

An efficient multiparty quantum secret sharing scheme using a single qudit

Wenwen Hu(胡文文), Bangshu Xiong(熊邦书), and Rigui Zhou(周日贵)

Citation: Chin. Phys. B, 2023, 32 (**8**): 080303. DOI: 10.1088/1674-1056/aca391
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Efficient semi-quantum secret sharing protocol using single particles

Ding Xing(邢丁), Yifei Wang(王艺霏), Zhao Dou(窦钊), Jian Li(李剑),Xiubo Chen(陈秀波), and Lixiang Li(李丽香)
Chin. Phys. B, 2023, 32 (**7**): 070308. DOI: 10.1088/1674-1056/ace159

Realization of the iSWAP-like gate among the superconducting qutrits

Peng Xu(许鹏), Ran Zhang(张然), and Sheng-Mei Zhao(赵生妹)
Chin. Phys. B, 2023, 32 (**2**): 020306. DOI: 10.1088/1674-1056/ac89e7

Measurement-device-independent quantum secret sharing with hyper-encoding

Xing-Xing Ju(居星星), Wei Zhong(钟伟), Yu-Bo Sheng(盛宇波), and Lan Zhou(周澜)
Chin. Phys. B, 2022, 31 (**10**): 100302. DOI: 10.1088/1674-1056/ac70bb

Finite-key analysis of practical time-bin high-dimensional quantum key distribution with afterpulse effect

Yu Zhou(周雨), Chun Zhou(周淳), Yang Wang(汪洋), Yi-Fei Lu(陆宜飞), Mu-Sheng Jiang(江木生), Xiao-Xu Zhang(张晓旭), and Wan-Su Bao(鲍皖苏)
Chin. Phys. B, 2022, 31 (**8**): 080303. DOI: 10.1088/1674-1056/ac6017

Dynamic quantum secret sharing protocol based on two-particle transform of Bell states

Yu-Tao Du(杜宇韬), Wan-Su Bao(鲍皖苏)
Chin. Phys. B, 2018, 27 (**8**): 080304. DOI: 10.1088/1674-1056/27/8/080304

An efficient multiparty quantum secret sharing scheme using a single qudit

Wenwen Hu(胡文文)[1,†], Bangshu Xiong(熊邦书)[2], and Rigui Zhou(周日贵)[3]

[1] *School of Information Engineering, Nanchang Hangkong University, Nanchang* 330063, *China*
[2] *Key Laboratory of Image Processing and Pattern Recognition of Jiangxi Province, Nanchang Hangkong University, Nanchang* 330063, *China*
[3] *College of Information Engineering, Shanghai Maritime University, Shanghai* 201306, *China*

(Received 4 July 2022; revised manuscript received 7 November 2022; accepted manuscript online 17 November 2022)

The aim of quantum secret sharing, as one of most promising components of quantum cryptograph, is one-to-multiparty secret communication based on the principles of quantum mechanics. In this paper, an efficient multiparty quantum secret sharing protocol in a high-dimensional quantum system using a single qudit is proposed. Each participant's shadow is encoded on a single qudit via a measuring basis encryption method, which avoids the waste of qudits caused by basis reconciliation. Security analysis indicates that the proposed protocol is immune to general attacks, such as the measure-resend attack, entangle-and-measure attack and Trojan horse attack. Compared to former protocols, the proposed protocol only needs to perform the single-qudit measurement operation, and can share the predetermined dits instead of random bits or dits.

Keywords: quantum secret sharing, high-dimensional, measurement basis encrypted, security analysis

PACS: 03.67.–a, 03.67.Ac, 03.67.Hk **DOI:** 10.1088/1674-1056/aca391

1. Introduction

Quantum computation and communication have been considered a revolution and has made numerous scientific breakthroughs. The main resources that enable quantum computation and communication to surpass the conventional classical methods are quantum parallelism, quantum entanglement and quantum coherence. In recent years, quantum physics has greatly promoted the development of communication and computation. Compared to classical communication, quantum communication demonstrates higher security and efficiency due to the special properties of quantum mechanics. On the other hand, since quantum computation demonstrates overwhelming computing power compared to its classical counterparts,[1,2] it seriously threatens the security of classical cryptography. Consequently, researchers have devoted their efforts to the search for more secure communication methods, and accordingly promote the development of quantum cryptography. Until now, quantum cryptography research has been applied to many different applications, such as quantum key distribution (QKD),[3–5] quantum secure direct communication (QSDC),[6,7] quantum secret sharing (QSS),[8–14] quantum private query (QPQ)[15,16] quantum digital signatures[17] and quantum conference key agreement.[18]

Secret sharing was independently proposed by Shamir[19] and Blakley[20] in 1979. As one of the primitive forms of cryptography, secret sharing plays a fundamental role in secure multiparty computation that is used to protect highly confidential information. Without question, it has been naturally extended into quantum versions, known as QSS. However, in contrast with classical secret sharing, the shared information in a QSS protocol can be classical or quantum. Accordingly, QSS protocols are classified into two categories. When the shared information is an unknown quantum state, it is called quantum state sharing (QSTS).[10] In the other case, it is categorized as QSS for sharing classical information. Herein, this paper only focuses on the second category, in which a QSS protocol shares the classical information.

The pioneering work of QSS was proposed by Hillery *et al.* in 1999 based on the three-particle and four-particle entangled Greenberger–Horne–Zeilinger (GHZ) state.[11] Following this, Cleve *et al.*[21] investigated the (k,n) threshold QSS protocol. Karlsson *et al.*[22] proposed the concept of a QSS protocol based on quantum entanglement swapping of Bell states. Gottesman[23] shows that any mixed state quantum secret sharing scheme can be derived by discarding a share from a pure-state scheme. In 2003, Guo G P and Guo G C first proposed a QSS protocol without using quantum entanglement.[24] Li et al. generalized Hillery *et al.*'s protocol into an arbitrary multiparty version via approaches that used a favored-measuring-basis and a measuring-basis-encryption scheme.[25] Since then, QSS protocols with different properties have been proposed, such as threshold QSS protocols,[26,27] multiparty to multiparty QSS protocols,[28,29] access structure based QSS protocols,[30,31] dynamic QSS protocols,[32,33] semi QSS protocols,[34,35] measurement-device-independent QSS protocols[36,37] and mediated QSS protocols.[38] However, most of above mentioned QSS protocols are only based on theory, which means that the security of

†Corresponding author. E-mail: 71141@nchu.edu.cn

© 2023 Chinese Physical Society and IOP Publishing Ltd

these protocols is only theoretically verified. Based on the differential phase shift and twinfield technologies used in QKD protocols, Yin *et al*. proposed a three-party QSS protocol that used weak coherent states instead of single-photon states,[13] which improved the secret key rate by three orders of magnitude in a 300-km-long fiber. Furthermore, to improve the poor performance of this protocol over channels with asymmetric transmittances, Yin *et al*. proposed a differential phase shift quantum secret sharing protocol with asymmetric source intensities.[14]

It is worth noting that most of the aforementioned QSS protocols are designed based on multi-particle entangled states because it is easy to split quantum information into multiple pieces due to the inherent correlation of quantum entanglement, such as the Bell state and the GHZ state. However, a major difficulty in quantum communication is the limit on the number of particles that can be coupled experimentally, which makes the multi-particle entangled state extremely fragile and thus their preparation and transmission difficult. Hence, due to the highly fragile characteristics of multi-particle entangled quantum states, it seems that a multiparty QSS (MQSS) protocol designed without quantum entanglement will become more practical. Some QSS protocols[12,28,29,39,40] that do not utilize quantum entanglement have been proposed. Furthermore, communication protocols that have been designed based on quantum resources of high-dimensional quantum systems (qudit) demonstrate higher resource capacity and security than qubits.[41,42] Undoubtedly, QSS protocols designed on quantum resources of qudits have become a new research hotspot.[43–48]

In this paper, inspired by the idea of the measuring-basis-encryption QSS protocol in Ref. [25], we propose the MQSS protocol using the single qudit state. Therein, a dit secret is split into n pieces of shadows via modulus operation, and each shadow is randomly encoded in the eigenstate of two mutually unbiased measurement bases (MBs). By transmitting the MBs via the QSDC protocol, each participant can obtain their shadows by measuring the received qudits in the correct MBs and avoids the waste of qudits arising from basis reconciliation. In contrast to (k,n)-threshold QSS protocols, the proposed scheme is a special case of the (k,n)-threshold QSS scheme in which all participants are authorized ($k \equiv n$) and the dealer's secret recovery needs the combination of all the participants' secret shadows. Thus, the present protocol has a slightly narrower application than the threshold QSS scheme, while the protocol implementation is much easier. Compared to most of the former QSS protocols, the proposed protocol poses some distinct advantages: (1) the proposed protocol is designed on single qudit states without using quantum entanglement; (2) the participant only performs single-qudit measurement operation without additional local quantum unitary operations; (3) the proposed protocol is asymptotically 100% efficient.

