Single-Photon-Memory Measurement-Device-Independent Quantum Secure Direct Communication - Part II: A Practical Protocol and Its Secrecy Capacity

Xiang-Jie Li, Dong Pan, *Member, IEEE*, Gui-Lu Long, *Member, IEEE*, and Lajos Hanzo, *Life Fellow, IEEE*

***Abstract*—In Part I of this two-part letter on single-photon-memory measurement-device-independent quantum secure direct communication (SPMQC), we reviewed the fundamentals and evolution of quantum secure direct communication (QSDC). In this Part II, we propose a practical protocol and analyze its secrecy capacity. In order to eliminate the security loopholes resulting from practical detectors, the measurement-device-independent (MDI) QSDC protocol has been proposed. However, block-based transmission of quantum states is utilized in MDI-QSDC, which requires practical quantum memory that is still unavailable at the time of writing. For circumventing this impediment, we propose the SPMQC protocol for dispensing with high-performance quantum memory. The performance of the proposed protocol is characterized by simulations considering realistic experimental parameters, and the results show that it is feasible to implement SPMQC by relying on existing technology.**

***Index Terms*—Quantum secure direct communication, measurement-device-independent quantum communication, entanglement, secrecy capacity.**

I. Introduction

QUANTUM secure direct communication (QSDC) uses a quantum channel for directly transmitting secret messages. **As mentioned in Part I,** Long and Liu proposed the first QSDC protocol in 2000 [1], in which the messages are mapped onto block-based entangled pairs. Then, in 2003, Deng *et al.* [2] developed the so-called two-step QSDC protocol for encoding messages. Inspired by these protocols, later many other entanglement-based QSDC protocols have been conceived, such as the high-dimensional QSDC protocol of [3], the multi-step QSDC protocol of [4], the quantum secure direct dialogue protocol of [5], the single-photon-memory two-step QSDC of [6], the continuous-variable QSDC of [7], the QSDC network of [8], and so on. Single-photon QSDC protocol was proposed by Deng and Long in 2004 [9], which is termed as the DL04 protocol. **The details of this protocol are described in Part I**

To dispense with high-performance quantum memory which has not yet been realized, quantum-memory-free (QMF) protocols were proposed [10], [11]. In short, the information is transformed by the transmitter to the ciphertext using a shared secure transmission sequence (SSTS), which is similar to the classical one-time pad philosophy. Then Alice encodes the ciphertext into a codeword by using an error correction code, which is then mapped to quantum states to be transmitted to Bob. Bob then demodulates, decodes and recovers the plaintext message. The SSTS is then extracted from the ciphertext by the pair of communicating parties for later transmission. In the communication process, the coding efficiency and the length of the SSTS extracted from the ciphertext are determined by the channel's security capacity, which can be calculated from the error rate, as detailed in Part I. The QMF coding scheme facilitates simultaneous ciphertext transmission and SSTS negotiation. In this scheme, the ciphertext bits can be transmitted one by one upon mapping them to the quantum state, hence eliminating the requirement for the block-based transmission of quantum states relying on quantum memory. The security of the message will be guaranteed by SSTS encryption, which is effectively the classic one-time-pad encryption. QMF-DL04-QSDC using dynamic joint encryption and error-control coding has been experimentally demonstrated over a maximum communication distance of 18.5 km [11]. QMF coding is suitable not only for single-photon QSDC, but also for entanglement-based QSDC [6]. Nonetheless, there are differences between the QMF and the one-time pad. Explicitly, the negotiation of STSS and ciphertext transmission are completed by a single transmission of quantum states in QMF. By contrast, there are two channels for the communication based on the one-time pad - one for secret key negotiation and one for ciphertext transmission.

There is always a gap between theory relying on idealized simplifying assumptions and practice in any technology, thus quantum communication is no exception. Hence, realistic imperfect devices cannot meet the idealized simplifying assumptions of the theory, which might lead to security loopholes. The measurement-device-independent [12], [13], [14], [15], [16], [17] and device-independent [18] versions of quantum communication protocols bridge this gap between theory and practice by removing the detector-side and signal-detector-side channels, respectively. The MDI QSDC protocol uses quantum teleportation and message encoding to send the messages [13]. It has a pair of eavesdropping detection facilities. The first one is used to detect whether there is an eavesdropper in the vicinity before encoding the information, while the

This work is supported by the National Natural Science Foundation of China under Grants No. 11974205 and No. 12205011, the Key R&D Program of Guangdong province (2018B030325002), Beijing Advanced Innovation Center for Future Chip (ICFC), Tsinghua University Initiative Scientific Research Program.

