Quantum Information & Computation
ISSN 1533-7146 Volume 25 (2025) pp. 542–551
©Cerebration Science Publishing

Article

Deterministic Quantum Key Distribution with Untrusted Relay and Finite Sources

Guo-Dong Kang [1,2,3,*], Li-Jun Zhang [1], Xiao-Lu Wu [1,2], Qing-Ping Zhou [1,2] and Mao-Fa Fang [3]

[1] School of Computer Science and Engineering, Jishou University, Jishou 416000, Hunan Province, China
[2] School of Physics and Mechanical and Electrical Engineering, Jishou University, Jishou 416000, Hunan Province, China
[3] Key Laboratory of Low Dimensional Quantum Structures and Quantum Control of Ministry of Education, College of Physics and Electronic Science, Hunan Normal University, Changsha 410081, Hunan Province, China
* Corresponding author: gdkang@jsu.edu.cn

Received date: 9 April 2025; Accepted date: 13 October 2025; Published online: 18 October 2025

Abstract: Measurement-device-independent quantum key distribution (MDI-QKD) is proposed to close all loopholes of detection devices in QKD systems, and it holds the potential to double the limit transmission distance of those one-way QKD protocols. However, most MDI-QKD protocols are nondeterministic, which reduces the potential key rate by nearly half. In this paper, we propose a deterministic QKD protocol with an untrusted detection relay and finite sources, and based on the current technology of QKD devices, we derive the performance formula for it. The simulation results show that the performance of this protocol can exceed the MDI-QKD within the long limit transmission distance range, about 445km.

Keywords: Deterministic Quantum Key Distribution; Untrusted Relay; Finite Sources.

1. Introduction

Quantum key distribution (QKD) [1,2], whose security relies on the fundamental laws of quantum mechanics, is one of the most successful directions in practice in quantum information processing. Since Bennett and Brassard proposed the first standard one-way QKD protocol, namely the BB84 [1], for nearly four decades of efforts, the security proof problem of these BB84-type QKD protocols have been solved in ideal-devices settings [3–6], and the communication distance has been extended from the early 32cm [7] to 1200km satellite-to-ground [8]. In practice, the imperfect factors of QKD devices, such as imperfect single-photon sources, channel decay, and imperfect photon detectors, are vulnerable to powerful eavesdroppers, thus reducing the key performances and even compromising the security of QKD. Recently, the decoy technique [9,10] and the measurement-device-independent (MDI) proposal [11] not only close nearly all (except the characteristic of the sources) of the main current loopholes in real-life QKD devices but also significantly improve the key performance with imperfect single-photon sources. Later, MDI-QKD protocols with imperfect sources were presented, making QKD more robust in real-world applications [12,13]. However, most one-way QKD protocols are nondeterministic (in the post-processing, bases reconciliation is needed, and nearly half of the effective signal sources are sifted off to obtain raw key bits, which reduces the key rate by nearly half). Another relatively new proposal, deterministic QKD (DQKD), was proposed to amend the nondeterministic factor of one-way QKD. The two classical deterministic protocols are the Ping-Pong (PP) protocol and the LM05 protocol [14,15]. The distinct feature of the DQKD is the two-way (forward and backward) quantum channel, usually called TWQKD. The security proof is more complex as Eve can invade it in both the quantum forward channel (QFC) and the quantum backward channel (QBC). Over the past two decades, through hard work, the security of TWQKD has been proven under ideal-device settings [16–19]. It demonstrated that the performance of TWQKD can even surpass that of one-way QKD within a specific distance range, showing great potential to achieve good performance [20]. However, due to its two-way nature, TWQKD is more vulnerable when considering the loopholes of imperfect measurement devices. Eve can use it to steal partial or even complete key information [21], and the communication distance limit is relatively shorter than that of one-way QKD. Remarkably, Lu et al. take the first step

DOI: 10.2478/qic-2025-0029

to prove that DQKD is MDI secure in the QBC, while the photon detector at Alice's side for check mode (to ensure security, check the fidelity of the QFC) is assumed to be perfect [22]. In this paper, we propose a DQKD protocol to double the limit transmission distance under the assumption that all measurement detectors, the relay, is untrusted (controlled by Eve). Later, we refer to it as the untrusted relay DQKD (UR-DQKD). The main work of this paper is to derive the performance formula for the UR-DQKD based on the current technology of QKD devices with finite sources.

The rest of this paper is arranged as follows. Details of the UR-DQKD protocol are presented in Section 2, whose key performance formula and simulation results are given in Section 3. Finally, a discussion and conclusion are made in Section 4.

2. Protocol

As in Figure 1, without loss of generality, Bob and Alice run the protocol according to the following steps.

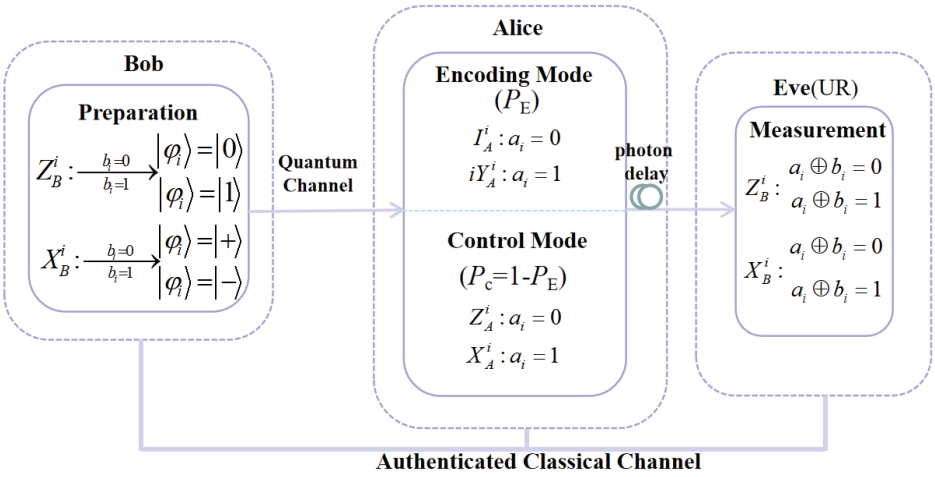

Figure 1. Schematic illustration of the UR-DQKD Classic.

