Measurement-device-independent quantum key distribution with uncharacterized qubit sources

Zhen-Qiang Yin,[1] Chi-Hang Fred Fung,[2,*] Xiongfeng Ma,[3,†] Chun-Mei Zhang,[1] Hong-Wei Li,[1] Wei Chen,[1,‡] Shuang Wang,[1,§] Guang-Can Guo,[1] and Zheng-Fu Han[1,¶]

[1]*Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, China and Synergetic Innovation Center of Quantum Information & Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China*

[2]*Department of Physics and Center of Theoretical and Computational Physics, University of Hong Kong, Pokfulam Road, Hong Kong*

[3]*Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing, China*

(Received 24 September 2013; published 18 December 2013)

Measurement-device-independent quantum key distribution (MDIQKD) is proposed to be secure against any possible detection attacks. The security of the original proposal relies on the assumption that the legitimate users can fully characterize the encoding systems including sources. Here, we propose a MDIQKD protocol where we allow uncharacterized encoding systems as long as qubit sources are used. A security proof of the MDIQKD protocol is presented that does not need the knowledge of the encoding states. Simulation results show that the scheme is practical.

DOI: 10.1103/PhysRevA.88.062322 PACS number(s): 03.67.Dd

I. INTRODUCTION

Quantum key distribution (QKD) [1,2] allows two distant parties (Alice and Bob) to share secret key bits. In the most commonly implemented QKD protocol, BB84 [1], Alice randomly encodes her qubits into one of the four quantum states $|0\rangle$, $|1\rangle$, $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, and $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$, where $|0\rangle$ and $|1\rangle$ represent the two eigenstates in the Z basis and $|+\rangle$ and $|-\rangle$ represent the two eigenstates in the X basis, respectively. Then, she transmits photons to Bob through a quantum channel which may be controlled by an eavesdropper, Eve. A key can be generated by postprocessing the measurement results [3–5]. The security of BB84 can be proved by considering the equivalence between BB84 and an entanglement distillation protocol (EDP). Many other QKD protocols are also proven to be secure with similar techniques [6–8]. Meanwhile, tremendous progress in experimental QKD has also been achieved in the past decade [9–18]. For a review of the subject, one can refer to Ref. [19] and references therein.

Despite the proven security in theory, Eve may still be able to crack practical QKD systems by exploiting imperfections in actual implementations. Quantum hacking strategies, taking advantage of practical loopholes, were studied in recent years, such as fake-state attack [20,21], time-shift attack [22,23], phase-remapping attack [24,25], detector-blinding attack [26,27], and unambiguous state discrimination (USD) attack [28]. In order to close all possible loopholes existing in practical QKD systems, device-independent (DI) QKD [29,30] protocols have been proposed, whose security does not rely on the details of implementation devices but on the violation of Bell's inequalities or other nonlocality tests. The security is only built on a few reasonable assumptions such as having good random numbers and trusted user operation systems. Unfortunately, DIQKD requires very high detection efficiency and low channel loss to yield secure keys. A recent DIQKD scheme with local Bell test [31] overcomes the channel loss limitation and extends the achievable distance to 17 km using current experimental parameters. However, this is still a short distance for practical interest and, so far, no DIQKD experiment has been demonstrated.

A close examination on hacking strategies indicates that most loopholes exist in the detection part of QKD systems [20–23,26,27]. Along this line, QKD protocols against detection loopholes are proposed [32,33]. Like DIQKD, unfortunately, these protocols still require high performance of implementation devices. In 2012, Lo *et al.* presented their seminal work, measurement-device-independent QKD (MDIQKD) [34], which is practical and is immune to all possible detector side channel attacks (see also Ref. [35]). Recently, a few experimental demonstrations of MDIQKD have been performed [36–39]. Secret key generation with MDIQKD over a distance of 50 km has been shown [38], which is significantly longer than the achievable distance of DIQKD.

In MDIQKD, Alice and Bob each sends their encoded qubits to a measurement unit (MU), controlled by an untrusted party Eve, who might collaborate with Eve, to perform a Bell-state measurement (BSM). A secure key can be established between Alice and Bob given Eve's announcements of the BSM results. The disadvantage of the original MDIQKD in comparison to DIQKD is that the security of MDIQKD relies on the assumption that Alice and Bob are able to characterize their encoding systems. For qubit sources, ideal four BB84 encoding states $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$ are assumed. For coherent-state sources, the decoy-state method is assumed [40–42]. In practice, such requirements might not be strictly satisfied. For example, two imperfect encoding systems could be misaligned. In this work, we remove the security assumption that Alice and Bob must characterize their encoding states for MDIQKD. We show that by modifying the original MDIQKD and using qubit sources, one can use uncharacterized encoding systems. When Alice (Bob) selects to output a state with index x (y), her (his) encoding device emits a mixed-qubit state $\rho_{A,x}$ ($\rho_{B,y}$) to Eve. In our framework, the initial joint state with

*chffung@hku.hk
†xma@tsinghua.edu.cn
‡kooky@mail.ustc.edu.cn
§wshuang@ustc.edu.cn
¶zfhan@ustc.edu.cn

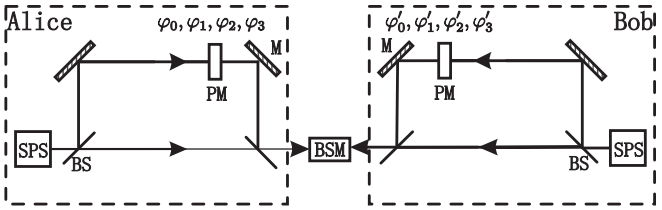

FIG. 1. A schematic diagram for the QMDIQKD protocol. SPS: single-photon source; BS: beam splitter; M: mirror; PM: phase modulator; BSM: Bell-state measurement, which is an untrusted device and may be controlled by Eve; φ_0, φ_1, φ_2, φ_3 (φ_0', φ_1', φ_2', φ_3') represent Alice's (Bob's) four encoding choices.

Eve's system is

$$\rho_{\mathrm{A},x} \otimes \rho_{\mathrm{B},y} \otimes \rho_{\mathrm{E}} \quad \text{for all } x, y,$$

where Eve's state ρ_{E} is independent of x and y. This excludes the case of a joint encoding device where the state is $\rho_{\mathrm{AB},x,y} \otimes \rho_{\mathrm{E}}$ and the case of hidden classical variables (unknown to Alice and Bob but known to Eve). The latter case is often considered as "black boxes" in DIQKD papers [29,30], and the state is $\sum_\lambda p(\lambda)\rho^\lambda_{\mathrm{A},x} \otimes \rho^\lambda_{\mathrm{B},y} \otimes \rho^\lambda_{\mathrm{E}}$, in which $p(\lambda)$ represents the probability distribution of the hidden variable λ. Similarly, the case of preshared entanglements with Eve is excluded in our framework. Therefore, our encoding devices emit mixed-qubit states, which are uncharacterized to Alice and Bob. Eve may learn about the encoding states by only performing quantum operations on them. There are no other means for her to obtain information. The additional requirement of devices we put here is that the BSM is able to identify at least two of the four Bell states. Denote the modified protocol as qubit-MDIQKD (QMDIQKD). The QMDIQKD protocol may be particularly relevant to the situation that Alice and Bob can make sure their encoding states are two dimensional (i.e., the phase encoding system) while they do not trust the accuracy of their phase modulators.

The rest of the paper is organized as follows. In Sec. II, we present the QMDIQKD protocol with qubit sources, whose security is proven in Sec. III for the case of pure-state sources. The security of the general (mixed-) qubit source case is given in Sec. IV. In Sec. V, we present simulation results of the QMDIQKD protocol, comparing to the original one. Finally, we conclude in Sec. VI with discussions.