The rest of this paper is organized as follows: Section 2 introduces the two mutually unbiased MBs in the context of the qudit. Section 3 describes the proposed MQSS protocol in detail. Section 4 proves that the present QSS protocol is secure against common attacks. Section 5 demonstrates the secret key rate analyses of the present protocol in four different quantum noise channels. Section 6 presents the comparisons of the present protocol with former QSS protocols. Finally, Section 7 draws the conclusions.

2. Two mutually unbiased measurement bases

For a single qudit, an unknown quantum state can be described as

$$|\psi\rangle = \sum_{j=0}^{d-1} a_j |\boldsymbol{j}\rangle, \tag{1}$$

where a_j is a complex number, and satisfies the normalization condition $\sum_{j=0}^{d-1} |a_j|^2 = 1$.

Similar to MBs of the Z basis and X basis in the context of the qubit, the Z basis and X basis for the single qudit[49] are defined as

$$\begin{aligned} &Z \text{ basis}: \left|\boldsymbol{Z}_j\right\rangle = |\boldsymbol{j}\rangle, \quad j = 0,1,\ldots,d-1, \\ &X \text{ basis}: \left|\boldsymbol{X}_j\right\rangle = \frac{1}{\sqrt{d}} \mathrm{e}^{\frac{2\pi \mathrm{i}}{d} k} |\boldsymbol{k}\rangle. \end{aligned} \tag{2}$$

The reason why the Z basis and X basis are recognized as mutually unbiased MBs is

$$\left|\langle \boldsymbol{Z}_j | \boldsymbol{X}_k \rangle\right|^2 = \frac{1}{d}, \quad j,k \in \{0,1,\ldots,d-1\}. \tag{3}$$

This means that when a single qudit stays in the eigenstate of the Z basis (X basis), but it is measured by X basis (Z basis), the final obtained measurement result is absolutely random.

3. Proposed MQSS protocol

Suppose that a dealer, Alice, wants to share the m-dit secret $\boldsymbol{K} = k_1 k_2 \ldots k_m$, $k_j \in \{0,1,\ldots,d-1\}$ among n participants Bob_1, Bob_2, …, Bob_n, and only when all the participants collaborate can they recover Alice's secret. The proposed MQSS protocol can be described by the following steps:

Step 1. Resources preparation and distribution

1.1 Alice generates n pair strings $(\boldsymbol{A}_i, \boldsymbol{B}_i)$ randomly, for i =1, 2, …, n, wherein $\mathrm{A}_i = a_i^1 a_i^2 \ldots a_i^m$, $a_i^j \in \{0, 1, \ldots, d-1\}$, $\mathrm{B}_i = b_i^1 b_i^2 \ldots b_i^m$, $b_i^j \in \{0, 1\}$. Herein, let us assume that the dit string shared by Alice is $\boldsymbol{K} = k_1 k_2 \ldots k_m$, $k_j = a_1^j + a_2^j + \cdots a_{n-1}^j + a_n^j \,(\mathrm{mod}\, d)$.

1.2 Alice encodes each pair string $(\boldsymbol{A}_i, \boldsymbol{B}_i)$ as a sequence of m qudits, in which each qudit is randomly encoded in an

eigenstate of Z basis or X basis as

$$\left|\psi_{a_i^j b_i^j}\right\rangle = \begin{cases} |\boldsymbol{a}_i^j\rangle, & b_i^j = 0, \\ \dfrac{1}{\sqrt{d}} \sum\limits_{k=0}^{d-1} \mathrm{e}^{\frac{2\pi \mathrm{i} \cdot a_i^j}{d} k} |\boldsymbol{k}\rangle, & b_i^j = 1. \end{cases} \tag{4}$$

Specifically, Alice encodes the dit value a_i^j in the eigenstate of Z basis when $b_i^j = 0$; otherwise, she encodes a_i^j in the eigenstate of X basis.

1.3 Assume that each encoded m qudits of a pair string ($\boldsymbol{A}_i$, $\boldsymbol{B}_i$) is denoted as an ordered particle sequence $\boldsymbol{S}_i = s_i^1 s_i^2 \ldots s_i^m$, $s_i^j = |\psi_{a_i^j b_i^j}\rangle$. For each sequence $\boldsymbol{S}_i$, Alice prepares enough detecting particles (herein, we suppose that the number of detecting particles is h) so that each particle is randomly chosen from $\left\{\left|\boldsymbol{Z}_j\right\rangle, \left|\boldsymbol{X}_j\right\rangle\right\}_{j=0}^{d-1}$, and then inserts these detecting particles randomly into $\boldsymbol{S}_i$ to obtain a new ordered particle sequence $\boldsymbol{S}_i^*$. Note that Alice keeps a record of the insertion position and the initial states of these detecting particles in each sequence $\boldsymbol{S}_i^*$. Then, she delivers sequence $\boldsymbol{S}_i^*$ to participant Bob_i, for $i = 1$ to n, via a quantum channel.

Step 2. Eavesdropping check

2.1 Each Bob_i stores the received particles in local quantum memory, and finally returns the number of received particles to Alice after receiving the sequence. Alice goes to the next step if the number is $m + h$; or else, she terminates the protocol.

2.2 Alice publicly announces the positions of these detecting particles in $\boldsymbol{S}_i^*$ to Bob_i via an authenticated classical channel. Bob_i measures these detecting particles randomly in Z basis or X basis and then publicly declares his measurement results. It is expected that there will be four different cases:

Case 1: For approximately $h/4$ qudits, Alice prepares it in Z basis and Bob_i measures them in Z basis. Accordingly, Alice expects her value to be unchanged.

Case 2: For approximately $h/4$ qudits, Alice prepares it in Z basis and Bob_i measures them in X basis. Accordingly, Alice expects a uniform distribution.

Case 3: For approximately $h/4$ qudits, Alice prepares it in X basis and Bob_i measures them in Z basis. Accordingly, Alice expects a uniform distribution.

Case 4: For approximately $h/4$ qudits, Alice prepares it in X basis and Bob_i measures them in X basis. Accordingly, Alice expects her value to be unchanged.

According to Bob_i's measurement results, Alice can compute the error rate and compare with the pre-defined threshold determined by the channel noise. If the error rate exceeds the prior threshold, then Alice asks Bob_i to abort the process and starts a new one; otherwise, Bob_i accepts the received particle sequence and obtains the particle sequence $\boldsymbol{S}_i$, for $i = 1$ to n.

Step 3. Secret recovery

3.1 Alice sends the measurement bases (MBs), i.e., the sequence B_i, to Bob_i via the QSDC protocol,[6–8] for $i = 1$ to n.

3.2 All the participants, Bob_1, Bob_2, …, Bob_n, measure their particles $\boldsymbol{S}_i$ in the correct MBs to obtain their shadows. That is, if $b_i^j = 0$, then Bob_i measures his particle $|\psi_{a_i^j b_i^j}\rangle$ in Z basis; otherwise, Bob_i measures his particle $|\psi_{a_i^j b_i^j}\rangle$ in X basis. Herein, the measurement results of the quantum states $\left|\boldsymbol{Z}_j\right\rangle$ and $\left|\boldsymbol{X}_j\right\rangle$ correspond to the classical dit value j and each participant's Bob_i's shadows are denoted as $\boldsymbol{B}_i = k_i^1 k_i^2 \ldots k_i^m$.

