




OPEN Security analysis of qutrit quantum secret sharing with linear optical correlation measurement

Yonggi Jo , Taek Jeong, Nam Hun Park, Zaeill Kim, Dong-Gil Im, Kyungdeuk Park & Yong Sup Ihn

In this paper, we investigate a possibility of three-dimensional extension of correlation measurement based quantum secret sharing (QSS) with a three-dimensional cyclic-entangled state, called qutrit cyclic-entangled state. The qutrit cyclic-entangled state can be post-selected by a correlation measurement setup with linear optical elements. Thus, this protocol can provide a measurement-device-independent security against a potential eavesdropper, since the measurement results reveals only a correlation among qutrits sent from the three parties, not the exact quantum states. We show that our protocol can be implemented with current state-of-the-art technologies. The security of QSS with a qutrit cyclic-entangled state is analyzed for the cases, when all players are trusted as well as there are malicious players. Possibility of higher-dimensional, qudit extension and conditions for an advantage with qudit are investigated as well.

In the emergence of quantum technologies, various quantum-secured protocols have been studied including quantum key distribution (QKD)^{1,2}, blind quantum computation^{3–5}, and quantum-secured sensing^{6–8}. These protocols provides security based on the principles of quantum mechanics, such as the no-cloning theorem⁹ and nonlocality¹⁰, rather than the computational complexity.

In 1999, quantum secret sharing (QSS) was introduced by Hillery *et al.* Secret sharing is a scheme proposed for distributing a secret among participants^{11,12}. In the scheme, one party, called a dealer, gives a part of the secret to participants, called players. Each player cannot access full information on the secret, since a player has only a share of the secret. The secret can be reconstructed only when the sufficient number of players cooperates by combining their shares. The scheme is called a (k, n) -threshold secret sharing, when the number of players is n and the sufficient number of players for reconstructing the secret is k . In QSS, a quantum secret or a classical secret can be shared by using a Greenberger–Horne–Zeilinger (GHZ) type entangled state¹³ without an information leakage of the share not only to a potential eavesdropper, conventionally called Eve, but also to the other players. After its first proposal, the information-theoretic security of the QSS has been studied^{14–17}, and experimental demonstrations of QSS protocols have been conducted as well^{18–24}.

After the first proposal of QKD, significant efforts were made to improve efficiency of a secret key rate such as the protocol involving high-dimensional quantum states, called qudits. A qudit naturally carry more classical information than a qubit. QSS using qudits^{25–29} have been studied as well as a multiparty extension of QKD using qudits^{30,31}. These results show that QSS based on qudits can achieve a higher secret key rate and a higher upper bound on the allowed error rate than the original protocols exploiting two-dimensional quantum states, called qubits, because of the structure of a qudit. From the results, it is known that a quantum communication protocol adopting qudit is noise robust compared to that with qubit. Moreover, there were the studies that fidelity of an optimal state estimation and the optimal fidelity of the $1 \rightarrow 2$ universal optimal quantum cloning machine decrease for increasing d , the dimension of a target quantum state^{32,33}. Therefore, Eve can obtain less information when a qudit is exploited as an information carrier in QSS, i.e., qudits can make a quantum communication protocol more secure.

However, generation of a qudit GHZ state, which needs demanding technologies, is necessary to implement the QSS protocols using qudits. In 2018, there was the first generation of a tripartite three-dimensional GHZ state, called tripartite qutrit GHZ state, using orbital angular momentum (OAM) modes of a single photon³⁴, but its generation efficiency and fidelity were not enough to implement a practical QSS protocol using qudits. Under the situation, it is natural to investigate a QSS protocol based on correlation measurement^{35,36}. In QKD, Bell state measurement (BSM)³⁷ based protocols have been widely studied rather than generation of entangled states³⁸. Moreover, they provide measurement-device-independent (MDI) security, i.e., security loopholes from

Agency for Defense Development, Yuseong P.O.Box 35, Daejeon 34186, Republic of Korea. ✉email: yonggi@add.re.kr

imperfection of measurement devices are closed, since BSM reveals only correlation between the two quantum state, not the exact key information. To enhance the efficiency, high-dimensional version of MDIQKD protocols have been studied^{39–42}. However, there is an obstacle to implementing high-dimensional MDIQSS protocols that a high-dimensional BSM and a high-dimensional GHZ state analyzer cannot be implemented with linear optical elements⁴³.

In this article, we investigate a possibility of QSS with a qudit cyclic-entangled state (3d-CQSS). It is known that implementation of a qudit GHZ state analyzer is not possible with linear optics. However, high-dimensional correlation measurement projecting on the cyclic-entangled state is possible with linear optical elements^{41,44}, especially based on a multiport interferometer^{45,46}, and it was successfully implemented for qudit quantum teleportation^{47,48}. With the correlation measurement setup, we propose an implementable 3d-CQSS protocol for (2, 2)-threshold QSS; there are a dealer, called Alice, and two Bobs who are authorized. The protocol would be generalized to d -dimensional CQSS (d -CQSS), and a class of the proposed protocol is $(d-1, d-1)$ -threshold QSS; there are a dealer, called Alice, and $(d-1)$ players, called Bob₁ to Bob _{$d-1$} . In this protocol, Charlie, an untrusted third party, is introduced, and only Charlie has the correlation measurement setup, which is performed on the three photons sent from the authorized parties. We analyze the security of d -CQSS and investigate conditions for security enhancement using qudits. We show the security of the protocol is not trivial like other high-dimensional quantum communication protocol, since the cyclic-entangled state has different properties to a GHZ-type entangled state. The conditions for the proposed protocol has higher secret sharing rate compared to two-dimensional QSS or entanglement-based d -CQSS are investigated as well.

Results

Three-dimensional correlation measurement with linear optical elements

In this section, an implementation of experimental elements to construct the three-dimensional correlation measurement with linear optical elements is introduced. For a qudit, it is impossible to construct a measurement setup with linear optical elements of which projector is a maximally entangled state or a GHZ-type state even if ancillary modes or systems are introduced⁴³. Thus, a direct high-dimensional generalization of BSM or GHZ state analyzer is not implementable with linear optical elements. However, it is possible to construct a correlation measurement for a certain type of d -partite d -dimensional entangled state^{39,44}. We investigate an entangled state exactly discriminated by the setup.

Here, we utilize the OAM mode of a single photon as an information carrier, but another mode could also be used. OAM modes, whose dimensionality can, in principle, be infinite, have been employed as high-dimensional information carriers not only in classical optical communication⁴⁹, but also in quantum information processing^{50,51}, including QKD^{52,53}. Encoding information in OAM modes enhances both channel capacity and resilience to noise^{54,55}. Despite these advantages, OAM-based systems face certain challenges, such as state-dependent diffraction⁵⁶ and sensitivity to atmospheric turbulence in free-space links⁵⁷. Various strategies have been proposed to improve the efficiency of OAM-encoded protocols, including the use of focusing techniques to address state-dependent diffraction⁵⁸, and vortex-mode-division multiplexing to mitigate inter-mode crosstalk caused by turbulence⁵⁹.

A single photon OAM state is written as follows:

$$|0\rangle = \hat{a}_{l=-1}^\dagger |\text{vac}\rangle, \quad |1\rangle = \hat{a}_{l=0}^\dagger |\text{vac}\rangle, \quad |2\rangle = \hat{a}_{l=1}^\dagger |\text{vac}\rangle, \quad (1)$$

where $\hat{a}_{l=x}^\dagger$ denotes the photon creation operator of which the OAM mode is x , and $|\text{vac}\rangle$ is a vacuum state. Two mutually unbiased bases (MUBs), called ordinary basis and bar basis, will be exploited for QSS. The quantum states in the bar basis can be obtained from the three-dimensional Fourier transformation of the states in the ordinary basis as follows:

$$\begin{aligned} |\bar{0}\rangle &= \frac{1}{\sqrt{3}} (|0\rangle + |1\rangle + |2\rangle), \\ |\bar{1}\rangle &= \frac{1}{\sqrt{3}} (|0\rangle + \omega_3 |1\rangle + \omega_3^2 |2\rangle), \\ |\bar{2}\rangle &= \frac{1}{\sqrt{3}} (|0\rangle + \omega_3^2 |1\rangle + \omega_3 |2\rangle), \end{aligned} \quad (2)$$

where $\omega_d = \exp(2\pi i/d)$. These two bases are MUBs, since $|\langle \bar{\alpha} | \beta \rangle|^2 = 1/3$ is always satisfied for all $\alpha, \beta \in \{0, 1, 2\}$, i.e., a quantum state from one MUB can be expressed as an equal-probability superposition of the quantum states forming another MUB.

An example of schematic setup of the three-dimensional correlation measurement is presented in Fig. 1. The three photons sent from three users, called Alice, Bob₁, and Bob₂, enter each input port of a three-port interferometer, called a tritter^{45,46,60}. The tritter consists of linear optical elements including beam splitters, mirrors, and phase modulators⁴⁶. In linear optics, the response of a material to incident light is directly proportional to the intensity of the light. In contrast, nonlinear optics involves more complex interactions, where the material's response depends nonlinearly on the light intensity. As a result, linear optical systems are generally less sensitive to input power fluctuations and are simpler to align and maintain, making them more stable than their nonlinear counterparts. Owing to these advantages, linear optical quantum interferometers play a significant role in quantum information processing⁶¹. The tritter performs the three-dimensional Fourier transformation on path modes of the photons as described in the following equation:

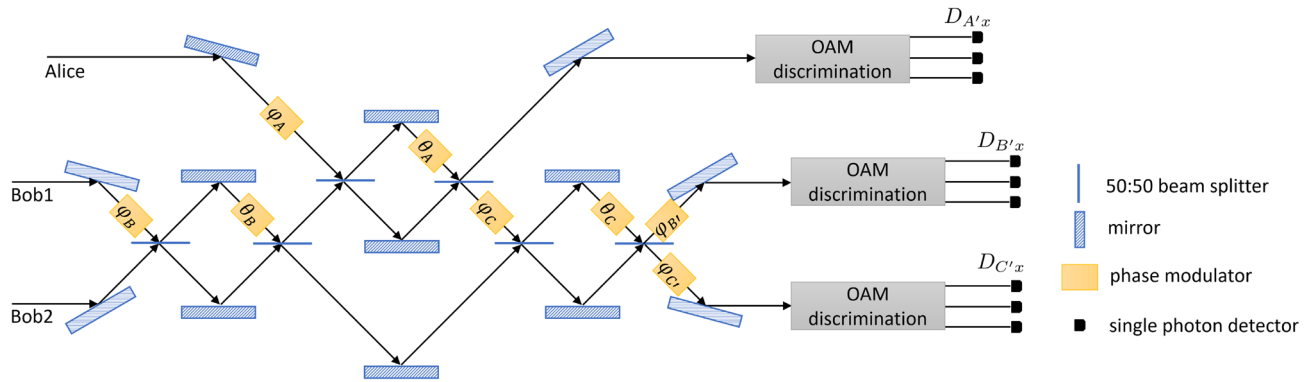


Fig. 1. A schematic diagram of a tripartite three-dimensional correlation measurement setup. Three photons enter into a 3-port interferometer, called a tritter. After interference in the tritter constructed by Clements' method⁴⁶, an OAM value and a label of existing output port of the photons are measured by means of OAM discrimination elements and single photon detectors. The setup can discriminate a part of tripartite qutrit entangled states from a combination of clicked detectors. For the tritter operation in Eq. (4), the parameters are $\theta_A = \arccos(1/\sqrt{3})$; $\theta_B = \pi/4$; $\theta_C = \pi/4$; $\varphi_A = 0$; $\varphi_B = \pi$; $\varphi_C = 3\pi/2$; $\varphi_{B'} = \pi/4$; and $\varphi_{C'} = \pi/4$. D_{Xy} : a detector corresponding to the OAM state $|y\rangle$ on the path X .