II. MODIFIED MDIQKD PROTOCOL

Similar to the original MDIQKD, Alice and Bob have symmetric encoding systems in the QMDIQKD protocol. They send their encoded qubits to Eve for BSM, as shown in Fig. 1. Here, without loss of generality, we assume a phase encoding scheme is used. Alice (Bob) can choose different phases φ_0, φ_1, φ_2, φ_3 (φ_0', φ_1', φ_2', φ_3') to perform the encoding step. Then, Eve performs a BSM on the incoming states and announces results to Alice and Bob.

We plan to analyze its security with the EDP method [4,5], which is widely used for security proofs of QKD. The essence of this method is to convert the QMDIQKD protocol into an equivalent EDP, then obtain the relation between the phase-error rate and the bit-error rate, which can be estimated in experiments. In this section, we give the equivalent EDP version of QMDIQKD and focus on a description where the encoding states are pure (extension to the mixed-state description is trivial):

(1) Alice and Bob prepare N pairs of entangled states,

$$|\phi^+\rangle_{\mathrm{AC}} = |0\rangle_A|\varphi_0\rangle_C + |1\rangle_A|\varphi_1\rangle_C + |2\rangle_A|\varphi_2\rangle_C + |3\rangle_A|\varphi_3\rangle_C,$$
$$|\phi^+\rangle_{\mathrm{BD}} = |0\rangle_B|\varphi_0'\rangle_D + |1\rangle_B|\varphi_1'\rangle_D + |2\rangle_B|\varphi_2'\rangle_D + |3\rangle_B|\varphi_3'\rangle_D, \tag{1}$$

respectively, where normalization factors are omitted. Subscripts A and B denote Alice's and Bob's classical key bits, respectively, of which values 0 and 1 represent encodings in basis 0, and values 2 and 3 represent encodings in basis 1. The states $|\varphi_x\rangle_C$ and $|\varphi_x'\rangle_D$ ($x = 0,1,2,3$) are Alice's and Bob's uncharacterized encoding states, respectively, to be sent to the MU and in general they are not orthogonal to each other. Alice and Bob ensure that $|\varphi_x\rangle_C$ and $|\varphi_x'\rangle_D$ are fixed pure states in a two-dimensional Hilbert (qubit) space but do not know the details. Later, we will extend the results to general mixed-qubit systems. Here, we describe Alice and Bob's encoding systems in an equivalent measurement-based way. By measuring her only half of the system, Alice collapses the system C to one of $|\varphi_i\rangle_C$ with $i = 0,1,2,3$ with equal probabilities, which is equivalent to saying that Alice prepares the system C into four states with equal probabilities. The same argument holds for Bob. Hence, Eq. (1) shows a mathematical equivalent description of Alice's and Bob's encoding systems.

(2) Alice and Bob send the states, labeled by C and D, respectively, to Eve who announces her BSM result. There are three possible outcomes: BSM failure; a successful measurement result in either of the Bell states

$$|\phi^+\rangle_{\mathrm{CD}} = (|0\rangle_C|0\rangle_D + |1\rangle_C|1\rangle_D)/\sqrt{2}, \tag{2}$$

$$|\psi^+\rangle_{\mathrm{CD}} = (|0\rangle_C|1\rangle_D + |1\rangle_C|0\rangle_D)/\sqrt{2}. \tag{3}$$

One must note that Eve might not honestly announce her measurement results. The beauty of MDIQKD [34] is that the security does not depend on whether the measurement results are faithfully obtained by Alice and Bob. Another important point is that it is enough to assume that the MU only needs to identify one of the Bell states in the original MDIQKD, whereas in the QMDIQKD, at least two Bell states need to be distinguished.

(3) After receiving Eve's message, Alice and Bob perform bit sift: discarding bits when Eve announces failed BSM ($z = 0$). Then, they project systems A and B in Eq. (1) onto $|0\rangle\langle 0| + |1\rangle\langle 1|, |2\rangle\langle 2| + |3\rangle\langle 3|$, which correspond to bases 0 and 1, respectively. Then, they perform basis sift: discarding bits when their systems collapse into different bases. By sacrificing certain bits for error testing,[1] they can then deduce a conditional probability distribution $p(z|x,y)$ [where $z = 0,1,2$ stands for Eve's announcements] failure, Eqs. (2) or (3), respectively; x and y ($x,y \in \{0,1,2,3\}$) represent the states of systems A and B.

(4) Finally, Alice and Bob perform EDP to systems A and B and obtain maximally entangled Bell states

[1] An alternative way to do that is by performing error verification after error correction [43,44].

TABLE I. List of conditional probabilities $p(z|x,y)$ for the case where Alice and Bob choose four BB84 states with equal probabilities. Only the cases where they choose the same basis are considered. No loss is considered.

z \ x,y	0,0	0,1	1,0	1,1	2,2	2,3	3,2	3,3
0	1/2	1/2	1/2	1/2	0	1	1	0
1	1/2	0	0	1/2	1/2	0	0	1/2
2	0	1/2	1/2	0	1/2	0	0	1/2

$|\phi^{+\theta}\rangle_{AB} = (|0\rangle_A|0\rangle_B + e^{i\theta}|1\rangle_A|1\rangle_B)/\sqrt{2}$, where secure-key bits can be extracted.

Let us first take a look at the original MDIQKD case where Alice and Bob each sends four BB84 states with equal probabilities. The conditional probabilities of the measurement result by a lossless MU are listed in Table I, from where one can see that there is a 50% intrinsic loss for the original MDIQKD scheme when two Bell states can be distinguished. In the case of $xy = 01,10$ and $z = 2$, a bit flip is operated on either Alice's or Bob's side.

In step 2, it is crucial in the QMDIQKD protocol to assume that the MU can distinguish at least two Bell states. In the following, we will show that the MDIQKD protocol using the uncharacterized qubit encoding system is insecure if only one Bell state can be measured by the MU, or $z \in \{0,1\}$. In this case, the row of $z = 2$ in Table I will be emerged to the one of $z = 0$. Now, let us consider the following two scenarios.

(1) Alice's and Bob's encoding systems emit four perfect BB84 states. Then, in the bit-sift procedure, Alice and Bob will discard the cases of $z = 0$ and 2 as listed in Table I. Thus, the key bits remain only when Alice and Bob send out the same states.

(2) Alice and Bob's encoding systems emit states from a set of two orthogonal states $|0\rangle$ and $|1\rangle$ regardless of their basis choices. Obviously, no secure key can be generated from this case since Eve can simply perform a projection measurement on the qubits sent out by Alice and Bob to get the full information.

From Alice's and Bob's points of view, they can not distinguish above two scenarios from their observed results. Thus, such a scheme is not secure. It is not hard to verify that the same conclusion holds when the MU projects onto any other Bell state instead of Eq. (2).

Moreover, note that not any two of Bell states will work for the QMDIQKD protocol. From the attack mentioned above, one can see that it is critical for a joint state of Alice and Bob to be able to yield two Bell-state measurement results when they choose the same basis. Table II shows such possibilities for each case of x,y and four Bell states. One can see that neither the pair $|00+11\rangle$ and $|01-10\rangle$ nor the pair $|01+10\rangle$ and $|00-11\rangle$ can be used for the QMDIQKD protocol.

