_B, \nu_B, \omega_B\}$) and finite data size. The upper-bounding of photon number yields using linear programming, as well as the finite-key analysis, are both described in more detail in appendix. We can see that similar result holds—our method has an advantage over either using symmetric intensities directly or adding fibre. More interestingly, we include both the case where we only allow s_A, s_B to be

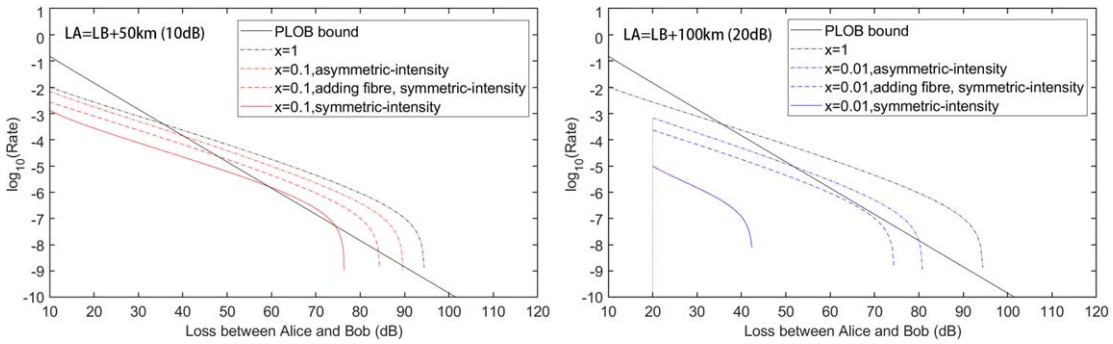

Figure 3. Key rate versus loss between Alice and Bob, for protocol with symmetric intensities ($s_A = s_B$), symmetric intensities with fibre added until channels are equal, and asymmetric intensities (s_A, s_B fully optimized). The PLOB [2] linear bound is included for comparison. The channel mismatch x is fixed at $x = \eta_A/\eta_B = 0.1$ (left) and $\eta_A/\eta_B = 0.01$ (right), i.e. Alice–Charles always has 10 dB (20 dB) higher loss than Bob–Charles. Note that the right plot starts from 20 dB of total distance (which is the case where Bob–Charles loss is 0dB and Alice–Charles loss is 20 dB). The dark count rate is set to 10^{-8}, misalignment is 2% for Alice and Bob each, and detector efficiency is incorporated into channel loss. As can be seen, allowing the use of asymmetric intensities greatly improves key rate when channels are asymmetric, and compared with a symmetric protocol, it can consistently provide approximately one order of magnitude higher key rate when there is a 10 dB channel mismatch, and two orders of magnitude when there is a 20 dB mismatch, for most distances. Interestingly, adding fibre can improve the key rate considerably too—but it still has lower key rate than the asymmetric-intensity protocol (the latter has about 2–3 times higher key rate), and has the additional inconvenience of having to modify the physical channel.

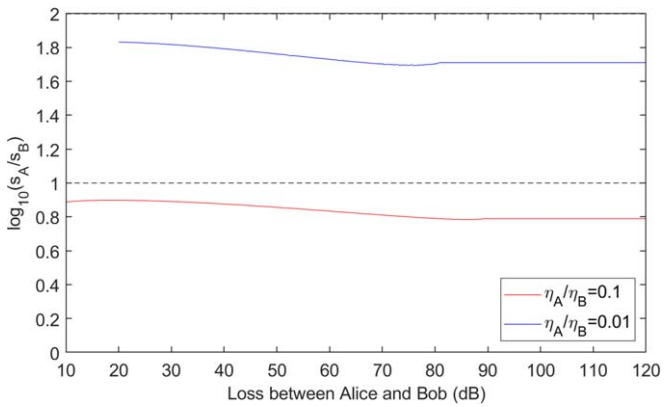

Figure 4. Ratio of optimal intensities $\log_{10}(s_A/s_B)$ over loss between Alice and Bob. Here we test two cases where the channel mismatch $x = \eta_A/\eta_B = 0.1$ and $\eta_A/\eta_B = 0.01$. As can be seen, s_A/s_B is rather close to η_B/η_A (here respectively 10^1 and 10^2). However, due to signal states being involved in key generation and phase-error rate estimation too, it slightly deviates from the value that minimizes X basis QBER (and instead takes the value that maximizes key rate).

asymmetric, versus the case where all intensities and probabilities can be optimized, and as shown in the plot, we see that using asymmetric signal intensities alone is sufficient to compensate for channel asymmetry.