3.3 When, and only when, all participants Bob_1, Bob_2, …, Bob_n collaborate together can they reconstruct Alice's m-dit secret $\boldsymbol{K}$ as

$$\begin{aligned} \boldsymbol{K} &= \textstyle\prod_{j=1}^{m} \left(k_1^j + k_2^j + \cdots + k_{n-1}^j + k_n^j\right) \bmod d \\ &= \textstyle\prod_{j=1}^{m} \left(a_1^j + a_2^j + \cdots + a_{n-1}^j + a_n^j\right) \bmod d \\ &\equiv k_1 k_2 \ldots k_m. \end{aligned} \tag{5}$$

4. General attacks analysis

This section demonstrates that our present MQSS protocol is secure against general attacks, such as the measure-resend attack, entangle-and-measure attack and Trojan horse attack. Besides, we consider that an internal dishonest participant knows a part of secret share, which means he has more powerful eavesdropping capabilities than an outside eavesdropper (Eve). Consequently, the attack behavior of the malicious participant, instead of Eve, is analyzed in detail.

4.1. Measure-resend attack

In the proposed MQSS protocol, the measure-resend attack can be described as: a malicious participant (say Bob_k) may try to measure other participants' particles sent by Alice directly and prepare the fresh particles according to his measurement results. The detecting particles in the present protocol, i.e., $\{|\boldsymbol{Z}_j\rangle, |\boldsymbol{X}_j\rangle, j = 0, 1, \ldots, d-1\}$, are randomly inserted into the transmitted particles sequence and then sent to participants. Without any prior knowledge of the specific positions and correct MBs of these inserted detecting particles, Bob_k will select the wrong measurement basis with probability $1/2$ for each detecting particle. If he selects the wrong MBs and prepares the new particle according to his measurement results, then the receiver can only get the correct measurement result with probability $1/d$. Thus, the error rate introduced by Bob_k is $(d-1)/(2d)$ for each detecting particle. Therefore, Eve's existence can be theoretically detected in public discussion with probability of $1 - [(d+1)/(2d)]^h$, where h is the number of detecting particles. It is obvious that the eavesdropping detection probability $1 - [(d+1)/(2d)]^h$ will quickly approach 1 with the increase in h. Therefore, the present MQSS protocol is secure against measure-resend attack.

4.2. Entangle-and-measure attack

Herein, we demonstrate that the present protocol is completely robust to entangle-and-measure attack to prove its security.[50] For the entangle-and-measure attack, the malicious participant Bob_k may use a unitary operation $\boldsymbol{U}_E$ to entangle an ancillary particle $|\boldsymbol{E}\rangle$ on the transmitted particle, and then measures the ancillary particle to steal secret information. If the transmitted qudit is encoded in the eigenstate of Z basis, the effect of the unitary operation $\boldsymbol{U}_E$ performed on the detecting particle can be shown as

$$\begin{aligned}\boldsymbol{U}_E|\boldsymbol{j}\rangle|\boldsymbol{E}\rangle =\ & |0\rangle|\boldsymbol{e}_{j,0}\rangle+|1\rangle|\boldsymbol{e}_{j,1}\rangle+\cdots+|\boldsymbol{j}\rangle|\boldsymbol{e}_{j,j}\rangle+\cdots\\ &+|\boldsymbol{d}-1\rangle|\boldsymbol{e}_{j,d-1}\rangle,\end{aligned}\tag{6}$$

where $|\boldsymbol{e}_{j,k}\rangle$, $k\in\{0,\,1,\,\ldots,\,d-1\}$ are d un-normalized states that belong to the Hilbert space of Bob_k's ancillary particle $\boldsymbol{H}_E$, which can be distinguished by Bob_k. Obviously, to avoid introducing errors to the transmitted particle, it holds that

$$\begin{aligned}|\boldsymbol{e}_{j,0}\rangle=|\boldsymbol{e}_{j,1}\rangle &=\cdots=|\boldsymbol{e}_{j,j-1}\rangle=|\boldsymbol{e}_{j,j+1}\rangle\\ &=\cdots=|\boldsymbol{e}_{j,d-1}\rangle=0.\end{aligned}\tag{7}$$

Therefore, the effect of $\boldsymbol{U}_E$ performed on the transmitted qudit can be simplified as

$$\boldsymbol{U}_E|\boldsymbol{j}\rangle|\boldsymbol{E}\rangle=|\boldsymbol{j}\rangle|\boldsymbol{e}_{j,j}\rangle=|\boldsymbol{j}\rangle|\boldsymbol{e}_j\rangle.\tag{8}$$

Accordingly if the particle is encoded in the eigenstate of X basis, the effect of the unitary operation $\boldsymbol{U}_E$ performed on the detecting particle can be shown as

$$\begin{aligned}\boldsymbol{U}_E|\boldsymbol{X}_j\rangle|\boldsymbol{E}\rangle &=\boldsymbol{U}_E\left(\frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\mathrm{e}^{\frac{2\pi\mathrm{i}\cdot j}{d}k}|\boldsymbol{k}\rangle\right)|\boldsymbol{E}\rangle\\ &=\frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\mathrm{e}^{\frac{2\pi\mathrm{i}\cdot j}{d}k}\boldsymbol{U}_E|\boldsymbol{k}\rangle|\boldsymbol{E}\rangle\\ &=\frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\mathrm{e}^{\frac{2\pi\mathrm{i}\cdot j}{d}k}|\boldsymbol{k}\rangle|\boldsymbol{e}_k\rangle.\end{aligned}\tag{9}$$

Since each eigenstate in Z basis can be expressed as the composition of a sequence of eigenstates in X basis defined as $|\boldsymbol{k}\rangle=\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}\mathrm{e}^{-\frac{2\pi\mathrm{i}\cdot k}{d}j}|\boldsymbol{X}_j\rangle$, we can deduce that

$$\begin{aligned}&\boldsymbol{U}_E|\boldsymbol{X}_j\rangle|\boldsymbol{E}\rangle\\ &=\frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\mathrm{e}^{\frac{2\pi\mathrm{i}\cdot j}{d}k}|\boldsymbol{k}\rangle|\boldsymbol{e}_k\rangle\\ &=\frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\mathrm{e}^{\frac{2\pi\mathrm{i}\cdot j}{d}k}\frac{1}{\sqrt{d}}\sum_{h=0}^{d-1}\mathrm{e}^{-\frac{2\pi\mathrm{i}\cdot k}{d}h}|\boldsymbol{X}_h\rangle\ |\boldsymbol{e}_k\rangle\\ &=\frac{1}{d}\sum_{k=0}^{d-1}\sum_{h=0}^{d-1}\mathrm{e}^{\frac{2\pi\mathrm{i}}{d}(j-h)k}|\boldsymbol{X}_h\rangle\ |\boldsymbol{e}_k\rangle\\ &=\frac{1}{d}\left(|\boldsymbol{X}_0\rangle\sum_{k=0}^{d-1}\mathrm{e}^{\frac{2\pi\mathrm{i}(j-0)}{d}k}\ |\boldsymbol{e}_k\rangle+|\boldsymbol{X}_1\rangle\sum_{k=0}^{d-1}\mathrm{e}^{\frac{2\pi\mathrm{i}(j-1)}{d}k}\ |\boldsymbol{e}_k\rangle\right.\\ &\quad\left.+\cdots+|\boldsymbol{X}_{d-1}\rangle\sum_{k=0}^{d-1}\mathrm{e}^{\frac{2\pi\mathrm{i}[j-(d-1)]}{d}k}|\boldsymbol{e}_k\rangle\right).\end{aligned}\tag{10}$$

Equation (10) can be further expressed as

$$\begin{aligned}\boldsymbol{U}_E|\boldsymbol{X}_j\rangle|\boldsymbol{E}\rangle =\ & \sum_{h=0,h\neq j}^{d-1}|\boldsymbol{X}_h\rangle\frac{1}{d}\sum_{k=0}^{d-1}\mathrm{e}^{\frac{2\pi\mathrm{i}}{d}(j-h)k}|\boldsymbol{e}_k\rangle\\ &+|\boldsymbol{X}_j\rangle\frac{1}{d}\sum_{k=0}^{d-1}|\boldsymbol{e}_k\rangle.\end{aligned}\tag{11}$$

