Quantum Inf Process (2013) 12:1125–1139
DOI 10.1007/s11128-012-0459-7

High-efficient quantum secret sharing based on the Chinese remainder theorem via the orbital angular momentum entanglement analysis

Ying Guo · Yuqian Zhao

Received: 18 March 2012 / Accepted: 18 July 2012 / Published online: 2 August 2012

Abstract We investigate a novel quantum secret sharing (QSS) based on the Chinese remainder theory (CRT) in multi-dimensional Hilbert space with the orbital angular momentum (OAM) entanglement analysis. The secret is divided and then allotted to two or more participants who prepare pairs of photons in the OAM-entanglement states. The initial secret can be restored jointly by legal participants via the OAM-entanglement analysis on the corresponding photons. Its security is guaranteed from the OAM entanglement of photons that are established through the spin angular momentum (SAM) entanglement analysis performed on the generated SAM-based OAM hybrid entanglement photons. It provides an alternative technique for the QSS while producing the OAM entanglement photons in the combined multi-dimensional OAM Hilbert space, where the CRT is conducted properly for sharing the conventional secret among legal participants.

Keywords Quantum secret sharing · Chinese remainder theory · OAM-entanglement · Entanglement swapping · Bell-state analysis

1 Introduction

Entanglement, a fascinating effect of multi-photon system that could prevent the secret from being eavesdropped [1,2], can be executed via the spontaneous parametric

Y. Guo · Y. Zhao (✉)
School of Information Science and Engineering, Central South University, Changsha 410083, China
e-mail: csuzhaoan@gmail.com

Y. Guo · Y. Zhao
Institute of Information and Communication, Chonbuk National University, Jeonju 561-756, Korea

down-conversion (SPDC). It attracts many attentions of scholars to the practical quantum information and quantum computing [3–5].

Entanglement swapping, one application of entanglement, has been experimentally demonstrated to transfer entanglement in the pulsed or continuous-wave source [6–8]. It plays a significant role in long-distance quantum communications while being implemented in terms of qubits encoded in polarization states [9,10]. Fortunately, for a single photon, it has at least two degrees of freedom, e.g. spin and orbital angular momentums [11]. Spin angular momentum (SAM) is associated with the polarization state that produces a qubit in two-dimensional Hilbert space [12], while orbital angular momentum (OAM) is associated with the helical phase front $e^{il\phi}$, utilizing an additional degree of freedom to allow for encoding information in qudit (state in multi-dimensional OAM Hilbert space) [13]. Currently, entanglement swapping based on the SAM or OAM entanglement has been developed in the theory or practice [12–15].

Quantum secret sharing (QSS), another application of entanglement, is known as the threshold scheme [20]. Suppose a secret is divided into p pieces such that any k of p pieces could recover it, but any sets of $k-1$ or fewer pieces fail to, which is called the (k, p)-threshold scheme. In this way, it forbids at most $k-1$ dishonest participants from restoring the secret [21–23]. For example, Hillery et al. [24] implemented an initial QSS with the Greenberger-Horne-Zeilinger (GHZ) state analysis in qubits. Zhang and Man presented the generalized multiparty QSS based on entanglement swapping with the Bell-state analysis [25]. Moreover, an experimental QSS was shown with generation of the four-photon-entangled states [26]. Bogdanski et al. [27] reported the practical QSS in telecommunication fiber for five-party implementation. Han et al. [28] illustrated an improved QSS with random phase shift operations. Markham and Sanders [29] illustrated the extended QSS with graph states. Sarvepalli et al. [30] proposed the QSS based on the Calderbank-Shor-Steane (CSS) codes. Furthermore, Sarvepalli proved the entropy inequalities [31] and calculated the bounds on the information rate of the QSS [32]. Scherpelz et al. [33] proposed a single-qubit QSS with polarization entanglement. In brief, the above-mentioned QSS can be designed on the basis of the qubits represented in two-dimensional Hilbert space with binary spin variables, i.e., the horizontal and vertical polarizations. In any case, the QSS has offered a powerful approach for sharing the secret in the multi-photon-entangled channels in polarizations. Unfortunately, the conventional processor in qubits can not always work for participants transmitting information with large capacity in the independent multi-dimensional Hilbert spaces simultaneously, and thus we are faced with a new challenge that extends to the QSS with qudits in multi-dimensional OAM Hilbert space.

In order to transmit the secret with high-rate and large-capacity in the practical QSS, it is much convenient to deploy qudits instead of pure qubits in experiments. This work has been devoted to the QSS with qudits generated by the OAM states in multi-dimensional OAM Hilbert spaces. It places a particular emphasis on the emerging technological solution leading to an application of the OAM entanglement in the QSS, where the secret is transferred without transmitting the carrier itself. After performing the SAM entanglement measurement to create the OAM entanglement, legal participants perform the OAM-entanglement analysis on the corresponding photons to restore the initial secret, which not only offers the high information-density

coding but also enhances the security of transmissions while packing much data in the twisted photons.