6. Conclusion

In this paper we present a simple method to obtain good performance for TF-QKD even if channels are asymmetric. We present a theoretical understanding of why signal states (and not decoy states) should be adjusted to compensate for asymmetry, and we also show that the method is still compatible with existing security proofs. With our method, there is no need to add additional fibre, and Alice and Bob can implement the method in software-only. This provides great convenience for TF-QKD in practice—where realistic channels might likely be asymmetric—and can also be used in quantum networks (where adding fibre for each pair of users is impractical) where a central service-provider can easily optimize the intensities for each pair of users.

Acknowledgments

This work was supported by the Natural Sciences and Engineering Research Council of Canada (NSERC), U.S. Office of Naval Research (ONR). Computations were performed on the Niagara supercomputer at the SciNet

HPC Consortium. SciNet is funded by: the Canada Foundation for Innovation; the Government of Ontario; Ontario Research Fund—Research Excellence; and the University of Toronto.

We thank Koji Azuma for providing the corrected security proof [18] that incorporates mixed states after the measurement.

Note added

We note that, during the preparation of the current manuscript, it came into our knowledge that another work on asymmetric TF-QKD is under preparation [20], which is independently completed from this work. Our works are posted simultaneously on the preprint server [20, 21].

Appendix. Numerically estimating photon-number yields with linear programs

In this section we briefly describe the linear programming approach we used to estimate the upper bounds for the photon-number yields $p_{ZZ}(k_c, k_d|n_A, n_B)$—which for simplicity here we will denote as Y_{nm}—which is the probability to obtain a set of detection events k_c, k_d given that Alice and Bob respectively sent n_A, n_B (or, n, m) photons. Such an approach has been widely discussed in literature as in [22–24], and is also described in the simple TF-QKD proof paper [9]. We also used a similar linear programming approach for some of the results in [15] appendix E, but it was not described in detail in that paper.

For simplicity, in this section we denote the observable gain in Z basis $p_{ZZ}(k_c, k_d|\beta_A, \beta_B)$ as Q_{μ_i,μ_j} where $\mu_i = \beta_A^2$ and $\mu_j = \beta_B^2$, and k_c, k_d are omitted (since the same expressions hold true for $k_c, k_d = (0, 1)$ or $k_c, k_d = (1, 0)$, and we can substitute the observable data for each k_c, k_d respectively to obtain the corresponding $p_{ZZ}(k_c, k_d|n_A, n_B)$). Also, as mentioned above, we denote the yields $p_{ZZ}(k_c, k_d|n_A, n_B)$ as Y_{nm}.

A.1. Linear program model

Following [4], the yields Y_{nm} where Alice sends n photons and Bob sends m photons, satisfy the constraints:

$$\sum_n \sum_m P_n^{\mu_i} P_m^{\mu_j} Y_{nm} = Q^Z_{\mu_i\mu_j}, \tag{A.1}$$

where the photon number distributions are Poissonian:

$$P_n^{\mu_i} = \mathrm{e}^{\mu_i} \frac{\mu_i^n}{n!}$$
$$P_m^{\mu_j} = \mathrm{e}^{\mu_j} \frac{\mu_j^m}{m!}. \tag{A.2}$$

Here, the right-hand-side constants $Q^Z_{\mu_i\mu_j}$ are the 'observables', i.e. the gain and error-gain respectively for the intensity combination μ_i, μ_j (which can be any intensity among the set of decoy intensities). For the case of 3-decoys each for Alice and Bob, equation (A.1) corresponds to 9 sets of constraints. Using equation (A.1) as linear constraints, and $\{Y_{nm}\}$ as variables, we can apply linear programming, to maximize or minimize any linear combination of any of the variables (called an objective function)—for instance, here we can run the linear program multiple times, each time acquiring the upper bound for a given Y_{nm} where (n, m) can be $(0, 0)$, $(2, 0)$, $(0, 2)$, $(1, 1)$, $(2, 2)$.