1. ***Preparation***. First, Bob sends a communication request to Alice through an authenticated classical channel. Then, according to a random bit string with length N, denoted as $\mathbf{b} = b_1 b_2 \ldots b_N$ with $b_i \in \{0,1\}$ and $i \in \{1,2,\ldots,N\}$, Bob prepares and sends N qubits, written as a density matrix$\rho_B = \otimes_{i=1}^{N} \rho_B^i$, to Alice. Where $\rho_B^i = \sum \frac{1}{4} \left|\varphi^i\right\rangle \left\langle\varphi^i\right|, \left|\varphi^i\right\rangle$ denotes the state of the i-th qubit that is randomly (with probability 1/4)in one of the four states: $\{Z_B : |0\rangle, |1\rangle\}$, $\{X_B : |+\rangle, |-\rangle\}$. $\{|0\rangle,|1\rangle\}$ represent the eigenstates of the Pauli operator Z, and $|\pm\rangle = \frac{1}{\sqrt{2}}|0\rangle \pm |1\rangle$ represent the eigenstates of the Pauli operator X. Alice responses to the request from Bob and prepares a random bit string with length N, denoted as $\mathbf{a} = a_1 a_2 \ldots a_N$ with $a_i \in \{0,1\}$ and $i \in \{1,2,\ldots,N\}$. Then, after receiving the i-th qubitρ_B^i, Alice randomly chooses between the control mode (CM) with probability P_C and the encoding mode (EM) with probability P_E, $P_E + P_C = 1$.
2. ***Encoding mode***. In the EM, Alice randomly (with equal probability) performs with two operators, I and iY, on the k-th qubit $\left|\varphi^k\right\rangle$ to encode bits $\mathbf{a}_k$. Where $\mathbf{a}_k$ is part of $\mathbf{a}$, and it will be used as the raw key bits. The unitary operator $I = |0\rangle\langle 0| + |1\rangle\langle 1|$ encodes bit $a_k = 0$ and $iY = |0\rangle\langle 1| - |1\rangle\langle 0|$ encodes bit $a_k = 1$.iY flips on all four prepared states as follows: $iY|0\rangle = -|1\rangle, iY|1\rangle = |0\rangle, iY|+\rangle = |-\rangle, iY|-\rangle = -|+\rangle$. After passing through the EM, all encoded qubits are sent to t+he UR.
3. ***Control mode***. In the control mode (CM), according to the rest part of $\mathbf{a}$, denoted as $\mathbf{a}_j, j \in [1,N]$ and $j \neq k$. Alice randomly (with equal probability) performs the Pauli Z operator ($a_j = 0$) or the Pauli X operator ($a_j = 1$) on the j-th qubit $\left|\varphi^j\right\rangle$and then sends them to the UR.
   Here, we emphasize that instead of measuring all the qubits from the CM and the EM by legitimate parties, Bob delegates the decoding measurement process to Eve and informs Eve the basis of $\left|\varphi^i\right\rangle$ through an authenticated classic channel. Eve measures each of Alice's qubits via Bob's basis in the UR, and then reports all of the measurement results (N bits), denoted as E_i, to Bob. Without noise, in the EM, Eve's measurement outcomes are $E_k : a_k \oplus b_k$, while in the CM, Eve's outcomes are more complex, i.e., $E_j = b_j$ if the basis used by Alice matches the basis chosen by Bob, otherwise, E_j are randomly to be 0 or 1.

4. ***Security Check***. Alice announces the serial number j of each $\left|\varphi^j\right\rangle$ and the corresponding control operator that is used in the CM. According to Alice's announcement, Bob computes the quantum bit error rate (QBER) of $\mathbf{a}_j$, denoted as Q_{CM}. If Q_{CM} exceeds the security threshold, they regard Eve as having seriously invaded the quantum channel and abort the rest of the bits.
5. ***Key distillation***. If Q_{CM} is acceptable, Alice randomly announces part of the $\mathbf{a}_k$ to compute the QBER of $\mathbf{a}_k$, denoted asQ_{EM}. If Q_{EM} is acceptable (note, in the asymptotic case $Q_{EM} = Q_{CM}$), Alice and Bob perform the error-correction (EC) and the privacy amplification (PA) to distillate the final secure key bits.

Here, a photon delay with a small time slot may be needed in Alice's module, as Bob only tells Eve the basis of$\rho_B^i$to execute the decoding measurement after Alice announces receiving a qubit. Note that photon delay is not a significant obstacle, as substantial progress has been made in [23].

3. Performance

3.1. Security Basis and Rigorous Proof

Here, we first emphasize and list the assumptions on which the security of this protocol is based.

1. First, the sources are security, i.e., the preparation basis of $\left|\varphi^i\right\rangle$ is not leaked to Eve before step 3, or in other words, the bit string **b** is unknown to Eve before step 3. Pre-shared entanglement between $\left|\varphi^i\right\rangle$ and Eve's ancilla $|\varepsilon\rangle_E$is also excluded.
2. Second, Alice's bit string **a** is not leaked to Eve. Alice has free will to choose the encoding and the control operators randomly.
3. Third, Eve can access quantum memory devices that have for arbitrary long coherence time.

Based on the above assumptions, we can infer that the security basis of this protocol is founded on two key points. First, Eve cannot distinguish between the qubits that pass through the EM and the ones that pass through the CM until Alice's announcements in step 4. Second, the density matrix of ρ_B^i is invariant under Alice's operations in the EM (CM), $\rho_{AB|EM(CM)}^i = \rho_B^i = \frac{I}{2}$. Thus, in the view of Eve, the evolution of ρ_i^B has nothing to do with Bob's preparation bases. Then, three conclusions can be drawn in the following.

1. Eve cannot get any information about the encoding bits a_k from the measurement results $E_k : a_k \oplus b_k$.
2. In the view of Eve, this protocol is equivalent to the one in which Alice randomly uses four operations $\{I, iY, Z, X\}$ for encoding. Thus, due to the CM, Eve will inevitably introduce QBER if she tries to get the information of a_k via attacks.