This paper is organized as follows. In Sect. 2, some notations and basic properties of the OAM Bell-states are presented. In Sect. 3, a simple (2, 2)-threshold QSS is perfectly generated on the basis of the OAM Bell-state analysis in the combined multi-dimensional OAM Hilbert space. In Sect. 4, we generalize the (2, 2)-threshold QSS scheme to the (p, p)-threshold one with the p-photon OAM GHZ-state analysis. After that, we investigate the coincidence rate of the OAM Bell-states as an example in the combined multi-dimensional OAM Hilbert space $\mathcal{H}$ in order to show the efficiency in Sect. 5. Finally, conclusions are drawn in Sect. 6.

2 Generations of the OAM Bell-states in multi-dimensional Hilbert space

As an ideal candidate to represent signals in multi-dimensional Hilbert space, the OAM state has drawn many attentions since it creates an opportunity for increasing the security in quantum communications.

In order to generate an OAM Bell-state, one should produce the SAM-Based OAM hybrid-entanglement states through the Pancharatnam-Berry optical phase, known as q plates [34–37]. It is a planar slab of an uniaxial birefringent medium. The orientation of its optical axis is represented in a polar coordinate, i.e., $\alpha(\phi) = q\phi + \alpha_0$, where α_0 and q are constants [38,39]. It shows that input spin polarization can reshape output orbit wavefront. As an application, Nagali et al. [36,37] performed entanglement swapping to transfer the entanglement from SAM to OAM. What we are interested in is the OAM generation in a case where only a single photon is considered with a q plate given by

$$\hat{Q}(q) = |R, l + 2q\rangle\langle L, l| + |L, l - 2q\rangle\langle R, l|, \tag{1}$$

where $|l\rangle$ is an OAM eigenstate used for encoding qudits [40,41], while $|R\rangle$ and $|L\rangle$ are two spin eigenstates, i.e., left-handed and right-handed circular polarizations. It is obvious that SAM can result in a qubit for the binary variables while OAM allows for a qudit in corresponding multi-dimensional OAM Hilbert space [16,42].

The violation of the Bell inequality has been demonstrated in two-photon multi-dimensional OAM Hilbert space [16], where an OAM Bell-state can be prepared

$$|\Theta^{\pm}\rangle_{si} = \frac{1}{\sqrt{2}}\left(|m\rangle_s|-n\rangle_i \pm |-m\rangle_s|n\rangle_i\right) \tag{2}$$

where $|m\rangle$ and $|n\rangle$ are identical OAM states, i.e., $m = n$, and the subscript s (or i) denotes the signal (or idler) photon. What we are concerned about is to create the OAM Bell-state in two-photon combined multi-dimensional OAM Hlibert space, where signal OAM state $|m\rangle_s$ and idler OAM state $|n\rangle_i$ are not necessarily identical, i.e., m and n are arbitrary numbers.

A schematic diagram of the setup is sketched in Fig. 1. We employ a pulsed high-intensity ultraviolet (uv) laser (100 MHz, 150 mW) with a central wave-length of

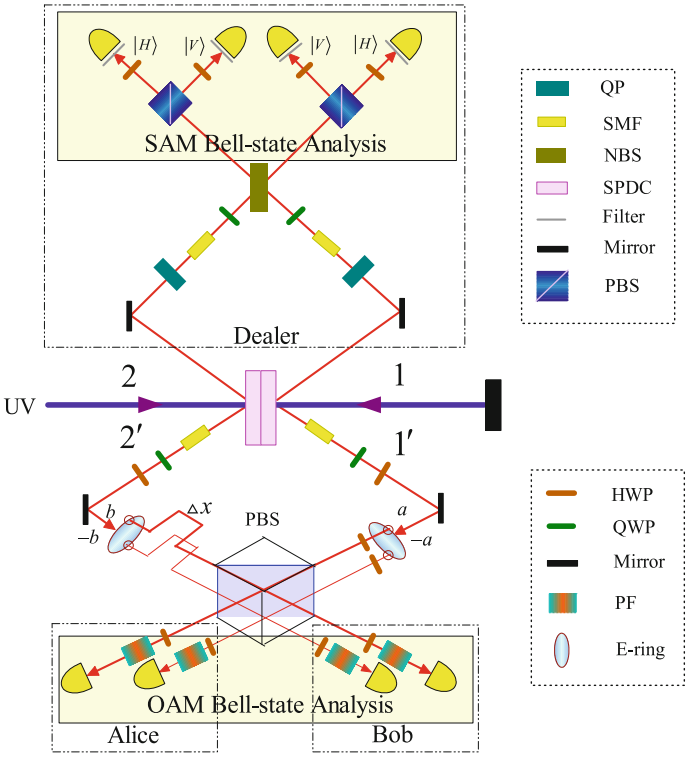

Fig. 1 Schematic diagram showing the principle for the QSS based on the OAM Bell-state analysis