Xiang-Jie Li is with State Key Laboratory of Low-dimensional Quantum Physics and Department of Physics, Tsinghua University, Beijing 100084, China.

Dong Pan is with Beijing Academy of Quantum Information Sciences, Beijing 100193, China.

Gui-Lu Long is with State Key Laboratory of Low-dimensional Quantum Physics and Department of Physics, Tsinghua University, Beijing 100084, China; Beijing Academy of Quantum Information Sciences, Beijing 100193, China; Frontier Science Center for Quantum Information, Beijing 100084, China; Beijing National Research Center for Information Science and Technology, Beijing 100084, China.(e-mail:gllong@mail.tsinghua.edu.cn).

Lajos Hanzo is with School of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, United Kingdom.

L. Hanzo would like to acknowledge the financial support of the Engineering and Physical Sciences Research Council projects EP/W016605/1 and EP/X01228X/1 as well as of the European Research Council's Advanced Fellow Grant QuantCom (Grant No. 789028)

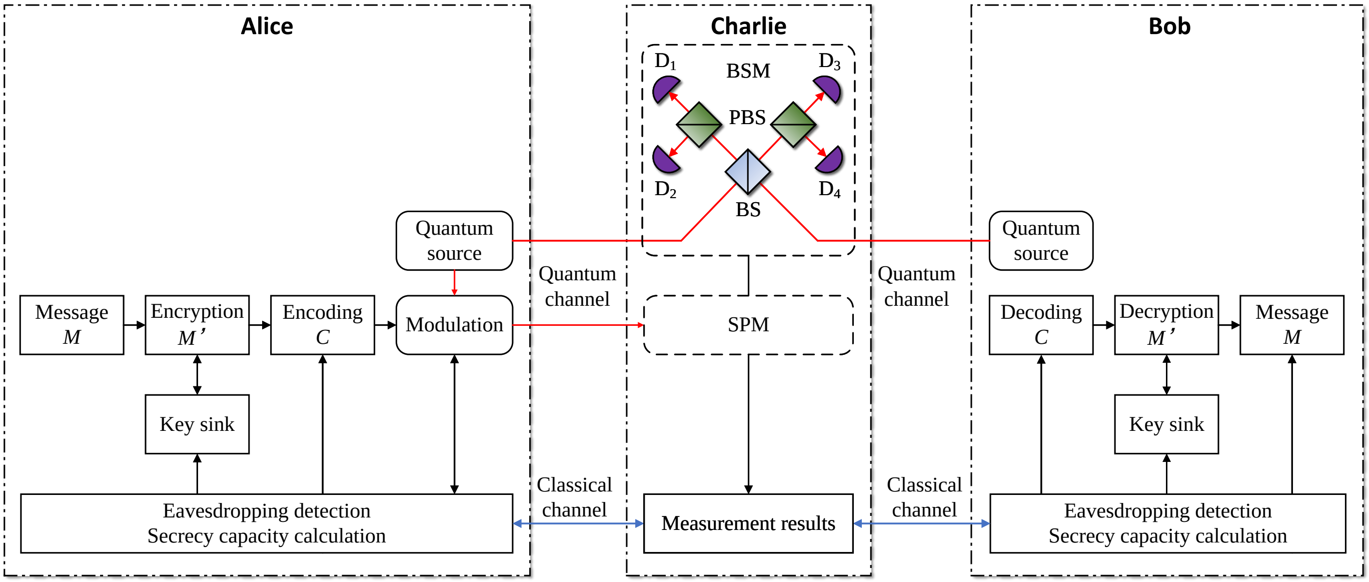

Fig. 1. Schematic diagram of SPMQC. BS, beam splitter; BSM, Bell-state measurement; D_1, D_2, D_3, D_4, detector; PBS, polarizing beam splitter; SPM, single photon measurement.

second one is for integrity detection, namely for detecting whether the transmitted information is tampered with. The eavesdropping detection relies on block-based transmission, since some samples of qubits will be randomly chosen for eavesdropping detection, and the remaining qubits in the block will wait for the results of checking in quantum memory. However, similar to the original QSDC protocol's block-based transmission regime, it is difficult to realize it with current quantum memory technology. Normally, we use an optical delay line instead of quantum memory to store photons [19], which inevitably introduces high attenuation. Hence, for the practical application of MDI QSDC, the conception of a new quantum-memory-free coding-assisted MDI QSDC protocol is essential.