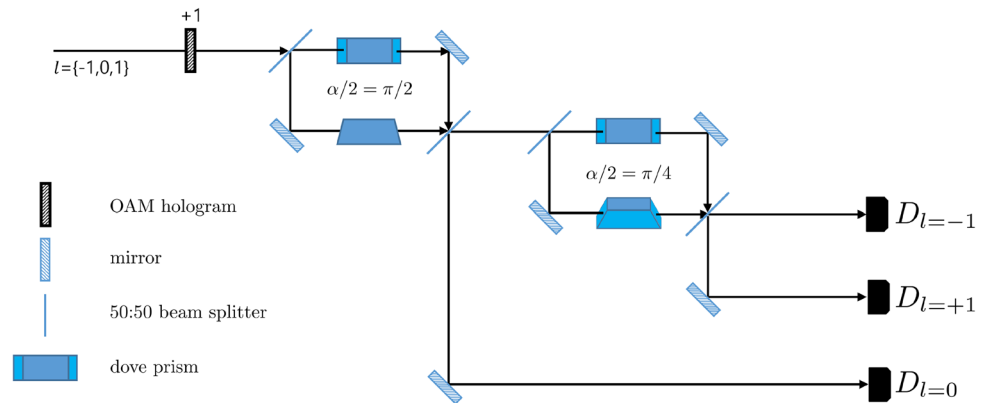


Fig. 2. A schematic diagram for measuring an OAM value of a single photon. The OAM BSs change a direction of propagation of an incoming single photon according to its OAM value. OAM BS consists of a Mach-Zehnder interferometer with Dove prisms. The relative angle between the two Dove prisms in each arm of the Mach-Zehnder interferometer is denoted as $\alpha/2$. In the setup, value one is added in the OAM value of an incoming photon by using an OAM hologram (+1). Then the first OAM BS ($\alpha/2 = \pi/2$) splits photons whose OAM value is odd and even, and the second OAM BS ($\alpha/2 = \pi/4$) does photons whose OAM value is $l = 0$ and $l = 2$. Finally, the incoming photon enters into corresponding single photon detector.

$$\hat{U}_3|a, b_1, b_2\rangle_{ABC} = \frac{1}{3\sqrt{3}} \left[(|a\rangle + |b_1\rangle + |b_2\rangle)_{A'} \otimes (|a\rangle + \omega_3|b_1\rangle + \omega_3^2|b_2\rangle)_{B'} \otimes (|a\rangle + \omega_3^2|b_1\rangle + \omega_3|b_2\rangle)_{C'} \right], \quad (3)$$

where a , b_1 , and b_2 are the encoded information of Alice, Bob1, and Bob2, respectively. The input ports and output ports are distinguished by the subscripts, A , B , and C for the input ports, and A' , B' , and C' for the output ports. Then the unitary operation on the path modes, \hat{U}_3 , performed by the tritter can be written as shown in the following equation:

$$\hat{U}_3 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega_3 & \omega_3^2 \\ 1 & \omega_3^2 & \omega_3 \end{pmatrix}. \quad (4)$$

Subsequently, an OAM value of the photons is measured. Figure 2 shows a possible setup with linear optical elements that changes a direction of propagation of incoming photons according to their OAM value. The OAM hologram, which adds (+1) to the OAM value of an incoming photon, and OAM beam splitters (OAM BSs) are exploited in the setup⁶². An OAM BS consists of a Mach-Zehnder interferometer and two Dove prisms

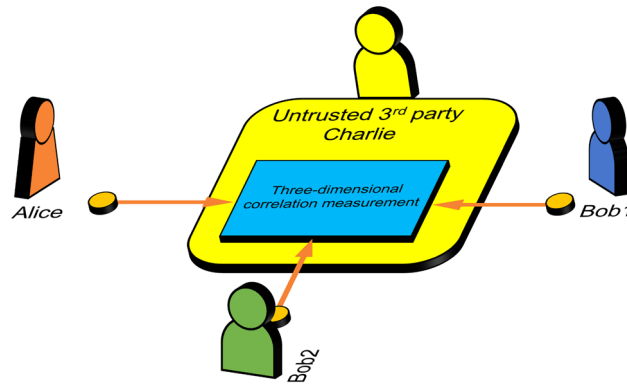


Fig. 3. A schematic diagram of our protocol. There are three authorized parties, Alice, Bob₁, and Bob₂, and one untrusted party, Charlie. Each of the authorized parties generates a single photon state according to their choice of an encoding basis and three-dimensional information. They send the quantum states to Charlie who measures a correlation among the OAM mode of the three photons by means of a tripartite three-dimensional correlation measurement. The three authorized parties can share a secret by using their encoded information and the result of the measurement.

in each arm. The relative angle between the two Dove prisms is $\alpha/2$, and the relative phase between photons in the two arms is given by $e^{i\alpha}$. The first OAM BS ($\alpha = \pi$) splits photons whose OAM value is even and odd, and the second OAM BS ($\alpha = \pi/2$) does photons whose OAM value is 0 and 2. Then there is one-to-one correspondence between the OAM value of an incoming single photon and the label of clicked detector. In our proposal, the OAM value discrimination setup should be able to measure an OAM value of the three incoming photons simultaneously, since there can be at most three photons on the same output port of the tritter. Direct measurements of an OAM value of a single photon are also considerable, such as the OAM value measurement by using refractive optical elements^{63,64}, the measurement separating OAM modes spatially^{65,66}, and the measurement using a single phase screen⁶⁷.

To describe our protocol, we define 27 orthonormal tripartite qutrit entangled states $|\Phi^3\rangle$ as follows:

$$|\Phi_{(2i+j,\sigma)}^3\rangle = \frac{1}{\sqrt{6}} \sum_{k=0}^2 \omega_3^{\sigma k} |k\rangle [|k+i+1, k+i+2\rangle + (-1)^j |k+i+2, k+i+1\rangle], \quad (5)$$

$$|\Phi_{(6+m,\sigma)}^3\rangle = \frac{1}{\sqrt{3}} \sum_{k=0}^2 \omega_3^{\sigma k} |k, k+m, k+m\rangle, \quad (6)$$

where $\omega_3 = \exp(2\pi/3)$, $i, m, \sigma \in \{0, 1, 2\}$, and $j \in \{0, 1\}$. With these states, the relation between the three-photon quantum states that enter the tritter and its corresponding detector click events are investigated. The correlation measurement setup cannot discriminate all of the tripartite qutrit entangled state written in Eqs. (5) and (6). The only state that can be exactly discriminated and its click events are described as follows:

$$|\Phi_{(0,0)}^3\rangle \rightarrow \begin{cases} D_{A'0}, D_{B'1}, D_{C'2} & \text{with probability } 1/12 \\ D_{A'0}, D_{B'2}, D_{C'1} & \text{with probability } 1/12 \\ D_{A'1}, D_{B'2}, D_{C'0} & \text{with probability } 1/12 \\ D_{A'1}, D_{B'0}, D_{C'2} & \text{with probability } 1/12 \\ D_{A'2}, D_{B'0}, D_{C'1} & \text{with probability } 1/12, \\ D_{A'2}, D_{B'1}, D_{C'0} & \text{with probability } 1/12 \\ D_{A'0}, D_{A'1}, D_{A'2} & \text{with probability } 1/6 \\ D_{B'0}, D_{B'1}, D_{B'2} & \text{with probability } 1/6 \\ D_{C'0}, D_{C'1}, D_{C'2} & \text{with probability } 1/6 \end{cases} \quad (7)$$

where D_{Xy} denotes a click event of the detector corresponding to the quantum state $|y\rangle$ in the output port X . The three click events of which probability is $1/6$ can be used in our protocol, since the other events are overlapped with the click events of $|\Phi_{(1,0)}^3\rangle$ as shown in the following equation:

$$|\Phi_{(1,0)}^3\rangle \rightarrow \begin{cases} D_{A'0}, D_{B'1}, D_{C'2} & \text{with probability } 1/6 \\ D_{A'0}, D_{B'2}, D_{C'1} & \text{with probability } 1/6 \\ D_{A'1}, D_{B'2}, D_{C'0} & \text{with probability } 1/6 \\ D_{A'1}, D_{B'0}, D_{C'2} & \text{with probability } 1/6 \\ D_{A'2}, D_{B'0}, D_{C'1} & \text{with probability } 1/6 \\ D_{A'2}, D_{B'1}, D_{C'0} & \text{with probability } 1/6 \end{cases} \quad (8)$$

There are always overlaps of click events for the other states, so only $|\Phi_{(0,0)}^3\rangle$ is exactly discriminated by using the correlation measurement setup. The details of calculation are drawn in the Methods section. We call this state as qutrit cyclic-entangled state⁶⁸, since the state has the form of the following equation:

$$|\Phi_{(0,0)}^3\rangle = \frac{1}{\sqrt{6}} [|0\rangle(|1, 2\rangle + |2, 1\rangle) + |1\rangle(|2, 0\rangle + |0, 2\rangle) + |2\rangle(|0, 1\rangle + |1, 0\rangle)]. \quad (9)$$

We expect that the existing setup⁴¹ also can be used for the $3d$ -CQSS protocol as well, which can exactly discriminate three tripartite qutrit entangled states, but it needs nondestructive photon number measurement setups that require demanding technologies.

This setup could be generalized to a d -dimensional correlation measurement which consists of a d -port interferometer and d -dimensional OAM mode discrimination elements. The d -port interferometer performs the d -dimensional Fourier transformation on the path modes, and its operator is shown in Eq. (10):

$$\hat{U}_d = \frac{1}{\sqrt{d}} \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega_d & \omega_d^2 & \omega_d^3 & \cdots & \omega_d^{d-1} \\ 1 & \omega_d^2 & \omega_d^4 & \omega_d^6 & \cdots & \omega_d^{2(d-1)} \\ 1 & \omega_d^3 & \omega_d^6 & \omega_d^9 & \cdots & \omega_d^{3(d-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_d^{d-1} & \omega_d^{2(d-1)} & \omega_d^{3(d-1)} & \cdots & \omega_d^{(d-1)(d-1)} \end{pmatrix}, \quad (10)$$

where $\omega_d = \exp(2\pi i/d)$. In this case, a d -dimensional cyclic-entangled state, which is a d -partite d -dimensional entangled state, is written as follows:

$$|\Phi_{(0,0)}^d\rangle = \frac{1}{\sqrt{d!}} \text{perm}(\Lambda) |\text{vac}\rangle, \quad (11)$$

where $\text{perm}(A)$ is the permanent of the matrix A . The matrix Λ is defined as shown in the following equation:

$$\Lambda = \begin{pmatrix} \hat{a}_{00}^\dagger & \hat{a}_{01}^\dagger & \cdots & \hat{a}_{0(d-1)}^\dagger \\ \hat{a}_{10}^\dagger & \hat{a}_{11}^\dagger & \cdots & \hat{a}_{1(d-1)}^\dagger \\ \vdots & \vdots & \ddots & \vdots \\ \hat{a}_{(d-1)0}^\dagger & \hat{a}_{(d-1)1}^\dagger & \cdots & \hat{a}_{(d-1)(d-1)}^\dagger \end{pmatrix}, \quad (12)$$

where \hat{a}_{xy}^\dagger denotes the photon creation operator. The subscript x denotes an OAM value of the single photon. The subscript y means a label of the party who sent the photon to Charlie, where $y = 0$ means Alice, and $y = n$ means Bob _{n} for $n \in \{1, 2, \dots, d-1\}$.

Schematic description of QSS with correlation measurement

In this section, a schematic description of $3d$ -CQSS is presented. In this protocol, three authorized parties, Alice, Bob₁, and Bob₂, participate in secret sharing, and an untrusted third party, Charlie, performs a measurement. Each authorized party has a single photon generator and a three-dimensional information encoder, such as a spatial light modulator (SLM) to encode in OAM modes of a single photon. Note that another degree-of-freedom of a single photon can be used in this protocol for three-dimensional encoding, such as multi time-bin modes. In QSS, it is necessary that one party cannot expect distributed secrets of the others. If the system of one party is traced out, the quantum states of the others are entangled for Eq. (5). Therefore, it is impossible to exactly predict the secret of the other party in this case. For the quantum state described in the form of Eq. (6), when the system of one party is traced out, the quantum states of the others are a fully mixed state.

The procedure of the $3d$ -CQSS protocol is as follows:

1. Alice (Bob₁, Bob₂) randomly generates binary information to choose a basis, and three-dimensional information, a (b_1 , b_2).
2. Each authorized party generates a single photon state, $|i\rangle$ or $|\bar{i}\rangle$, according to his/her three-dimensional information, i .
3. The authorized parties send their single photon states to Charlie, who has a correlation measurement setup.
4. Charlie performs the correlation measurement onto the incoming photons, and he announces the result of the measurement.
5. The authorized parties compare their encoding bases through classical communication. They keep the encoded information if the encoding bases are the same. The trials that Alice's and Bobs' bases are not identical, are discarded.
6. If Charlie's measurement result is one of the states described in Eq. (5), Alice performs a local operation to satisfy the following condition: $a + b_1 + b_2 = 0 \pmod{3}$. (See Table 1.)
7. After several repetition of steps 2.2–2.2, they estimate parameters for security analysis by revealing a part of data.

Basis	Alice's operation
ordinary basis	$a \rightarrow a + i(\bmod 3)$
bar basis	$\bar{a} \rightarrow \bar{a} + \sigma(\bmod 3)$

Table 1. Alice's local operation when the result of the three-dimensional correlation measurement is $|\Phi_{(2i+j,\sigma)}^3\rangle$. To satisfy the condition, $a + b_1 + b_2 = 0(\bmod 3)$, a local operation is necessary, where a , b_1 , and b_2 are encoded number of Alice, Bob₁, and Bob₂, respectively.

- A portion of the data is revealed when all authorized parties choose the ordinary basis and Charlie's measurement outcome corresponds to one of the states given in Eq. (5).
 - The entire dataset is revealed when all authorized parties choose the ordinary basis and Charlie's measurement outcome corresponds to one of the states described in Eq. (6).
 - All of the data is revealed if all authorized parties used the bar basis.
8. At this point, Alice and the Bobs are prepared to share a classical secret based on their measurement outcomes and proceed with the analysis of security parameters.

The parameters for security analysis will be described in the Security Analysis section. Measurement statistics from both the ordinary and bar bases are required for security analysis. However, outcomes obtained in the bar basis are used solely for parameter estimation, not for secret sharing, since a party could potentially infer the encoded values of the others when the encoding is done in the bar basis. For example, the $3d$ -cyclic-entangled state is written in the bar basis as follows:

$$|\Phi_{(0,0)}^3\rangle = \frac{1}{3\sqrt{2}} \sum_{k=0}^2 (2|\bar{k}, \bar{k}, \bar{k}\rangle - |\bar{k}, \bar{k}+1, \bar{k}+2\rangle + |\bar{k}, \bar{k}+2, \bar{k}+1\rangle). \quad (13)$$

If Alice sent $|\bar{0}\rangle$ to Charlie, the number of possible cases is three. The two cases are that Bob₁ and Bob₂ sent $|\bar{1}\rangle$ and $|\bar{2}\rangle$, or $|\bar{2}\rangle$ and $|\bar{1}\rangle$ to Charlie, respectively, and the probability of each case is one fourth. The other case is that both Bob₁ and Bob₂ sent $|\bar{0}\rangle$ to Charlie, and its probability is one half. Since these three cases are not equally probable, the encoded number of the other parties is not random for one party. Therefore, the bar basis cannot be used to share a secret. In conclusion, measurement results obtained in the ordinary basis are used for both QSS and its security analysis, whereas those obtained in the bar basis are used exclusively for security analysis.