355 nm. The pump uv pulse is weakly passed through two barium oxide crystals, where the type-I non-collinear spontaneous parametric down-conversions (SPDC) are simultaneously utilized and the degenerated 710 nm signal and idler beams are separated by the non-polarizing beam splitters (NBS). One pair of photons $(1, 1')$ can be produced with multi-dimensional entanglement in the OAM degree of freedom, i.e.,

$$|\Phi\rangle_{1,1'}^{(0)} = \sum_{l} C_{l,-l}|l\rangle_1|-l\rangle_{1'}|H\rangle_1|H\rangle_{1'}, \tag{3}$$

where $C_{l,-l}$ denotes the probability amplitude of detecting a signal photon with the OAM of $l\hbar$ and an idler photon with $-l\hbar$ while $|H\rangle$ represents the horizontal polarization. After being reflected by a mirror, the type-I SPDC can be done again. Then another pair of photons $(2, 2')$ are similarly created with the OAM-entanglement

$$|\Phi\rangle_{2,2'}^{(0)} = \sum_{l} C_{l,-l}|l\rangle_2|-l\rangle_{2'}|H\rangle_2|H\rangle_{2'}. \tag{4}$$

It is obvious that two states in Eqs. (3,4) show the similar OAM entanglement in multi-dimensional OAM Hilbert spaces but no SAM-entanglement between photons.

For each pair of photons (t, t'), $\forall\, t \in \{1, 2\}$, one implements entanglement transferring via the q_t plate, denoted by QP_t, and obtains

$$|\Phi\rangle_{1,1'}^{(1)} = \sum_l C_{l,-l}\big(|R, l+a\rangle_1|L, l-a\rangle_1\big)|-l, H\rangle_{1'}, \tag{5}$$

$$|\Phi\rangle_{2,2'}^{(1)} = \sum_l C_{l,-l}\big(|R, l+b\rangle_2|L, l-b\rangle_2\big)|-l, H\rangle_{2'}, \tag{6}$$

where $|a = 2q_1\rangle$ and $|b = 2q_2\rangle$ denote the OAM states in the independent multi-dimensional OAM Hilbert spaces generated by the QP_1 and QP_2, respectively. The subsequent single-mode fiber (SMF) is employed for selecting the fundamental Gaussian mode with the zero OAM. According to the symmetry of the SPDC process, i.e., $C_{l,-l} = C_{-l,l}$, one obtains

$$|\Phi\rangle_{1,1'} = \frac{1}{\sqrt{2}}\big(|R\rangle_1|a\rangle_{1'} + |L\rangle_1|-a\rangle_{1'}\big), \tag{7}$$

$$|\Phi\rangle_{2,2'} = \frac{1}{\sqrt{2}}\big(|R\rangle_2|b\rangle_{2'} + |L\rangle_2|-b\rangle_{2'}\big). \tag{8}$$

Combining Eqs. (7,8), one achieves the combined SAM-based OAM hybrid-entanglement state

$$|\Gamma\rangle_{11'22'} = |\Phi\rangle_{1,1'} \otimes |\Phi\rangle_{2,2'}, \tag{9}$$

which can be rewritten in the formula

$$\begin{aligned}|\Gamma\rangle_{121'2'} = \frac{1}{2}\big(&|\Lambda^+\rangle_{12}|\Omega^+\rangle_{1'2'} + |\Lambda^-\rangle_{12}|\Omega^-\rangle_{1'2'} \\ &+|\Upsilon^+\rangle_{12}|\Theta^+\rangle_{1'2'} + |\Upsilon^-\rangle_{12}|\Theta^-\rangle_{1'2'}\big)\end{aligned} \tag{10}$$

$$\begin{aligned}= \frac{1}{2}\big(&|\Phi^+\rangle_{12}|\Theta^+\rangle_{1'2'} + |\Phi^-\rangle_{12}|\Omega^+\rangle_{1'2'} \\ &+i|\Psi^+\rangle_{12}|\Omega^-\rangle_{1'2'} - i|\Psi^-\rangle_{12}|\Theta^-\rangle_{1'2'}\big)\end{aligned} \tag{11}$$