II. Details of our protocol

Here we use QMF coding to replace the quantum memory required for block-transition-based MDI QSDC. Our SPMQC-DL04 protocol is illustrated in Fig. 1. We use the following single qubit states:$|0\rangle$, $|1\rangle$, $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$, and $|\tilde{\pm}\rangle = (|0\rangle \pm i|1\rangle)/\sqrt{2}$. The four Bell-basis states are, $|\phi^{\pm}\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2}$, $|\psi^{\pm}\rangle = (|01\rangle \pm |10\rangle)/\sqrt{2}$ and $M \in \{0,1\}^m$ represents the message that Alice wants to transmit to Bob. Furthermore, $K \in \{0,1\}^m$ represents the keys in the key sink used for encryption and decryption, while $M' \in \{0,1\}^m$ and $C \in \{0,1\}^c$ represent the ciphertext and code word, respectively. We divide the code word into frames, and each round of communication includes the following six steps to send a frame of information. We note that the key sink is empty in the first round. So Alice and Bob should select the appropriate values to estimate the secrecy capacity and the key K [11].

TABLE I
Correspondence between Alice's states and Bob's initial state as well as BSM results [13]. The first column represents Bob's initial state, the four Bell states in the first row are Charlie's measurement results, and the rest are Alice's retained qubits.

For instance, if the BSM result is $|\psi^+\rangle$ and Bob's initial state is $|0\rangle_{\mathrm{B}}$, the retained qubit of Alice will be $|0\rangle_{\mathrm{A}}$. The state of qubit retained by Alice is only known to Bob, since the initial state is prepared by Bob.

Bob's initial state	$\lvert\psi^-\rangle$	$\lvert\psi^+\rangle$	$\lvert\phi^-\rangle$	$\lvert\phi^+\rangle$
$\lvert 0\rangle_{\mathrm{B}}$	$-\lvert 0\rangle_{\mathrm{A}}$	$\lvert 0\rangle_{\mathrm{A}}$	$-\lvert 1\rangle_{\mathrm{A}}$	$-\lvert 1\rangle_{\mathrm{A}}$
$\lvert 1\rangle_{\mathrm{B}}$	$-\lvert 1\rangle_{\mathrm{A}}$	$-\lvert 1\rangle_{\mathrm{A}}$	$-\lvert 0\rangle_{\mathrm{A}}$	$\lvert 0\rangle_{\mathrm{A}}$
$\lvert +\rangle_{\mathrm{B}}$	$-\lvert +\rangle_{\mathrm{A}}$	$\lvert -\rangle_{\mathrm{A}}$	$-\lvert +\rangle_{\mathrm{A}}$	$\lvert -\rangle_{\mathrm{A}}$
$\lvert -\rangle_{\mathrm{B}}$	$-\lvert -\rangle_{\mathrm{A}}$	$\lvert +\rangle_{\mathrm{A}}$	$\lvert -\rangle_{\mathrm{A}}$	$-\lvert +\rangle_{\mathrm{A}}$

Step 1, state preparation. Alice randomly prepares a Bell-state $|\psi^-\rangle$ or a single photon state which is randomly in one of the four states $\{|+\rangle_{\mathrm{A}}, |-\rangle_{\mathrm{A}}, |0\rangle_{\mathrm{A}}, |1\rangle_{\mathrm{A}}\}$. The entangled state is used for information transmission, as shown in Fig. 2a. While the single photon state is used for security checks. Bob prepares a single photon state, which is randomly in one of the four states $\{|+\rangle_{\mathrm{B}}, |-\rangle_{\mathrm{B}}, |0\rangle_{\mathrm{B}}, |1\rangle_{\mathrm{B}}\}$.