Thus, to avoid introducing errors to the transmitted particle, it should hold that $\sum_{k=0}^{d-1}\mathrm{e}^{\frac{2\pi\mathrm{i}}{d}(j-h)k}|\boldsymbol{e}_k\rangle=0$ for $j\neq h$. Note that when $(j-h)\neq 0\,(\mathrm{mod}\,d)$, it holds that $\mathrm{e}^{\frac{2\pi\mathrm{i}}{d}(j-h)k}\neq 0$. On the other hand, the sum of $\sum_{k=0}^{d-1}\mathrm{e}^{\frac{2\pi\mathrm{i}}{d}(j-h)k}$ can be calculated as

$$\begin{aligned}\sum_{k=0}^{d-1}\mathrm{e}^{\frac{2\pi\mathrm{i}}{d}(j-h)k} &=\frac{1-\mathrm{e}^{\frac{2\pi\mathrm{i}}{d}(j-h)(d-1)}\times\mathrm{e}^{\frac{2\pi\mathrm{i}}{d}(j-h)}}{1-\mathrm{e}^{\frac{2\pi\mathrm{i}}{d}(j-h)}}\\ &=\frac{1-\mathrm{e}^{2\pi\mathrm{i}(j-h)}}{1-\mathrm{e}^{\frac{2\pi\mathrm{i}}{d}(j-h)}}=\frac{1-1}{1-\mathrm{e}^{\frac{2\pi\mathrm{i}}{d}(j-h)}}=0.\end{aligned}\tag{12}$$

Hence, only when $|\boldsymbol{e}_i\rangle\equiv|\boldsymbol{e}_j\rangle$ for any $i,j\in\{0,1,\ldots,d-1\}$, it holds that $\sum_{k=0}^{d-1}\mathrm{e}^{\frac{2\pi\mathrm{i}}{d}(j-h)k}|\boldsymbol{e}_k\rangle\equiv 0$ for $j\neq h$. Accordingly, we can obtain that $\boldsymbol{U}_E|\boldsymbol{X}_j\rangle|\boldsymbol{E}\rangle=|\boldsymbol{X}_j\rangle|\boldsymbol{e}_j\rangle$. Apparently, to avoid an eavesdropping check, Bob_k's entangle-and-measure attack can only get the same information from his ancillary particle. In other words, if he wants to steal any useful information from the transmitted particle, he would definitely introduce the error to the detecting particle and then could be detected. Thus, the present protocol is completely robust to entangle-and-measure attack.

4.3. Trojan horse attack

The Trojan horse attack is generally classified into two types.[51,52] The first type uses so-called delayed photon technology. In this attack, an attacker intercepts a particle transmitted to a participant and then inserts a probing photon in the particle with a delay time that is shorter than the original time window. Using this method, a participant cannot detect the fake photon because it does not register on their detector. The second type of Trojan horse attack uses an invisible photon, i.e., the attacker attaches an invisible photon to each particle sent to the participant. In the two types of Trojan horse attacks mentioned above, when a participant performs the unitary operation on the transmitted particle, the inserted particle, i.e., the probing photon or invisible photon that attaches to it will also receive the same operation simultaneously. Therefore, when the participant returns the particle, the attacker can intercept the particle again and separates the probing photon or invisible photon. The attacker can obtain full information regarding a participant's operation by measuring the previously

inserted separated photon. Since the participants cannot detect this fake photon, the Trojan horse attack cannot be detected.

In summary, the quantum communication protocols are considered vulnerable to Trojan horse attacks if they adopt two-way or circular communication. In contrast, in a one-way communication protocol, since the attacker has no chance to collect the malicious photons from the Trojan horse attacks because no particle is returned by the participant, the protocol will be robust to Trojan horse attacks. In the proposed MQSS protocol, the qudit transmission applies a one-way transmission strategy in which the qudits are sent only from the dealer to the participants. Although the attacker can insert probing photons or invisible photons into each transmitted qudit, the information of the participants' secret shadow bits cannot be obtained due to the fact that the probing photons will not be sent out after they are received by the participants. From the above analysis, we know that the proposed MQSS is congenitally free from Trojan horse attacks and all the participants do not have to install costly special optical devices such as the photon number splitter and the optical wavelength filter.

5. Secret key rate analysis in noise channel

In real quantum communication, each qudit transmitted in a channel will be unavoidably affected by channel noise, which certainly affects the present MQSS protocol's performance (i.e., secret key rate). Thus, this section illustrates the key rate analysis of the present MQSS protocol under different quantum noisy channels in detail. To simplify the analysis, each time we only consider one type of noise model in the quantum channel and no qudit loss during the transmission.

5.1. Noise models

The generally encountered noise models for describing a single qudit transmitted in a quantum channel are the dit-flip, d-phase-flip, amplitude damping and depolarizing noise.[53] The Kraus operator is an effective method that is used to describe the effect of a single qudit that is transmitted in these four noise models, and it can be represented by every completely positive trace-preserving map ε defined as

$$\rho' = \varepsilon(\rho) = \sum_K E_K \rho E_K^{\dagger}, \tag{13}$$

where ρ and ρ' respectively correspond to the density matrices of input and output quantum states, and the Kraus operator E_K is represented by the Weyl operator.[54] The Weyl operator is a quantum unitary transformation defined as

$$U_{m,n} = \sum_{k=0}^{d-1} w^{k\cdot m} |(k+n) \bmod d\rangle \langle k|, \quad m,n = 0,1,\ldots,d-1. \tag{14}$$

The dit-flip noise would flip the Z basis state $|j\rangle$ either to any other states of $|(j+1) \bmod d\rangle$, $|(j+2) \bmod d\rangle$, $\cdots$, or $|(j+d-1) \bmod d\rangle$ with probability p and leave it unchanged with probability $1-p$. Thus, the corresponding Kraus operators are described as

$$E_{0,0} = \sqrt{1-p}\, U_{0,0}, \quad E_{0,j} = \sqrt{\frac{p}{d-1}}\, U_{0,j}, \quad j = 1,2,\ldots,d-1. \tag{15}$$

The d-phase-flip noise describes the loss of quantum information without energy dissipation. This kind of noise channel would cause any state $|j\rangle$ with probability p to suffer one out of $d-1$ phases of the form $w|j\rangle$, $w^2|j\rangle$, ..., or $w^{d-1}|j\rangle$. Its Kraus operators are written as

$$E_{0,0} = \sqrt{1-p}\, U_{0,0}, \quad E_{0,j} = \sqrt{\frac{p}{d-1}}\, U_{j,0}, \ j = 1,2,\ldots,d-1. \tag{16}$$

Amplitude-damping noise describes the energy dissipation effects due to loss of energy from a quantum system, which would flip any state $|j\rangle$ into $|0\rangle$ with probability p except the state $|0\rangle$. The corresponding Kraus operators can be expressed as

$$E_0 = |0\rangle\langle 0| + \sqrt{1-p} \sum_{j=1}^{d-1} |j\rangle\langle j|, \quad E_1 = \sqrt{p} \sum_{j=1}^{d-1} |0\rangle\langle j|. \tag{17}$$

Depolarizing noise means that a quantum system initially prepared in an arbitrary state would evolve to a maximally mixed state I_d/d with probability p. The Kraus operators for this noise are given as

$$E_{0,0} = \sqrt{1 - \frac{d^2-1}{d^2} p}\, U_{0,0}, \quad E_{m,n} = \sqrt{\frac{p}{d^2}}\, U_{m,n}, \quad 0 \le m,n \le d-1, \ (m,n) \neq (0,0). \tag{18}$$

5.2. Secret key rate in noise channel

Fidelity is an effective index that measures the distance of two quantum states. Here we adopt it to evaluate the secret key rate of the proposed MQSS protocols in a quantum noisy channel. Fidelity is defined as $F = \mathrm{tr}(\rho_1 \cdot \rho_2)$, where tr() denotes the trace operation of the matrix, and ρ_1 and ρ_2 respectively denote the density matrices of two quantum states.