The notations $|\Lambda^\pm\rangle$, $|\Upsilon^\pm\rangle$, $|\Phi^\pm\rangle$ and $|\Psi^\pm\rangle$ denote the SAM Bell-states in different bases, i.e.,

$$\begin{aligned}|\Lambda^\pm\rangle &= \frac{1}{\sqrt{2}}(|L\rangle|L\rangle \pm |R\rangle|R\rangle), \\ |\Upsilon^\pm\rangle &= \frac{1}{\sqrt{2}}(|L\rangle|R\rangle \pm |R\rangle|L\rangle),\end{aligned} \tag{12}$$

and

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|H\rangle|H\rangle \pm |V\rangle|V\rangle),$$
$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|H\rangle|V\rangle \pm |V\rangle|H\rangle), \tag{13}$$

while $|\Theta^{\pm}\rangle$ and $|\Omega^{\pm}\rangle$ represent the OAM Bell-states

$$|\Omega^{\pm}\rangle = \frac{1}{\sqrt{2}}(|a\rangle|b\rangle \pm |-a\rangle|-b\rangle),$$
$$|\Theta^{\pm}\rangle = \frac{1}{\sqrt{2}}(|a\rangle|-b\rangle \pm |-a\rangle|b\rangle). \tag{14}$$

The key procedure in the above transformation is due to the relations of the horizontal and circular polarizations [14,15,43], i.e.,

$$|H\rangle = \frac{1}{\sqrt{2}}(|L\rangle + |R\rangle),\ |V\rangle = \frac{i}{\sqrt{2}}(|L\rangle - |R\rangle). \tag{15}$$

According to relation of the SAM and OAM states in Eqs. (10,11), it illustrates the principle of SAM entanglement swapping when photons (1, 2) are projected onto the SAM Bell-state, as shown in Fig. 1. In essence, an SAM Bell-state measurement of photons (1, 2) results in another OAM Bell-state on photons $(1', 2')$. The practical difficulty of this process is to identify unambiguously four SAM Bell-states $|\Phi^{\pm}\rangle$ and $|\Psi^{\pm}\rangle$. However, it is sufficient to project photons (1, 2) while superposing them at the NBS and registering coincidence counts between outputs. After performing the SAM Bell-state measurement, the entanglement of the OAM Bell-state is achieved in multi-dimensional OAM Hilbert space $\mathcal{H} = H_a \otimes H_b$.

As an example, we consider a case where photons (1, 2) have collapsed into $|\Phi^{+}\rangle_{12}$ as a result of the SAM Bell-state measurement. The remaining photons $(1', 2')$ will be correspondingly projected to the OAM Bell-state $|\Theta^{+}\rangle_{1'2'}$, illustrated in Eq.(11). It shows that the emerging state of photons $(1', 2')$ has an intimate relationship with the SAM Bell-state measurement on photons (1, 2), which is the deployed OAM Bell-state for implementing the QSS among the legally designated participants.

3 The CRT-based QSS via the OAM Bell-state Analysis

Prior to proposing the CRT-based QSS, we should briefly describe the principle of the well known CRT over finite field [17–19], which is a result of the congruences in number theory or abstract algebra.

Proposition 1 *For the given coprime numbers in* $\mathcal{M} = \{m_i : 1 \le i \le p\}$, *such that* $\gcd(m_i, m_j) = 1$, *where* $1 \le j \le p$, *the system of equations*

Table 1 The secret results X with two shadows $a = s_1$ and $b = s_2$ for $m_1 = 2$ and $m_2 = 3$ based on the CRT

$X(m_1, m_2)$	0	1	2	3	4	5
$a \mod m_1$	0	1	0	1	0	1
$b \mod m_2$	0	1	2	0	1	2

$$\begin{cases} X = s_1 \mod m_1, \\ X = s_2 \mod m_2, \\ \quad \vdots \\ X = s_p \mod m_p, \end{cases} \tag{16}$$

has a unique solution in $\mathbb{Z}_M = \{0, 1, \ldots, M-1\}$ for $M = \prod_{i=1}^{p} m_i$. The solution can be calculated as follows

$$X = \sum_{i=1}^{p} T_i M_i s_i \mod M \tag{17}$$

where T_i and M_i are parameters satisfying constraints $M_i = M/m_i$ and $T_i M_i \mod m_i = 1$.

According to Eq. (16), the number $X \in \mathbb{Z}_M$, which is a secret of the dealer in the QSS, can be mapped to p shadows in $\mathcal{S}$ given by

$$\mathcal{S} = \{s_i = X \mod m_i : 1 \le i \le p\}, \tag{18}$$

which are then distributed to p distant participants. It is known that it is difficult for anyone to recover X without shadows $\mathcal{S}$ [18]. However, when all participants exchange their shadows, they can jointly recover X from Eq. (17).

For example, taking $m_1 = 2$ and $m_2 = 3$, the number X gives the value in $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ with two shadows a and b, respectively, shown in Table 1.

According to the CRT, for the given system of simultaneous congruence equations in Eq. (16), the solution X is unique over finite field $\mathbb{Z}_M$ under some appropriate conditions on the congruences, which can be exquisitely employed for the present QSS. Namely, the CRT can be employed to produce several shares using different shadows in $\mathcal{S}$ embedded in the OAM Bell-states in multi-dimensional OAM Hilbert space $\mathcal{H}$ represented in the congruence equations where the secret could then be recovered by solving the system of congruences to get the unique solution X.