III. SECURITY AGAINST COLLECTIVE ATTACKS AND KEY-RATE LOWER BOUND: PURE-STATE CASE

Following the similar argument used in Ref. [5], we design an EDP that is equivalent to the QMDIQKD protocol. Given that the initial states of Alice's, Bob's, and Eve's ancillas are

TABLE II. The relation between the states depending on x,y values and four Bell states: ✓ means there is overlap between the state xy and the corresponding Bell states, while × means the two states are orthogonal.

x,y \ Bell state	$\|00+11\rangle$	$\|01-10\rangle$	$\|01+10\rangle$	$\|00-11\rangle$
0,0	✓	×	×	✓
1,1	✓	×	×	✓
0,1	×	✓	✓	×
1,0	×	✓	✓	×
2,2	✓	×	✓	×
3,3	✓	×	✓	×
2,3	×	✓	×	✓
3,2	×	✓	×	✓

separable, we first define Eve's collective attack by a unitary transformation:

$$\begin{aligned} &U_{\mathrm{Eve}}|\varphi_x\rangle_C|\varphi'_y\rangle_D|e\rangle_{\mathrm{Ea}}|0\rangle_M \\ &\quad = \sqrt{p(0|x,y)}|\Gamma_{xy0}\rangle_E|0\rangle_M + \sqrt{p(1|x,y)}|\Gamma_{xy1}\rangle_E|1\rangle_M \\ &\qquad + \sqrt{p(2|x,y)}|\Gamma_{xy2}\rangle_E|2\rangle_M, \end{aligned} \tag{4}$$

where $x,y = \{0,1,2,3\}$, $|e\rangle_{\mathrm{Ea}}$ is Eve's arbitrary ancilla, $|0\rangle_M$ is the message which will be sent to Alice and Bob, and $|\Gamma_{xy0}\rangle_E$, $|\Gamma_{xy1}\rangle_E$, and $|\Gamma_{xy2}\rangle_E$ are all normalized Eve's arbitrary quantum states for Eve's ancilla and photons C, D. Here, we emphasize that our collective attack modeled by Eq. (4) has taken the basis-independent attack and basis-dependent attack [45] into account. The basis-independent attack is a situation where the density matrix of the states transmitted in the channel when Alice's and Bob's bases choices are both 0 is the same as the case of basis 1. The basis-dependent attack is a situation where the two density matrices are different. The basis dependence can be measured by fidelity. In general, for basis-dependent attacks, Eve may obtain basis information through certain measurements and then adopt different operations accordingly. Any measurement that Eve may utilize to learn the basis and the followup operations can be seen as part of an extended unitary transformation on Alice's and Bob's encoding states and her ancilla given by Eq. (4).

A. Example: General four-dimensional case

Before proceeding, we first prove that when two-dimensional photon pairs C and D are general four-dimensional quantum states $|\varphi_{xy}\rangle_{\mathrm{CD}}$, the protocol will not be secure. Generally, we assume when Alice's input is x and Bob's input is y, the state is $|\varphi_{xy}\rangle_{\mathrm{CD}}$. Let us consider a counterexample, where

$$\begin{aligned} \langle\varphi_{00}|\varphi_{11}\rangle_{\mathrm{CD}} &= 0, \\ \langle\varphi_{00}|\varphi_{01}\rangle_{\mathrm{CD}} &= -1/\sqrt{2}, \\ |\varphi_{01}\rangle_{\mathrm{CD}} &= |\varphi_{10}\rangle_{\mathrm{CD}}, \\ |\varphi_{22}\rangle_{\mathrm{CD}} = |\varphi_{33}\rangle_{\mathrm{CD}} &= |\varphi_{00}\rangle_{\mathrm{CD}} + |\varphi_{01}\rangle_{\mathrm{CD}}, \\ |\varphi_{23}\rangle_{\mathrm{CD}} &= |\varphi_{32}\rangle_{\mathrm{CD}}, \end{aligned} \tag{5}$$

TABLE III. QMDIQKD: probability table for bases 0 and 1 for a particular joint sender.

z \ x,y	0,0	0,1	1,0	1,1	2,2	2,3	3,2	3,3
0	1/2	1/2	1/2	1/2	0	1	1	0
1	1/2	0	0	1/2	1/2	0	0	1/2
2	0	1/2	1/2	0	1/2	0	0	1/2

$$\langle\varphi_{23}|\varphi_{00}\rangle_{\mathrm{CD}} = \langle\varphi_{23}|\varphi_{11}\rangle_{\mathrm{CD}} = \langle\varphi_{23}|\varphi_{01}\rangle_{\mathrm{CD}} = \langle\varphi_{23}|\varphi_{22}\rangle_{\mathrm{CD}} = 0.$$

Obviously, the above states are defined in a four-dimensional Hilbert space. Define a conditional probability $p(z|x,y)$ to be the probability for the BSM's result z conditioned on the values set by Alice and Bob, x,y. In the case without eavesdropping, Alice and Bob will verify that their conditional probabilities $p(z|x,y)$ are as shown in Table III. These conditional probabilities can be satisfied by the following attack strategy:

$$\begin{aligned}
U_{\mathrm{Eve}}|\varphi_{xy}\rangle_{\mathrm{CD}}|0\rangle_{\mathrm{Ea}}|0\rangle_M &= (|\Gamma_{xy0}\rangle_E|0\rangle_M + |\Gamma_{xy1}\rangle_E|1\rangle_M)/\sqrt{2} \\
&\quad \text{when } x=y=0 \text{ or } x=y=1, \\
U_{\mathrm{Eve}}|\varphi_{xy}\rangle_{\mathrm{CD}}|0\rangle_{\mathrm{Ea}}|0\rangle_M &= (|\Gamma_{xy0}\rangle_E|0\rangle_M + |\Gamma_{xy2}\rangle_E|2\rangle_M)/\sqrt{2} \\
&\quad \text{when } x=1,y=0 \text{ or } x=0,y=1, \\
U_{\mathrm{Eve}}|\varphi_{23}\rangle_{\mathrm{CD}}|0\rangle_{\mathrm{Ea}}|0\rangle_M &= |\Gamma_{230}\rangle_E|0\rangle_M, \\
|\Gamma_{000}\rangle_E &= -|\Gamma_{010}\rangle_E.
\end{aligned}$$

When Alice and Bob declare their basis choices, Eve can know all key values in basis 0 since $|\Gamma_{001}\rangle_E$ and $|\Gamma_{111}\rangle_E$ can be orthogonal. One can verify that the same probability tables are obtained when the senders of Alice and Bob emit perfect BB84 states without any channel error. Therefore, it is not possible for Alice and Bob to distinguish whether their senders transmit genuine BB84 states (in which security can hold) or this set of general four-dimensional quantum states $|\varphi_{xy}\rangle_{\mathrm{CD}}$ (in which security can not hold). Thus, to avoid this case, we restrict $|\varphi_{xy}\rangle_{\mathrm{CD}} = |\varphi_x\rangle_C|\varphi'_y\rangle_D$. Before discussing the general case, we first give a simple example for the case that Alice and Bob observe a set of specific probabilities $p(z|x,y)$.

B. Example: Ideal case

Let us prove the security of the QMDIQKD protocol by considering an ideal case where no disturbance is allowed in the quantum channels. In this case, Alice and Bob would find that $p(0|0,0) = p(1|0,0) = p(0|1,1) = p(1|1,1) = p(0|0,1) = p(2|0,1) = p(0|1,0) = p(2|1,0) = p(1|2,2) = p(2|2,2) = p(1|3,3) = p(2|3,3) = 1/2$, and $p(0|2,3) = p(0|3,2) = 1$. Then, from Eve's collective attack (described by U_{Eve}) point of view, she needs to satisfy the following conditions:

$$\begin{aligned}
&U_{\mathrm{Eve}}|\varphi_0\rangle_C|\varphi'_0\rangle_D|e\rangle_{\mathrm{Ea}}|0\rangle_M \\
&\quad = \frac{1}{\sqrt{2}}|\Gamma_{000}\rangle_E|0\rangle_M + \frac{1}{\sqrt{2}}|\Gamma_{001}\rangle_E|1\rangle_M, \\
&U_{\mathrm{Eve}}|\varphi_1\rangle_C|\varphi'_1\rangle_D|e\rangle_{\mathrm{Ea}}|0\rangle_M \\
&\quad = \frac{1}{\sqrt{2}}|\Gamma_{110}\rangle_E|0\rangle_M + \frac{1}{\sqrt{2}}|\Gamma_{111}\rangle_E|1\rangle_M, \\
&U_{\mathrm{Eve}}|\varphi_0\rangle_C|\varphi'_1\rangle_D|e\rangle_{\mathrm{Ea}}|0\rangle_M \\
&\quad = \frac{1}{\sqrt{2}}|\Gamma_{010}\rangle_E|0\rangle_M + \frac{1}{\sqrt{2}}|\Gamma_{012}\rangle_E|2\rangle_M, \\
&U_{\mathrm{Eve}}|\varphi_1\rangle_C|\varphi'_0\rangle_D|e\rangle_{\mathrm{Ea}}|0\rangle_M \\
&\quad = \frac{1}{\sqrt{2}}|\Gamma_{100}\rangle_E|0\rangle_M + \frac{1}{\sqrt{2}}|\Gamma_{102}\rangle_E|2\rangle_M
\end{aligned} \tag{6}$$