We first consider the ideas of the so-called zero-error attacks [24,25]. Suppose that, in the i-th round, Eve emits a fake state $\left|\varphi_E^i\right\rangle$, randomly in the bases $\{Z, X\}$, to Alice and then tries to extract Alice's encoding bits a_k by measuring $\left|\varphi_E^{a_k}\right\rangle$ in the UR after passing $|\varphi_E\rangle$ through the EM(CM)($|\varphi_E\rangle$ is transformed to be $\left|\varphi_E^{a_k}\right\rangle$). Through this attack, on the one hand, Eve can get all the information of a_k after Alice announces the index i of each EM(CM) round. On the other hand, Eve will inevitably introduce errors when she reports, honestly or dishonestly, the measurement results E_k to Bob for EC and PA. Eve faces two folds in each round as she has a 1/2 probability of misguessing Bob's preparation basis: if Alice chooses the CM, the error rate of the measurement result is Q_{CM}; If Eve, to escape from being detected by the CM, tampers with a measurement result (i.e.,$1 \to 0$) with a probability $p_t (0 \le p_t \le 1)$ and reports it to Bob, it will cause errors if Alice had chosen the EM in this round, the error rate is denoted as Q_{EM}. It is easy to figure out that $Q_{EM} = 0.5 \bullet p_t \bullet (1 - P_{CM})$ and $Q_{CM} = 0.25 \bullet (1 - p_t) \bullet P_{CM}$. By the above attacks (individual attacks), Eve can get all of a_k at the cost of introducing the maximum noise, $Q_{CM}^{\max} = 0.25 \bullet P_{CM}$. For specific, in this protocol, we set $P_{CM} = 0.25$, thus $Q_{CM}^{\max} = 6.25\%$ $(Q_{EM} = 0)$ which can be easily detected by Alice and Bob. Of course, theoretically speaking, P_{CM} can be arbitrarily chosen within the interval (0, 1) by legitimate parties, i.e., set $P_{CM} = 0.125$ and so on. The only difference is that increasing the value of P_{CM} increases security of the protocol, but at the expense of the encoding rate. It is proper to choose $P_{CM} = 0.25$, which guarantees both security (typically, the error rate of information transfer on a standard optical fiber with length 120∼400km is below 5%) and a relatively high encoding rate of this UR-DQKD. Therefore, Eve should balance her strategy to keep $Q_{CM} = Q_{EM}$, while Alice and Bob can fight against this kind of attack by setting the noise threshold, $Q_{CM} = Q_{EM} = Q_{\max} \approx 5.4\%$. Then the security of this protocol can be well captured by considering collective attacks.

Now we consider the security bound for this protocol under the general collective attacks [26]. Eve performs the attacks $\widehat{U}_E$ on each ρ_B^i and her initial ancilla $|\varepsilon\rangle_E$, then, after Alice's encoding operation $\widehat{O}_{a_k} = \{I^{a_k=0}, iY^{a_k=1}\}$, she extracts a_k at any time from the entire quantum system $\rho^{ABE|\widehat{O}_{a_k}} = \sum_{a_k} \widehat{O}_{a_k} \{\widehat{U}_E (\rho_B^k \otimes |\varepsilon\rangle_E\langle\varepsilon|) \widehat{U}_E^\dagger\} \widehat{O}_{a_k}^\dagger$ $(a_k = 0, 1)$ after completing the decoding measurement in the UR (She can randomly report the measurement results to Bob

at the premise of maintaining the balance $Q_{CM} = Q_{EM} = Q_{\max} \approx 5.4\%$). The maximum amount of information that Eve can get from $\rho^{ABE|\widehat{O}_{a_k}}$ is $I_E = h(Q_{EM})$ in a depolarizing quantum channel (QC) (we emphasize that the depolarizing quantum channel can characterize the noise of most of the current optical quantum hardware in practice), where $h(x)$ (the binary Shannon entropy) is given by $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$. Under ideal settings (perfect single-photon sources, no channel losses, and perfect photon-detector efficiency), the key rate of this protocol is given by (details of the rigorous security proof are presented in Appendix A).

$$K = 1 - 2h(Q_{EM}), \tag{1}$$

It reveals that the quantum channel noise in this protocol constrains Eve's ability to steal the maximum amount of information.

Here we argue that, in this protocol, Eve can not obtain more information by performing the general coherent attack mentioned in the LM05 protocol [15] than the one via the above general collective attack. In the coherent attack, in each round, Eve performs the first unitary attack $\widehat{U}_1$ on $\left|\varphi^i\right\rangle$ with one of her ancillas $|\varepsilon\rangle_E$ and stores the resulting ancillas $|\varepsilon_X\rangle_E$ after the first attack. Then, after passing $\left|\varphi^i\right\rangle$ through the EM(CM), Eve performs the second unitary attack $\widehat{U}_2$ on $\left|\varphi^i_{a_i}\right\rangle$ with her fresh ancilla $|\eta\rangle_E$ and stores the resulting ancillary states $|\eta_Y\rangle_E$. Of course, the second attack includes the resulting state of the first ancilla, where X and Y denote, respectively, the indices of her ancillary nonorthogonal vectors (i.e., $X = 00, 01, 10, 11$, $Y = 000000, 000001, \ldots, 111111$). This attack aims to create coherence between $|\varepsilon_X\rangle_E$ and $|\eta_Y\rangle_E$ thus creating coherence between $\left|\varphi^i\right\rangle$ and $\left|\varphi^i_{a_k}\right\rangle$. Eve takes advantage of the coherence to make an optimal guess of a_k by measuring $|\varepsilon_X\rangle_E$,$|\eta_Y\rangle_E$ and $\left|\varphi^i_{a_k}\right\rangle$ after step 3. From equation (14) in Ref. [15], we can figure out that the QBER Eve can introduce is $Q_{EM} = 1/2 - 1/8(1+cosx)^2$. Setting $x = x'$ in equation (13) of Ref. [15], we can obtain the upper bound of $I_{AE} = 1 - h[(1+sinx)/2]$, where $\cos x = \langle\varepsilon_{00}|\varepsilon_{11}\rangle$ specifies the angle between ε_{00} and ε_{11} (two normalized and nonorthogonal vectors of Eve's first ancilla). Then finally, we can obtain the upper bound of $I_{AE} = 1 - h(\frac{1+\sqrt{1-4(\zeta-1/2)^2}}{2})$ under the coherent attack, where $\zeta = \sqrt{1-2Q_{CM}}$. It takes the maximum($I_{AE} \approx 0.54$) at the cost of introducing the maximum noise ($Q_{EM} \approx 18\%$) under the coherent attack (ensuring the key rate $K = 0$). While in this protocol, I_E takes its maximum ($I_E \approx 0.5$) at $Q_{EM} \approx 11.4\%$ under the collective attack (ensuring the key rate $K = 0$). Note that Alice breaks the coherence in the CM (Alice randomly performs the Pauli Z operator or the Pauli X operator in the CM), thus, the maximum Q_{CM} that Eve can introduce is equal for any coherent and incoherent attack. With the noise threshold $Q_{CM} = Q_{EM} = Q_{\max} \approx 5.4\%$, the upper bound of $I_{AE} = 0.157$ under the general coherent attack, while $I_E = h(Q_{CM}) = 0.303$ under the general collective attack. It indicates that, in this protocol, the general coherent attack is not the optimal one for Eve as the CM breaks the coherence between $\left|\varphi^i\right\rangle$ and $\left|\varphi^i_{a_k}\right\rangle$.