The QSS consists of dividing and recovering the secret X from a set of shares for two participants, each containing partial information of OAM state $|a\rangle$ or $|b\rangle$ for the secret X. Suppose the dealer wants to distribute a secret $X \in \mathbb{Z}_6$ to two participants, Alice and Bob, respectively. Two pairs of photons $(1, 1')$ and $(2, 2')$ are prepared in advance, as shown in Fig. 1, where photons $(1, 2)$ are kept by the dealer while photons $1'$ and $2'$ are sent to Alice and Bob, respectively. It goes as follows.

Step A1: *Moduli negotiation.* Suppose Alice and Bob choose two coprime numbers m_1 and m_2 as their modulus, which correspond to the OAM Bell-states in $\mathcal{H}$.

Step A2: *Shadows mapping.* The dealer prepares the secret X on finite field $\mathbb{Z}_{m_1 m_2}$, which can be mapped to two shadows $a = X \mod m_1$ and $b = X \mod m_2$ for m_1-dimensional and m_2-dimensional OAM Hilbert spaces, respectively.
Step A3: *Secret distributing.* The dealer performs the SAM Bell-state measurement on photons (1, 2) to produce an OAM Bell-state in $\{|\Omega^{\pm}\rangle_{AB}, |\Theta^{\pm}\rangle_{AB}\}$ in the combined multi-dimensional OAM Hilbert space $\mathcal{H}$, i.e.,

$$
\begin{aligned}
|\Omega^{\pm}\rangle_{AB} &= \frac{1}{\sqrt{2}}\big(|a\rangle_{1'}|b\rangle_{2'} \pm |-a\rangle_{1'}|-b\rangle_{2'}\big), \\
|\Theta^{\pm}\rangle_{AB} &= \frac{1}{\sqrt{2}}\big(|a\rangle_{1'}|-b\rangle_{2'} \pm |-a\rangle_{1'}|b\rangle_{2'}\big),
\end{aligned} \tag{19}
$$

where photons $1'$ and $2'$ are in the OAM states in a-dimensional and b-dimensional OAM Hilbert spaces kept by Alice and Bob, respectively.
Step A4: *Secret recovering.* Alice and Bob perform the OAM-Bell state measurement to sort OAM states $|a\rangle$ and $|b\rangle$ on photons $1'$ and $2'$, respectively. Finally, Alice and Bob jointly recover X via the CRT.

Due to insecure channels, one may be challenged by eavesdropping. Moreover, dishonest participants may cheat others to reveal X. According to the CRT [17–19], the QSS is secure against dishonest participants since only authorized participants can have access to their photons on which they perform the OAM state analysis to achieve the respective shadows, where X appears from Eq.(17). In addition, since all legal participants decide the joint coefficients of the OAM Bell-state, any dishonest participant who randomly selects one OAM state of another photon from $2m_2$ (or $2m_1$) OAM states in its own multi-dimensional OAM Hilbert space could guess the specific OAM state with probability $1/(2m_2)$ (or $1/(2m_1)$) before gathering together to recover X. Accordingly, the probability to guess the correct basis of the OAM Bell-state is $1/(4m_1m_2)$. Therefore, it is more difficulty for any dishonest participants to steal X by applying the individual attack strategy on the OAM Bell-state than that of the conventional attack strategy on the SAM Bell-state.

4 Extension of the CRT-based QSS

So far we have proposed a simple QSS with two participants based on the OAM Bell-state analysis. Let us now show how to implement the QSS among three or more participants who share the p-qudit OAM Greenberger-Horne-Zeilinger (GHZ) state prepared by the dealer with p pairs of photons in the SAM-based OAM hybrid entanglement states.

According to the CRT, the extended QSS for p participants, Alice, Bob, ..., Charlie, should be on the basis of the p-qudit OAM GHZ-states. For the given p pairs of photons (t, t'), $1 \le t \le p$, we obtain

$$
|\Phi\rangle_{t,t'} = \frac{1}{\sqrt{2}}\big(|R\rangle_t|m_t\rangle_{t'} + |L\rangle_t|-m_t\rangle_{t'}\big), \tag{20}
$$

where $m_t = 2q_t$ denotes the OAM increasing from QP_t. Then we have the combined SAM-based OAM hybrid entanglement state on p pairs of photons $\{(t, t') : 1 \le t \le p\}$, i.e.,

$$|\Gamma\rangle_{11'\cdots pp'} = \otimes_{t=1}^{p} |\Phi\rangle_{t,t'}, \tag{21}$$

which is rewritten as

$$|\Gamma\rangle_{1\cdots p,1'\cdots p'} = \sum \left(|\mathrm{GHZ}\rangle_{1\cdots p}^{\mathrm{SAM}} \otimes |\mathrm{GHZ}\rangle_{1'\cdots p'}^{\mathrm{OAM}} \right), \tag{22}$$