when Alice and Bob prepare the 0 basis, and

$$\begin{aligned}
&U_{\mathrm{Eve}}|\varphi_2\rangle_C|\varphi'_2\rangle_D|e\rangle_{\mathrm{Ea}}|0\rangle_M \\
&\quad = \frac{1}{\sqrt{2}}|\Gamma_{221}\rangle_E|1\rangle_M + \frac{1}{\sqrt{2}}|\Gamma_{222}\rangle_E|2\rangle_M, \\
&U_{\mathrm{Eve}}|\varphi_3\rangle_C|\varphi'_3\rangle_D|e\rangle_{\mathrm{Ea}}|0\rangle_M \\
&\quad = \frac{1}{\sqrt{2}}|\Gamma_{331}\rangle_E|1\rangle_M + \frac{1}{\sqrt{2}}|\Gamma_{332}\rangle_E|2\rangle_M, \\
&U_{\mathrm{Eve}}|\varphi_2\rangle_C|\varphi'_3\rangle_D|e\rangle_{\mathrm{Ea}}|0\rangle_M = |\Gamma_{230}\rangle_E|0\rangle_M, \\
&U_{\mathrm{Eve}}|\varphi_3\rangle_C|\varphi'_2\rangle_D|e\rangle_{\mathrm{Ea}}|0\rangle_M = |\Gamma_{320}\rangle_E|0\rangle_M
\end{aligned} \tag{7}$$

when Alice and Bob prepare the 1 basis. This definition is just a special case of Eq. (4). We again assume that Alice and Bob do not know the details of $|\varphi_x\rangle_C$ and $|\varphi'_y\rangle_D$ $(x,y = 0,1,2,3)$. Recall that $|\varphi_x\rangle_C$ and $|\varphi'_y\rangle_D$ are both in the two-dimensional Hilbert space and they are disjoint $(|\varphi_{xy}\rangle_{\mathrm{CD}} = |\varphi_x\rangle_C|\varphi'_y\rangle_D)$ (see previous Sec. III A), and we may arbitrarily assign a phase to each of them. Thus,

$$\begin{aligned}
|\varphi_2\rangle_C &= C_{20}|\varphi_0\rangle_C + C_{21}|\varphi_1\rangle_C, \\
|\varphi_3\rangle_C &= C_{30}|\varphi_0\rangle_C + C_{31}e^{i\theta}|\varphi_1\rangle_C, \\
|\varphi'_2\rangle_D &= C'_{20}|\varphi'_0\rangle_D + C'_{21}|\varphi'_1\rangle_D, \\
|\varphi'_3\rangle_D &= C'_{30}|\varphi'_0\rangle_D + C'_{31}e^{i\theta'}|\varphi'_1\rangle_D
\end{aligned} \tag{8}$$

must hold for some complex numbers C_{xy} and C'_{xy}. By considering that $|\varphi_0\rangle_C$ and $|\varphi_1\rangle_C$ can have some trivial overall phases, we can assume C_{20} and C_{21} are both non-negative real numbers. Next, by omitting the trivial overall phase of $|\varphi_3\rangle_C$, we can simply assume that C_{30} and C_{31} are also non-negative real numbers. In the same way, C'_{xy} are also non-negative real numbers. Substitute Eqs. (6) to the last two equations of (7), and we obtain

$$\begin{aligned}
C_{30}C'_{20}|\Gamma_{001}\rangle_E + C_{31}C'_{21}e^{i\theta}|\Gamma_{111}\rangle_E &= 0, \\
C_{30}C'_{21}|\Gamma_{012}\rangle_E + C_{31}C'_{20}e^{i\theta}|\Gamma_{102}\rangle_E &= 0, \\
C_{20}C'_{30}|\Gamma_{001}\rangle_E + C_{21}C'_{31}e^{i\theta'}|\Gamma_{111}\rangle_E &= 0, \\
C_{20}C'_{31}|\Gamma_{012}\rangle_E + C_{21}C'_{30}e^{-i\theta'}|\Gamma_{102}\rangle_E &= 0.
\end{aligned} \tag{9}$$

From the above equation, one can verify that if any one of $\{C_{xy}, C'_{xy}|x = 2,3, y = 0,1\}$ equals to 0, Eq. (7) and the normalized conditions of $|\varphi_2\rangle_C$, $|\varphi'_2\rangle_D$, $|\varphi_3\rangle_C$, $|\varphi'_3\rangle_D$ can not be all satisfied. Hence, $C_{xy} \neq 0$, $C'_{xy} \neq 0$, and furthermore we have

$$|\Gamma_{001}\rangle_E + e^{i\theta}|\Gamma_{111}\rangle_E = 0. \tag{10}$$

Obviously, Eq. (10) makes sure that Eve has no information on Alice's and Bob's bits in basis 0 when Eve announces the message $|1\rangle_M$. Therefore, the above-observed probabilities can promise Alice and Bob to share secure-key bits even when their encoding states are not characterized. In other words, we have proven the security of the QMDIQKD protocol in the case of no error and no loss.

C. Proof: General pure-qubit case

To begin our analysis, without loss of generality, we can assume in Eq. (4) $|\Gamma_{xyz}\rangle_E = \sum_n \gamma_{xyzn}|n\rangle_E$, in which $|n\rangle_E$ are a set of normalized orthogonal bases of Eve's states, and complex number $\gamma_{xyzn} =_E \langle n|\Gamma_{xyz}\rangle_E$, satisfying $\sum_n |\gamma_{xyzn}|^2 = 1$. Thus, we can give the density matrix for the case that Alice and Bob both select basis 0:

$$\begin{aligned}\rho = {} & \frac{1}{p(1|0,0)+p(1|1,1)+p(1|0,1)+p(1|1,0)} \\ & \times \sum_n P\{\sqrt{p(1|0,0)}\gamma_{001n}|0\rangle_A|0\rangle_B \\ & + \sqrt{p(1|1,1)}\gamma_{111n}|1\rangle_A|1\rangle_B + \sqrt{p(1|0,1)}\gamma_{011n}|0\rangle_A|1\rangle_B \\ & + \sqrt{p(1|1,0)}\gamma_{101n}|1\rangle_A|0\rangle_B\}, \end{aligned} \tag{11}$$

in which $P\{|x\rangle\} = |x\rangle\langle x|$. The aim of this EDP is to obtain perfect Bell states $|\phi^{-\theta}\rangle_{\mathrm{AB}} = (|0\rangle_A|0\rangle_B - e^{-i\theta}|1\rangle_A|1\rangle_B)/\sqrt{2}$. Accordingly, we can define the bit-error rate e_b and phase-error rate e_p under basis 0:

$$e_b = {}_A\langle 0|_B\langle 1|\rho|1\rangle_B|0\rangle_A + {}_A\langle 1|_B\langle 0|\rho|0\rangle_B|1\rangle_A = \frac{p(1|0,1)+p(1|1,0)}{p(1|0,0)+p(1|1,1)+p(1|0,1)+p(1|1,0)}, \tag{12}$$

$$e_p = {}_{\mathrm{AB}}\langle\phi^{+\theta}|\rho|\phi^{+\theta}\rangle_{\mathrm{AB}} + {}_{\mathrm{AB}}\langle\psi^{+\theta}|\rho|\psi^{+\theta}\rangle_{\mathrm{AB}} \tag{13}$$