3.2. Performance Formula

In this section, we derive the performance formula for this protocol, close to the real-world QKD system. We first present the reasonable models of the devices for this protocol, based on current technology.

We assume that Bob uses single photons as the source (SPS). In each round, Bob successfully emits a single-photon state to the quantum channel with probability P_1 (efficiency of single-photon state collection) or a vacuum state due to random losses with the probability P_0, $P_1 + P_0 = 1$. Note that high-performance single-photon sources (SPS) have made significant progress in recent QKD experiments and P_1 can be over 99% in practice [27]. Here we set $P_1 = 90\%$.

The quantum channel (optical fiber) transmittance t_{AB} can be expressed as $t_{AB} = 10^{-\frac{\beta L_{AB}}{10}}$ where, β is the decay coefficient of the fiber between Alice and Bob, and L_{AB} is the length of the fiber.

We consider a threshold photon detector in the UR that cannot resolve the photon number of each photon pulse, but can only distinguish a vacuum pulse from a non-vacuum pulse.

Then, the total efficiency of the QKD system is $\eta = t_{AB}\eta_{AB}$, where $\eta_{AB} = t_A t_B \eta_E$ denotes the total transmittance of the devices in Alice and Bob's sides ($t_A t_B$) and the UR (η_E). Here, the efficiency of the photon delay on Alice's side, which can be nearly unity with today's technology, is merged into the UR.

From the above models, the performance formula for this protocol can be written as

$$K_{finite} \geq P_{EM} \bullet g\{Y_1[1 - h(e_1)] - f_{EC}h(e_g)\}, \tag{2}$$

Details of each term in Equation (2) are listed below.

1. The factor P_{EM} is the probability of implementing the EM, and g is the total gain in the UR from Bob's SPS.
2. Y_1 is defined as the yield of a single-photon pulse, i.e., the condition probability of a detection event in the UR given that Bob sends out a single-photon pulse. Note that Y_0 (typically $10^{-5} \sim 10^{-6}$) is the background detection rate that is independent of the SPS detection.
3. e_1 and e_g are, respectively, the error rate of single-photon pulses and the overall QBER. $f_{EC} \geq 1$ is the directional error correction efficiency.

Usually, g and e_g can be obtained directly from experiments, while the parameters Y_1 and e_1 must be estimated tightly. Here, we give the theoretically expected bound of each term in Equation (2) to get the bound of K_{finite}.

The total gain g is given by

$$g = \sum_{i=0}^{i=1} Y_i P_i = Y_0 P_0 + Y_1 P_1. \tag{3}$$

The total QBER is given by

$$e_g \bullet g = \sum_{i=0}^{1} e_i Y_i P_i = e_0 Y_0 P_0 + Q_{EM} Y_1 P_1, \tag{4}$$

where, Q_{EM} in Equation (4) is the QBER induced by optical devices, thus attributed to Eve. In a depolarizing quantum channel with high visibility, Q_{EM} typically is 1%∼5%. e_0 in Equation (4) denotes the error rate of the random background, and is reasonably set to be 0.5.

Based on the assumption presented in [28], in the finite sources scenario, the lower bound of Y_1 in this protocol can be written as

$$Y_1^L = Y_0 + (1 - Y_0)\eta - \delta_{Y1}/g, \tag{5}$$

where δ_{Y_1} denotes the statistic fluctuation of the single-photon gain.

The upper bound of e_1 is given by

$$e_1^u = \frac{e_g + \delta_e}{Y_1^L}, \tag{6}$$

where δ_e is the statistic fluctuation of e_g in a finite source scenario.

According to the law of large numbers and the finite sources theorem [29–31], δ_{Y_1} and δ_e are, respectively, given by

$$\delta_{Y_1} = \sqrt{\frac{2\ln(1/\varepsilon_{PE}) + 4\ln(N+1)}{4N}}, \tag{7}$$

$$\delta_e = \sqrt{\frac{2\ln(1/\varepsilon_{PE}) + 4\ln(N \bullet P_{EM} + 1)}{4N \bullet P_{EM}}}. \tag{8}$$

Note, Y_1 should be tightly estimated over all N pulses, while δ_e should be tightly estimated only over the pulses from the EM, and this protocol has four outcomes of the positive operator-valued measurement,POVM, in the UR). Then, with the above Equations (3)–(8), we can calculate the lower bound of K_{finite}. Simulation results of Equation (2) are presented in Figure 2 with the parameters of today's QKD technology, as listed in Table 1.