where $|\mathrm{GHZ}\rangle_{1\cdots p}^{\mathrm{SAM}}$ and $|\mathrm{GHZ}\rangle_{1'\cdots p'}^{\mathrm{OAM}}$ denote the SAM and OAM GHZ states, i.e.,

$$|\mathrm{GHZ}\rangle_{1\cdots p}^{\mathrm{SAM}} = \frac{1}{\sqrt{2}} \left(\prod_{t=1}^{p} |\omega(t)\rangle_t + \prod_{t=1}^{p} |\bar{\omega}(t)\rangle_t \right), \tag{23}$$

$$|\mathrm{GHZ}\rangle_{1'\cdots p'}^{\mathrm{OAM}} = \frac{1}{\sqrt{2}} \left(\prod_{t=1}^{p} |\mu(t')\rangle_{t'} + \prod_{t'=1}^{p} |-\mu(t')\rangle_{t'} \right). \tag{24}$$

Here $|\omega(t)\rangle, |\bar{\omega}(t)\rangle \in \{|R\rangle, |L\rangle\}$ and $|\mu(t')\rangle \in \{|m_t\rangle, |-m_t\rangle\}$ satisfy the constraints that if $|\omega(t)\rangle = |R\rangle$ (or $|\omega(t)\rangle = |L\rangle$), then $|\bar{\omega}(t)\rangle = |L\rangle$ and $|\mu(t')\rangle = |m_t\rangle$ (or $|\bar{\omega}(t)\rangle = |R\rangle$ and $|\mu(t')\rangle = |-m_t\rangle$), respectively. There are 2^p SAM and OAM GHZ-states in the sum of Eq. (22), respectively. After performing the joint SAM GHZ-state analysis with $|\mathrm{GHZ}\rangle_{1\cdots p}^{\mathrm{SAM}}$ on photons $\{1, \ldots, p\}$, one obtains the OAM GHZ-state $|\mathrm{GHZ}\rangle_{1'\cdots p'}^{\mathrm{OAM}}$ in the combined multi-dimensional OAM Hilbert space $\mathcal{H}_p = \otimes_{t=1}^{p} H_{m_t}$. Namely, the detection of the SAM GHZ-state $|\mathrm{GHZ}\rangle_{1\cdots p}^{\mathrm{SAM}}$ creates the OAM GHZ-state $|\mathrm{GHZ}\rangle_{1\cdots p}^{\mathrm{SAM}}$ in $\mathcal{H}_p$, i.e.,

$$\langle \mathrm{GHZ}_{1\cdots p}^{\mathrm{SAM}} | \Gamma \rangle_{1\cdots p,1'\cdots p'} = |\mathrm{GHZ}\rangle_{1'\cdots p'}^{\mathrm{OAM}}. \tag{25}$$

Based on the OAM GHZ state analysis on photons $\{1', \ldots, p'\}$, one achieves the extended QSS in $\mathcal{H}_p$.

Suppose the dealer wants to distribute a secret $X \in \mathbb{Z}_M$ to p participants, Alice, Bob, ..., and Charlie, respectively, where $M = \Pi_{t=1}^{p} m_t$. There are p pairs of photons $\{(t, t') : 1 \le t \le p\}$ prepared in advance, where photons $\{1, 2, \ldots, p\}$ are kept by the dealer and photons $1', 2', \ldots, p'$ are sent to Alice and Bob, ..., Charlie, respectively. This QSS can be described as follows.

Step B1: Alice, Bob, ..., and Charlie, select p coprime numbers $\mathcal{M} = \{m_t : 1 \le t \le p\}$ as their modulus, corresponding to the OAM GHZ-states in $\mathcal{H}_p$.

Step B2: The dealer prepares the secret X in $\mathbb{Z}_M$, which can be mapped to shadows

$$\mathcal{S} = \{a_t = X \mod m_t : 1 \le t \le p\} \tag{26}$$

corresponding to the OAM state $|a_t\rangle$ or $|-a_t\rangle$ on each photon t'.

Step B3: The dealer performs the SAM GHZ-state measurement with $|\mathrm{GHZ}\rangle_{1\cdots p}^{\mathrm{SAM}}$ on photons $\{1, 2, \ldots, p\}$ to generate the OAM GHZ-state $|\mathrm{GHZ}\rangle_{1'\cdots p'}^{\mathrm{OAM}}$ in $\mathcal{H}_p$, where photon t' is in the OAM state $|a_t\rangle$ or $|-a_t\rangle$.
Step B4: Each participant performs the OAM state analysis in m_t-dimensional OAM Hilbert space to sort the OAM state $|a_t\rangle$ or $|-a_t\rangle$ on photon t' to obtain shadow a_t on finite field $\mathbb{Z}_{m_t}$. Finally, all legal participants lay heads together to recover X via the CRT.