In step 5 of the protocol, the probability that all players choose the same basis is $(1/2)^2$, since each player independently selects between two bases with equal probability, and there are two players involved. Therefore, only a fraction $(1/2)^2$ of the trials is retained after basis sifting. In step 7, although there are 27 orthonormal entangled states in total, secret sharing is performed only using the quantum states defined in Eq. (5). As a result, only one-third of the sifted trials contribute to secret sharing, while the remaining two-thirds are used solely for security analysis under the assumption of ideal correlation measurements. When using the practical correlation measurement introduced in Fig. 1, it can successfully distinguish only one entangled state with probability $1/2$. Thus, the success probability of this measurement is $(1/27) \times (1/2)$, and the total sifting probability becomes the product of the basis-sifting probability from step 5 and the success probability of the correlation measurement, yielding $(1/2)^2 \times (1/54)$.

When Alice, Bob₁, and Bob₂ distributed three-dimensional classical information, a , b_1 , and b_2 , then the procedure of sharing a three-dimensional classical number is as follows:

1. The dealer, Alice, chooses a classical secret, S , where $S \in \{0, 1, 2\}$.
2. Alice announces the message, M , through classical communication. M is defined from the equation: $M = S + a(\bmod 3)$.
3. Players, Bob₁ and Bob₂, can decode the classical secret by sharing their encoded numbers, but cannot without collaboration. The decoding is shown in the following equation:

$$M + b_1 + b_2(\bmod 3) = S + a + b_1 + b_2(\bmod 3) = S.$$

The protocol can be extended to d -dimensional CQSS (d -CQSS) among a dealer, Alice, and players, Bob₁ to Bob _{$d-1$} . In the d -CQSS protocol, each of the authorized parties send a d -dimensionally encoded photon to Charlie who has a d -dimensional correlation measurement setup. They use two different bases, the ordinary basis $\{|0\rangle, |1\rangle, \dots, |d-1\rangle\}$ and the bar basis $\{|\bar{0}\rangle, |\bar{1}\rangle, \dots, |\bar{d-1}\rangle\}$. Similarly with the three-dimensional case, the relation between the two bases is the d -dimensional Fourier transformation. They can distribute a d -dimensional classical secret with the d -partite d -dimensional quantum state written in Eq. (11). If the result of the d -partite d -dimensional correlation measurement is $|\Phi_{(0,0)}^d\rangle$, a sum on $(\bmod d)$ of the encoded numbers of all the quantum state always becomes zero. A participant cannot predict the encoded number of the others, since if k photons in $|\Phi_{(0,0)}^d\rangle$ are traced out, for $k < d-1$, the rest of the photons are entangled with the same

probabilities. Therefore, the authorized parties can employ $(d - 1, d - 1)$ -threshold QSS by using this quantum state.

Security analysis of our QSS protocol

Strategy for security analysis

Before we analyze security of the $3d$ -CQSS protocol, we should define constraints to construct a secure QSS protocol: (i) The single photon generators and the OAM encoders, which the authorized parties have, should be characterized and not be influenced by Eve. (ii) The authorized parties hold trusted random number generators to select an encoding basis and encoding information. (iii) Successive rounds of the protocol must be completely independent, i.e., we assume an independent and identically distributed (i.i.d.) attack of Eve. (iv) The laboratory of each authorized party must be isolated from the outside to prevent unintended information leakage or inflow. Under these assumptions, we analyze security of the $3d$ -CQSS protocol in the asymptotic limit.

Here, we introduce the security analysis for $3d$ -CQSS. To analyze the security, we exploit the entanglement distillation process (EDP)^{69–71} of an equivalent protocol of the $3d$ -CQSS protocol, which the authorized parties share a tripartite qutrit entangled state $|\Phi_{(0,0)}^3\rangle$. The equivalent protocol can be constructed by replacing the qutrit generation setups of the authorized parties to bipartite qutrit maximally entangled state generation setups and qutrit discrimination measurement setups. Each authorized party generates the bipartite three-dimensional maximally entangled state described in the following equation:

$$|\Theta\rangle = \frac{1}{\sqrt{3}} (|0, 0\rangle + |1, 1\rangle + |2, 2\rangle), \quad (14)$$

and send one photon to Charlie. Subsequently, Charlie performs the three-dimensional correlation measurement and announces the result. The six-photon quantum state is described as follows:

$$\begin{aligned} |\Xi\rangle_{AA'B_1B'_1B_2B'_2} &= |\Theta\rangle_{AA'} \otimes |\Theta\rangle_{B_1B'_1} \otimes |\Theta\rangle_{B_2B'_2} \\ &= \sum_{\sigma=0}^2 \sum_{j=0}^8 \left[|\Phi_{(j,\sigma)}^3\rangle_{A'B'_1B'_2} \otimes |\Phi_{(j,3-\sigma)}^3\rangle_{AB_1B_2} \right], \end{aligned} \quad (15)$$

where the subscripts A , B_1 , and B_2 denote the photons that Alice, Bob₁, and Bob₂ keep, and A' , B'_1 , and B'_2 are the photons sent from Alice, Bob₁, and Bob₂ to Charlie, respectively. If Charlie's result is $|\Phi_{(j,\sigma)}^3\rangle$ where j is an even number and $j < 6$, the authorized parties can share $|\Phi_{(0,0)}^3\rangle_{AB_1B_2}$ by means of local operations and classical communication (LOCC). Finally, the authorized parties choose a measurement basis and measure their photon. If the measurement bases are the same, $a + b_1 + b_2 = 0 \pmod{3}$ is always satisfied where a , b_1 , and b_2 are the outcome of Alice, Bob₁, and Bob₂, respectively.

In order to assure the information-theoretic security, the authorized parties analyze their security under the assumption that Eve can exploit everything allowed by the quantum mechanics for an attack. The worst case is that Eve has full control over the shared quantum state. This attack can be realized by means of purification of the total quantum system, including Eve's ancillary system. The total system can be described in the form of a pure state as shown in Eq. (16):

$$\sum_{\sigma=0}^2 \sum_{j=0}^8 \sqrt{\lambda_{(j,\sigma)}} |\Phi_{(j,\sigma)}^3\rangle_{AB_1B_2} \otimes |e_{(j,\sigma)}\rangle_E, \quad (16)$$

where $\{|e_{(j,\sigma)}\rangle\}$ is Eve's orthonormal basis. Then the quantum system of the authorized parties can be obtained by tracing out Eve's system as described in the following equation:

$$\hat{\rho}_{AB_1B_2} = \sum_{\sigma=0}^2 \sum_{j=0}^8 \lambda_{(j,\sigma)} |\Phi_{(j,\sigma)}^3\rangle \langle \Phi_{(j,\sigma)}^3|. \quad (17)$$

Now, we analyze the amount of a shared classical secret through a single sifted pulse in the asymptotic limit, which we refer a secret key rate for simplicity from now on. A sifted pulse means that a pulse can be used for generating a secret key. In the $3d$ -CQSS protocol, the sifted pulse is obtained when all the authorized parties use the ordinary basis, and the result of the three-dimensional correlation measurement is $|\Phi_{(0,0)}^3\rangle$. The asymptotic secret key rate of the $3d$ -CQSS protocol can be calculated from the Devetak–Winter formula⁷¹, which is used in various QSS protocols^{72–74}, shown in Eq. (18):

$$r_{\min} = I(A, \overline{B}) - \chi(A; E) = I(A, 3 - B_1 - B_2) - \chi(A; E), \quad (18)$$

where \overline{B} denotes joint measurement result of Bobs and $(\text{mod } 3)$ is omitted in the bracket of the mutual information. Hereafter, we omit \min in the subscript of the secret key rate r . The first term of the right-hand side in Eq. (18) is defined as the mutual information between Alice's encoded information, A , and joint measurement result of players, which is a modular sum of Bob₁ and Bob₂'s encoded information, $3 - B_1 - B_2 \pmod{3}$. In a multiparty QKD, all the authorized parties share a symmetric secret key, so the smallest mutual information

between two parties is necessary to obtain a secret key rate^{75,76}. Unlike multiparty QKD, in QSS, it is necessary to consider the mutual information between Alice's information and the modular sum of the others to evaluate a secret key rate since a classical secret is shared by using Alice's encoded information and the modular sum of the others. The second term is the Holevo information which is defined as an upper bound to the amount of information that Eve can know about a quantum state transmitted through the quantum channel⁷⁷. By subtracting the Holevo information from the mutual information, we can obtain the amount of information that the authorized parties can share securely by using the quantum state.

There is another case that one of the authorized players is malicious. For instance, Bob₁ can collaborate with Eve to obtain Alice's information without Bob₂'s information. In this case, the security of the proposed protocol becomes more vulnerable compared with a QSS protocol using a tripartite qutrit GHZ state shown in the following equations:

$$\begin{aligned} |3d\text{-GHZ}_3\rangle &= \frac{1}{\sqrt{3}} (|0, 0, 0\rangle + |1, 1, 1\rangle + |2, 2, 2\rangle) \\ &= \frac{1}{3} \sum_{k=0}^2 (|\bar{k}, \bar{k}+1, \bar{k}+2\rangle + |\bar{k}, \bar{k}+2, \bar{k}+1\rangle + |\bar{k}, \bar{k}, \bar{k}\rangle). \end{aligned} \quad (19)$$

In a QSS protocol using the GHZ state, if Bob₁'s measurement outcome is $\bar{0}$, then there are three possible outcomes of Alice and Bob₂, $\{0, 0\}$, $\{1, 2\}$, and $\{2, 1\}$. However, in the proposed protocol, only the two cases, $\{1, 2\}$ and $\{2, 1\}$, are possible from Eq. (5) when Bob₁'s measurement outcome is 0. Therefore, intuitively, a secret key rate of the proposed protocol with a malicious player could be low compared with that of a QSS protocol using the GHZ state with a malicious player. To analyze the security of the proposed protocol with the malicious Bob₁, the Devetak–Winter formula is shown in Eq. (20) can be used:

$$r = I(A, 3 - B_1 - B_2) - \chi(A; EB_1), \quad (20)$$

where (mod 3) is omitted in the bracket of the mutual information.

Like the case of 3d-CQSS, a secret key rate of d-CQSS can be obtained from the Devetak–Winter formula as shown in Eq. (21):

$$r = I\left(A, d - \sum_{n=1}^{d-1} B_n\right) - \chi(A; E), \quad (21)$$

when all the authorized parties are trusted. The secret key rate is changed to the following equation:

$$r = I\left(A, d - \sum_{n=1}^{d-1} B_n\right) - \chi\left(A; E \prod_{n=1}^k B_n\right), \quad (22)$$

when Bob₁ to Bob_k are malicious players who collaborate with Eve.

Error parameters

We define three groups of the tripartite qutrit entangled states, $\{|\Phi_{(2i,\sigma)}^3\rangle\}$, $\{|\Phi_{(2i+1,\sigma)}^3\rangle\}$, and $\{|\Phi_{(6+i,\sigma)}^3\rangle\}$, where $i, \sigma \in \{0, 1, 2\}$. A state can be transformed to another state in the same group by means of LOCC but cannot be transformed to a state in another group. To simplify the analysis, the density matrix described in Eq. (17) is transferred to the depolarized state written in Eq. (23):

$$\begin{aligned} \hat{\rho}_{\text{dp}} &= \sum_{\sigma=0}^2 \left(\lambda_{(0,\sigma)} |\Phi_{(0,\sigma)}^3\rangle \langle \Phi_{(0,\sigma)}^3| + \sum_{i=1}^2 \lambda_{-} |\Phi_{(2i,\sigma)}^3\rangle \langle \Phi_{(2i,\sigma)}^3| \right. \\ &\quad \left. + \sum_{j=0}^2 \lambda_{+} |\Phi_{(2j+1,\sigma)}^3\rangle \langle \Phi_{(2j+1,\sigma)}^3| + \sum_{k=6}^8 \lambda_{=} |\Phi_{(k,\sigma)}^3\rangle \langle \Phi_{(k,\sigma)}^3| \right), \end{aligned} \quad (23)$$

by means of LOCC like the multipartite qubit description⁷⁸ under the assumption that Eve performs a symmetric attack to obtain encoded information in the both bases well⁷⁹. The coefficients, λ_{-} , λ_{+} , and $\lambda_{=}$, can be obtained from the following equations:

$$\lambda_{-} = \frac{1}{6} \sum_{\sigma=0}^2 \sum_{j=1}^2 \lambda_{(2j,\sigma)}, \quad (24)$$

$$\lambda_{+} = \frac{1}{9} \sum_{\sigma=0}^2 \sum_{j=0}^2 \lambda_{(2j+1,\sigma)}, \quad (25)$$

$$\lambda_{-} = \frac{1}{9} \sum_{\sigma=0}^2 \sum_{j=6}^8 \lambda_{(j,\sigma)}. \quad (26)$$