For simplicity of analysis, let us assume that Alice has equal probability $1/2$ to prepare each encoded qudit in the eigenstate of Z basis or X basis The mean fidelity can be calculated as

$$F^m = \frac{1}{2}(F_Z^m + F_X^m), \tag{19}$$

where the subscripts Z and X denote the mean fidelity of each qudit respectively encoded in eigenstates of Z basis and

X basis, and the superscript $m \in \{\mathrm{df}, \mathrm{dph}, \mathrm{ad}, \mathrm{d}\}$ corresponds to different noise models of dit-flip, d-phase-flip, amplitude-damping and depolarizing.

Therefore, given all possible choices of encoding eigenstates in Z basis or X basis, the mean fidelity F_Z^m and F_X^m are calculated in following forms:

$$\{F_Z^m, F_X^m\} = \frac{1}{d}\sum_{j=0}^{d-1} \mathrm{tr}\left(\rho_{\mathrm{in}}^j \rho_{\mathrm{out}}^j\right), \tag{20}$$

where ρ_{in}^j represents the density matrix of the initial qudit state while ρ_{out}^j represents the final density matrix after the qudit is transmitted in the quantum noise channel.

For any state $|k\rangle$ of Z basis transmitted via dit-flip, d-phase-flip, amplitude damping and depolarizing quantum channels, the corresponding effect can be expressed as

$$\begin{aligned}
\rho_{\mathrm{df}}^k &= \varepsilon^{\mathrm{df}}\left(\rho_{\mathrm{in}}^k\right) = (1-p)\,U_{00}\,|k\rangle\langle k|\,U_{00}^\dagger \\
&\quad + \sum_{j=1}^{d-1}\frac{p}{d-1}\left(U_{0j}\,|k\rangle\langle k|\,U_{0j}^\dagger\right) \\
&= (1-p)\,|k\rangle\langle k| + \frac{p}{d-1}\sum_{j=0,j\neq k}^{d-1}|j\rangle\langle j|, \qquad (21)\\
\rho_{\mathrm{dpf}}^k &= \varepsilon^{\mathrm{dpf}}\left(\rho_{\mathrm{in}}^k\right) = (1-p)\,U_{00}\,|k\rangle\langle k|\,U_{00}^\dagger \\
&\quad + \sum_{j=1}^{d-1}\frac{p}{d-1}\left(U_{j0}\,|k\rangle\langle k|\,U_{j0}^\dagger\right) = |k\rangle\langle k|, \qquad (22)\\
\rho_{\mathrm{ad}}^k &= \varepsilon^{\mathrm{ad}}\left(\rho_{\mathrm{in}}^k\right) \\
&= |0\rangle\langle 0|\,\rho_{\mathrm{in}}^k\,|0\rangle\langle 0| + |0\rangle\langle 0|\,\rho_{\mathrm{in}}^k\sqrt{1-p}\sum_{j=1}^{d-1}|j\rangle\langle j| \\
&\quad + \sqrt{1-p}\sum_{j=1}^{d-1}|j\rangle\langle j|\rho_{\mathrm{in}}^k\,|0\rangle\langle 0| + (1-p) \\
&\quad \times \sum_{j=1}^{d-1}|j\rangle\langle j|\rho_{\mathrm{in}}^k\,|j\rangle\langle j| + p\sum_{j=1}^{d-1}|0\rangle\langle j|\rho_{\mathrm{in}}^k\,|j\rangle\langle 0| \\
&= (|0\rangle\langle 0|)(|k\rangle\langle k|)(|0\rangle\langle 0|) \\
&\quad + \sqrt{1-p}\,(|0\rangle\langle 0|)(|k\rangle\langle k|)\sum_{j=1}^{d-1}(|j\rangle\langle j|) \\
&\quad + \sqrt{1-p}\left(\sum_{j=1}^{d-1}|j\rangle\langle j|\right)(|k\rangle\langle k|)(|0\rangle\langle 0|) \\
&\quad + (1-p)\sum_{j=1}^{d-1}(|j\rangle\langle j|)(|k\rangle\langle k|)(|j\rangle\langle j|) \\
&\quad + p\sum_{j=1}^{d-1}(|0\rangle\langle j|)(|k\rangle\langle k|)(|j\rangle\langle 0|), \qquad (23)\\
\rho_{\mathrm{d}}^k &= \varepsilon^{\mathrm{d}}\left(\rho_{\mathrm{in}}^k\right) = \left(1-\frac{d^2-1}{d^2}p\right)U_{00}\,|k\rangle\langle k|\,U_{00}^\dagger \\
&\quad + \frac{p}{d^2}\sum_{\substack{m,n=0,\\(m,n)\neq(0,0)}}^{d-1}\left(U_{mn}\,|k\rangle\langle k|\,U_{mn}^\dagger\right) \\
&= \left(1-\frac{d-1}{d}p\right)|k\rangle\langle k| + \frac{P}{d}\sum_{j=0,j\neq k}^{d-1}|j\rangle\langle j|, \qquad (24)
\end{aligned}$$

where the subscripts df, dpf, ad and d in Eqs. (21)–(24) correspond to dit-flip, d-phase-flip, amplitude damping and depolarizing quantum channels here and thereafter.

Accordingly, the mean fidelity of any qudit state in Z basis when it is transmitted in four types of quantum noisy channels is calculated as

$$\begin{aligned}
F_Z^{\mathrm{df}} &= \frac{1}{d}\sum_{k=0}^{d-1}\mathrm{tr}\left\{(|k\rangle\langle k|)\left[(1-p)\,|k\rangle\langle k| \right.\right. \\
&\quad \left.\left. + \frac{p}{d-1}\sum_{j=0,j\neq k}^{d-1}|j\rangle\langle j|\right]\right\} = (1-p), \qquad (25)\\
F_Z^{\mathrm{dpf}} &= \frac{1}{d}\sum_{k=0}^{d-1}\mathrm{tr}\left\{(|k\rangle\langle k|)(|k\rangle\langle k|)\right\} = 1, \qquad (26)\\
F_Z^{\mathrm{ad}} &= \frac{1}{d}\sum_{k=0}^{d-1}\mathrm{tr}\left\{\rho_{\mathrm{in}}^k\rho_{\mathrm{out}}^k\right\} \\
&= \frac{1}{d}(|0\rangle\langle 0|\,|0\rangle\langle 0|) + \frac{1}{d}\sum_{k\neq 0}^{d-1}(|k\rangle\langle k|) \\
&\quad \times [p\,|0\rangle\langle 0| + (1-p)\,|k\rangle\langle k|] = 1 + \frac{p}{d} - p, \qquad (27)\\
F_Z^{\mathrm{d}} &= \frac{1}{d}\sum_{k=0}^{d-1}\mathrm{tr}\left\{(|k\rangle\langle k|)\left[\left(1-\frac{d-1}{d}p\right)|k\rangle\langle k| \right.\right. \\
&\quad \left.\left. + \frac{P}{d}\sum_{j=0,j\neq k}^{d-1}|j\rangle\langle j|\right]\right\} = 1 + \frac{p}{d} - p. \qquad (28)
\end{aligned}$$