$$= \frac{\sum_n |\sqrt{p(1|0,0)}\gamma_{001n} + e^{i\theta}\sqrt{p(1|1,1)}\gamma_{111n}|^2 + \sum_n |e^{i\theta}\sqrt{p(1|0,1)}\gamma_{011n} + \sqrt{p(1|1,0)}\gamma_{101n}|^2}{2[p(1|0,0)+p(1|1,1)+p(1|0,1)+p(1|1,0)]}, \tag{14}$$

in which $|\phi^{+\theta}\rangle_{\mathrm{AB}} = (|0\rangle_A|0\rangle_B + e^{-i\theta}|1\rangle_A|1\rangle_B)/\sqrt{2}$ and $|\psi^{+\theta}\rangle_{\mathrm{AB}} = (e^{-i\theta}|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B)/\sqrt{2}$. The task is to find a way to estimate an effective upper bound of e_p. Before proceeding, we remark that we just focus on the e_p and final key-bits rate for the 0 basis for simplicity, and thus we do not need to calculate the density matrix for the 1 basis. But, the e_p of this 0 basis must be related to some probabilities of the 1 basis, such as $p(1|2,3)$. Now, we begin to detail how to obtain an upper bound of e_p.

We substitute the relations (8) into Eq. (4) to obtain the following constraints:

$$\begin{aligned} & C_{x0}C'_{y0}\sqrt{p(z|0,0)}|\Gamma_{00z}\rangle_E + C_{x0}C'_{y1}e^{ia\theta'}\sqrt{p(z|0,1)}|\Gamma_{01z}\rangle_E + C_{x1}C'_{y0}e^{ib\theta}\sqrt{p(z|1,0)}|\Gamma_{10z}\rangle_E + C_{x1}C'_{y1}e^{i(a\theta'+b\theta)}\sqrt{p(z|1,1)}|\Gamma_{11z}\rangle_E \\ & = \sqrt{p(z|x,y)}|\Gamma_{xyz}\rangle_E, \end{aligned} \tag{15}$$

in which $x,y = \{0,1,2,3\}$, $z = \{0,1,2\}$, $a = 0$ when $y \neq 3$, $a = 1$ when $y = 3$, $b = 0$ when $x \neq 3$, and $b = 1$ when $x = 3$. Considering that $|\Gamma_{xyz}\rangle_E$ can be spanned by a set of basis $|n\rangle_E$ and with Eq. (15), we obtain

$$\begin{aligned} & \sum_n |C_{30}C'_{20}\sqrt{p(1|0,0)}\gamma_{001n} + C_{31}C'_{21}\sqrt{p(1|1,1)}e^{i\theta}\gamma_{111n}|^2 \leqslant [\sqrt{p(1|3,2)} + C_{30}C'_{21}\sqrt{p(1|1,0)} + C_{31}C'_{20}\sqrt{p(1|0,1)}]^2 \triangleq \xi, \\ & \sum_n |C_{30}C'_{21}\sqrt{p(2|0,1)}\gamma_{012n} + C_{31}C'_{20}\sqrt{p(2|1,0)}e^{i\theta}\gamma_{102n}|^2 \leqslant [\sqrt{p(2|3,2)} + C_{30}C'_{20}\sqrt{p(2|0,0)} + C_{31}C'_{21}\sqrt{p(2|1,1)}]^2 \triangleq \zeta. \end{aligned} \tag{16}$$

Note that $|\varphi_x\rangle_C$ must be normalized, and thus we have

$$\begin{aligned} C_{30}^2 + C_{31}^2 + 2C_{30}C_{31}\mathrm{Re}\left(e_C^{i\theta}\langle\varphi_0|\varphi_1\rangle_C\right) = 1, \\ C_{20}'^2 + C_{21}'^2 + 2C'_{20}C'_{21}\mathrm{Re}({}_D\langle\varphi'_0|\varphi'_1\rangle_D) = 1, \end{aligned} \tag{17}$$

where $\mathrm{Re}(x)$ represents the real part of complex number x. From Eq. (4), it is easy to verify that

$$\begin{aligned} \left|\mathrm{Re}\left(e_C^{i\theta}\langle\varphi_0|\varphi_1\rangle_C\right)\right| \leqslant \sqrt{p(0|1,0)p(0|0,0)} + \sqrt{p(1|1,0)p(1|0,0)} + \sqrt{p(2|1,0)p(2|0,0)} \triangleq \chi, \\ |\mathrm{Re}({}_D\langle\varphi'_0|\varphi'_1\rangle_D)| \leqslant \sqrt{p(0|0,1)p(0|0,0)} + \sqrt{p(1|0,1)p(1|0,0)} + \sqrt{p(2|0,1)p(2|0,0)} \triangleq \chi'. \end{aligned} \tag{18}$$

From constraints (16), we also know that

$$\begin{aligned} [C_{30}C'_{20}\sqrt{p(1|0,0)} - C_{31}C'_{21}\sqrt{p(1|1,1)}]^2 \leqslant \xi, \\ [C_{30}C'_{21}\sqrt{p(2|0,1)} - C_{31}C'_{20}\sqrt{p(2|1,0)}]^2 \leqslant \zeta \end{aligned} \tag{19}$$

easily. Assuming that one obtains C_{30}, C_{31}, C'_{20}, and C'_{21} satisfying the above constraints, the only remaining task is to find the maximum of $\sum_n |\sqrt{p(1|0,0)}\gamma_{001n} + \sqrt{p(1|1,1)}e^{i\theta}\gamma_{111n}|^2$. By observing the first inequality of (16) and with the help of triangle

inequality and Cauchy-Schwarz inequality, we have

$$\begin{aligned}
\xi &\geqslant \sum_n [C_{30}C'_{20}|\sqrt{p(1|0,0)}\gamma_{001n} + \sqrt{p(1|1,1)}e^{i\theta}\gamma_{111n}| - |C_{30}C'_{20} - C_{31}C'_{21}|\sqrt{p(1|1,1)}|\gamma_{111n}|]^2 \\
&= C_{30}^2 C_{20}'^2 \sum_n |\sqrt{p(1|0,0)}\gamma_{001n} + e^{i\theta}\sqrt{p(1|1,1)}\gamma_{111n}|^2 + (C_{30}C'_{20} - C_{31}C'_{21})^2 p(1|1,1) \\
&\quad - 2C_{30}C'_{20}|C_{30}C'_{20} - C_{31}C'_{21}|\sqrt{p(1|1,1)}\sum_n |\sqrt{p(1|0,0)}\gamma_{001n} + e^{i\theta}\sqrt{p(1|1,1)}\gamma_{111n}||\gamma_{111n}| \\
&\geqslant C_{30}^2 C_{20}'^2 \sum_n |\sqrt{p(1|0,0)}\gamma_{001n} + \sqrt{p(1|1,1)}e^{i\theta}\gamma_{111n}|^2 + (C_{30}C'_{20} - C_{31}C'_{21})^2 p(1|1,1) \\
&\quad - 2C_{30}C'_{20}|C_{30}C'_{20} - C_{31}C'_{21}|\sqrt{p(1|1,1)}\sqrt{\sum_n |\sqrt{p(1|0,0)}\gamma_{001n} + e^{i\theta}\sqrt{p(1|1,1)}\gamma_{111n}|^2} \\
&= \left(C_{30}C'_{20}\sqrt{\sum_n |\sqrt{p(1|0,0)}\gamma_{001n} + \sqrt{p(1|1,1)}e^{i\theta}\gamma_{111n}|^2} - |C_{30}C'_{20} - C_{31}C'_{21}|\sqrt{p(1|1,1)}\right)^2. \qquad (20)
\end{aligned}$$