To evaluate a secret key rate, it is necessary to define parameters which can be obtained from the revealed data. The four different error rates are defined as shown in the following equations:

$$Q_s = \sum_{j=2}^8 \lambda_{(j,0)} = 2\lambda_{+} + 2\lambda_{-} + 3\lambda_{=}, \quad (27)$$

$$Q_{\omega} = \sum_{\sigma=1}^2 \sum_{j=0}^8 \lambda_{(j,\sigma)} = \lambda_{(0,1)} + \lambda_{(0,2)} + 6\lambda_{+} + 4\lambda_{-} + 6\lambda_{=}, \quad (28)$$

$$Q_{\pm} = \lambda_{(1,0)} = \lambda_{+}, \quad (29)$$

$$Q_u = \frac{1}{9} \sum_{k,\sigma=0}^2 \lambda_{(k+6,\sigma)} = \lambda_{=}. \quad (30)$$

The Q_s is called a state error rate, which is defined as the probability that the result state does not have a ω_3 phase change; however, it is not the wanted state. The Q_{ω} is a three-dimensional phase error rate, the probability that the result state has a phase of ω_3 . The Q_{\pm} is a two-dimensional phase error rate, the probability that the (+) sign in $|\Phi_{(0,0)}^3\rangle$ is changed to (−). Finally, the Q_u is called a user error rate, the probability of a state for which the two players, Bob₁ and Bob₂, have the same encoded information. The parameters can be obtained from the statistics of the authorized parties as shown in the following equations:

$$Q_s = p(a + b_1 + b_2 \neq 0 \ \& \ b_1 \neq b_2) - p(\bar{a} + \bar{b}_1 + \bar{b}_2 \neq 0) + \frac{1}{3} [2p(a + b_1 + b_2 = 0 \ \& \ b_1 \neq b_2) - (\langle \hat{X} \hat{X} \hat{X} \rangle + \text{c.c.})], \quad (31)$$

$$Q_{\omega} = p(\bar{a} + \bar{b}_1 + \bar{b}_2 \neq 0), \quad (32)$$

$$Q_{\pm} = |1 - 2p(\bar{a} = \bar{b}_1 = \bar{b}_2 \mid \bar{a} + \bar{b}_1 + \bar{b}_2 = 0)|, \quad (33)$$

$$Q_u = \frac{1}{9} p(b_1 = b_2), \quad (34)$$

where $p(x)$ can be obtained from (the number of pulses for which x is true)/(the number of sifted pulses for which the basis including x is used), and (mod 3) is omitted in all the brackets. In Eq. (31), c.c. denotes complex conjugate of $\langle \hat{X} \hat{X} \hat{X} \rangle$. The operator \hat{X} is defined as the following equation:

$$\hat{X} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad (35)$$

where the bases of the matrix are the OAM modes.

Secret key rate

In this section, the secret key rate for 3d-CQSS is evaluated using Eqs. (17) and (18) under the assumption that all authorized parties are trusted, as shown in Eq. (36):

$$r = \log 3 + \sum_{j=0}^8 \sum_{\sigma=0}^2 (\lambda_{(j,\sigma)} \log \lambda_{(j,\sigma)}) - \sum_{j=0}^8 \left[\left(\sum_{\sigma=0}^2 \lambda_{(j,\sigma)} \right) \log \left(\sum_{\sigma=0}^2 \lambda_{(j,\sigma)} \right) \right] + \sum_{i=0}^2 \Lambda_i \log \Lambda_i. \quad (36)$$

In the absence of isotropy, the secret key rate can be determined through numerical analysis based on the measurement outcomes from the authorized parties. This analysis seeks to identify a shared quantum state that minimizes the secret key rate⁸⁰.

To compare our protocol with others, we consider a depolarizing channel, which has been commonly used in the literature for such comparisons^{81,82}. With the depolarized state in Eq. (23), an analytic secret key rate of 3d-CQSS can be evaluated by using the Eqs. (23–30), as shown in Eq. (37):

$$r = (1 - 3Q_u - 3Q_{\pm}) \log 3 - (Q_{\omega} + Q_s - 2Q_{\pm} - 3Q_u) + (1 - Q_{\omega} - Q_s - Q_{\pm}) \log(1 - Q_{\omega} - Q_s - Q_{\pm}) + 3(Q_s - Q_u) \log(Q_s - Q_u) + (Q_{\omega} - 2Q_s - 2Q_{\pm}) \log(Q_{\omega} - 2Q_s - 2Q_{\pm}) - (1 - 3Q_s - 3Q_{\pm}) \log(1 - 3Q_s - 3Q_{\pm}). \quad (37)$$

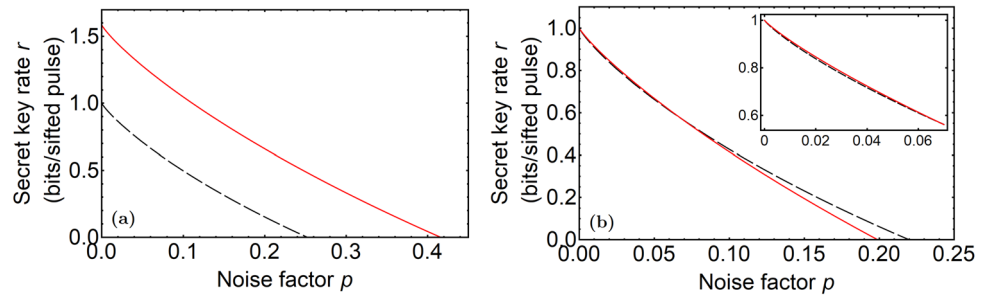


Fig. 4. Secret key rates per sifted pulse under a depolarizing channel. The secret key rate of the three-party QSS protocol using qubits (black, dashed line) and that of the 3d-CQSS protocol (red, solid line) are drawn. p is the ratio of white noise. **(a)** The secret key rates when all the authorized parties are trusted. **(b)** The secret key rates when Bob₁ cooperates with Eve.

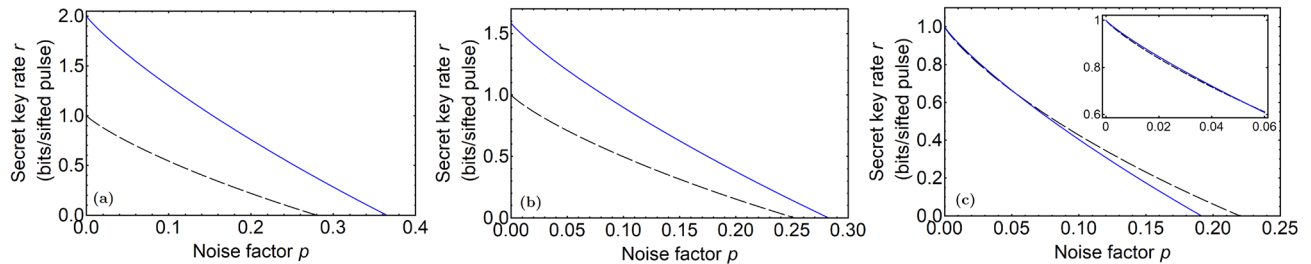


Fig. 5. Secret key rates per sifted pulse under a depolarizing channel. The secret key rate of the four-party QSS protocol using qubits (black, dashed line) and that of the 4d-CQSS protocol (blue, solid line) are drawn. p is the ratio of white noise. **(a)** The secret key rates when all the authorized parties are trusted. **(b)** The secret key rates when Bob₁ cooperates with Eve. **(c)** The secret key rates when Bob₁ and Bob₂ cooperate with Eve.

The unit of the secret key rate is (bits)/(sifted pulse). This equation can be used to evaluate not only the secret key rate of the 3d-CQSS protocol, but also that of an entanglement-based 3d-QSS protocol that exploits the tripartite qutrit cyclic-entangled state, $|\Phi_{(0,0)}^3\rangle$. By using the same method, a secret key rate of d -CQSS can be calculated as well. Calculation details are drawn in the Methods section.

Now, let us compare the secret key rate of QSS using qudit. To compare the secret key rates, we consider a depolarizing channel with white noise. The depolarized state for d -CQSS is shown in Eq. (38):

$$\hat{\rho}_{d,\text{dp}} = (1-p)|\Phi_{(0,0)}^d\rangle\langle\Phi_{(0,0)}^d| + \frac{p}{d^d}\mathbb{1}_{d^d}, \quad (38)$$

where $\mathbb{1}_x$ is the $x \times x$ identity operator. For 2d-QSS, we calculate the secret key rate evaluated by using the Devetak–Winter formula and a N -partite qubit GHZ state under a depolarizing channel is described in the following equation:

$$\hat{\rho}_{2,\text{dp}} = (1-p)|2d\text{-GHZ}_N\rangle\langle 2d\text{-GHZ}_N| + \frac{p}{2^N}\mathbb{1}_{2^N}. \quad (39)$$

where the N -partite qubit GHZ state is defined as shown in the following equation:

$$|2d\text{-GHZ}_N\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes N} + |1\rangle^{\otimes N}). \quad (40)$$

Figure 4(a) shows the secret key rate of 3d-CQSS (red solid line) and that of three-party 2d-QSS (black dashed line) evaluated under a depolarizing channel when all the parties are trusted. 3d-CQSS has a higher secret key rate than 2d-QSS since d -dimensional information is transferred by a single quantum, rather than binary information. The plots show 3d-CQSS has noise robustness compared with 2d-QSS as well. Figure 4(b) shows the secret key rate of 3d-CQSS (red solid line) and that of 2d-QSS (black dashed line) when Bob₁ cooperates with Eve. Since Bob₁ can expect values of the others from his number, the security becomes more vulnerable against a dishonest authorized party compared with three-party 2d-QSS. The secret key rate of 3d-CQSS is slightly higher only when the noise factor is smaller than approximately 7%, and then 2d-QSS becomes more efficient when the noise factor is larger than the value.

Figure 5 shows the secret key rate of 4d-CQSS (blue solid line) and that of four-party 2d-QSS (black dashed line) evaluated under a depolarizing channel. Figure 5(a) shows the secret key rates when all players are

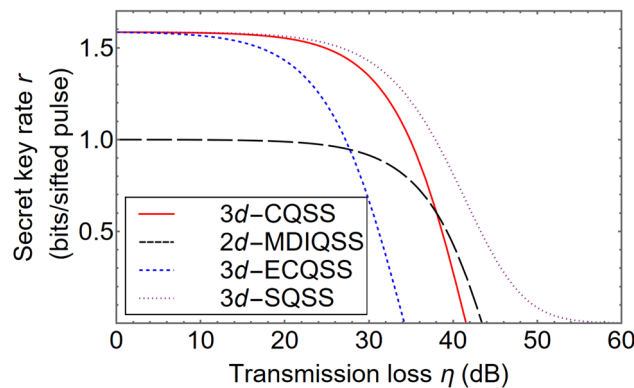


Fig. 6. The secret key rates per sifted pulse with experimental factors when all players are trusted. The secret key rates of the $2d$ -MDIQSS protocol (black dashed line), the entangled state based $3d$ -CQSS ($3d$ -ECQSS) protocol (blue dotted line), the correlation measurement based $3d$ -CQSS protocol (red solid line), and single photon based $3d$ -QSS ($3d$ -SQSS) protocol (Purple dotted line) are plotted. Experimental factors, transmission loss η and a dark count rate of a single photon detector, are considered in the plots. The dark count rate is assumed as 10^{-5} per pulse.

trusted. Similarly with three-dimensional case, $4d$ -CQSS has the higher secret key rate and the protocol can be accomplished when the noise is larger compared with four-party $2d$ -QSS. Figure 5(b) shows the secret key rates when Bob₁ collaborates with Eve to obtain Alice's encoded number without encoded numbers of Bob₂ and Bob₃. Since the mutual information between Alice and Bob₁ is $2 - \log 3$ for the ideal situation, i.e., the authorized parties share $|\Phi_{(0,0)}^4\rangle$, the maximum secret key rate of the protocol can be obtained the mutual information among the authorized parties subtracted by the mutual information between Alice and Bob₁, $\log 3$. Therefore, $4d$ -CQSS has the higher secret key rate compared with four-party $2d$ -QSS even when there is one malicious player. If there are two malicious players, Bob₁ and Bob₂, the secret key rate becomes almost similar with that of four-party $2d$ -QSS as shown in Fig. 5(c) since the mutual information between Alice's number and the numbers of Bob₁ and Bob₂ becomes one for the ideal situation.

For d -CQSS, the maximum secret key rate per sifted pulse can be obtained as $\log(d - m)$ where m is the number of malicious players for $0 \leq m \leq d - 2$. This value comes from the mutual information among the authorized parties, $\log d$, and the mutual information among Alice and malicious players, $\log d - \log(d - m)$, for the ideal situation, i.e., the authorized parties share the quantum state $|\Phi_{(0,0)}^d\rangle$. Because of the structure of the quantum state, d -CQSS cannot guarantee the same security with d -party QSS using d -dimensional GHZ state when there are malicious players. However, if there are more than two trusted players in d -CQSS, the protocol can be more efficient compared with d -party $2d$ -QSS.

In Fig. 6, the secret key rates of the $2d$ -MDIQSS protocol³⁵ (black dashed line), the entangled state based $3d$ -CQSS ($3d$ -ECQSS) protocol (blue dotted line), the correlation measurement based $3d$ -CQSS protocol (red solid line), and single photon based $3d$ -QSS ($3d$ -SQSS) protocol⁸³ (Purple dotted line) are compared under the consideration of experimental factors, transmission loss of a photon and a dark count rate of a single photon detector. The other conditions are assumed as the ideal, for instance, there is no Eve, state preparation is perfect, and the all authorized parties are trusted. In the plot, it is shown that the secret key rate of the $3d$ -CQSS protocol is higher than that of the $2d$ -MDIQSS protocol, when the transmission loss is lower than approximately 39 dB. This effect also can be seen in QKD, as it was known that a high-dimensional QKD protocol is vulnerable to the transmission loss compared with the same type of QKD protocol using qubits^{84,85}.