Note that, since there are infinitely many photon number states, to solve the linear program on an actual computer, we have to perform a cut-off and discard higher-order terms with large photon number. In practice we choose $S_{\mathrm{cut}} = 10$, such that a term is only discarded when both $n \geqslant 10$ and $m \geqslant 10$. For the discarded terms, we can either set them to zero (for lower bounds) or 1 (for upper bounds).

$$\sum_n \sum_m P_n^{\mu_i} P_m^{\mu_j} Y_{nm} \geqslant \sum_{n<10} \sum_{m<10} P_n^{\mu_i} P_m^{\mu_j} Y_{nm}$$
$$\sum_n \sum_m P_n^{\mu_i} P_m^{\mu_j} Y_{nm} \leqslant \sum_{n<10} \sum_{m<10} P_n^{\mu_i} P_m^{\mu_j} Y_{nm} + \left(1 - \sum_{n<10} \sum_{m<10} P_n^{\mu_i} P_m^{\mu_j}\right). \tag{A.3}$$

Therefore, in practice, the linear constraints can be written as:

$$Q^Z_{\mu_i\mu_j} - \left(1 - \sum_{n<10} \sum_{m<10} P_n^{\mu_i} P_m^{\mu_j}\right) \leqslant \sum_{n<10} \sum_{m<10} P_n^{\mu_i} P_m^{\mu_j} Y_{nm} \leqslant Q^Z_{\mu_i\mu_j} \tag{A.4}$$

with the additional constraint on variables:

$$0 \leqslant Y_{nm} \leqslant 1. \tag{A.5}$$

The linear program is run multiple times, each time maximizing a given Y_{mn}, where (n, m) can be (0, 0), (2, 0), (0, 2), (1, 1), (2, 2).

A.2. Finite-size effects

In this section we consider finite-size effects for the privacy amplification process. Because of the statistical fluctuations, the observables (gains) we obtain in the Z basis might deviate from their respective expected values, which will lie within a certain 'confidence interval' around the observed values. Here we will perform a standard error analysis, similar to that in [15, 22, 25], which is meant to be a straightforward estimation of the performance of TF-QKD under asymmetry and with practical data size, but not as a rigorous proof for composable security.

Consider a random variable, whose observed value is n, we can bound its expected value $\langle n \rangle$ with the upper and lower bounds

$$\underline{n} = n - \gamma\sqrt{n} \leqslant \langle n \rangle \leqslant n + \gamma\sqrt{n} = \overline{n} \tag{A.6}$$

with a confidence (success probability) of $\mathrm{erf}(\gamma/\sqrt{2})$, where γ is the number of standard deviations the confidence interval lies above and below the observed value, and erf is the error function. In the simulations we consider a security failure probability of $\epsilon = 10^{-7}$, which means we should set $\gamma \approx 5.3$.

In the Z basis, let us denote the observed counts for a given intensity setting $\{\mu_i, \mu_j\}$ as $n^Z_{\mu_i,\mu_j}$, which satisfies

$$n^Z_{\mu_i,\mu_j} = Q^Z_{\mu_i,\mu_j} \times (NP_{\mu_i}P_{\mu_j}), \tag{A.7}$$

where N is the total number of signals sent and P_{μ_i}, P_{μ_j} are the probabilities for Alice and Bob to respectively choose intensities μ_i and μ_j. By applying equation (A.6), we can acquire the upper and lower bounds to $Q^Z_{\mu_i,\mu_j}$:

$$\begin{aligned}\overline{Q^Z_{\mu_i\mu_j}} &= Q^Z_{\mu_i\mu_j} + \gamma\sqrt{\frac{Q^Z_{\mu_i\mu_j}}{NP_{\mu_i}P_{\mu_j}}} \\ \underline{Q^Z_{\mu_i\mu_j}} &= Q^Z_{\mu_i\mu_j} - \gamma\sqrt{\frac{Q^Z_{\mu_i\mu_j}}{NP_{\mu_i}P_{\mu_j}}}.\end{aligned} \tag{A.8}$$

Then, we can substitute them into the upper and lower bounds in the linear program when estimating Y_{nm}:

$$\underline{Q^Z_{\mu_i\mu_j}} - \left(1 - \sum_{n<10}\sum_{m<10} P^{\mu_i}_n P^{\mu_j}_m\right) \leqslant \sum_{n<10}\sum_{m<10} P^{\mu_i}_n P^{\mu_j}_m Y_{nm} \leqslant \overline{Q^Z_{\mu_i\mu_j}} \tag{A.9}$$

which loosens the bounds and will result in a slightly higher upper bound for Y_{nm} (which is understandable, since we expect lower key rate with finite-size effect considered). Similar linear programs for finite-size decoy-state have also been considered in [23].