Therefore, we obtain

$$\sum_n |\sqrt{p(1|0,0)}\gamma_{001n} + \sqrt{p(1|1,1)}e^{i\theta}\gamma_{111n}|^2 \leqslant \frac{[\sqrt{\xi} + |C_{30}C'_{20} - C_{31}C'_{21}|\sqrt{p(1|1,1)}]^2}{C_{30}^2 C_{20}'^2}. \qquad (21)$$

Furthermore, by the same way, we can obtain that

$$\sum_n |\sqrt{p(1|0,0)}\gamma_{001n} + \sqrt{p(1|1,1)}e^{i\theta}\gamma_{111n}|^2 \leqslant \frac{[\sqrt{\xi} + |C_{30}C'_{20} - C_{31}C'_{21}|\sqrt{p(1|0,0)}]^2}{C_{31}^2 C_{21}'^2}. \qquad (22)$$

Combining constraints (21) and (22), we have

$$\begin{aligned}
&\sum_n |\sqrt{p(1|0,0)}\gamma_{001n} + \sqrt{p(1|1,1)}e^{i\theta}\gamma_{111n}|^2 \\
&\quad \leqslant \min\left\{\max_{C,C'}\left\{\frac{[\sqrt{\xi} + |C_{30}C'_{20} - C_{31}C'_{21}|\sqrt{p(1|1,1)}]^2}{C_{30}^2 C_{20}'^2}\right\}\max_{C,C'}\left\{\frac{[\sqrt{\xi} + |C_{30}C'_{20} - C_{31}C'_{21}|\sqrt{p(1|0,0)}]^2}{C_{31}^2 C_{21}'^2}\right\}\right\} \triangleq \varepsilon, \qquad (23)
\end{aligned}$$

in which $\max_{C,C'}$ means searching over all C_{30}, C_{31}, C'_{20}, and C'_{21} satisfying constraints (17) and (19), and $\max\{a,b\}$ ($\min\{a,b\}$) yields the larger (smaller) one of a and b. Although finding an analytical expression of ε may be difficult, one can get ε with numerical methods. When ε is obtained, the phase-error rate is given by

$$e_p \leqslant \frac{[\sqrt{p(1|0,1)} + \sqrt{p(1|1,0)}]^2 + \varepsilon}{2[p(1|0,0) + p(1|1,1) + p(1|0,1) + p(1|1,0)]}. \qquad (24)$$

One should note that Eq. (24) requires that $C_{30}C'_{20}$ and $C_{31}C'_{21}$ can not be both zero. If the constraints (17) and (19) allow $C_{30}C'_{20}$ and $C_{31}C'_{21}$ to be both zero, e_p can take on an arbitrary value.[2] The secure-key rate is given by

$$R = 1 - H(e_b) - H(e_p), \qquad (25)$$

where $H(x) = -x\ln x - (1-x)\ln(1-x)$ is the Shannon's binary entropy function. Based on this lower bound of the secret key rates, in Sec. V we will show a numerical simulation of real-life QMDIQKD. But before that, we argue in the next section that the secret key rate obtained here for the pure-state case is applicable to the mixed-state case as well.

IV. SECURITY PROOF FOR THE MIXED-STATE CASE

We proved the security of our QMDIQKD scheme when Alice and Bob send pure-qubit states in Sec. III. In this case, the key rate is given by Eq. (25) with e_p bounded by Eq. (24). Here, we prove in the following that the exact same key-rate formula and e_p bound are applicable to the case where Alice and Bob send mixed-qubit states. The proof strategy is to reuse the pure-state results by relying on linearity.

We first purify the mixed states of Alice and Bob in a system F. Then, the entire state of Alice and Bob can be conditional on value i of system F, and we denote it as $\rho_{\mathrm{ABCD},i}$. Note that for each i, Alice's and Bob's states in $\rho_{\mathrm{ABCD},i}$ are pure. The channel by Eve converts the state $\rho_{\mathrm{ABCD},i}$ to a final state in systems A and B as in Eq. (11):

$$\rho_{\mathrm{ABCD},i} \longrightarrow \rho_{\mathrm{AB},i} = \mathcal{E}(\rho_{\mathrm{ABCD},i}),$$

where $\rho_{\mathrm{AB},i}$ is the expression in Eq. (11), and $\mathcal{E}$ represents the channel. For simplicity, we denote $\rho_i = \rho_{\mathrm{ABCD},i}$. We may

[2]This situation can occur when $|\varphi_0\rangle = |\varphi_2\rangle = |0\rangle$ and $|\varphi_1\rangle = |\varphi_3\rangle = |1\rangle$ for both Alice and Bob. In this case, security is obviously impossible, which is consistent with that both $C_{30}C'_{20}$ and $C_{31}C'_{21}$ can be zero.

calculate $e_{p,i}$ as in Eq. (13) for each i of system F, which we denote as follows:

$$e_{p,i} = g'(\rho_{\mathrm{AB},i}),$$

where $g'(\rho)$ is defined as the right-hand side of Eq. (13). Note that g' is linear. Furthermore, g' only depends on the measurement statistics of $\rho_{\mathrm{AB},i}$, denoted as $s_{i,j} = \mathrm{Tr}(O_j \rho_{\mathrm{AB},i})$ for some measurement O_j (e.g., projection onto a Bell state $|\phi^{+\theta}\rangle$). Let $\vec{s}(\rho_{\mathrm{AB},i}) = [s_{i,1}, s_{i,2}, \ldots]$ denote the operation that returns a collection of measurement statistics. Thus, we can express $e_{p,i}$ as a function of the statistics instead:

$$e_{p,i} = g(\vec{s}(\mathcal{E}(\rho_i))), \tag{26}$$

where $g \circ \vec{s} = g'$.

Denote the key rate taking into account privacy amplification only by $R_{\mathrm{PA}}(e_p) = 1 - H(e_p)$.

Remark 1. $R_{\mathrm{PA}}(e_{p,i})$ is a secure-key rate since for each i, Alice's and Bob's states in $\rho_{\mathrm{ABCD},i}$ are pure and thus the key-rate formula and the bound for the phase-error rate in Sec. III apply.

Remark 2. $\sum_i p_i R_{\mathrm{PA}}(e_{p,i})$ is a secure-key rate because Alice and Bob could use the value of system F to compute a key for each i.

Lemma 1. Given that $\sum_i p_i R_{\mathrm{PA}}(e_{p,i})$ is a secure-key rate, $R_{\mathrm{PA}}(\sum_i p_i e_{p,i})$ is a secure-key rate. This corresponds to the case where Alice and Bob do not use the value of system F, and so only the average phase-error rate $\sum_i p_i e_{p,i}$ is used.

Proof. This is true because of the convexity of $R_{\mathrm{PA}}(\ldots)$ in the domain $[0,1/2]$. ∎

Remark 3. We express Eq. (24) in a generic manner:

$$g(\vec{s}) \leqslant f(\vec{s}) \text{ for any collection of measurement statistics } \vec{s}, \tag{27}$$

where $g(\vec{s})$ represents e_p generated by some measurement statistics $\vec{s}$ [cf. Eqs. (26) and (13)] and $f(\vec{s})$ represents the right-hand side of Eq. (24). Note that $\vec{s}$ contains $p(1|0,0)$, $p(1|0,1)$, for example.

Lemma 2. $R_{\mathrm{PA}}(f(\vec{s}(\mathcal{E}(\rho))))$ is a secure-key rate, where $\rho = \sum_i p_i \rho_i$ is the average state obtained by ignoring system F.

Proof. Note that Lemma 1 shows that

$$R_{\mathrm{PA}}\left(\sum_i p_i e_{p,i}\right) \tag{28}$$

is secure. (This corresponds to giving system F to Eve. But this point is not relevant to our current discussion.) Three facts are important: $\mathcal{E}$ is linear, g is linear because g' is linear, and $\vec{s}$ is linear. This means that the parameter in the above equation is

$$\begin{aligned}\sum_i p_i e_{p,i} &= \sum_i p_i g(\vec{s}(\mathcal{E}(\rho_i))) \\ &= g\left(\vec{s}\left(\mathcal{E}\left(\sum_i p_i \rho_i\right)\right)\right) \\ &\leqslant f\left(\vec{s}\left(\mathcal{E}\left(\sum_i p_i \rho_i\right)\right)\right),\end{aligned}$$

where the last line is due to Eq. (27).