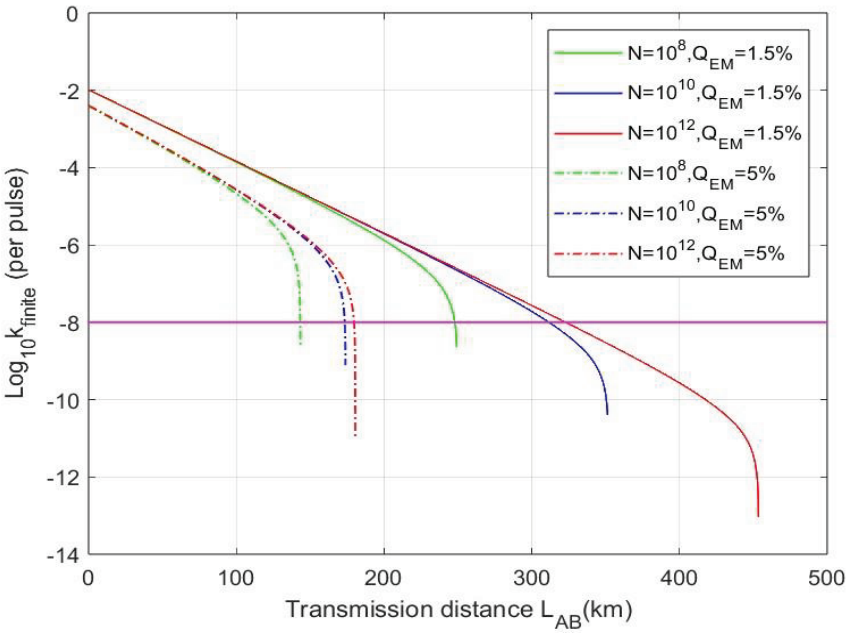

Figure 2. As a function of the transmission distance L_{AB} between Alice and Bob. We simulate the lower bounds of the finite-key-rate K_{finite} in three cases: (N=10^8) green-solid-line, (N=10^{10}) blue-solid-line, and (N=10^{12}) red-solid-line, $Q_{EM} = 1.5\%$, $\eta_E = 14.5\%$; (N=10^8) green-dash-dotted-line, (N=10^{10}) blue-dash-dotted-line, and ($N = 10^{12}$) red-dash-dotted-line, $Q_{EM} = 5\%$, $\eta_E = 14.5\%$.

Table 1. Experimental parameters of today's QKD technology.

$\beta(dB/km)$	Q_{EM}	Y_0	η_E	f_{EC}	ε_{PE}
0.2	1.5%∽5%	8×10^{-8}	14.5% ∽ 45%	1.15	10^{-8}

Figure 2 shows that: the finite lengths of sources have significant effects on the limit transmission distance; with $Q_{EM} = 1.5\%$, $N \geq 10^8$, cut off those key rates below 10^{-8}, the performance is over 248km∽10^{-8} bits/pulse, and the limit transmission distance can be extended over 320 km with $N \geq 10^{12}$; even with $Q_{EM} = 5\%$, much higher than the current value in practice, the performance is over 143km∽10^{-8} bits/pulse, and the limit transmission distance can be extended over 180 km with $N \geq 10^{12}$.

Figure 3 shows that: the UR-DQKD doubles the performance of the current DQKD, and the effect of the finite lengths of sources is negligible when N is large enough, i.e., $N \geq 10^{16}$; brief comparison with the performance of the MDI-QKD, i.e., the dashed line in Figure 3 in Ref. [32], the key rate and the limit transmission distance of this protocol perform better than that of the MDI-QKD. All critical parameters for comparison are the same as those in Table 1 ($Q_{EM} = 1.5\%$, $Y_0 = 8 \times 10^{-8}$, $\eta_E = 14.5\%$, $f_{EC} = 1.15$, and $\beta = 0.2$) except for the sources: infinite decoy states of coherent pulses in the MDI-QKD, finite SPS based on the recent experiment progress in this protocol. Theoretically speaking, for the MDI-QKD with infinite decoy states, besides the signal coherent pulses with intensity $\mu_{\text{Alice}} = \mu_{\text{Bob}} = \mu$, Alice and Bob send infinite faint coherent pulses with intensities $v_i (v_i \in \{v_1, v_2, \ldots, v_m\}$, $m \to \infty$, and $v_i < \mu$) to the UR to tightly estimate the gain Y_{11} and the error rate e_{11} of the key rate equation (B31) in Ref. [32], which makes the key rate of the MDI-QKD with infinite coherent pulses asymptotic to that of the MDI-QKD with infinite single photons. Note that the optimal μ, approximately 0.2∽0.6, slightly varies with the transmission distance L_{AB} and is numerically optimized in Figure 3. Therefore, under the above conditions, it is justified to make a performance comparison between the infinite decoy states MDI-QKD and this UR-DQKD with finite SPS.

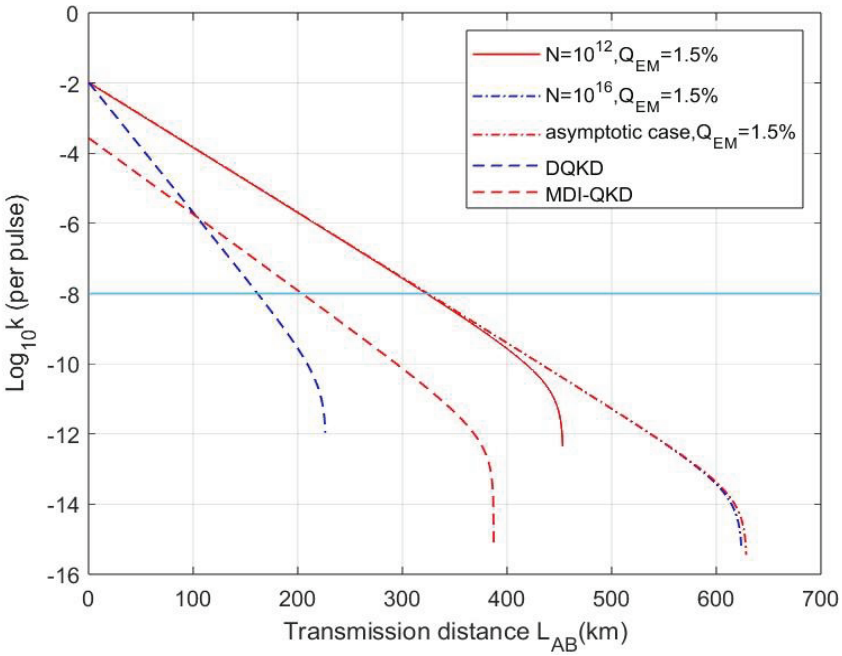

Figure 3. As a function of the transmission distance L_{AB} between Alice and Bob. We take a brief comparison of the performance of the UR-DQKD with that of the current DQKD such as the LM05 [15] and the MDIQKD [32].