As shown in the plot, the $3d$ -CQSS with the correlation measurement has an advantage compared with the entanglement-based $3d$ -CQSS ($3d$ -ECQSS) protocol regarding resistance to the transmission loss when all authorized parties are trusted. Note that this advantage appears even when the preparation efficiency of an entangled state is not considered. This effect comes from the number of errors which occur when two or more photons are lost. For example, let us consider the case that Bob₁'s and Bob₂'s photons are lost. In the correlation measurement based $3d$ -CQSS protocol, if Alice's photon clicks the detector $D_{A'0}$, then the three-dimensional correlation measurement succeeds only when $D_{A'1}$ and $D_{A'2}$ are clicked due to the dark count. In this situation, if Bob₁ and Bob₂ did not send quantum states having an OAM mode of 1 and 2, the trial introduces an error. In the $3d$ -ECQSS protocol, if one photon clicks Alice's detector D_0 , where D_x is the detector corresponding to the OAM mode x , there are two cases that an error does not occur. The first case is that Bob₁'s detector D_1 and Bob₂'s detector D_2 are clicked, and the other is that Bob₁'s detector D_2 and Bob₂'s detector D_1 are clicked. Errors are introduced for the other cases, for which Bob₁'s one detector and Bob₂'s one detector are clicked due to the dark count. Therefore, the transmission loss and the dark count introduce more errors in the $3d$ -ECQSS. In conclusion, the $3d$ -CQSS protocol has the advantage of its practicality compared with the $3d$ -ECQSS even though the state generation rate is not considered. A QSS protocol based on a 3-dimensional GHZ state would yield similar results, as the measurement setup for the 3-dimensional GHZ state QSS protocol is identical to that of the $3d$ -ECQSS protocol. Details of the calculation are described in the Methods section.

We compare the performance of our protocol with that of another high-dimensional QSS protocol. As an example, we consider the single-photon-based d -QSS (d -SQSS) protocol^{29,83}. In this protocol, a dealer generates a single-photon quantum state and sends it to the players. The players then sequentially perform unitary operations chosen from a predefined set and return the results to the dealer. The dealer selects a measurement basis from the players' broadcasts to obtain a deterministic outcome. Therefore, the protocol relies on just a single photon, and with active basis choice, only three detectors are needed. The mutual information for $3d$ -SQSS is shown in Fig. 6 for performance comparison. Since $3d$ -SQSS uses only three detectors, it is less susceptible to photon loss and detector dark counts compared to other protocols. Although SQSS appears to be the best QSS protocol in this comparison, our protocol offers certain advantages.

Transmission loss can be translated into communication distance. For instance, a typical single-mode fiber (SMF) has a loss of about 0.25 dB/km at a 1550 nm wavelength signal. Thus, the maximum distance for QSS protocols can be obtained from Fig. 6. However, due to the differences in protocol constructions, some corrections are needed in the conversion. In the case of $3d$ -SQSS, since the dealer generates the single photon and the photon must return to the dealer, the communication distance is effectively half of the photon transmission distance. For CQSS and MDIQSS, an untrusted third party with the correlation measurement setup can serve as an intermediary between the authorized parties, meaning the communication distances in these protocols can be doubled in the conversion of the plots in Fig. 6. In the case of $3d$ -ECQSS, due to the trusted device assumption, Alice must possess the entangled state generator, so the plot in Fig. 6 can be directly translated into the communication distance. With these conditions in mind, we conclude that QSS protocols with correlation measurement capabilities can achieve longer-distance quantum communication compared to other QSS protocols.

Discussion

In this article, the $(d-1, d-1)$ -threshold d -CQSS was investigated. It was shown that the d -CQSS protocol can be implemented with the current state-of-the-art technologies and is more practical compared with the entanglement-based d -QSS protocol since generation of qudit GHZ state is not necessary. By employing correlation measurement, our protocol inherently ensures MDI security^{35,36,38,39}, meaning that all types of potential side-channel attacks exploiting detector imperfections are mitigated, especially when such imperfections pose significant security risks⁸⁶. Even if an untrusted party attempts to deceive the authorized parties, the deception will influence their measurement statistics, making the attempt detectable.

The security of the d -CQSS protocol was analyzed, showing improvement on the secret key rate compared with $2d$ -QSS. The security when there are malicious players was investigated as well. Due to the properties of the entangled state discriminated by the correlation measurement, the advantage of high-dimensional system decreases with malicious players. However, it was shown that there is enhancement on the secret key rate compared with the $2d$ -QSS when there are more than two trusted players. Even when there is only one trusted player, the enhancement exists at low error regime. It was also shown that the $3d$ -CQSS protocol with the correlation measurement would have robustness against transmission loss compared with the entanglement-based $3d$ -CQSS protocol. A single-photon-based $3d$ -QSS protocol^{29,83} offers a higher secret key rate for the same transmission loss compared to our protocol. However, when translated into communication distance, our protocol outperforms in terms of the maximum achievable communication distance due to its design.

We have analyzed the security of our protocol under certain assumptions to highlight its characteristics through a simple comparison. However, in practical scenarios, these assumptions may not always hold. Several studies have focused on relaxing these assumptions, such as finite key analysis^{82,87–89} as opposed to asymptotic key rates, and analysis against coherent attacks without the i.i.d. assumption^{90,91}. Additionally, device-independent (DI) security analysis, based on nonlocality tests, can eliminate most of the assumptions^{74,92–95}. In DI analysis, only two assumptions are required: first, that quantum physics is correct; and second, that there is no unintended information leakage in the laboratories of each authorized party. Nonlocality tests, often referred to as Bell-type inequalities^{10,96}, reveal correlations that cannot be explained by classical means based on measurement statistics. In other words, quantum correlations are confirmed when measurement statistics violate the Bell inequality, without assuming any specific device. For DI analysis, an appropriate Bell inequality is necessary. While the Clauser–Horne–Shimony–Holt (CHSH) inequality⁹⁶ satisfies tightness and maximal violation with maximal entanglement (MVME) conditions, no such inequality exists for high-dimensional systems. The Collins–Gisin–Linden–Massar–Popescu (CGLMP) inequality⁹⁷ is known as the unique tight inequality for 3-dimensional bipartite quantum systems⁹⁸, but its maximal violation occurs with a partially entangled state. A nonlocality test for high-dimensional bipartite quantum systems that satisfies MVME has been proposed⁹⁹. However, since our protocol relies on cyclic-entangled states for security analysis, the GHZ-type generalization cannot be applied. Therefore, it is crucial to construct a suitable nonlocality test for cyclic-entangled states to ensure the DI security of our protocol.

Methods

Three-dimensional correlation measurement

Here, click events of the three-dimensional correlation measurement are investigated. The interference among the three photons sent from the authorized parties is performed by using the tritter described in Eq. (3) and Eq. (4). The tripartite quantum states, $|\Phi_{(0,\sigma)}^3\rangle$ and $|\Phi_{(1,\sigma)}^3\rangle$ are considered where $\sigma \in \{0, 1, 2\}$. In the other states, there are photons whose OAM mode is identical. This causes the two photons to enter the same detector. These states cannot be discriminated, since photon number resolving detectors are not involved in the setup.

With the tritter operation shown in Eq. (4), the detector click events can be calculated. A quantum state $|0, 1, 2\rangle_{ABC}$ is transformed with the tritter operation as follows:

$$\begin{aligned}
|0, 1, 2\rangle_{ABC} &\xrightarrow{\text{tritter}} \frac{1}{3\sqrt{3}} \left[(|0\rangle_{A'} + |0\rangle_{B'} + |0\rangle_{C'}) (|1\rangle_{A'} + \omega_3 |1\rangle_{B'} + \omega_3^2 |1\rangle_{C'}) (|2\rangle_{A'} + \omega_3 |2\rangle_{B'} + \omega_3^2 |2\rangle_{C'}) \right] \\
&= \frac{1}{3\sqrt{3}} \left(|0, 1, 2\rangle_{A'A'A'} + |0, 1, 2\rangle_{B'B'B'} + |0, 1, 2\rangle_{C'C'C'} + \omega_3^2 |0, 1, 2\rangle_{A'B'C'} + \omega_3 |0, 2, 1\rangle_{A'B'C'} \right. \\
&\quad \left. + \omega_3^2 |1, 2, 0\rangle_{A'B'C'} + \omega_3 |1, 0, 2\rangle_{A'B'C'} + \omega_3^2 |2, 0, 1\rangle_{A'B'C'} + \omega_3 |2, 1, 0\rangle_{A'B'C'} + \dots \right). \quad (41)
\end{aligned}$$

Similarly, quantum states after tritter operation can be obtained as follows:

$$\begin{aligned}
|0, 2, 1\rangle_{ABC} &\xrightarrow{\text{tritter}} \frac{1}{3\sqrt{3}} \left(|0, 1, 2\rangle_{A'A'A'} + |0, 1, 2\rangle_{B'B'B'} + |0, 1, 2\rangle_{C'C'C'} + \omega_3 |0, 1, 2\rangle_{A'B'C'} + \omega_3^2 |0, 2, 1\rangle_{A'B'C'} \right. \\
&\quad \left. + \omega_3 |1, 2, 0\rangle_{A'B'C'} + \omega_3^2 |1, 0, 2\rangle_{A'B'C'} + \omega_3 |2, 0, 1\rangle_{A'B'C'} + \omega_3^2 |2, 1, 0\rangle_{A'B'C'} + \dots \right), \quad (42)
\end{aligned}$$

$$\begin{aligned}
|1, 2, 0\rangle_{ABC} &\xrightarrow{\text{tritter}} \frac{1}{3\sqrt{3}} \left(|0, 1, 2\rangle_{A'A'A'} + |0, 1, 2\rangle_{B'B'B'} + |0, 1, 2\rangle_{C'C'C'} + \omega_3^2 |0, 1, 2\rangle_{A'B'C'} + \omega_3 |0, 2, 1\rangle_{A'B'C'} \right. \\
&\quad \left. + \omega_3^2 |1, 2, 0\rangle_{A'B'C'} + \omega_3 |1, 0, 2\rangle_{A'B'C'} + \omega_3^2 |2, 0, 1\rangle_{A'B'C'} + \omega_3 |2, 1, 0\rangle_{A'B'C'} + \dots \right), \quad (43)
\end{aligned}$$

$$\begin{aligned}
|1, 0, 2\rangle_{ABC} &\xrightarrow{\text{tritter}} \frac{1}{3\sqrt{3}} \left(|0, 1, 2\rangle_{A'A'A'} + |0, 1, 2\rangle_{B'B'B'} + |0, 1, 2\rangle_{C'C'C'} + \omega_3 |0, 1, 2\rangle_{A'B'C'} + \omega_3^2 |0, 2, 1\rangle_{A'B'C'} \right. \\
&\quad \left. + \omega_3 |1, 2, 0\rangle_{A'B'C'} + \omega_3^2 |1, 0, 2\rangle_{A'B'C'} + \omega_3 |2, 0, 1\rangle_{A'B'C'} + \omega_3^2 |2, 1, 0\rangle_{A'B'C'} + \dots \right), \quad (44)
\end{aligned}$$

$$\begin{aligned}
|2, 0, 1\rangle_{ABC} &\xrightarrow{\text{tritter}} \frac{1}{3\sqrt{3}} \left(|0, 1, 2\rangle_{A'A'A'} + |0, 1, 2\rangle_{B'B'B'} + |0, 1, 2\rangle_{C'C'C'} + \omega_3^2 |0, 1, 2\rangle_{A'B'C'} + \omega_3 |0, 2, 1\rangle_{A'B'C'} \right. \\
&\quad \left. + \omega_3^2 |1, 2, 0\rangle_{A'B'C'} + \omega_3 |1, 0, 2\rangle_{A'B'C'} + \omega_3^2 |2, 0, 1\rangle_{A'B'C'} + \omega_3 |2, 1, 0\rangle_{A'B'C'} + \dots \right), \quad (45)
\end{aligned}$$

$$\begin{aligned}
|2, 1, 0\rangle_{ABC} &\xrightarrow{\text{tritter}} \frac{1}{3\sqrt{3}} \left(|0, 1, 2\rangle_{A'A'A'} + |0, 1, 2\rangle_{B'B'B'} + |0, 1, 2\rangle_{C'C'C'} + \omega_3 |0, 1, 2\rangle_{A'B'C'} + \omega_3^2 |0, 2, 1\rangle_{A'B'C'} \right. \\
&\quad \left. + \omega_3 |1, 2, 0\rangle_{A'B'C'} + \omega_3^2 |1, 0, 2\rangle_{A'B'C'} + \omega_3 |2, 0, 1\rangle_{A'B'C'} + \omega_3^2 |2, 1, 0\rangle_{A'B'C'} + \dots \right). \quad (46)
\end{aligned}$$

Then, the quantum states after tritter operation with $|\Phi_{(0,0)}^3\rangle_{ABC}$ and $|\Phi_{(1,0)}^3\rangle_{ABC}$ can be calculated as follows:

$$\begin{aligned}
|\Phi_{(0,0)}^3\rangle_{ABC} &\xrightarrow{\text{tritter}} \frac{1}{3\sqrt{2}} \left[2(|0, 1, 2\rangle_{A'A'A'} + |0, 1, 2\rangle_{B'B'B'} + |0, 1, 2\rangle_{C'C'C'}) + (\omega_3 + \omega_3^2) (|0, 1, 2\rangle_{A'B'C'} + |0, 2, 1\rangle_{A'B'C'} \right. \\
&\quad \left. + |1, 2, 0\rangle_{A'B'C'} + |1, 0, 2\rangle_{A'B'C'} + |2, 0, 1\rangle_{A'B'C'} + |2, 1, 0\rangle_{A'B'C'}) \right] \\
&= \frac{1}{3\sqrt{2}} \left[2(|0, 1, 2\rangle_{A'A'A'} + |0, 1, 2\rangle_{B'B'B'} + |0, 1, 2\rangle_{C'C'C'}) - |0, 1, 2\rangle_{A'B'C'} - |0, 2, 1\rangle_{A'B'C'} \right. \\
&\quad \left. - |1, 2, 0\rangle_{A'B'C'} - |1, 0, 2\rangle_{A'B'C'} - |2, 0, 1\rangle_{A'B'C'} - |2, 1, 0\rangle_{A'B'C'} \right], \quad (47) \\
|\Phi_{(1,0)}^3\rangle_{ABC} &\xrightarrow{\text{tritter}} \frac{\omega_3^2 - \omega_3}{\sqrt{6}} (|0, 1, 2\rangle_{A'B'C'} - |0, 2, 1\rangle_{A'B'C'} + |1, 2, 0\rangle_{A'B'C'} - |1, 0, 2\rangle_{A'B'C'} \\
&\quad + |2, 0, 1\rangle_{A'B'C'} - |2, 1, 0\rangle_{A'B'C'}). \quad (48)
\end{aligned}$$

As shown in the above equations, the rest terms, denoted as \dots in Eqs. (41–46), are canceled with the definitions, $\omega_3^2 + \omega_3 + 1 = 0$ and $\omega_3^3 = 1$. From the equations, we can obtain the detector click events and their probabilities written in Eqs. (7) and (8).