Step 2, transmission and measurement. Alice and Bob send their own qubit to Charlie at the same time. Note that if Alice has prepared a pair of entangled qubits, one of the qubits will be forwarded to Charlie and the remaining one is retained by Alice, as shown in Fig. 2b. Charlie receives the qubits sent by Alice as well as Bob, and then he performs a Bell-state measurement (BSM) and announces the measurement result through classical channels.

Step 3, security check. If Alice prepares a single photon, she informs Bob through the classical channel and then they complete the eavesdropping detection and estimate the detection bit error rate (DBER), as detailed in Ref. [13]. This procedure completes the first security check. If the DBER is below the maximum tolerable threshold, then they move to the next step. Otherwise, they return to **Step 1**.

Step 4, state recovery and transmitted message coding. As shown in Table I, if Alice prepares an entangled state, the

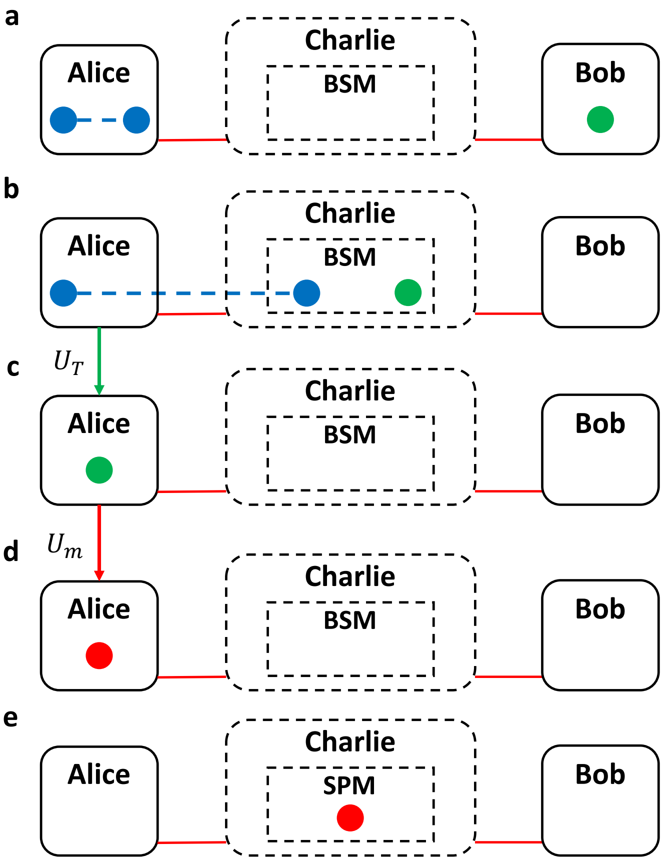

Fig. 2. Photon transmission process of SPMQC when Alice prepares a Bell state. BSM: Bell-state measurement; SPM: single photon measurement.

qubit which is retained by her will have one of the four single-photon states with equal probabilities after Charlie's BSM. Bob announces the basis that he used for preparing the initial state. Alice then recovers the qubit she retained by performing the unitary operation $U_T \in \{I, i\sigma_y\}$ according to the BSM result, as shown in Fig. 2c. To elaborate a little further, if Bob's initial state is prepared in the basis Z and the BSM result is $|\phi^-\rangle$ or $|\phi^+\rangle$, applying a unitary operation $U_T = i\sigma_y$ to Alice' qubit will transform it to the same state as Bob's initial state. We refer to this step as the state recovery, since it completes the teleportation of Bob's initial state to Alice.

Alice applies the Exclusive OR (XOR) operation both to the message M and to the key K distilled from the previous round of information transmission for producing an encrypted ciphertext M', where we have $M' = M \oplus K$. Next Alice performs dynamic joint encryption and error-control coding [11] to ensure the secure and reliable transmission of the ciphertext. Then Alice maps the ciphertext onto a qubit by using $U_m \in \{I, i\sigma_y\}$, where I is used for bit 0, $i\sigma_y$ for bit 1, as shown in Fig. 2d. Alice also randomly chooses some qubits for transmission to carry out a subsequent integrity check, rather than mapping them to the ciphertext.

Step 5, qubit transmission and measurement. Alice sends the qubit containing the ciphertext to Charlie, as shown in Fig. 2e. Charlie measures it on the specific preparation basis that Bob has announced and publishes the measurement results through the classical channel.