4. Conclusion and Discussion

In this work, we propose a UR-DQKD protocol. The main work of this paper focuses on deriving the lower bound of the performance formula for it with a practical model based on today's technology. Moreover, with the current parameters, the simulation results show that this protocol can achieve good performance. It nearly doubles the performance of the current DQKD employing a trusted relay [15] and outperforms the MDI-QKD within a considerable distance (320km). It is foreseeable that the performance will be over 470km$\backsim 10^{-8}$ bits/pulse if the critical parameters of the QKD system are set to the optimal values of today's technology, i.e., use ultralow-loss fiber ($\beta = 0.17$) and high-efficiency detector ($\eta_E \geq 45\%$) [33], thus expected to be comparable with the performance of the PM-QKD [32]. We also note the recent progress in the experimental demonstration of quantum secure direct communication (QSDC) with single-photons and entanglement-pairs, which also indicates the potential of achieving high-performance MDI-DQKD with current devices (over 200km with relatively high secure key rates) [34]. In conclusion, this protocol is feasible with today's technology, allowing high-performance, secure networks with a relay controlled by an untrusted third party.

Author Contributions

Conceptualization, Guo-Dong Kang, Qing-Ping Zhou, and Mao-Fa Fang; methodology, Guo-Dong Kang; software, Guo-Dong Kang, Li-Jun Zhang, and Xiao-Lu Wu; validation, Guo-Dong Kang; formal analysis, Guo-Dong Kang, Qing-Ping Zhou, and Mao-Fa Fang; investigation, Guo-Dong Kang and Mao-Fa Fang; writing—original draft preparation, Guo-Dong Kang; writing—review and editing, Guo-Dong Kang, Li-Jun Zhang, and Xiao-Lu Wu; funding acquisition, Guo-Dong Kang and Mao-Fa Fang. All authors have read and agreed to the published version of the manuscript.

Funding

This work was supported by the National Natural Science Foundation of China under Grant Nos. (12604012, 11464015, 62565010), the Natural Science Foundation of Hunan Province under Grant No. 2020JJ4496, and the Science Research Foundation of the Education Department of Hunan Province under Grant No.20A0585.

Conflicts of Interest Statement

The authors declare that they have no conflicts of interest.

Data Availability Statement

The authors declare that the data supporting the findings of this study are available within the article.

Appendix A

In the collective attacks scenario [26], in each round, Eve starts her strategy on the quantum channel (QC) by performing unitary operations $\widehat{U}_E$ on her ancilla $|\varepsilon\rangle_E$ and Bob's preparation states $\left|\varphi^i\right\rangle$, then after passing through the EM(CM) on Alice's side, Eve tries to extract Alice's encoding bit a_k with the measurement results from the UR and her ancilla(after Alice publicly announcing the index i of each EM round). Since $\rho_i^B = \rho_i^{AB|EM(CM)} = \frac{I}{2}$ (the analysis in Sect. 3.1), Eve can only distinguish the difference between the density matrix ρ_i^B and the one, denoted as $\rho_i^{B|\widehat{O}_{0,1}}$, after Alice's encoding operation $\widehat{O}_{a_k}$ by performing $\widehat{U}_E$ on the joint Hilbert space of the ancilla $|\varepsilon\rangle_E\langle\varepsilon|$ and ρ_i^B. The action of Eve's unitary attacks$\widehat{U}_E$ can be represented by

$$\widehat{U}_E \left|i_{\widehat{k}}\right\rangle|\varepsilon\rangle_E = \left|0_{\widehat{k}}\right\rangle|\varepsilon_{i0}\rangle_E + \left|1_{\widehat{k}}\right\rangle|\varepsilon_{i1}\rangle_E \; i{=}0,1 \tag{A1}$$

where $\left\{\left|0_{\widehat{k}}\right\rangle, \left|1_{\widehat{k}}\right\rangle\right\}$ denote the eigenstates of the Pauli operators , $\widehat{k} = \{X, Z\}$ is Bob's preparation vector of the Bloch sphere. Without loss of generality, the unitarity of $\widehat{U}_E$ is guaranteed by the following constraints(neglecting the preparation vector $\widehat{k}$)

$$\langle\varepsilon_{i0}|\varepsilon_{i0}\rangle + \langle\varepsilon_{i1}|\varepsilon_{i1}\rangle = 1, \langle\varepsilon_{00}|\varepsilon_{10}\rangle = \langle\varepsilon_{01}|\varepsilon_{11}\rangle = 0. \tag{A2}$$

The maximum information of a_k that Eve can get is given by

$$I_E = \{S(\rho^{ABE}) - \frac{1}{2}[S(\rho^{ABE|\widehat{O}_0}) + S(\rho^{ABE|\widehat{O}_1})]\}_{max}, \tag{A3}$$

where the *max* is taken over all possible unitary attacks $\widehat{U}_E$,$S(\rho) = Tr(\rho\log_2\rho)$ is the von Neumann entropy, $\rho^{ABE} = \frac{1}{2}(\rho^{ABE|\widehat{O}_0} + \rho^{ABE|\widehat{O}_1})$, $\rho^{ABE|\widehat{O}_0} = \widehat{U}_E\ (\frac{I_B}{2}\otimes|\varepsilon\rangle_E\langle\varepsilon|)\ \widehat{U}_E^\dagger$, $\rho^{ABE|\widehat{O}_1} = iY_A\ \widehat{U}_E\ (\frac{I_B}{2}\otimes|\varepsilon\rangle_E\langle\varepsilon|)\ \widehat{U}_E^\dagger\ iY_A^\dagger$. Note that $\rho^{ABE|\widehat{O}_0}$ ($\rho^{ABE|\widehat{O}_1}$) would only differ from $\frac{I_B}{2}\otimes|\varepsilon\rangle_E\langle\varepsilon|$ by Eve's unitary attacks $\widehat{U}_E$, it is easy to figure out that $S(\rho^{ABE|\widehat{O}_0}) = S(\rho^{ABE|\widehat{O}_1}) = 1$. Then we obtain