The other detector click events of the quantum states exploited in the protocol are described in the following equation:

$$|\Phi_{(0,1)}^3\rangle, |\Phi_{(0,2)}^3\rangle, |\Phi_{(1,1)}^3\rangle, |\Phi_{(1,2)}^3\rangle \rightarrow \left\{ \begin{array}{ll} D_{A'0}, D_{A'2}, D_{B'1} & \text{with probability } 1/18 \\ D_{A'0}, D_{A'1}, D_{C'2} & \text{with probability } 1/18 \\ D_{A'0}, D_{A'2}, D_{B'1} & \text{with probability } 1/18 \\ D_{A'0}, D_{A'2}, D_{C'1} & \text{with probability } 1/18 \\ D_{A'0}, D_{B'1}, D_{B'2} & \text{with probability } 1/18 \\ D_{A'0}, D_{C'1}, D_{C'2} & \text{with probability } 1/18 \\ D_{A'1}, D_{A'2}, D_{B'0} & \text{with probability } 1/18 \\ D_{A'1}, D_{A'2}, D_{C'0} & \text{with probability } 1/18 \\ D_{A'1}, D_{B'0}, D_{B'2} & \text{with probability } 1/18 \\ D_{A'1}, D_{C'0}, D_{C'2} & \text{with probability } 1/18 \\ D_{A'2}, D_{B'0}, D_{B'1} & \text{with probability } 1/18 \\ D_{A'2}, D_{C'0}, D_{C'1} & \text{with probability } 1/18 \\ D_{B'0}, D_{B'1}, D_{C'2} & \text{with probability } 1/18 \\ D_{B'1}, D_{B'2}, D_{C'1} & \text{with probability } 1/18 \\ D_{B'0}, D_{C'1}, D_{C'2} & \text{with probability } 1/18 \\ D_{B'1}, D_{B'2}, D_{C'0} & \text{with probability } 1/18 \\ D_{B'1}, D_{C'0}, D_{C'2} & \text{with probability } 1/18 \\ D_{B'2}, D_{C'0}, D_{C'1} & \text{with probability } 1/18 \end{array} \right. \quad (49)$$

where D_{Xy} denotes a click event of the detector corresponding to the state $|y\rangle$, the photon exists in the output port X , and the fractional numbers denote the probability of the click events. The click events of $|\Phi_{(0,0)}^3\rangle$ and $|\Phi_{(1,0)}^3\rangle$ are described in the maintext.

Even if photon number resolving detectors are involved, the other states cannot be discriminated. An example is described in the following equation:

$$|\Phi_{(2,0)}^3\rangle, |\Phi_{(2,1)}^3\rangle, |\Phi_{(2,2)}^3\rangle, |\Phi_{(3,0)}^3\rangle, |\Phi_{(3,1)}^3\rangle, |\Phi_{(3,2)}^3\rangle \rightarrow \begin{cases} D_{A'2}, D_{B'0}^2 \\ D_{B'0}^2, D_{B'2}^2 \\ D_{B'0}, D_{B'1}^2 \\ \vdots \end{cases}, \quad (50)$$

where the superscripts 2 in the right-hand side mean that two photons enter the detector. In conclusion, only $|\Phi_{(0,0)}^3\rangle$ is exactly discriminated by using the three-dimensional correlation measurement.

Calculations for a secret key rate of 3d-CQSS

Main results

In this section, calculation details of the secret key rate written in Eq. (37) are described. To calculate the secret key rate, it is necessary to obtain the mutual information and the Holevo information written in Eq. (18). The mutual information can be obtained from the following equation:

$$I(A, 3 - B_1 - B_2) = H(A) + H(3 - B_1 - B_2) - H(A, 3 - B_1 - B_2), \quad (51)$$

where (mod 3) is omitted in the all brackets, A , B_1 , and B_2 are encoded information of Alice, Bob₁, and Bob₂, respectively, $H(x)$ is the Shannon entropy, and $H(x, y)$ is the joint entropy. The entropies can be evaluated by using the tripartite quantum state written in Eq. (17) and they are shown in Eqs. (52–54):

$$H(A) = \log 3, \quad (52)$$

$$H(3 - B_1 - B_2) = \log 3, \quad (53)$$

$$H(A, 3 - B_1 - B_2) = \log 3 - \sum_{i=0}^2 \Lambda_i \log \Lambda_i, \quad (54)$$

where

$$\Lambda_i = \sum_{\sigma=0}^2 [\lambda_{(2i,\sigma)} + \lambda_{(2i+1,\sigma)} + \lambda_{(6+i,\sigma)}], \quad (55)$$

and the base 2 of all the logarithms is omitted.

The definition of the Holevo information is given as

$$\chi(A; E) = S(\hat{\rho}_{AE}) - \sum_{a=0}^2 p(a) S(\hat{\rho}_{E|A=a}),$$

where $S(\hat{\rho})$ is the von Neumann entropy. The Holevo information means that the maximum information that Eve can obtain through the quantum state. Since Alice will encrypt a classical secret by using her encoded information, a , Eve's attack strategy is obtaining the maximum information about Alice's encoded number. The reduced density matrix between Alice and Eve is obtained by tracing out Bob₁'s and Bob₂'s systems from the full quantum state written in Eq. (16). Eve's conditional density matrix, $\hat{\rho}_{E|A=a}$, can be obtained by performing projection of Alice's system onto $|a\rangle\langle a|$. Then the two terms in the Holevo information can be calculated as shown in Eq. (56) and Eq. (57):

$$S(\hat{\rho}_{AE}) = - \sum_{j=0}^8 \sum_{\sigma=0}^2 \lambda_{(j,\sigma)} \log \lambda_{(j,\sigma)}, \quad (56)$$

$$\sum_{a=0}^2 p(a) S(\hat{\rho}_{E|A=a}) = - \sum_{j=0}^8 \left[\left(\sum_{\sigma=0}^2 \lambda_{(j,\sigma)} \right) \log \left(\sum_{\sigma=0}^2 \lambda_{(j,\sigma)} \right) \right]. \quad (57)$$

From the equations, the secret key rate is obtained as shown in Eq. (58):

$$r = \log 3 + \sum_{j=0}^8 \sum_{\sigma=0}^2 (\lambda_{(j,\sigma)} \log \lambda_{(j,\sigma)}) - \sum_{j=0}^8 \left[\left(\sum_{\sigma=0}^2 \lambda_{(j,\sigma)} \right) \log \left(\sum_{\sigma=0}^2 \lambda_{(j,\sigma)} \right) \right] + \sum_{i=0}^2 \Lambda_i \log \Lambda_i. \quad (58)$$

When the depolarized state written in Eq. (23) is considered, the secret key rate becomes the equation shown in Eq. (59):

$$\begin{aligned}
 r = & (\langle \text{spanclass} = 'convertEndash' \rangle 1 - 3 \langle /span \rangle \lambda_+ - 3\lambda_-) \log 3 \\
 & + \left[\left(\sum_{\sigma=0}^2 \lambda_{(0,\sigma)} \right) + 3\lambda_+ + 3\lambda_- \right] \log \left[\left(\sum_{\sigma=0}^2 \lambda_{(0,\sigma)} \right) + 3\lambda_+ + 3\lambda_- \right] \\
 & + \sum_{\sigma=0}^2 (\lambda_{(0,\sigma)} \log \lambda_{(0,\sigma)}) - \left(\sum_{\sigma=0}^2 \lambda_{(0,\sigma)} \right) \log \left(\sum_{\sigma=0}^2 \lambda_{(0,\sigma)} \right) + 6(\lambda_+ + \lambda_- + \lambda_-) \log (\lambda_+ + \lambda_- + \lambda_-).
 \end{aligned} \quad (59)$$

Finally, the secret key rate becomes the form described in Eq. (37) by substituting the λ s to the error rates defined in Eqs. (27–30).

$$\begin{aligned}
 r = & (1 - 3Q_u - 3Q_{\pm}) \log 3 - (Q_{\omega} + Q_s - 2Q_{\pm} - 3Q_u) \\
 & + (1 - Q_{\omega} - Q_s - Q_{\pm}) \log(1 - Q_{\omega} - Q_s - Q_{\pm}) + 3(Q_s - Q_u) \log(Q_s - Q_u) \\
 & + (Q_{\omega} - 2Q_s - 2Q_{\pm}) \log(Q_{\omega} - 2Q_s - 2Q_{\pm}) - (1 - 3Q_s - 3Q_{\pm}) \log(1 - 3Q_s - 3Q_{\pm}).
 \end{aligned} \quad (60)$$

Error parameters

Here, we describe how the error rates written in Eqs. (27–30) can be calculated in the 3d-CQSS protocol. First, Q_p is the most simple error rate to calculate. As it is shown in Eq. (28), the 3d-phase error rate is a sum of the probabilities of the tripartite quantum states which have ω and ω^2 phases. The 3d-phase error rate can be calculated from the statistics of the bar basis, since $\bar{a} + \bar{b} + \bar{c} = 0 \pmod{3}$ is satisfied only when there are no ω and ω^2 phases in the state. Therefore, the 3d-phase error rate can be calculated as shown in Eq. (61):

$$p(\bar{a} + \bar{b}_1 + \bar{b}_2 \neq 0) = \sum_{\sigma=1}^2 \sum_{j=0}^8 \lambda_{(j,\sigma)} = \lambda_{(0,1)} + \lambda_{(0,2)} + 6\lambda_+ + 4\lambda_- + 6\lambda_- = Q_{\omega}, \quad (61)$$

where $p(x)$ is defined as (the number of signals that x is true)/(the number of sifted signals of which bases including x are used), and $\pmod{3}$ is omitted in the bracket in the left-hand side of the equation.

The state error rate is defined as a sum of the probabilities of the states $|\Phi_j^0\rangle$, where $j \in \{0, 1, 2, \dots, 8\}$ as shown in Eq. (27). To evaluate the state error rate written in Eq. (27), we use the equations shown in Eq. (62):

$$\begin{aligned}
 p(a + b_1 + b_2 \neq 0 \ \& \ b_1 \neq b_2) = \sum_{\sigma=0}^2 \sum_{j=2}^5 \lambda_{(j,\sigma)} = 6\lambda_+ + 6\lambda_-, \\
 p(a + b_1 + b_2 = 0 \ \& \ b_1 \neq b_2) = \sum_{\sigma=0}^2 (\lambda_{(0,\sigma)} + \lambda_{(1,\sigma)}) = \left(\sum_{\sigma=0}^2 \lambda_{(0,\sigma)} \right) + 3\lambda_+,
 \end{aligned} \quad (62)$$

and an expectation value of the operator \hat{X} , which is defined in Eq. (35). The expectation value of one party, for example Alice's, can be obtained from the following equation:

$$\langle \hat{X} \rangle_A = p(a = 0) + \omega p(a = 1) + \omega^2 p(a = 2).$$

By using the depolarized state in Eq. (23), we can obtain the value shown in Eq. (63):

$$\langle \hat{X} \hat{X} \hat{X} \rangle + \text{c.c.} = \sum_{j=0}^8 (2\lambda_{(j,0)} - \lambda_{(j,1)} - \lambda_{(j,2)}) = 2\lambda_{(0,0)} - \lambda_{(0,1)} - \lambda_{(0,2)}. \quad (63)$$

Then the state error rate can be obtained by using the probabilities described in Eqs. (62) and (63) as shown in Eq. (64):

$$\begin{aligned}
 Q_s = & 2\lambda_+ + 2\lambda_- + 3\lambda_- \\
 = & p(a + b_1 + b_2 \neq 0 \ \& \ b_1 \neq b_2) - p(\bar{a} + \bar{b}_1 + \bar{b}_2 \neq 0) + \frac{1}{3} [2p(a + b_1 + b_2 = 0 \ \& \ b_1 \neq b_2) - (\langle \hat{X} \hat{X} \hat{X} \rangle + \text{c.c.})].
 \end{aligned} \quad (64)$$

The user error rate is easily obtained when the depolarized state is considered as shown in Eq. (30) and Eq. (34), but the 2d-phase error rate is difficult to be exactly evaluated. Therefore, the error rate is approximated by using the probability shown in Eq. (65):

$$p(\bar{a} = \bar{b}_1 = \bar{b}_2 \mid \bar{a} + \bar{b}_1 + \bar{b}_2 = 0). \quad (65)$$

This probability is 1/2 for the states $\{|\Phi_{(2j,0)}^3\rangle\}$, zero for the states $\{|\Phi_{(2j+1,0)}^3\rangle\}$, and 1/3 for the states $\{|\Phi_{(6+j,0)}^3\rangle\}$, where $j \in \{0, 1, 2\}$. From these probabilities, we define the 2d-phase error rate as Eq. (34) of which value is zero for the ideal state, $|\Phi_{(0,0)}^3\rangle$, and one for the state $|\Phi_{(1,0)}^3\rangle$. The 2d-phase error rate is not always the same as $\lambda_{(1,0)}$, since the probability is affected by other states as well.