Similarly, for any state $|X_k\rangle$ of X basis transmitted via dit-flip, d-phase-flip, amplitude damping and depolarizing quantum channels, the corresponding effect can be expressed as

$$\begin{aligned}
\rho_{\mathrm{out}}^k &= \varepsilon^{\mathrm{df}}\left(\rho_{\mathrm{in}}^k\right) = (1-p)U_{00}\left(\frac{1}{d}\sum_{j_1,j_2=0}^{d-1}w^{(j_1-j_2)k}\,|j_1\rangle\langle j_2|\right)U_{00}^\dagger + \frac{p}{d-1}\sum_{j=1}^{d-1}\left[U_{0j}\left(\frac{1}{d}\sum_{j_1,j_2=0}^{d-1}w^{(j_1-j_2)k}\,|j_1\rangle\langle j_2|\right)U_{0j}^\dagger\right] \\
&= (1-p)\rho_{\mathrm{in}}^k + \sum_{j=1}^{d-1}\frac{p}{(d-1)\cdot d}\times\left[\sum_{j_1,j_2=0}^{d-1}w^{(j_1-j_2)k}\left(U_{0j}\,|j_1\rangle\langle j_2|\,U_{0j}^\dagger\right)\right] \\
&= (1-p)\rho_{\mathrm{in}}^k + \frac{p}{(d-1)\cdot d}\times\left[\sum_{j_1,j_2=0}^{d-1}w^{(j_1-j_2)k}\sum_{j=1}^{d-1}\left(\sum_{s_1=0}^{d-1}|s_1\rangle\langle s_1+j|\,(|j_1\rangle\langle j_2|)\sum_{s_2=0}^{d-1}|s_2+j\rangle\langle s_2|\right)\right]
\end{aligned}$$

$$= (1-p)\rho_{\text{in}}^k + \frac{p}{(d-1)\cdot d}\sum_{j_1=j_2=0,\ j=1}^{d-1} w^{(j_1-j_2)k}\,|j_1-j\rangle\langle j_2-j|, \tag{29}$$

$$\begin{aligned}
\rho_{\text{out}}^k &= \varepsilon^{\text{dpf}}\left(\rho_{\text{in}}^k\right) = (1-p)\,U_{00}\left(\frac{1}{d}\sum_{j_1,j_2=0}^{d-1} w^{(j_1-j_2)k}\,|j_1\rangle\langle j_2|\right)U_{00}^{\dagger} + \frac{p}{d-1}\sum_{j=1}^{d-1}\left[U_{j0}\left(\frac{1}{d}\sum_{j_1,j_2=0}^{d-1} w^{(j_1-j_2)k}\,|j_1\rangle\langle j_2|\right)U_{j0}^{\dagger}\right]\\
&= (1-p)\,\rho_{\text{in}}^k + \frac{p}{d-1}\times\left[\frac{1}{d}\sum_{j_1,j_2=0}^{d-1} w^{(j_1-j_2)k}\times\sum_{j=1}^{d-1}\left(U_{j,0}\,|j_1\rangle\langle j_2|\,U_{j,0}^{\dagger}\right)\right]\\
&= (1-p)\,\rho_{\text{in}}^k + \frac{p}{d-1}\times\left[\frac{1}{d}\sum_{j_1,j_2=0}^{d-1} w^{(j_1-j_2)k}\sum_{j=1}^{d-1}\left(\sum_{s_1=0}^{d-1} w^{s_1 j}\,|s_1\rangle\langle s_1|\,(|j_1\rangle\langle j_2|)\sum_{s_2=0}^{d-1} w^{-s_2 j}\,|s_2\rangle\langle s_2|\right)\right]\\
&= (1-p)\,\rho_{\text{in}}^k + \frac{p}{d-1}\times\left[\frac{1}{d}\sum_{j_1,j_2=0,j=1}^{d-1} w^{(j_1-j_2)(k+j)}\,|j_1\rangle\langle j_2|\right],
\end{aligned} \tag{30}$$

$$\begin{aligned}
\rho_{\text{out}}^k &= \varepsilon^{\text{ad}}\left(\rho_{\text{in}}^k\right)\\
&= (|0\rangle\langle 0|)\left(\frac{1}{d}\sum_{j_1,j_2=0}^{d-1} w^{k(j_1-j_2)}\,|j_1\rangle\langle j_2|\right)(|0\rangle\langle 0|) + (|0\rangle\langle 0|)\left(\frac{1}{d}\sum_{j_1,j_2=0}^{d-1} w^{k(j_1-j_2)}\,|j_1\rangle\langle j_2|\right)\sqrt{1-p}\sum_{j_3=1}^{d-1}|j_3\rangle\langle j_3|\\
&\quad + \sqrt{1-p}\sum_{j_3=1}^{d-1}|j_3\rangle\langle j_3|\left(\frac{1}{d}\sum_{j_1,j_2=0}^{d-1} w^{k(j_1-j_2)}\,|j_1\rangle\langle j_2|\right)(|0\rangle\langle 0|)\\
&\quad + (1-p)\sum_{j_3=1}^{d-1}|j_3\rangle\langle j_3|\left(\frac{1}{d}\sum_{j_1,j_2=0}^{d-1} w^{k(j_1-j_2)}\,|j_1\rangle\langle j_2|\right)\sum_{j_3'=1}^{d-1}\left|j_3'\right\rangle\left\langle j_3'\right|\\
&\quad + p\sum_{j_3=1}^{d-1}|0\rangle\langle j_3|\left(\frac{1}{d}\sum_{j_1,j_2=0}^{d-1} w^{k(j_1-j_2)}\,|j_1\rangle\langle j_2|\right)\sum_{j_3'=1}^{d-1}\left|j_3'\right\rangle\langle 0|\\
&= \frac{1}{d}\,|0\rangle\langle 0| + \frac{\sqrt{1-p}}{d}\sum_{j=1}^{d-1} w^{-k\cdot j}\,|0\rangle\langle j| + \frac{\sqrt{1-p}}{d}\sum_{j=1}^{d-1} w^{k\cdot j}\,|j\rangle\langle 0| + \frac{1-p}{d}\sum_{j_1,j_2=1}^{d-1} w^{k(j_1-j_2)}\,|j_1\rangle\langle j_2| + \frac{p}{d}\sum_{j_1,j_2=1}^{d-1} w^{k(j_1-j_2)}\,|0\rangle\langle 0|,
\end{aligned} \tag{31}$$

$$\begin{aligned}
\rho_{\text{out}}^k &= \varepsilon^{\text{d}}\left(\rho_{\text{in}}^k\right)\\
&= \left(1-\frac{d^2-1}{d^2}p\right)U_{00}\left(\frac{1}{d}\sum_{j_1,j_2=0}^{d-1} w^{(j_1-j_2)k}\,|j_1\rangle\langle j_2|\right)U_{00}^{\dagger} + \frac{p}{d^2}\sum_{\substack{m,n=0,\\(m,n)\neq(0,0)}}^{d-1}\left(U_{mn}\left(\frac{1}{d}\sum_{j_1,j_2=0}^{d-1} w^{(j_1-j_2)k}\,|j_1\rangle\langle j_2|\right)U_{mn}^{\dagger}\right)\\
&= \left(1-\frac{d^2-1}{d^2}p\right)\rho_{\text{in}}^k + \frac{d-1}{d^2}p\cdot\frac{1}{d}\sum_{j=0}^{d-1}|j\rangle\langle j| + \frac{d-1}{d^2}p\cdot\frac{1}{d}\sum_{j=0}^{d-1}|j\rangle\langle j| + \frac{(d-1)^2}{d^2}p\cdot\frac{1}{d}\sum_{j=0}^{d-1}|j\rangle\langle j|\\
&= \left(1-\frac{d^2-1}{d^2}p\right)\cdot\frac{1}{d}\sum_{j_1,j_2=0}^{d-1} w^{(j_1-j_2)k}\,|j_1\rangle\langle j_2| + \frac{d^2-1}{d^2}p\cdot\frac{1}{d}\sum_{j=0}^{d-1}|j\rangle\langle j|.
\end{aligned} \tag{32}$$