$$I_E = [S(\rho^{ABE}) - 1]_{max}, \tag{A4}$$

where $\rho^{ABE} = \widehat{O}_0\ [\widehat{U}_E\ (\frac{I_B}{4}\otimes|\varepsilon\rangle_E\langle\varepsilon|)\ \widehat{U}_E^\dagger]\ \widehat{O}_0^\dagger + \widehat{O}_1\ [\widehat{U}_E\ (\frac{I_B}{4}\otimes|\varepsilon\rangle_E\langle\varepsilon|)\ \widehat{U}_E^\dagger]\ \widehat{O}_1^\dagger$. With infinite sources (in asymptotic cases), the secret key rate of this protocol is given by

$$K = 1 - h(Q_{EM}) - I_E. \tag{A5}$$

where $h(Q_{EM}) = -Q_{EM}\log_2 Q_{EM} - (1-Q_{EM})\log_2(1-Q_{EM})$, denotes the bits that will be sacrificed in the EC, and Q_{EM}, the QBER of the raw key bits, can be seen as the noise of the QC (also can be seen as the QBER that Eve can introduce). This paper considers the condition of a depolarizing QC, and it follows that $Q_{EM}(Q_{CM})$ is independent of Bob's preparation vector $\widehat{k}$, and $Q_{EM} = Q_{CM}$ with infinite sources. For simplicity and without loss of generality, we set the specific form of Eve's unitary attacks as follows.

$$\begin{aligned}&\langle\varepsilon_{00}|\varepsilon_{01}\rangle = \langle\varepsilon_{10}|\varepsilon_{11}\rangle = \langle\varepsilon_{00}|\varepsilon_{10}\rangle = \langle\varepsilon_{01}|\varepsilon_{11}\rangle = \langle\varepsilon_{01}|\varepsilon_{10}\rangle = 0,\\ &\langle\varepsilon_{00}|\varepsilon_{11}\rangle = 1 - 2Q_{EM}, \langle\varepsilon_{01}|\varepsilon_{01}\rangle = \langle\varepsilon_{10}|\varepsilon_{10}\rangle = Q_{EM}.\end{aligned} \tag{A6}$$

Now, to obtain the final formula of K in Eq. (A5), we should firstly work out the eigenvalues of ρ^{ABE} to get I_E in Eq. (A4). Note that the eigenvalues of ρ^{ABE} are the same with the ones of its Gram matrix G [35], and the dimension of G is 4×4 which is much more easier for eigenvalues computing. We write ρ^{ABE}in the Gram matrix(G) representation [35] in the following. For a mixture of non-orthogonal pure states $\rho = \sum_i p_i|\varphi_i\rangle\langle\varphi_i|$, $\sum_i p_i = 1$, the elements of the Gram matrix G are defined as

$$G_{ij} = \sqrt{p_i p_j\left\langle\varphi_i\middle|\varphi_j\right\rangle}, \tag{A7}$$

where the sets of $G\{|\varphi_i\rangle\}$ are given by

$$|\varphi_1\rangle = |0\rangle|\varepsilon_{00}\rangle + |1\rangle|\varepsilon_{01}\rangle, |\varphi_2\rangle = |0\rangle|\varepsilon_{10}\rangle + |1\rangle|\varepsilon_{11}\rangle,$$
$$|\varphi_3\rangle = |0\rangle|\varepsilon_{01}\rangle - |1\rangle|\varepsilon_{00}\rangle, |\varphi_4\rangle = |0\rangle|\varepsilon_{11}\rangle - |1\rangle|\varepsilon_{10}\rangle. \tag{A8}$$

Then, with Eqs. (A6) and (A8), ρ^{ABE} can be written as

$$G(\rho^{ABE}) = \begin{pmatrix} 1 & 0 & 0 & 1-2Q_{EM} \\ 0 & 1 & 2Q_{EM}-1 & 0 \\ 0 & 2Q_{EM}-1 & 1 & 0 \\ 1-2Q_{EM} & 0 & 0 & 1 \end{pmatrix}. \tag{A9}$$

Now, we can obtain the eigenvalues of $G(\rho^{ABE})$ which are given by

$$\lambda_{1,2} = \frac{1}{2}(1-Q_{EM}), \lambda_{3,4} = \frac{1}{2}Q_{EM}. \tag{A10}$$

Then, $S(\rho^{ABE})_{max}$ is given by (its maximum is taken at $\langle\varepsilon_{00}|\,\varepsilon_{10}\rangle = 0$)

$$S(\rho^{ABE})_{max} = 1 + h(Q_{EM}). \tag{A11}$$

Finally, Eqs. (A4), (A5), and (A11) allow us to derive the formula of the secret key rate K for this protocol (see Eq. (1) in Sect. 3.1).