We note that the extension of the QSS for p participants via the CRT is in essence based on the generation of the p-qudit OAM GHZ-state $|\mathrm{GHZ}\rangle_{1'\cdots p'}^{\mathrm{OAM}}$. In order to create the OAM GHZ state among legal participants, one has to apply p QP_t to produce p OAM states $|m_t = 2q_t\rangle_{t'}$ on photons t' embedded in p pairs of the SAM-based OAM hybrid entanglement states, which establishes the p-qudit GHZ state in $\mathcal{H}_p$. As an example, for $q_1 = 1/2, q_2 = 1$ and $q_3 = 3/2$, one generates the three-qudit OAM GHZ-states

$$|\mathrm{GHZ}^{\pm}\rangle_{1'2'3'}^{\mathrm{OAM}} = \frac{1}{\sqrt{2}}(|1\rangle|2\rangle|3\rangle \pm |-1\rangle|-2\rangle|-3\rangle), \tag{27}$$

which can be elegantly employed in the CRT-based QSS in $\mathcal{H}_3$.

In brief, the extended QSS for p participants not only provides us an efficient approach to share the secret in $\mathcal{H}_p$, but also increases the security of the secret X since it is more difficult for dishonest participants or eavesdropper to steal any information on shadows $\mathcal{S}$ from the p-qudit OAM-entanglement states than that of the previous QSS with the p-qubit states in 2^p-dimensional Hilbert space.

5 Efficiency analysis

In what follows, we consider the efficiency of the CRT-based QSS via the OAM entanglement analysis in the combined multi-dimensional OAM Hilbert space.

As discussed in the previous sections, it is difficult for dishonest participants who have no knowledge of the whole shadows to recover the secret X [17–19]. Actually, since each shadow a_t is kept in the t^{th} qudit of the OAM entanglement state, it is impossible for dishonest participants to steal the remaining shares a_l for $l \neq t$ without disturbing the OAM states of other photons, where each qudit works as a carrier for the corresponding legal participant. In other words, the security of the QSS is based on the OAM entanglement of the Bell-state (or GHZ state) in the combined multi-dimensional OAM Hilbert space, on which the CRT is properly deployed for the secret sharing. Borrowing the security analysis in the conventional QSS with the multi-qubit entanglement state [28–30], we can show in a similar way that the proposed CRT-based QSS with the OAM entanglement analysis is at least secure against any dishonest participants and individual eavesdropping attack strategies.

In order to analyze the efficiency of the CRT-based QSS without loss of generality, we consider the generation of the OAM Bell-states in $\mathcal{H}$. According to Eq. (3), one can create the OAM entanglement channel, i.e., $|\Theta^{\pm}\rangle$ or $|\Omega^{\pm}\rangle$ for given shadows (a, b) embedded in Eq.(14), which corresponds to the secret X on finite field.

Based on the experimental setup in Fig. 1, we need to consider the rotational effect on QP_t while showing the practical application of the QSS. After being rotated with an arbitrary angle $\beta_t \in [0, 2\pi)$ of QP_t represented by a suitable parameter $q_t, \forall\, t \in \{1, 2, 3, 4\}$, it can be explicitly rewritten as

$$\hat{Q}(q_t, \beta_t) = \chi_{\beta_t} |R, l + 2q_t\rangle\langle L, l| + \chi^*_{\beta_t} |L, l - 2q_t\rangle\langle R, l|, \tag{28}$$

where parameter χ_{β_t} is given by

$$\chi_{\beta_t} = \begin{cases} e^{i4\pi q_t - 2(q_t-1)\beta_t}, & 0 < \phi < \beta_t; \\ e^{-2(q_t-1)\beta_t}, & \text{otherwise}, \end{cases} \tag{29}$$

and its conjugation by $\chi^*_{\beta_t}$. The yielded OAM state $|2q_t\rangle$ has a coherent decomposition in infinite dimensional OAM Hilbert space with a fractional form

$$|2q_t\rangle = \sum_n e^{i(2q_t - n)\pi} \mathrm{sinc}[2(q_t - n)\pi]|n\rangle. \tag{30}$$

In an OAM analyzer, the interaction of the SMF and polarizer sustains the fundamental Gaussian mode [14,37]. Therefore, it projects the incoming photons onto the hyper-entanglement state

$$|\mathcal{A}_t(q_t, \beta_t)\rangle = \frac{1}{\sqrt{2}} \sum_n \mathcal{N}_{\beta_t}(n)|L\rangle|-n\rangle + \mathcal{N}^*_{\beta_t}(n)|R\rangle|n\rangle, \tag{31}$$

where $\mathcal{N}_{\beta_t}(n) = \chi_{\beta_t} e^{i(2q_t - n)\pi} \mathrm{sinc}[(2q_t - n)\pi]$.