Secret key rate with experimental factors

Here, the secret key rate is evaluated by using the experimental factors, transmission loss, η , and a dark count of single photon detectors, μ . The situation is the ideal case, where there is no Eve, and there is no state error. In the 3d-CQSS protocol, there are nine single photon detectors and three photons propagate through quantum channels. A success probability of the 3d-CQSS protocol, $p_{3\text{MDI}}(x, y, z)$, is defined as the probability that when Alice, Bob₁, and Bob₂ send the quantum states, $|x\rangle$, $|y\rangle$, and $|z\rangle$ to Charlie, respectively, the result of the three-dimensional correlation measurement is $|\Phi_{(0,0)}^3\rangle$. Then the success probability can be calculated from the experimental factors as shown in Eq. (66):

$$p_{3\text{CM}}(a, b_1, b_2) = (1 - \mu)^6(1 - \eta)^3 + 3(1 - \mu)^6\mu(1 - \eta)^2\eta + 3(1 - \mu)^6\mu^2(1 - \eta)\eta^2 + 3(1 - \mu)^6\mu^3\eta^3, \quad (66)$$

when $a + b_1 + b_2 = 0 \pmod{3}$ and $a \neq b_1 \neq b_2 \neq a$ are satisfied. The subscript 3CM denotes the three-dimensional correlation measurement based protocol. The first term means the three photons sent from the authorized parties arrive at the measurement setup successfully, and there is no dark count. The second term is the case that one photon is lost, and the others arrive, but it is considered to be a successful trial, since one detector is clicked due to the dark count. The coefficient 3 comes from the number of possibilities that one photon is lost among the three photons. The success probability when two photons and when all the photons are lost are described in the third term and the final term, respectively. The coefficient 3 of the final term comes from the fact that there are three different click combinations considered for the successful trial, as shown in Eq. (7).

The case is considered when $a + b_1 + b_2 = 0 \pmod{3}$ and $a \neq b_1 \neq b_2 \neq a$ are not satisfied. If $a = b_1 = b_2$ is true, the success probability becomes as shown in Eq. (67):

$$p_{3\text{CM}}(a, b_1, b_2) = 3(1 - \mu)^6\mu^2(1 - \eta)\eta^2 + 3(1 - \mu)^6\mu^3\eta^3. \quad (67)$$

In this case, at least two photons should be lost, and two detectors are clicked due to the dark count for a successful trial. Therefore, the success probability has only two terms which are the cases that two photons are lost, and all the photons are lost.

If two photons have the same OAM mode, then the success probability can be obtained from Eq. (68):

$$p_{3\text{CM}}(a, b_1, b_2) = (1 - \mu)^6\mu(1 - \eta)^2\eta + 3(1 - \mu)^6\mu^2(1 - \eta)\eta^2 + 3(1 - \mu)^6\mu^3\eta^3. \quad (68)$$

By using the equations, Eqs. (66–68), the error rates can be calculated as an example is shown in Eq. (69):

$$Q_\omega = \frac{\sum_{\bar{a}+\bar{b}_1+\bar{b}_2 \neq 0} p_{3\text{CM}}(\bar{a}, \bar{b}_1, \bar{b}_2)}{\sum_{\bar{a}, \bar{b}_1, \bar{b}_2=0}^2 p_{3\text{CM}}(\bar{a}, \bar{b}_1, \bar{b}_2)}, \quad (69)$$

where $\pmod{3}$ is omitted.

For the entanglement-based 3d-CQSS protocol, the probabilities are changed. Assume that each party has three SPDs to discriminate three different OAM modes. The $p_{3\text{E}}(a, b_1, b_2)$ is defined as a probability that Alice's a detector, Bob₁'s b_1 detector, and Bob₂'s b_2 detector are clicked, and an entangled state generator produces the $|\Phi_{(0,0)}^3\rangle$ state. When $a + b_1 + b_2 = 0 \pmod{3}$ and $a \neq b_1 \neq b_2 \neq a$, the probability becomes as shown in Eq. (70):

$$p_{3\text{E}}(a, b_1, b_2) = (1 - \mu)^6(1 - \eta)^3 + 3(1 - \mu)^6\mu(1 - \eta)^2\eta + 6(1 - \mu)^6\mu^2(1 - \eta)\eta^2 + 12(1 - \mu)^6\mu^3\eta^3, \quad (70)$$

where the subscript 3E denotes three-dimensional entanglement-based protocol. As in Eq. (66), n -th term is defined as the probability that $(n - 1)$ photons are lost, but the measured values of Alice, Bob₁, and Bob₂ are a , b_1 , and b_2 , respectively, due to the dark count. The first term and the second term are the same with those of Eq. (66), but there are differences in the third term and the fourth term. In the correlation measurement based 3d-CQSS protocol, if one photon arrives at the corresponding detector, the other two detectors for the successful trial is determined as shown in Eq. (7). The other detector click events are not considered, since they are discarded in the correlation-measurement based 3d-CQSS protocol. However, in the entanglement-based 3d-CQSS protocol, if one photon arrives at the detector of one party, there are only two different cases for a successful trial. If Alice's detector D_0 is clicked by an arriving photon, the successful trial can occur when Bob₁'s D_1 and Bob₂'s D_2 are clicked, or when Bob₁'s D_2 and Bob₂'s D_1 are clicked. Therefore, the coefficient of the third term and that of the fourth term are different from Eq. (66), and this difference enlarges the error rates of the entanglement-based 3d-CQSS protocol.

The probability can be calculated when OAM value of all the authorized parties is the same, $a = b_1 = b_2$, as shown in Eq. (71):

$$p_{3\text{E}}(a, b_1, b_2) = 6(1 - \mu)^6\mu^2(1 - \eta)\eta^2 + 3(1 - \mu)^6\mu^3\eta^3. \quad (71)$$

The probability of two of the parties having the same results of the OAM mode detection is written in Eq. (72):

$$p_{3\text{E}}(a, b_1, b_2) = 6(1 - \mu)^6\mu(1 - \eta)^2\eta + 4(1 - \mu)^6\mu^2(1 - \eta)\eta^2 + 12(1 - \mu)^6\mu^3\eta^3. \quad (72)$$

By using the probabilities, the error rates can be calculated with Eq. (69), as well. Since the coefficient of the terms in Eq. (71) and Eq. (72) is greater than those in Eq. (67) and Eq. (68), the error rates of an entanglement-based 3d-CQSS protocol are greater than those of the correlation measurement based 3d-CQSS protocol.

Data availability

The datasets generated and/or analyzed during the current study are not publicly available due to the security policy of the Ministry of National Defense of South Korea, but are available from the corresponding author upon reasonable request.

Received: 25 March 2025; Accepted: 30 May 2025

Published online: 05 June 2025

References

- Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, 175 (IEEE, India, 1984).
- Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, 661–663 (1991).
- Childs, A. M. Secure assisted quantum computation. *Quantum Info. Comput.* **5**, 456–466 (2005).
- Arrighi, P. & Salvail, L. Blind quantum computation. *Int. J. of Quantum Inf.* **04**, 883–898. <https://doi.org/10.1142/S0219749906002171> (2006).
- Broadbent, A., Fitzsimons, J. & Kashefi, E. Universal blind quantum computation. In *2009 50th Annual IEEE Symposium on Foundations of Computer Science*, 517–526 (2009).
- Malik, M., Magaña-Loaiza, O. S. & Boyd, R. W. Quantum-secured imaging. *Appl. Phys. Lett.* **101**, 241103. <https://doi.org/10.1063/1.4770298> (2012).
- Heo, J. et al. Quantum-secured single-pixel imaging with enhanced security. *Optica* **10**, 1461–1470. <https://doi.org/10.1364/OPTICA.494050> (2023).
- Heo, J., Jeong, T., Park, N. H. & Jo, Y. True image construction in quantum-secured single-pixel imaging under spoofing attack. *APL Photonics* **9**, 076111. <https://doi.org/10.1063/5.0209041> (2024).
- Wootters, W. K. & Zurek, W. H. A single quantum cannot be cloned. *Nature* **299**, 802–803 (1982).
- Bell, J. S. On the Einstein Podolsky Rosen paradox. *Physics* **1**, 195–200 (1964).
- Shamir, A. How to share a secret. *Commun. ACM* **22**, 612–613 (1979).
- Blakley, G. R. Safeguarding cryptographic keys. In *Managing Requirements Knowledge, International Workshop on (AFIPS)*, 313 (1899).
- Greenberger, D. M., Horne, M. A., Shimony, A. & Zeilinger, A. Bell's theorem without inequalities. *Am. J. Phys.* **58**, 1131–1143 (1990).
- Gottesman, D. Theory of quantum secret sharing. *Phys. Rev. A* **61**, 042311 (2000).
- Scarani, V. & Gisin, N. Quantum communication between N partners and Bell's inequalities. *Phys. Rev. Lett.* **87**, 117901 (2001).
- Xiao, L., Lu Long, G., Deng, F.-G. & Pan, J.-W. Efficient multiparty quantum-secret-sharing schemes. *Phys. Rev. A* **69**, 052307 (2004).
- Qin, S.-J., Gao, F., Wen, Q.-Y. & Zhu, F.-C. Cryptanalysis of the Hillery-Bužek-Berthiaume quantum secret-sharing protocol. *Phys. Rev. A* **76**, 062324 (2007).
- Tittel, W., Zbinden, H. & Gisin, N. Experimental demonstration of quantum secret sharing. *Phys. Rev. A* **63**, 042301 (2001).
- Lance, A. M., Symul, T., Bowen, W. P., Sanders, B. C. & Lam, P. K. Tripartite quantum state sharing. *Phys. Rev. Lett.* **92**, 177903 (2004).
- Chen, Y.-A. et al. Experimental quantum secret sharing and third-man quantum cryptography. *Phys. Rev. Lett.* **95**, 200502 (2005).
- Gaertner, S., Kurtsiefer, C., Bourennane, M. & Weinfurter, H. Experimental demonstration of four-party quantum secret sharing. *Phys. Rev. Lett.* **98**, 020503 (2007).
- Bell, B. A. et al. Experimental demonstration of graph-state quantum secret sharing. *Nat. Commun.* **5**, 5480 (2014).
- Lu, H. et al. Secret sharing of a quantum state. *Phys. Rev. Lett.* **117**, 030501 (2016).
- Fu, Y., Yin, H.-L., Chen, T.-Y. & Chen, Z.-B. Long-distance measurement-device-independent multiparty quantum communication. *Phys. Rev. Lett.* **114**, 090501. <https://doi.org/10.1103/PhysRevLett.114.090501> (2015).
- Kim, W.-J., Cha, S.-H., Lee, S.-W. & Lee, J. Quantum secret sharing by high-dimensional systems. *J. Korean Phys. Soc.* **48**, 1218–1223 (2006).
- Keet, A., Fortescue, B., Markham, D. & Sanders, B. C. Quantum secret sharing with qudit graph states. *Phys. Rev. A* **82**, 062315 (2010).
- Tang, D., Wang, T.-J., Mi, S., Geng, X.-M. & Wang, C. High-dimensional circular quantum secret sharing using orbital angular momentum. *Int. J. Theor. Phys.* **55**, 4963–4971 (2016).
- Song, X.-L., Liu, Y.-B., Deng, H.-Y. & Xiao, Y.-G. (t, n) threshold d-level quantum secret sharing. *Sci. Rep.* **7**, 6366 (2017).
- de Oliveira, M., Nape, I., Pinnell, J., TabeBordbar, N. & Forbes, A. Experimental high-dimensional quantum secret sharing with spin-orbit-structured photons. *Phys. Rev. A* **101**, 042303. <https://doi.org/10.1103/PhysRevA.101.042303> (2020).
- Cerf, N. J., Bourennane, M., Karlsson, A. & Gisin, N. Security of quantum key distribution using d-level systems. *Phys. Rev. Lett.* **88**, (2002).
- Durt, T., Kaszlikowski, D., Chen, J.-L. & Kwek, L. C. Security of quantum key distributions with entangled qudits. *Phys. Rev. A* **69**, 032313 (2004).
- Bruß, D. & Macchiavello, C. Optimal state estimation for d -dimensional quantum systems. *Phys. Lett. A* **253**, 249–251 (1999).
- Bouchard, F., Fickler, R., Boyd, R. W. & Karimi, E. High-dimensional quantum cloning and applications to quantum hacking. *Sci. Adv.* **3** (2017).
- Erhard, M., Malik, M., Krenn, M. & Zeilinger, A. Experimental Greenberger-Horne-Zeilinger entanglement beyond qubits. *Nat. Photon.* **12**, 759–764 (2018).
- Fu, Y., Yin, H.-L., Chen, T.-Y. & Chen, Z.-B. Long-distance measurement-device-independent multiparty quantum communication. *Phys. Rev. Lett.* **114**, 090501 (2015).
- Zhang, C. et al. Memory-assisted measurement-device-independent quantum secret sharing. *Phys. Rev. A* **111**, 012602. <https://doi.org/10.1103/PhysRevA.111.012602> (2025).
- Lütkenhaus, N., Calsamiglia, J. & Suominen, K.-A. Bell measurements for teleportation. *Phys. Rev. A* **59**, 3295–3300 (1999).
- Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).
- Jo, Y. & Son, W. Key-rate enhancement using qutrit states for quantum key distribution with askew aligned sources. *Phys. Rev. A* **94**, 052316 (2016).
- Hwang, W.-Y., Su, H.-Y. & Bae, J. N-dimensional measurement-device-independent quantum key distribution with $N + 1$ uncharacterized sources: zero quantum-bit-error-rate case. *Sci. Rep.* **6**, 30036 (2016).