References

1. C. H. Bennett, and G. Brassard (1984). "Quantum cryptography: Public key distribution and coin tossing". *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, 175–179.
2. A. K. Ekert (1991). "Quantum cryptography based on Bell's theorem". *Physical Review Letters*, 67: 6, 661–663.
3. H.-K. Lo, and H. Chau (1999). "Unconditional security of quantum key distribution over arbitrarily long distances". *Science*, 283: 5410, 2050–2056.
4. D. Mayers (1996). "Quantum key distribution and string oblivious transfer in noisy channels". *Advances in Cryptology—CRYPTO'96*, 343–357. Heidelberg: Springer.
5. P. W. Shor, and J. Preskill (2000). "Simple proof of security of the BB84 quantum key distribution protocol". *Physical Review Letter*, 85:2, 441–444.
6. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden (2002). "Quantum cryptography". *Reviews of Modern Physics*, 74: 1, 145–200.
7. C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin (1992). "Experimental quantum cryptography". *Journal. of Cryptology*, 5, 3–28.
8. S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, C.-W. Liao, H.-F. Zhang, Y.-J. Han, W.-Y. Zhou, H.-S. Zhong, H.-Z. Lu, Z.-Z. Zhang, X.-L. Chen, J.-Z. Zhang, F.-X. Li, Z.-S. Yuan, and J.-W. Pan (2017). "Satellite-to-ground quantum key distribution". *Nature*, 549: 43–47, 2017.
9. H. K. Lo, X. Ma, and K. Chen (2005). "Decoy state quantum key distribution". *Physical Review Letter*, 94, 230504.
10. X. B. Wang (2005). "Beating the photon-number-splitting attack in practical quantum cryptography". *Physical Review Letter*, 94, 230503.
11. H. K. Lo, M. Curty, and B. Qi (2012). "Measurement-device-independent quantum key distribution". *Physical Review Letter*, 108, 130503.
12. Z.-Q. Yin, C.-H. Fred Fung, X. Ma, C.-M. Zhang, H.-W. Li, Wei Chen, S. Wang, G.-C. Guo, and Z.-F. Han (2013). "Measurement-device-independent quantum key distribution with uncharacterized qubit sources". *Physical Review A*, 88: 6, 1–9.
13. G.-D. Kang, Q.-P. Zhou, and M.-F. Fang (2019). "Measurement-device-independent quantum key distribution with uncharacterized coherent sources". *Quantum Information Processing*, 19: 1, 1–18.
14. K. Boström and T. Felbinger (2002). "Deterministic secure direct communication using entanglement". *Physical Review Letter*, 89: 1, 187902.

15. M. Lucamarini, and S. Mancini (2005). “Secure deterministic communication without entanglement”. *Physical Review Letter*, 94: 14, 140501.
16. H. Lu, C.-H. Fred Fung, X.-F. Ma, and Q.-Y. Cai (2011). “Unconditional security proof of a deterministic quantum key distribution with a two-way quantum channel”. *Physical Review. A*, 84: 4, 1504–1512.
17. N. J. Beaudry, M. Lucamarini, S. Mancini, and R. Renner (2013). “Security of two-way quantum key distribution”. *Physical Review A*, 88: 6, 8617–8626.
18. C.-H. Fred Fung, X. Ma, H. Chau, and Q.-Y. Cai (2012). “Quantum key distribution with delayed privacy amplification and its application to the security proof of a two-way deterministic protocol”. *Physical Review A*, 85:3, 032308.
19. G.-D. Kang, Q.-P. Zhou, and M.-F. Fang (2019). “Two-way quantum key distribution in a uniformly distributed quantum space via a special mapping and its analytical security proofs”. *International Journal of Quantum Information*, 17: 1, 19500102.
20. M. Lucamarini, A. Cere’, G. D. Giuseppe, S. Mancini, D. Vitali, and P Tombesi (2007). “Two-way protocol for quantum cryptography with imperfect devices”. *Open System and Information Dynamics*, 14, 169–178.
21. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov. (2010). “Hacking commercial quantum cryptography systems by tailored bright illumination”. *Nature Photonics*, 4: 10, 686–689.
22. H. Lu, C.-H. F. Fung, and Q.-Y. Cai (2013). “Two-way deterministic quantum key distribution against detector-side-channel attacks”. *Physical Review A*, 88: 4, 044302.
23. Y. Ma, Y.-Z. Ma, Z.-Q. Zhou, C.-F. Li, and G.-C. Guo (2021). “One-hour coherent optical storage in an atomic frequency comb memory”. *Nature Communications*, 12: 1, 2381.
24. Q.-Y. Cai (2003). “The ping-pong protocol can be attacked without eavesdropping”. *Physical Review Letter*, 91, 109801.
25. A. Wójcik (2003). “Eavesdropping on the “ping-pong” quantum communication protocol”. *Physical Review Letter*, 90: 15: 157901.
26. R. Koenig, U. Maurer, and R. Renner (2022). “On the power of quantum memory”. *IEEE Transactions Information Theory*, 51, 2391–2401.
27. H.-Z. J. Zeng, M. A. P. Nguyen, X. Ai, A. Bennett, A. S. Solntsev, A. Laucht, M. T. L. S. L. Tang, and P. K. Lam, (2022). “Integrated room temperature single-photon source for quantum key distribution”. *Optics Letters*, 47: 7, 1673–1676.
28. X.-F. Ma, B. Qi, Y. Zhao, and H.-K. Lo (2025). “Practical decoy state for quantum key distribution”. *Physical Review A*, 72: 1, 012326.
29. A. El Gamal and Y. H. Kim (2011). *Network Information Theory*, Cambridge: Cambridge University Press.
30. H.-W. Li, Y.-B. Zhao, Z.-Q. Yin, S. Wang, Z.-F. Han, W- S. Bao, and G.-C. Guo (2009). “Security of decoy states QKD with finite resources against collective attacks”. *Optics Communications*, 282: 20, 4162–4166.
31. M. Christandl, R. Koenig, and R. Renner (2008). “Post-selection technique for quantum channels with applications to quantum cryptography”. *Physical Review Letter*, 102: 2, 020504.
32. X.-F. Ma, P. Zeng and H.-Y. Zhou (2018). “Phase-matching quantum key distribution”. *Physical Review X*, 8: 3, 0310431.
33. L. Zhou, J.-P. Lin, Y.-M. Xie, Y.-S. Lu, Y.-M. Jing, H.-L. Yin and Z.-L. Yuan (2023). “Experimental quantum communication overcomes the rate-loss limit without global phase tracking”. *Physical Review Letters*, 130, 250801.
34. Z.-R. Zhou, Y.-B. Sheng, P.-H. Niu, L.-G. Yin, G.-L. Long, and L. Hanzo (2019). “Measurement-device-independent quantum secure direct communication”. *Science China Physics, Mechanics & Astronomy*, 63: 3, 230362.
35. R. Jozsa, and J. Schlienz (1999). “Distinguishability of states and von Neumann entropy”. *Physical Review A*, 62, 012301.