Now, note that $R_{\mathrm{PA}}(x)$ is a decreasing function of x, i.e., $R_{\mathrm{PA}}(x) \geqslant R_{\mathrm{PA}}(y)$ for $y \geqslant x$ (in the domain $[0,1/2]$). Thus,

$$R_{\mathrm{PA}}\left(\sum_i p_i e_{p,i}\right) \geqslant R_{\mathrm{PA}}\left(f\left(\vec{s}\left(\mathcal{E}\left(\sum_i p_i \rho_i\right)\right)\right)\right). \tag{29}$$

Since the left-hand side is secure, the right-hand side must represent a secure-key rate when Alice and Bob ignore system F and use only the average state $\rho = \sum_i p_i \rho_i$ which contains the encoding state as a mixed state. ∎

This proves that bounding the phase-error rate by Eq. (24) with Alice and Bob sending mixed-qubit states produces a secure-key rate R_{PA}. For the error-correction part of the key-rate formula $R_{\mathrm{EC}}(e_b) \triangleq -H(e_b)$, it can be easily seen that it is applicable to the mixed-state case as well since e_b is directly measured. Alternatively, the same line of arguments in the above analysis for e_p could be used for e_b as well, showing that R_{EC} is secure. In essence, we have shown that the key rate given by Eq. (25) with e_p bounded by Eq. (24) is applicable to the case where Alice and Bob send mixed-qubit states.

V. SIMULATION

We first consider the case that Alice and Bob use ideal BB84 senders (not trusted by Alice and Bob) and an ideal Bell-state MU to perform QMDIQKD with noise-free channel and no Eve's attack, but with photon absorption taken into account. One must observe that $p(1|2,3) = p(1|0,1) = p(2|0,0) = p(2|1,1) = p(2|2,3) = 0$, then with constraint (16) we deduce that $\xi = \zeta = 0$. Then, through constraints (17) and (19), it is easy to verify that $C_{30} = C_{31} = C'_{20} = C'_{21} \neq 0$. Hence, $\varepsilon = 0$ and then $e_p = 0$. Therefore, in this case, Alice and Bob can share perfect Bell state $|\phi^{-\theta}\rangle_{\mathrm{AB}}$. Furthermore, MDIQKD can be secure in this situation, which fits in well with the example given in Sec. II.

For a general situation, an analytical expression is hard to obtain. However, according to $p(z|x,y)$ which is directly known from experiments, χ can be deduced. Then, all C_{30}, C_{31}, C'_{20}, and C'_{21} satisfying constraints (17) and (19) can be searched, and the maximum of ε can be obtained according to Eq. (23). Finally, an upper bound of e_p can be obtained.

To estimate the performance of QMDIQKD, a numeric simulation is given. For comparison, we assume that we use perfect BB84 senders and Bell-state MU (but we do not trust them) to perform the the QMDIQKD protocol. The MU, whose implementation can be imagined as the same as the one in Ref. [34], is equipped with four single-photon detectors (SPDs) with the detection efficiency η and dark counting rate d *per gate*. We assume that Eve is passive and ignore the channel disturbance and optical misalignment. We also define that l represents the distance from Alice or Bob to the MU and $p_s = 10^{-0.02l}\eta$ means the probability that a single photon from Alice or Bob can click a SPD of MU.

Consequently, if Alice and Bob both emit qubit $|0\rangle$ or $|1\rangle$, the MU will announce message 1 with probability $p(1|0,0) = p(1|1,1) = p_s^2(1-d)^2/2 + 2p_s(1-p_s)d(1-d)^2 + 2(1-p_s)^2 d^2(1-d)^2$, in which the first item corresponds to the case that the projection of the incoming photons into $|\phi^+\rangle_{\mathrm{CD}}$ is successful: the two photons click the

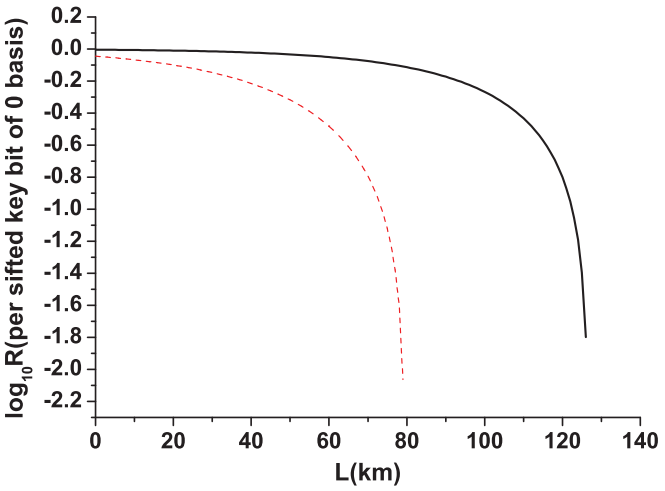

FIG. 2. (Color online) Secure-key rate R (unit: per sifted key bit of 0 basis) vs channel distance L (km) from Alice or Bob to MU: we set $\eta = 0.1$, $d = 10^{-5}$ per pulse. The solid line represents MDIQKD with perfect trustworthy BB84 senders' devices, MU without optics misalignment, which can distinguish one Bell state $|\phi^+\rangle_{CD}$, and no Eve's attack; the dashed line is for QMDIQKD with perfect BB84 senders' devices (but not trusted by Alice and Bob), MU without optics misalignment, which can distinguish two Bell states $|\phi^+\rangle_{CD}$ and $|\psi^+\rangle_{CD}$, and no Eve's attack.

two SPDs and the remaining two SPDs do not give dark clicks. The second item accounts for the case that only one photon clicks one SPD but a dark count occurs in one relevant SPD, and the last item represents the case that two photons are absorbed by the channel but two dark counts occur in two relevant SPDs. If Alice and Bob both emit qubit $|0\rangle$ or $|1\rangle$, the MU will announce message 2 with probability $p(2|0,0) = p(2|1,1) = 2(1-p)^2d^2(1-d)^2 + 2p(1-p)d(1-d)^2$, in which the first item accounts for the case that only one photon clicks one SPD but a dark count occurs in one relevant SPD, and the last item represents the case that two photons are absorbed by the channel but two dark counts occur in two relevant SPDs. And, $p(0|0,0) = p(0|1,1) = 1 - p(1|0,0) - p(2|0,0)$ also holds.

By the similar considerations, we set $p(1|1,0) = p(1|0,1) = 2(1-p_s)^2d^2(1-d)^2 + 2p_s(1-p_s)d(1-d)^2$, $p(2|0,1) = p(2|1,0) = p_s^2(1-d)^2/2 + 2p_s(1-p_s)d(1-d)^2 + 2(1-p_s)^2d^2(1-d)^2$, $p(0|0,1) = p(0|1,0) = 1 - p(1|0,1) - p(2|0,1)$, $p(1|2,3) = p(1|3,2) = p(2|2,3) = p(2|3,2) = 2(1-p_s)^2d^2(1-d)^2 + 2p_s(1-p_s)d(1-d)^2$, and $p(0|2,3) = p(0|3,2) = 1 - p(1|2,3) - p(2|2,3)$. The secure-key rate (unit: per sifted key bit under 0 basis) versus channel distance L (km) from Alice or Bob to the MU is given by Fig. 2.

In Fig. 2, the secure-key rate for MDIQKD is given by the solid line, in which we assume that Alice and Bob are aware that their encoding states are perfect, MU can only distinguish Bell state $|\phi^+\rangle_{CD}$, and Eve is passive. The secure-key rate for QMDIQKD is given by the dashed line, in which we have ideal BB84 senders (but we do not trust them now), MU can distinguish two Bell states $|\phi^+\rangle_{CD}$ and $|\psi^+\rangle_{CD}$, and Eve is passive.