Note that, although here we only consider a standard error analysis, in principle our results in this paper is applicable to e.g. composable security using Chernoff's bound [24]. The key point is, the dependence on channel asymmetry, and the compensation for asymmetry using intensities, are only relevant in the X basis (signal states). The asymptotic case (with infinite decoys, where only signal states are relevant) therefore defines the fundamental scaling of key rate versus asymmetric channels, and all types of finite size analysis on the decoy states (e.g. using standard error analysis, using Chernoff's bound [24], or adding a 'joint bounds' analysis to tighten the bounds on statistical fluctuation and obtain a higher key rate [25], versus not considering finite-size effects at all and assuming the asymptotic key rate [3, 7–10], i.e. assuming expected values of the gain and QBER to be identical to observed values in experiment) can be viewed of as correction terms (imperfections) on the yields and the key rate in the asymptotic limit. Our method is only related to the signal states and their intensities in the X basis, and is in principle always applicable regardless of the type of decoy state analysis (e.g. number of decoys) and the finite-size analysis used, as long as the Z basis is decoupled from the X basis.

With finite-size effect considered, the optimizable parameters for TF-QKD now include

$$[s_A, \mu_A, \nu_A, P_{s_A}, P_{\mu_A}, P_{\nu_A}, s_B, \mu_B, \nu_B, P_{s_B}, P_{\mu_B}, P_{\nu_B}], \tag{A.10}$$

where the implicit parameters are ω_A, ω_B (which for simplicity we assume to be zero), and $P_{\omega_A} = 1 - P_{s_A} - P_{\mu_A} - P_{\nu_A}$ and similarly $P_{\omega_B} = 1 - P_{s_B} - P_{\mu_B} - P_{\nu_B}$, and the choice of signal states s_A, s_B versus the decoy states automatically implies basis choice, too. The above parameters are optimized using the same coordinate descent algorithm as described in [15]. In figure A1, the dot-dash line (fully asymmetric) optimizes all 12 parameters, while the dashed line (signal-only asymmetric) optimizes only 7 parameters (where all

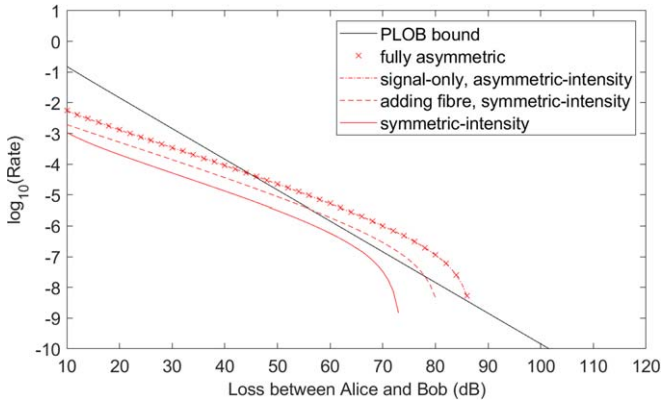

Figure A1. Key rate versus loss between Alice and Bob, for protocol with symmetric intensities and probabilities, with symmetric intensities and fibre added until channels are equal, with only asymmetric signal intensities (while all other parameters are symmetric between Alice and Bob), and with fully optimized parameters (all intensities and probabilities are freely optimized). The PLOB [2] linear bound is included for comparison. Here we consider 10^{-8} dark count rate, a 2% misalignment for Alice and Bob each, $N = 10^{12}$ total pulses sent, and channel mismatch of $x = \eta_A/\eta_B = 0.1$. Again, detector efficiency is incorporated into channel loss. As we can see, similar to the asymptotic case, using asymmetric intensities can greatly improve the key rate. Perhaps more interestingly, we can see that allowing asymmetry in signal intensities alone is sufficient in obtaining a good key rate through asymmetric channels (its key rate almost entirely overlaps with the fully optimized case).

parameters except s_A, s_B are identical for Alice and Bob):

$$[s_A,\ \mu,\ \nu,\ P_s,\ P_\mu,\ P_\nu,\ s_B,\ \mu,\ \nu,\ P_s,\ P_\mu,\ P_\nu]. \tag{A.11}$$

Performing coordinate descent on key rate versus parameters while estimating the yields with linear programming is rather CPU-intensive. We have used a 40-core (80-thread) machine (a single compute node in the Niagara supercomputer [26], each node with dual 20-core Intel Skylake CPUs) to generate figure A1, where the OpenMP multithreading library is used to parallelize the coordinate descent algorithm (to accelerate the search along each coordinate). The details of the algorithm can be found in [15, 22]. Also, we used Gurobi [27], a commercial linear program solver, to solve the linear programming models. Linear programs sometimes introduce multiple maxima, which means a local search on parameters sometimes might get trapped in a local maximum. To alleviate this, we can start a local search from multiple random starting points, and pick the largest search result, which can be viewed of as a form of global search. (In principle, we can permutate the search results and perform multiple iterations of random search using e.g. an evolution algorithm [28], but here using one iteration with multiple random starting points is usually sufficient in finding a good key rate.)