Accordingly, the mean fidelity of any qudit state in X basis when it is transmitted in four types of quantum noise channels is calculated as

$$\begin{aligned}
F_X^{\text{df}} &= \frac{1}{d}\sum_{k=0}^{d-1}\text{tr}\left\{\left(\frac{1}{d}\sum_{j_1,j_2=0}^{d-1} w^{(j_1-j_2)k}\,|j_1\rangle\langle j_2|\right)\right.\\
&\quad\left.\times\left[\frac{1-p}{d}\sum_{j_1,j_2=0}^{d-1} w^{(j_1-j_2)k}\,|j_1\rangle\langle j_2| + \frac{p}{(d-1)\cdot d}\sum_{j_1=j_2=0,\ j=1}^{d-1} w^{(j_1-j_2)k}\,|j_1-j\rangle\langle j_2-j|\right]\right\} = 1,
\end{aligned} \tag{33}$$

$$\begin{aligned}
F_X^{\text{dpf}} &= \frac{1}{d}\sum_{k=0}^{d-1}\text{tr}\left\{\left(\frac{1}{d}\sum_{j_1,j_2=0}^{d-1} w^{(j_1-j_2)k}\,|j_1\rangle\langle j_2|\right)\right.\\
&\quad\left.\times\left(\frac{1-p}{d}\sum_{j_1,j_2=0}^{d-1} w^{(j_1-j_2)k}\,|j_1\rangle\langle j_2| + \frac{p}{d-1}\times\left[\frac{1}{d}\sum_{j_1,j_2=0,j=1}^{d-1} w^{(j_1-j_2)(k+j)}\,|j_1\rangle\langle j_2|\right]\right)\right\} = (1-p)+\frac{p}{d},
\end{aligned} \tag{34}$$

$$F_X^{\text{ad}} = \frac{1}{d}\sum_{k=0}^{d-1}\text{tr}\left\{\left(\frac{1}{d}\sum_{j_1,j_2=0}^{d-1} w^{(j_1-j_2)k}\,|j_1\rangle\langle j_2|\right)\left[\left(\frac{1}{d}+\frac{p}{d}\sum_{j_1,j_2=1}^{d-1} w^{k(j_1-j_2)}\right)|0\rangle\langle 0| + \frac{\sqrt{1-p}}{d}\sum_{j=1}^{d-1} w^{-k\cdot j}\,|0\rangle\langle j|\right.\right.$$

$$+\frac{\sqrt{1-p}}{d}\sum_{j=1}^{d-1}w^{k\cdot j}\left|j\right\rangle\left\langle 0\right|+\frac{1-p}{d}\sum_{j_1,j_2=1}^{d-1}w^{k(j_1-j_2)}\left|j_1\right\rangle\left\langle j_2\right|\Bigg]\Bigg\}$$

$$=\frac{1}{d^2}+\frac{2(d-1)}{d^2}\sqrt{1-p}+\frac{(d-1)^2}{d^2}(1-p)+\frac{d-1}{d^2}p, \tag{35}$$

$$F_X^{\mathrm{d}}=\frac{1}{d}\sum_{k=0}^{d-1}\mathrm{tr}\Bigg\{\left(\frac{1}{d}\sum_{j_1,j_2=0}^{d-1}w^{(j_1-j_2)k}\left|j_1\right\rangle\left\langle j_2\right|\right)\Bigg[\left(1-\frac{d^2-1}{d^2}p\right)\cdot\frac{1}{d}\sum_{j_1,j_2=0}^{d-1}w^{(j_1-j_2)k}\left|j_1\right\rangle\left\langle j_2\right|+\frac{d^2-1}{d^2}p\cdot\frac{1}{d}\sum_{j=0}^{d-1}\left|j\right\rangle\left\langle j\right|\Bigg]\Bigg\}$$

$$=1+\frac{d+1}{d^2}p-p-\frac{1}{d^3}p. \tag{36}$$

According to Eqs. (19), (25)–(28) and (33)–(36), the mean fidelity of each qudit received by participants in different noise channels is deduced and illustrated in Table 1.

Table 1. The mean fidelity of different noise channels in our proposed MQSS protocol.

Mean fidelity \ Noise model	Dit-flip	d-phase-flip	Amplitude-damping	Depolarizing
Single qudit	$1-\frac{1}{2}p$	$1-\frac{d-1}{2d}p$	$\left[1-\frac{(d-2)}{d}p-\frac{1}{d}+\frac{1-p}{d^2}+\frac{d-1}{d^2}\sqrt{1-p}\right]$	$1+\frac{d-1}{2d^3}p-\frac{d-1}{d}p$

Therefore, on the basis of the mean fidelity of a single qudit transmitted in the noise channel, the secret key rate of the present MQSS protocol with n participants in four noise channels can be deduced as

$$S^{\mathrm{df}}=\left(1-\frac{1}{2}p\right)^n,\quad S^{\mathrm{dpf}}=\left(1-\frac{d-1}{2d}p\right)^n,$$
$$S^{\mathrm{ad}}=\left[1-\frac{(d-2)}{d}p-\frac{1}{d}+\frac{1-p}{d^2}+\frac{d-1}{d^2}\sqrt{1-p}\right]^n,$$
$$S^{\mathrm{d}}=\left(1+\frac{d-1}{2d^3}p-\frac{d-1}{d}p\right)^n, \tag{37}$$

where the superscripts df, dpf, ad and d respectively denote the dit-flip, d-phase-flip, amplitude-damping and depolarizing noise channels.

To demonstrate the performance of the present MQSS protocol in noise environments more intuitively, the fidelity of a simple example that involves a three-party protocol under quantum system dimensions $d=5$ in different noise models is plotted in Fig. 1.

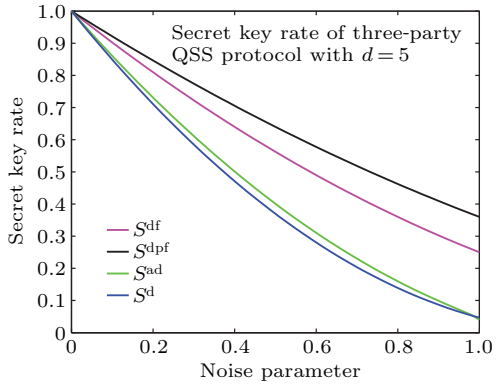


Fig. 1. The secret key rate of the present MQSS protocol with a three-party protocol in four different types of noise under different noise parameters p, where S^{df}, S^{dpf}, S^{ad} and S^{d} respectively denote the secret key in dif-flip, d-phase-flip, amplitude-damping and depolarizing noise channels.

As shown Fig. 1, we can see that the secret key rate of the present protocol decreases as the noise parameter p increases in four different noise channels. Under the same noise parameter p, the secret key rate satisfies $S^{\mathrm{dpf}}>S^{\mathrm{df}}>S^{\mathrm{ad}}>S^{\mathrm{d}}$. Besides, it is worth noting that as the noise parameter p increases, the secret key rates in the dit-phase-flip and dit-flip channels demonstrate a better performance than the amplitude-damping and depolarizing channels.

6. Comparisons

Table 2 presents the comparisons of the proposed protocol with some former protocols. Tsai *et al.*'s[38] QSS protocol is based on the measurement property of the GHZ state in the context of the qubit. In addition to single-qubit measurement operation, the dealer and each participant need to perform an additional local quantum unitary operation. Wang *et al.*'s protocol[44] shares the secret based on correlation of the Bell state and using quantum superdense coding. By performing quantum Fourier transform and a local quantum unitary operation, Yang *et al.*'s[45] protocol realizes secret sharing based on the correlation of GHZ states. Based on the measurement-delay strategy and the measurement properties of GHZ states, Wang *et al.*'s[46] protocol can share the random bits or dits with high efficiency.

Compared to MQSS protocols[38,44–46] designed on multi-particle entangled states, our proposed protocol is designed on a single qudit state. Due to the difficulty in preparing the entangled state in a laboratory and maintaining the coherence when the quantum state is transmitted in a channel, the present protocol seems more practical in real quantum communication. Furthermore, in the present protocols, all the participants do not need to perform additional quantum unitary operations, which makes its realization easier than former QSS protocols.

Table 2. Comparisons with some representative protocols.

Items \ Protocols	Tsai *et al*'s protocol[38]	Wang *et al*'s protocol[44]	Yang *et al*'s protocol[45]	Wang *et al*'s protocol[46]	Proposed protocol
Dimensions	2	d	d	2 or d	d
Quantum resources	Single qubit state, GHZ state	Bell state	GHZ state	GHZ state	Single qudit state
Participant's measurement	Single-qubit measurement	Single-qudit measurement, Bell-state measurement	Single-qudit measurement	Single-qubit measurement	Single-qudit measurement
Additional quantum operations	Yes	Yes	Yes	Yes	No
Shared secret key	Predetermined bits	Predetermined dits	Random dits	Random bits (dits)	Predetermined dits

7. Conclusion

Based on two mutually unbiased MBs in a high-dimensional quantum system, this paper proposes an efficient MQSS protocol using single qudit states. By adapting the approaches of measurement basis encryption and sending the MBs via the QSDC protocol, each participant can choose the correct MBs to obtain their secret shadows and avoid the waste of qudits arising from basis reconciliation. Thus, the proposed protocol is asymptotically 100% efficient. Security analysis proves that that the proposed protocol is secure against general attacks such as measure-resend attack, entangle-and-measure attack, and Trojan horse attack.