Step 6, message decoding and integrity check. Alice announces the random check bits and their position via the classical channel. Then the quantum bit error rate (QBER) is estimated both by Alice and Bob. If the QBER is below the maximum tolerable threshold, the ciphertext transmission is deemed reliable. This procedure represents the integrity check. Then Bob decodes the ciphertext to get the message M. If the message frame has not been transmitted, they return to **Step 1**. Otherwise, Alice and Bob use the DBER and the QBER to estimate the secrecy capacity of the current round of communication and calculate the number of keys they can distill from the ciphertext. Finally, both of them distill and insert the same keys into the key sink to encrypt and decrypt the next round of transmission. The current round of communication is over. Note that the recently proposed solution of increasing the channel capacity using masking (INCUM) [20] in QSDC can be invoked for improving performance as detailed in Ref. [21].

Note that only single-photon storage is required for the qubit retained by Alice, which can be realized by an optical delay line. This is a common characteristic of entanglement-based protocols [22], [6]. In this sense, we simply term the proposed protocol SPMQC.

III. Performance analysis

Based on the security analysis of MDI DL04 QSDC [15], there exists a secrecy capacity C_s, which allows us to use a forward encoding scheme having a coding rate lower than C_s to transmit the message reliably and securely to receivers. The associated asymptotic secrecy capacity lower bound C_s is given by [15]

$$C_s = Q[1 - h(e) - gh(\epsilon_u)], \tag{1}$$

where Q is the signal gain of Bob for message decoding and g is the gain difference between the channels of AB and AE, while e and ϵ_u represent the QBER and DBER, respectively. This is presented in more detail in Ref. [21]. The DBER ϵ_u originates from the three bases $u \in \{X, Y, Z\}$ that are used for the security check [15] in **Step 3**. Subsequently, Alice chooses one of the unitary operations $U_m \in \{\sigma_x, i\sigma_y, \sigma_z\}$ for encoding bit 1 in **Step 4**, and the paired qubits containing the eigenstate of the encoding operation σ_u will be discarded. However, this optimal procedure has not been taken into account in our protocol's description.

To determine the DBER of the proposed protocol using different bases, we perform simulations under the assumption of having ideal quantum sources. The detailed derivation is presented in Ref. [21]. The key parameter settings for our simulations are shown in Table II. As seen in Fig. 3, the DBER e_Z is higher than e_X and e_Y. Both the DBER e_X and e_Y exhibit the same trends. This means that Alice and Bob will have different secrecy capacity, if they use different security check bases. The difference between C_s^Z and C_s^X (C_s^Y) can only be seen, when we focus our attention on a very short distance, as shown in the inset graph of Fig. 4. Hence, we can

TABLE II
KEY PARAMETER SETTINGS OF SIMULATION.

Parameter	Value	Description
δ	0.2 dB/km	the attenuation coefficient
η_d	60%	the efficiency of detectors
e_0	1/2	the error rate of background
e_{det}	1.31%	the intrinsic detector error rate
p_d	1×10^{-6}	dark count
e_d	0.015	the misalignment probability

choose an optimized security check basis X or Y to obtain a higher secrecy capacity. Note that the above results were obtained under the simplifying assumption of having ideal quantum sources. It is plausible that the difference between C_s^Z and C_s^X (C_s^Y) will be larger, if practical light sources, such as weak-coherent pulses and parametric down-conversion, are considered. This is because the distribution of the multiphoton may play an important role in the associated DBER estimation.

Under such circumstances, the importance of choosing an optimized basis for security checks becomes plausible. The results demonstrate the feasibility of SPMQC for applications in metropolitan quantum communications with a range of a few tens of kilometers.