From Fig. 2, we see that QMDIQKD with only the two-dimensional assumption can offer near 160-km QKD service between Alice and Bob (i.e., twice the distance between the MU and Alice or Bob). One should note that the two lines in Fig. 2 do not converge at $L = 0$ due to the errors introduced by dark counts. Here, the detection efficiency is 10% and thus dark counts occur. It can be seen that these errors lower the key rate more significantly in QMDIQKD than in the original MDIQKD. On the other hand, if the efficiency is 100%, thus eliminating the effect of dark counts, the two lines will converge at $L = 0$. To see this, if $L = 0$ and the efficiency of SPDs is 1, we must have $p(1|0,1) = p(1|3,2) = p(2|0,0) = p(2|1,1) = p(2|3,2) = 0$ and $p(1|00) = p(1|11) = 1$. Then, $\xi = 0$ and $\zeta = 0$ according to their definitions in (16). By (19), we have $C_{30}C'_{20} = C_{31}C'_{21}$ since $p(1|0,0) = p(1|1,1) = 1$. Also, note that $C_{30}C'_{20} \neq 0$ in this case. Then, by (23), we obtain $\epsilon = 0$, $e_p = 0$, and finally $R = 1$. And, in this ideal situation, the original MDIQKD will also have $R = 1$. Thus, the lines will converge in this case.

VI. CONCLUSION

In this paper, we have proved the security of a new MDIQKD scheme where uncharacterized qubit source systems are used. The difference between MDIQKD and QMDIQKD lies in the knowledge of Alice and Bob on their encoding states and the requirement of MU announcement. In MDIQKD, the encoded states are assumed to be well characterized, and the MU only needs to identify any one of the Bell states [34]. In QMDIQKD, Alice and Bob do not need to worry about their encoding systems except that they need to be sure about the source-state dimensions, and the MU can distinguish at least two Bell states. The simulation results show that the scheme is practical. Thus, our work advances MDIQKD to be more device independent while keeping its main advantage: high loss and error tolerance.

There are a few extensions to our work that can be done in the future.

(i) Our security proof assumes that Eve's attack is collective. This restriction can be removed by employing the recently developed security proofs [46,47] to make our protocol secure against the most general attacks. It is an interesting future project to extend our proof to the most general attack case in the finite-size key scenario.

(ii) Currently, the QMDIQKD protocol is restricted to two-dimensional (qubit) source systems. However, direct extension of this protocol to higher dimensions is not fruitful. When the dimension is four or above, the protocol becomes insecure since the four BB84 states can be unambiguously represented by a four-dimensional state.

(iii) Weak coherent sources are widely used in QKD experiments. The decoy-state method can be employed to solve the multiphoton state issue. To extend the QMDIQKD protocol to coherent state sources, we can combine this protocol with the decoy-state method. Since the decoy-state method is proven to be secure under the Gottesman, Lo, Lutkenhaus, and Preskill (GLLP) scenario [41,45], such an extension is expected to be natural.

ACKNOWLEDGMENTS

The authors thank O. Gittsovich, H.-K. Lo, N. Lütkenhaus, B. Qi, K. Tamaki, and F. Xu for helpful discussions. This work was supported by the National Basic Research Program of

China (Grants No. 2011CBA00200 and No. 2011CB921200), National Natural Science Foundation of China (Grants No. 61101137 and No. 61201239). X.M. gratefully acknowledges the financial support from the National Basic Research Program of China Grants No. 2011CBA00300 and No. 2011CBA00301; and the 1000 Youth Fellowship program in China. C.-H.F.F. gratefully acknowledges the financial support of RGC Grant No. 700712P from the HKSAR Government.

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE Press, New York, 1984), pp. 175–179.
[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] D. Mayers, J. Assoc. Comput. Mach. **48**, 351 (2001).
[4] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[5] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[6] K. Tamaki, M. Koashi, and N. Imoto, Phys. Rev. Lett. **90**, 167904 (2003).
[7] J.-C. Boileau, K. Tamaki, J. Batuwantudawe, R. Laflamme, and J. M. Renes, Phys. Rev. Lett. **94**, 040503 (2005).
[8] Z.-Q. Yin, H.-W. Li, W. Chen, Z.-F. Han, and G.-C. Guo, Phys. Rev. A **82**, 042335 (2010).
[9] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, Phys. Rev. Lett. **96**, 070502 (2006).
[10] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, Phys. Rev. Lett. **98**, 010503 (2007).
[11] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, Phys. Rev. Lett. **98**, 010504 (2007).
[12] C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan, Phys. Rev. Lett. **98**, 010505 (2007).
[13] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, in *Proceedings of the IEEE ISIT* (IEEE Press, New York, 2006), p. 2094.
[14] Z. L. Yuan, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **90**, 011118 (2007).
[15] H. Takesue, S. Nam, Q. Zhang, R. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, Nat. Photonics **1**, 343 (2007).
[16] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, New J. Phys. **4**, 41 (2002).
[17] S. Wang, W. Chen, J.-F. Guo, Z.-Q. Yin, H.-W. Li, Z. Zhou, G.-C. Guo, and Z.-F. Han, Opt. Lett. **37**, 1008 (2012).
[18] B. Frolich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, Nature (London) **501**, 69 (2013).
[19] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[20] V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **74**, 022313 (2006).
[21] V. Makarov and J. Skaar, Quantum Inf. Comput. **8**, 0622 (2008).
[22] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Quantum Inf. Comput. **7**, 073 (2007).
[23] Y. Zhao, Chi-Hang Fred Fung, B. Qi, C. Chen, and H.-K. Lo, Phys. Rev. A **78**, 042333 (2008).
[24] Chi-Hang Fred Fung, B. Qi, K. Tamaki, and H.-K. Lo, Phys. Rev. A **75**, 032314 (2007).
[25] F. Xu, B. Qi, and H.-K. Lo, New J. Phys. **12**, 113026 (2010).
[26] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 686 (2010).
[27] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Nat. Commun. **2**, 349 (2011).
[28] Y.-L. Tang, H.-L. Yin, X. Ma, Chi-Hang Fred Fung, Y. Liu, H.-L. Yong, T.-Y. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, Phys. Rev. A **88**, 022308 (2013).
[29] D. Mayers and A. Yao, in *FOCS, 39th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society Press, Los Alamitos, 1998), p. 503.
[30] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).
[31] Charles Ci Wen Lim, C. Portmann, M. Tomamichel, R. Renner, and N. Gisin, Phys. Rev. X **3**, 031006 (2013).
[32] X. Ma and N. Lütkenhaus, Quantum Inf. Comput. **12**, 0203 (2012).
[33] M. Pawłowski and N. Brunner, Phys. Rev. A **84**, 010302 (2011).
[34] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
[35] S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).
[36] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Phys. Rev. Lett. **111**, 130501 (2013).
[37] T. da Silva, D. Vitoreti, G. Xavier, G. Temporão, and J. von der Weid, Phys. Rev. A **88**, 052303 (2013).
[38] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, X. Ma, J. S. Pelc, M. M. Fejer, Q. Zhang, and J.-W. Pan, Phys. Rev. Lett. **111**, 130502 (2013).
[39] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, arXiv:1306.6134.
[40] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[41] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[42] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[43] Chi-Hang Fred Fung, X. Ma, and H. F. Chau, Phys. Rev. A **81**, 012318 (2010).
[44] X. Ma, C.-H. F. Fung, J.-C. Boileau, and H. Chau, Computers Security **30**, 172 (2011).
[45] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).
[46] C. M. Caves, C. A. Fuchs, and R. Schack, J. Math. Phys. **43**, 4537 (2002).
[47] M. Christandl, R. König, and R. Renner, Phys. Rev. Lett. **102**, 020504 (2009).