Note that to prove the present protocol is secure against entangle-and-measure attack, we only demonstrate its complete robustness instead of performing its security analysis from the aspect of information theory. In a real situation, when a quantum state is transmitted via a channel, the quantum system will unavoidably interact with the outer environment and will definitely be affected by the channel noise. Hence, the secret key rate of the present protocol in quantum noise channels of dit-flip, dit-phase-flip, amplitude damping and depolarizing is further demonstrated. However, we found that the secret key rate of the present protocol decreases obviously with the channel noise parameter strength increase. Therefore, our future works will focus on security analysis of the quantum communication protocol from an information theoretical aspect and will attempt to find an effective method to improve the secret key rate under noise channels.

Acknowledgements

Project supported by the Doctoral Funding of Nanchang Hangkong University (Grant No. EA202204231); the National Natural Science Foundation of China (Grant Nos. 61866027 and 6217070290); the Key research project of Jiangxi Province (Grant No. 20212BBE53017); and the Shanghai Science and Technology Project (Grant Nos. 21JC1402800 and 20040501500).

References

[1] Shor P 1994 *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, November 20–22 1994, Santa Fe, NM, USA, p. 124
[2] Grover L K 1996 *28th Annual ACM Symposium on Theory of Computing*, May 29 1996, Philadelphia, PA, USA, p. 212
[3] Bennett C H, and Brassard G 1984 *IEEE International Conference on Computers, Systems and Signal Processing*, December 1984, Bangalore, India, p. 175
[4] Vahid K, Alireza B and Saber B 2002 *Phys. Rev. A* **65** 052331
[5] Xie Y M, Lu Y S, Weng C X, Cao X Y, Jia Z Y, Bao Y, Wang Y, Fu Y, Yin H L and Chen Z B 2022 *PRX Quantum* **3** 020315
[6] Cai Q Y and Li B W 2004 *Chin. Phys. Lett.* **21** 601
[7] Deng F G and Long G L 2004 *Phys. Rev. A* **69** 052319
[8] Marco L and Stefano M 2005 *Phys. Rev. Lett.* **94** 140501
[9] Bennett C H, Brassard G, Crépeau C, Jozsa R, Peres A and Wootters W K 1993 *Phys. Rev. Lett.* **70** 1895
[10] Lance A M, Symul T, Bowen W P, Sanders B C and Ping K L 2004 *Phys. Rev. Lett.* **92** 177903
[11] Hillery M, Bužek V and Berthiaume A 1999 *Phys. Rev. A* **59** 1829
[12] Schmid C, Trojek P, Bourennane M, Kurtsiefer C, Zukowski M and Weinfurter H 2005 *Phys. Rev. Lett.* **95** 230505
[13] Gu J, Cao X Y, Yin H L and Chen Z B 2021 *Opt. Express* **29** 9165
[14] Jia Z Y, Gu J, Li B H, Yin H L and Chen Z B 2021 *Entropy* **23** 716
[15] Jakobi M, Simon C, Gisin N, Bancal J D, Branciard C, Walenta N and Zbinden H 2011 *Phys. Rev. A* **83** 022301
[16] Yang Y G, Liu Z C, Chen X B, Zhou Y H and Shi W M 2017 *Sci. China-Phys. Mech. Astron.* **60** 120311
[17] Lu Y S, Cao X Y, Weng C X, Gu J, Xie Y M, Zhou M G, Yin H L and Chen Z B 2021 *Opt. Express* **29** 10162
[18] Li Z, Cao X Y, Li C L, Weng C X, Gu J, Yin H L and Chen Z B 2021 *Quantum Sci. Technol.* **6** 045019
[19] Shamir A 1979 *Commun. ACM* **22** 612
[20] Blakley G R 1979 *International Workshop on Managing Requirements Knowledge*, 04–07 June 1979, New York, NY, USA, p. 313
[21] Cleve R, Gottesman D and Lo H K 1999 *Phys. Rev. Lett.* **83** 648
[22] Karlsson A, Koashi M and Imoto N 1999 *Phys. Rev. A* **59** 162
[23] Gottesman D 2000 *Phys. Rev. A* **61** 042311
[24] Guo G P and Guo G C 2003 *Phys. Lett. A* **310** 247
[25] Li X, Long G L and Deng F G 2004 *Phys. Rev. A* **69** 052307
[26] Song X L, Liu Y B and Deng H Y 2017 *Sci. Rep.* **7** 6366
[27] Kartick S and Hari O 2020 *Quantum Inf. Process.* **19** 73
[28] Yan F L and Gao T 2005 *Phys. Rev. A* **72** 012304
[29] Yan F L, Gao T and Li Y C 2008 *Chin. Phys. Lett.* **25** 1187
[30] Wang M M, Chen X B and Yang Y X 2014 *Quantum Inf. Process.* **13** 429
[31] Bai C M, Li Z H, Si M M and Li Y M 2017 *Eur. Phys. J. D* **71** 255
[32] Yang C W and Tsai C W 2020 *Quantum Inf. Process.* **19** 162
[33] Hu W W, Zhou R G, Li X, Fan P and Tan C Y 2021 *Quantum Inf. Process.* **20** 159
[34] Li L Z, Qiu D W and Mateus P 2013 *J. Phys. A: Math. Theor.* **46** 045304
[35] Hu W W, Zhou R G and Luo J 2022 *Chin. J. Phys.* **77** 1701
[36] Fu Y, Yin H L, Chen T Y and Chen Z B 2015 *Phys. Rev. Lett.* **114** 090501
[37] Gao Z K, Li T and Li Z H 2020 *Sci. China-Phys. Mech. Astron.* **63** 120311
[38] Tsai C W, Yang C W and Lin J 2022 *Quantum Inf. Process.* **21** 63
[39] Han L F, Liu Y M and Liu J 2008 *Opt. Commun.* **281** 2690

[40] Qin H W 2016 *J. Chin. Inst. Eng.* **39** 623
[41] Molina-Terriza G, Vaziri A, Ursin R and Zeilinger A 2005 *Phys. Rev. Lett.* **94** 040501
[42] Inoue R, Yonehara T, Miyamoto Y, Koashi M and Kozuma M 2009 *Phys. Rev. Lett.* **103** 110503
[43] Vahid K, Alireza B and Saber B 2002 *Phys. Rev. A* **65** 042320
[44] Wang X, Liu Y M and Han L F 2008 *Int. J. Quantum Inf.* **6** 1155
[45] Yang W, Huang L S and Shi R H 2013 *Quantum Inf. Process.* **12** 2465
[46] Wang M M, Tian L T, and Qu Z G 2018 *International Conference on Cloud Computing and Security*, June 22–24, 2018, Haikou, Hainan, China, p. 23
[47] Mashhadi S 2019 *Quantum Inf. Process.* **18** 11
[48] Qin H W, Tang W K S and Tso R L 2020 *IEEE J. Sel. Top. Quant.* **26** 6600106
[49] Pittenge A O and Rubin M H 2004 *Linear Algebra Appl.* **390** 255
[50] Boyer M, Kenigsberg D and Mor T 2007 *Phys. Rev. Lett.* **99** 140501
[51] Deng F G, Li X H, Zhou H Y and Zhang Z J 2005 *Phys. Rev. A* **72** 044302
[52] Cai Q Y 2006 *Phys. Lett. A* **351** 23
[53] Fonseca A 2019 *Phys. Rev. A* **100** 062311
[54] Bertlmann R A and Krammer P 2008 *J. Phys. A* **41** 235303