References

[1] Takeoka M, Guha S and Wilde M 2014 Fundamental rate-loss tradeoff for optical quantum key distribution *Nat. Commun.* **5** 5235
[2] Pirandola S, Laurenza R, Ottaviani C and Banchi L 2017 Fundamental limits of repeaterless quantum communications *Nat. Commun.* **8** 15043
[3] Lucamarini M, Yuan Z L, Dynes J F and Shields A J 2018 Overcoming the rate-distance limit of quantum key distribution without quantum repeaters *Nature* **557** 400
[4] Lo H K, Curty M and Qi B 2012 Measurement-device-independent quantum key distribution *Phys. Rev. Lett.* **108** 130503
[5] Xu F, Ma X, Zhang Q, Lo H K and Pan J W 2019 Quantum cryptography with realistic devices arXiv:1903.09051
[6] Tamaki K, Lo H K, Wang W and Lucamarini M 2018 Information theoretic security of quantum key distribution overcoming the repeaterless secret key capacity bound arXiv:1805.05511
[7] Ma X F, Zeng P and Zhou H 2018 Phase-matching quantum key distribution *Phys. Rev.* X **8** 031043
[8] Wang X B, Yu Z W and Hu X L 2018 Twin-field quantum key distribution with large misalignment error *Phys. Rev.* A **98** 062323
[9] Curty M, Azuma K and Lo H K 2019 Simple security proof of twin-field type quantum key distribution protocol *npj Quantum Inf.* **5** 1–6
[10] Lin J and Lütkenhaus N 2018 Simple security analysis of phase-matching measurement-device-independent quantum key distribution *Phys. Rev.* A **98** 042332
[11] Zhong X, Hu J, Curty M, Qian L and Lo H K 2019 Proof-of-principle experimental demonstration of twin-field type quantum key distribution *Phys. Rev. Lett.* **123** 100506
[12] Liu Y *et al* 2019 Experimental twin-field quantum key distribution through sending or not sending *Phys. Rev. Lett.* **123** 100505
[13] Miner M, Pittaluga M, Roberts G L, Lucamarini M, Dynes J F, Yuan Z L and Shields A J 2019 Experimental quantum key distribution beyond the repeaterless secret key capacity *Nat. Photon.* **13** 334
[14] Wang S *et al* 2019 Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system *Phys. Rev.* X **9** 021046
[15] Wang W, Xu F and Lo H K 2019 Asymmetric protocols for scalable high-rate measurement-device-independent quantum key distribution networks *Phys. Rev.* X **9** 041012
[16] Liu H *et al* 2019 Experimental demonstration of high-rate measurement-device-independent quantum key distribution over asymmetric channels *Phys. Rev. Lett.* **122** 160501

[17] Zhou X Y, Zhang C H, Zhang C M and Wang Q 2019 Asymmetric sending or not-sending twin-field quantum key distribution in practice *Phys. Rev.* A **99** 062316
[18] Azuma K 2019 private communications
[19] Xu F, Curty M, Qi B and Lo H K 2013 Practical aspects of measurement-device-independent quantum key distribution *New J. Phys.* **15** 113007
[20] Grasselli F, Navarrete A and Curty M 2019 Asymmetric twin-field quantum key distribution arXiv:1907.05256
[21] Wang W and Lo H K 2019 Simple method for asymmetric twin field quantum key distribution arXiv:1907.05291
[22] Xu F, Xu H and Lo H K 2014 Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution *Phys. Rev.* A **89** 052333
[23] Ma X, Fung C H F and Razavi M 2012 Statistical fluctuation analysis for measurement-device-independent quantum key distribution *Phys. Rev.* A **86** 052305
[24] Curty M, Xu F, Lim C C W, Tamaki K and Lo H K 2014 Finite-key analysis for measurement-device-independent quantum key distribution *Nat. Commun.* **5** 3732
[25] Zhou Y H, Yu Z W and Wang X B 2016 Making the decoy-state measurement-device-independent quantum key distribution practically useful *Phys. Rev.* A **93** 042324
[26] Loken C *et al* 2010 *J. Phys.: Conf. Ser.* **256** 012026
[27] OPTIMIZATION, GUROBI INC. 2019 Gurobi Optimization LLC 2019 Gurobi optimizer reference manual http://gurobi.com
[28] Storn R and Price K 1997 Differential evolution-a simple and efficient heuristic for global optimization over continuous spaces *J. Glob. Optim.* **11** 341–59