41. Jo, Y., Bae, K. & Son, W. Enhanced Bell state measurement for efficient measurement-device-independent quantum key distribution using 3-dimensional quantum states. *Sci. Rep.* **9**, 687 (2019).
42. Dellantonio, L., Sørensen, A. S. & Bacco, D. High-dimensional measurement-device-independent quantum key distribution on two-dimensional subspaces. *Phys. Rev. A* **98**, 062301 (2018).
43. Calsamiglia, J. Generalized measurements by linear elements. *Phys. Rev. A* **65**, 030301 (2002).
44. Goyal, S. K., Boukama-Dzoussi, P. E., Ghosh, S., Roux, F. S. & Konrad, T. Qudit-teleportation for photons with linear optics. *Sci. Rep.* **4**, 4543 (2014).
45. Reck, M., Zeilinger, A., Bernstein, H. J. & Bertani, P. Experimental realization of any discrete unitary operator. *Phys. Rev. Lett.* **73**, 58–61 (1994).
46. Clements, W. R., Humphreys, P. C., Metcalf, B. J., Kolthammer, W. S. & Walmsley, I. A. Optimal design for universal multiport interferometers. *Optica* **3**, 1460–1465. <https://doi.org/10.1364/OPTICA.3.001460> (2016).
47. Luo, Y.-H. et al. Quantum teleportation in high dimensions. *Phys. Rev. Lett.* **123**, 070505. <https://doi.org/10.1103/PhysRevLett.123.070505> (2019).
48. Hu, X.-M. et al. Experimental high-dimensional quantum teleportation. *Phys. Rev. Lett.* **125**, 230501. <https://doi.org/10.1103/PhysRevLett.125.230501> (2020).
49. Wang, J., Chen, S. & Liu, J. Orbital angular momentum communications based on standard multi-mode fiber (invited paper). *APL Photon.* **6**, 060804. <https://doi.org/10.1063/5.0049022> (2021) https://pubs.aip.org/aip/app/article-pdf/doi/10.1063/5.0049022/14571621/060804_1_online.pdf.
50. Yao, A. M. & Padgett, M. J. Orbital angular momentum: origins, behavior and applications. *Adv. Opt. Photon.* **3**, 161–204. <https://doi.org/10.1364/AOP.3.000161> (2011).
51. Fickler, R. et al. Quantum entanglement of high angular momenta. *Science* **338**, 640–643. <https://doi.org/10.1126/science.1227193> (2012) <https://www.science.org/doi/pdf/10.1126/science.1227193>.
52. Vallone, G. et al. Free-space quantum key distribution by rotation-invariant twisted photons. *Phys. Rev. Lett.* **113**, 060503. <https://doi.org/10.1103/PhysRevLett.113.060503> (2014).
53. Mirhosseini, M. et al. High-dimensional quantum cryptography with twisted light. *New J. Phys.* **17**, 033033 (2015).
54. Islam, N. T., Lim, C. C. W., Cahall, C., Kim, J. & Gauthier, D. J. Provably secure and high-rate quantum key distribution with time-bin qudits. *Sci. Adv.* **3**, e1701491. <https://doi.org/10.1126/sciadv.1701491> (2017) <https://www.science.org/doi/pdf/10.1126/sciadv.1701491>.
55. Vagniluca, I. et al. Efficient time-bin encoding for practical high-dimensional quantum key distribution. *Phys. Rev. Appl.* **14**, 014051. <https://doi.org/10.1103/PhysRevApplied.14.014051> (2020).
56. Zhao, J. et al. Performance analysis of d -dimensional quantum cryptography under state-dependent diffraction. *Phys. Rev. A* **100**, 032319. <https://doi.org/10.1103/PhysRevA.100.032319> (2019).
57. Paterson, C. Atmospheric turbulence and orbital angular momentum of single photons for optical communication. *Phys. Rev. Lett.* **94**, 153901. <https://doi.org/10.1103/PhysRevLett.94.153901> (2005).
58. Zhao, T. et al. High-dimensional quantum key distribution with focused structured photons. *Opt. Express* **33**, 20258–20271. <https://doi.org/10.1364/OE.558986> (2025).
59. Zhou, Y. et al. Multiprobe time reversal for high-fidelity vortex-mode-division multiplexing over a turbulent free-space link. *Phys. Rev. Appl.* **15**, 034011. <https://doi.org/10.1103/PhysRevApplied.15.034011> (2021).
60. Żukowski, M., Zeilinger, A. & Horne, M. A. Realizable higher-dimensional two-particle entanglements via multiport beam splitters. *Phys. Rev. A* **55**, 2564–2579 (1997).
61. Tan, S.-H. & Rohde, P. P. The resurgence of the linear optics quantum interferometer - recent advances & applications. *Reviews in Physics* **4**, 100030. <https://doi.org/10.1016/j.revip.2019.100030> (2019).
62. Leach, J., Padgett, M. J., Barnett, S. M., Franke-Arnold, S. & Courtial, J. Measuring the orbital angular momentum of a single photon. *Phys. Rev. Lett.* **88**, 257901 (2002).
63. Lavery, M. P. J. et al. Refractive elements for the measurement of the orbital angular momentum of a single photon. *Opt. Express* **20**, 2110–2115 (2012).
64. Lavery, M. P. J. et al. Efficient measurement of an optical orbital-angular-momentum spectrum comprising more than 50 states. *New J. Phys.* **15**, 013024 (2013).
65. Mirhosseini, M., Malik, M., Shi, Z. & Boyd, R. W. Efficient separation of the orbital angular momentum eigenstates of light. *Nat. Commun.* **4**, 1–6 (2013).
66. Fontaine, N. K. et al. Laguerre-gaussian mode sorter. *Nat. Commun.* **10**, 1865. <https://doi.org/10.1038/s41467-019-09840-4> (2019).
67. Bouchard, F. et al. Measuring azimuthal and radial modes of photons. *Opt. Express* **26**, 31925–31941 (2018).
68. Cabello, A. n -particle n -level singlet states: Some properties and applications. *Phys. Rev. Lett.* **89**, 100402. <https://doi.org/10.1103/PhysRevLett.89.100402> (2002).
69. Mayers, D. Unconditional security in quantum cryptography. *J. ACM* **48**, 351–406 (2001).
70. Shor, P. W. & Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **85**, 441–444 (2000).
71. Devetak, I. & Winter, A. Distillation of secret key and entanglement from quantum states. *Proc. R. Soc. A Math. Phys. Eng. Sci.* **461**, 207–235 (2005).
72. Kogias, I., Xiang, Y., He, Q. & Adesso, G. Unconditional security of entanglement-based continuous-variable quantum secret sharing. *Phys. Rev. A* **95**, 012315. <https://doi.org/10.1103/PhysRevA.95.012315> (2017).
73. Choi, M., Lee, Y. & Lee, S. Quantum secret sharing and Mermin operator. *Quantum Inf. Process.* **17**, 258 (2018).
74. Zhang, Q. et al. Device-independent quantum secret sharing with noise preprocessing and postselection. *Phys. Rev. A* **110**, 042403. <https://doi.org/10.1103/PhysRevA.110.042403> (2024).
75. Epping, M., Kampermann, H., Macchiavello, C. & Bruß, D. Multi-partite entanglement can speed up quantum key distribution in networks. *New J. Phys.* **19**, 093012 (2017).
76. Jo, Y. & Son, W. Semi-device-independent multiparty quantum key distribution in the asymptotic limit. *OSA Continuum* **2**, 814–826 (2019).
77. Holevo, A. S. Bounds for the quantity of information transmitted by a quantum communication channel. *Problems Inform. Transmission* **9**, 177–183 (1973).
78. Dür, W. & Cirac, J. I. Classification of multiqubit mixed states: Separability and distillability properties. *Phys. Rev. A* **61**, 042314 (2000).
79. Ferenczi, A. & Lütkenhaus, N. Symmetries in quantum key distribution and the connection between optimal attacks and optimal cloning. *Phys. Rev. A* **85**, 052310 (2012).
80. Qin, Y. et al. Efficient and secure quantum secret sharing for eight users. *Phys. Rev. Res.* **6**, 033036. <https://doi.org/10.1103/PhysRevResearch.6.033036> (2024).
81. Scarani, V. et al. The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301–1350. <https://doi.org/10.1103/RevModPhys.81.1301> (2009).
82. Tomamichel, M., Lim, C. C. W., Gisin, N. & Renner, R. Tight finite-key analysis for quantum cryptography. *Nat. Commun.* **3**, 634. <https://doi.org/10.1038/ncomms1631> (2012).
83. Tavakoli, A., Herbauts, I., Żukowski, M. & Bourennane, M. Secret sharing with a single d -level quantum system. *Phys. Rev. A* **92**, 030302 (2015).

84. Nunn, J. et al. Large-alphabet time-frequency entangled quantum key distribution by means of time-to-frequency conversion. *Opt. Express* **21**, 15959–15973 (2013).
85. Jo, Y., Park, H. S., Lee, S.-W. & Son, W. Efficient high-dimensional quantum key distribution with hybrid encoding. *Entropy* **21**, 80 (2019).
86. Lo, H.-K., Curty, M. & Tamaki, K. *Secure quantum key distribution*. *Nat. Photon.* **8**, 595–604 (2014).
87. Sheridan, L., Le, T. P. & Scarani, V. Finite-key security against coherent attacks in quantum key distribution. *New J. Phys.* **12**, 123019. <https://doi.org/10.1088/1367-2630/12/12/123019> (2010).
88. Bunandar, D., Govia, L. C. G., Krovi, H. & Englund, D. Numerical finite-key analysis of quantum key distribution. *Npj Quantum Information* **6**, 104. <https://doi.org/10.1038/s41534-020-00322-w> (2020).
89. George, I., Lin, J. & Lütkenhaus, N. Numerical calculations of the finite key rate for general quantum key distribution protocols. *Phys. Rev. Res.* **3**, 013274. <https://doi.org/10.1103/PhysRevResearch.3.013274> (2021).
90. Fröhlich, B. et al. Long-distance quantum key distribution secure against coherent attacks. *Optica* **4**, 163–167. <https://doi.org/10.1364/OPTICA.4.000163> (2017).
91. Wang, Y.-Z., Sun, X.-R., Cao, X.-Y., Yin, H.-L. & Chen, Z.-B. Experimental coherent-state quantum secret sharing with finite pulses. *Phys. Rev. Appl.* **22**, 044018. <https://doi.org/10.1103/PhysRevApplied.22.044018> (2024).
92. Acín, A. et al. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.* **98**, 230501 (2007).
93. Roy, S. & Mukhopadhyay, S. Device-independent quantum secret sharing in arbitrary even dimensions. *Phys. Rev. A* **100**, 012319. <https://doi.org/10.1103/PhysRevA.100.012319> (2019).
94. Moreno, M. G. M., Brito, S., Nery, R. V. & Chaves, R. Device-independent secret sharing and a stronger form of bell nonlocality. *Phys. Rev. A* **101**, 052339. <https://doi.org/10.1103/PhysRevA.101.052339> (2020).
95. Zhang, Q. et al. Device-independent quantum secret sharing with advanced random key generation basis. *Phys. Rev. A* **111**, 012603. <https://doi.org/10.1103/PhysRevA.111.012603> (2025).
96. Clauser, J. F., Horne, M. A., Shimony, A. & Holt, R. A. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.* **23**, 880–884 (1969).
97. Collins, D., Gisin, N., Linden, N., Massar, S. & Popescu, S. Bell inequalities for arbitrarily high-dimensional systems. *Phys. Rev. Lett.* **88**, 040404 (2002).
98. Masanes, L. Tight bell inequality for d-outcome measurements correlations. *Quantum Inf. Comput.* **3**, 345–358. <https://doi.org/10.26421/QIC3.4-4> (2003).
99. Kaniewski, J. et al. Maximal nonlocality from maximal entanglement and mutually unbiased bases, and self-testing of two-qutrit quantum systems. *Quantum* **3**, 198. <https://doi.org/10.22331/q-2019-10-24-198> (2019).

Acknowledgements

This work was supported by the Agency for Defense Development Grant funded by the Korean Government.

Author contributions

Y.J. initiated the project. Y.J., T.J., N.H.P., and Z.K. conducted the simulations. Y.J., T.J., D.-G.I., K.P., and Y.S.I. designed the experimental concept. Y.J. wrote the article with help of all the authors. All authors have approved the final version of the manuscript.

Declarations

Competing interests

The authors declare no conflicts of interest.

Additional information

Correspondence and requests for materials should be addressed to Y.J.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Open Access This article is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License, which permits any non-commercial use, sharing, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if you modified the licensed material. You do not have permission under this licence to share adapted material derived from this article or parts of it. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

© The Author(s) 2025