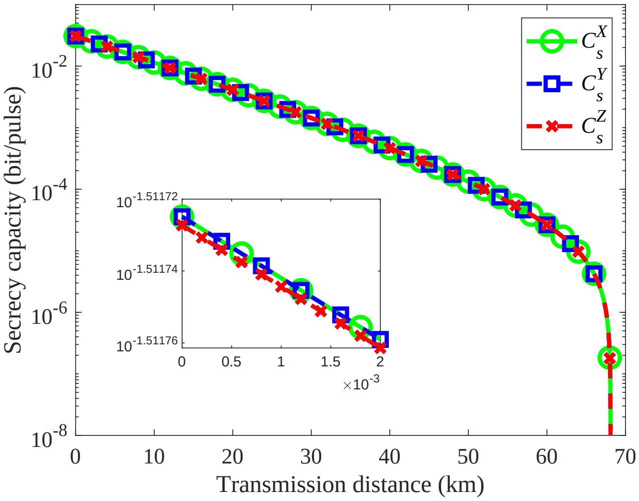

Fig. 4. The secrecy capacity of our SPMQC protocol vs. distance, parameterized by three different security check bases. There are three different lines. The green line labeled by circles represents the secrecy capacity C_s^X changing with transmission distance, while the blue dotted line labeled by squares and the red dotted line labeled by crosses represents C_s^Y and C_s^Z, respectively.

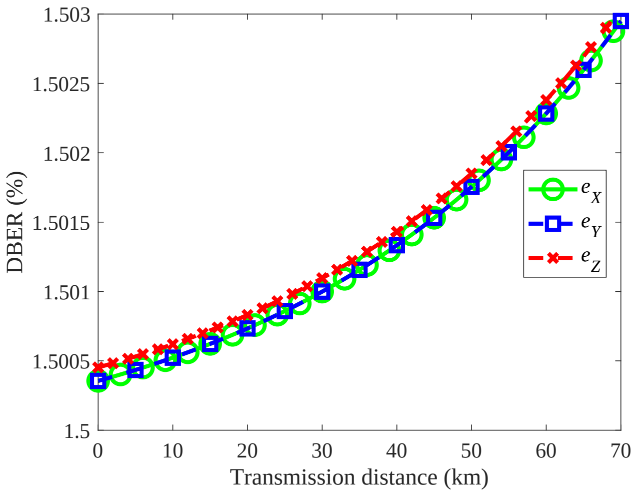

Fig. 3. The DBER vs. the transmission distance parameterized by three different security check bases. The green line labeled by circles represents the DBER e_X changing with the transmission, while the blue dotted line labeled by squares and the red dotted line labeled by crosses represents e_Y and e_Z, respectively.

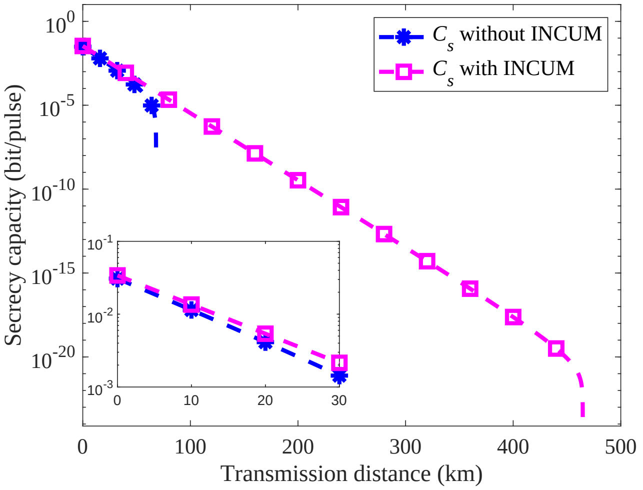

Fig. 5. The secrecy capacity of our SPMQC protocol vs. distance both with and without INCUM technology. The blue line labeled by asterisks and the red line labeled by squares represent the secrecy capacity C_s without and with INCUM technology changing with the transmission, respectively.

Fig. 5 shows the secrecy capacity of the SPMQC protocol both with and without increasing the capacity using masking (INCUM). In a relatively short transmission distance, such as 30 kilometers, the use of INCUM technology has little impact on the secrecy capacity. However, with the increase in transmission distance, the gap between them gradually expands. In particular, when the INCUM technology is not used, the maximum transmission distance of SPMQC is less than 100 kilometers. By contrast, when the INCUM technology is harnessed, the maximum transmission distance can reach hundreds of kilometers. Indeed, the INCUM technology [20] can substantially increase the secrecy capacity and the transmission distance of the protocol.

Finally, we performed numerical simulations for characterizing the influence of dark count on the upper limit of transmission distance. As shown in Fig. 6, the dark count has a significant impact on the transmission distance. As the transmission distance increases, the communication signal will be attenuated, but the dark count will not change. When the signal light intensity attenuation becomes comparable to the dark count, the detector will struggle to distinguish whether the arrival is caused by the signal light or the dark count, so its secrecy capacity will be significantly reduced. When the dark count is 10^{-5}, 10^{-6}, and 10^{-7}, the maximum transmission distance will be 350 kilometers, 450 kilometers,

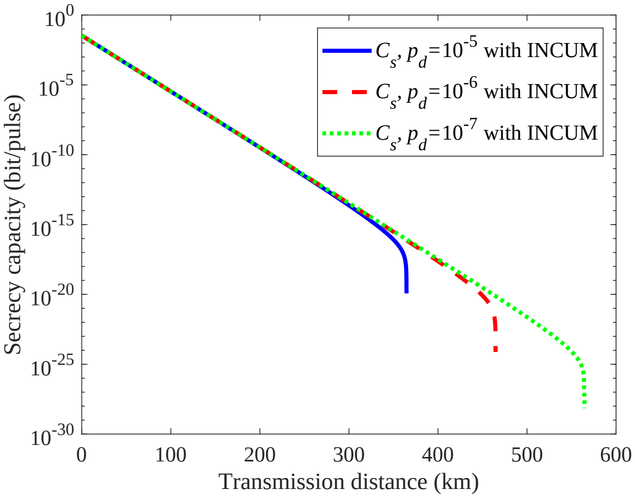

Fig. 6. The secrecy capacity of SPMQC protocol with different dark count rate. The blue line represents the secrecy capacity C_s changing with transmission distance in the dark count rate of 1×10^{-5}, while the red and the green line represents 1×10^{-6} and 1×10^{-7}, respectively.

and 550 kilometers, respectively. Therefore, we can improve the transmission distance of our SPMQC protocol by reducing the dark count rate of the detector.

IV. Conclusion

We have proposed the SPMQC protocol and analyzed its performance. Selecting the optimal security basis X or Y increases beneficially the security capacity of the proposed protocol. The results show our SPMQC is eminently suitable for metropolitan areas covering a range of a few tens of kilometers. with given the rapid evolution of experimental techniques, our SPMQC protocol has the potential of finding its way into practical applications.

But before that, there are some further open issues for future research. Firstly, practical imperfect light sources have to be integrated into our proposed protocol. Secondly, the method of decoy-state based techniques could be utilized to estimate the error rate and reception rate. Thirdly, the family of optimal QMF coding techniques may be combined with optimal MDI protocols [23], [24] for supporting high-rate and long-distance MDI QSDC.

References

[1] G.-L. Long and X.-S. Liu, "Theoretically efficient high-capacity quantum-key-distribution scheme," *Phys. Rev. A*, vol. 65, no. 3, Feb. 2002, Art. no. 032302. (arXiv preprint quant-ph/0012056, 2000).

[2] F.-G. Deng, G. L. Long, and X.-S. Liu, "Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block," *Phys. Rev. A* , vol. 68, no. 4, Oct. 2003, Art. no. 042317.

[3] C. Wang, F.-G. Deng, Y.-S. Li, X.-S. Liu, and G. L. Long, "Quantum secure direct communication with high-dimension quantum superdense coding," *Phys. Rev. A* , vol. 71, no. 4, Apr. 2005, Art. no. 044305.

[4] C. Wang, F. G. Deng, and G. L. Long, "Multi-step quantum secure direct communication using multi-particle Green–Horne–Zeilinger state," *Opt. Commun.* , vol. 253, no. 1-3, pp. 15–20, Sep. 2005.

[5] C. Zheng and G. Long, "Quantum secure direct dialogue using Einstein-Podolsky-Rosen pairs," *Sci. China Phys. Mech.* , vol. 57, pp. 1238–1243, Apr. 2014.

[6] D. Pan, K. Li, D. Ruan, S. X. Ng, and L. Hanzo, "Single-photon-memory two-step quantum secure direct communication relying on Einstein-Podolsky-Rosen pairs," *IEEE Access*, vol. 8, pp. 121146–121161, Jun. 2020.

[7] Z. Cao, L. Wang, K. Liang, G. Chai, and J. Peng, "Continuous-variable quantum secure direct communication based on Gaussian mapping," *Phys. Rev. Appl.*, vol. 16, no. 2, Aug. 2021, Art. no. 024012.

[8] Z. Qi, Y. Li, Y. Huang, J. Feng, Y. Zheng, and X. Chen, "A 15-user quantum secure direct communication network," *Light: Sci. Appl.*, vol. 10, Sep. 2021, Art. no. 183.

[9] F.-G. Deng and G.-L. Long, "Secure direct communication with a quantum one-time pad," *Phys. Rev. A*, vol. 69, no. 5, May 2004, Art. no. 052319.

[10] Z. Sun, R. Qi, Z. Lin, L. Yin, G. Long, and J. Lu, "Design and implementation of a practical quantum secure direct communication system," in *2018 IEEE Globecom Workshops (GC Wkshps)*, IEEE, Dec, 2018, pp. 1–6.

[11] Z. Sun, L. Song, Q. Huang, L. Yin, G. Long, J. Lu, and L. Hanzo, "Toward practical quantum secure direct communication: A quantum-memory-free protocol and code design," *IEEE T. Commun.*, vol. 68, no. 9, pp. 5778–5792, Sep. 2020.

[12] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, no. 13, Mar. 2012, Art. no. 130503.

[13] Z. Zhou, Y. Sheng, P. Niu, L. Yin, G. Long, and L. Hanzo, Z.-R. Zhou, Y.-B. Sheng, P.-H. Niu, L.-G. Yin, G.-L. Long, and L. Hanzo, "Measurement-device-independent quantum secure direct communication," *Sci. China Phys. Mech.*, vol. 63, no. 3, Dec. 2020, Art. no. 230362.

[14] P.-H. Niu, Z.-R. Zhou, Z.-S. Lin, Y.-B. Sheng, L.-G. Yin, and G.-L. Long, "Measurement-device-independent quantum communication without encryption," *Sci. Bull.*, vol. 63, no. 20, pp. 1345–1350, Oct. 2018.

[15] P.-H. Niu, J.-W. Wu, L.-G. Yin, and G.-L. Long, "Security analysis of measurement-device-independent quantum secure direct communication," *Quantum Inf. Process.*, vol. 19, Sep. 2020, Art. no. 356.

[16] D. Pan, S. X. Ng, D. Ruan, L. Yin, G. Long, and L. Hanzo, "Simultaneous two-way classical communication and measurement-device-independent quantum key distribution with coherent states," *Phys. Rev. A*, vol. 101, no. 1, Jan. 2020, Art. no. 012343.

[17] J.-W. Ying, L. Zhou, W. Zhong, and Y.-B. Sheng, "Measurement-device-independent one-step quantum secure direct communication," *Chin. Phys. B* , vol. 31, no. 12, pp. 120303–120303, Nov. 2022.

[18] L. Zhou and Y.-B. Sheng, "One-step device-independent quantum secure direct communication," *Sci. China Phys. Mech.*, vol. 65, no. 5, Mar. 2022, Art. no. 250311.

[19] F. Zhu, W. Zhang, Y. Sheng, and Y. Huang, "Experimental long-distance quantum secure direct communication," *Sci. Bull.*, vol. 62, no. 22, pp. 1519–1524, Nov. 2017.

[20] G.-L. Long and H.-R. Zhang, "Drastic increase of channel capacity in quantum secure direct communication using masking," *Sci. Bull.*, vol. 66, no. 13, pp. 1267–1269, Jul. 2021.

[21] X.-J. Li, D. Pan, G.-L. Long, and L. Hanzo, "Single-photon-memory measurement-device-independent quantum secure direct communication," *arXiv preprint arXiv:2212.05661*, Dec. 2022, https://arxiv.org/pdf/2212.05661.pdf.

[22] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, Aug. 1991.

[23] L. Liu, J. L. Niu, C. R. Fan, X. T. Feng, and C. Wang, "High-dimensional measurement-device-independent quantum secure direct communication," *Quantum Inf. Process.*, vol. 19, Nov. 2020, Art. no. 404.

[24] Z.-K. Zou, L. Zhou, W. Zhong, and Y.-B. Sheng, "Measurement-device–independent quantum secure direct communication of multiple degrees of freedom of a single photon," *EPL (Europhys. Lett.)*, vol. 131, no. 4, Sep. 2020, Art. no. 40005.