In order to illustrate the effect of $|\Theta^+\rangle_{1'2'}$ on the QSS, we deploy an OAM analyzer on photons in the combined hybrid entanglement state

$$|\mathcal{T}\rangle_{12} = |\mathcal{A}_1(q_1, \beta_1)\rangle \otimes |\mathcal{A}_2(q_2, \beta_2)\rangle. \tag{32}$$

After being performed the SAM Bell-state measurement with outcome $|\Psi^+\rangle$, it produces the OAM entanglement state on photons $(1', 2')$

$$\begin{aligned} |\Theta^+(\beta_1, \beta_2)\rangle_{1'2'} = \frac{1}{\sqrt{2}} \sum_{a,b} \big[& \mathcal{N}_{\beta_1}(a)\mathcal{N}^*_{\beta_2}(b)|a\rangle_{1'}|-b\rangle_{2'} \\ & + \mathcal{N}^*_{\beta_1}(a)\mathcal{N}_{\beta_2}(b)|-a\rangle_{1'}|b\rangle_{2'}\big]. \end{aligned} \tag{33}$$

Suppose an OAM analyzer on photon $1'$ is with $q_1 = -q$ and $\beta_1 = 0$ while another on photon $2'$ is with $q_2 = q$ and $\beta_2 = \beta \neq 0$. Photons $(1, 1')$ before threading this analyzer are collapsed into $|\mathcal{A}_1(-q, 0)\rangle$. Similarly, photons $(2, 2')$ become $|\mathcal{A}_2(q, \beta)\rangle$. Therefore, the OAM entanglement state in Eq.(33) can be described as

$$|\Theta^+(0, \beta)\rangle_{1'2'} = \frac{1}{\sqrt{2}} \sum_{a,b} \big[\mathcal{N}^*_{\beta}(b)|a\rangle_{1'}|-b\rangle_{2'} + \mathcal{N}_{\beta}(b)|-a\rangle_{1'}|b\rangle_{2'}\big]. \tag{34}$$

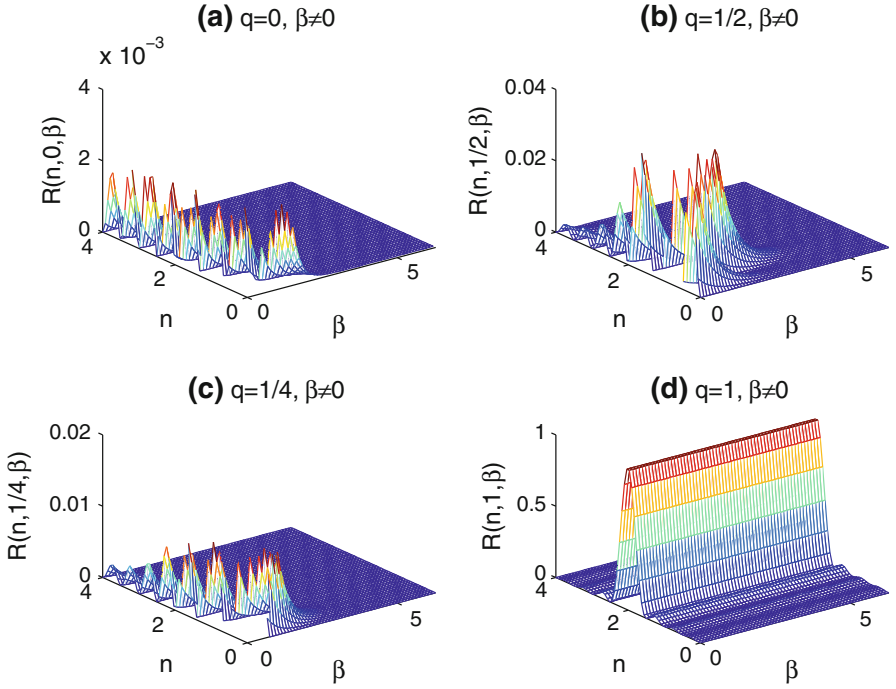

Fig. 2 Coincidence curves for four different q plates with the rotation angle $\beta \in (0, 2\pi)$

The OAM analyzer for different q plates with $\beta \neq 0$ results in the coincidence $R(n, q, \beta)$ while detecting $(1', 2')$ in state $|\Theta^+\rangle_{1'2'}$ and another in state $|\Theta^+(0, \beta)\rangle_{1'2'}$ as follows

$$\begin{aligned} R(n, q, \beta) &\propto |\langle\Theta^+(0, \beta)|\Theta^+\rangle|^2 \\ &= e^{4(q-1)\beta} \cos^2(4q\pi) \cos^2[(2q - n)\pi]\text{sinc}^2[(2q - n)\pi]. \end{aligned} \tag{35}$$

For $\beta = 0$, one obtains

$$R(n, q, 0) \propto \cos^2(4q\pi) \cos^2[(2q - n)\pi]\text{sinc}^2[(2q - n)\pi]. \tag{36}$$

We plot the coincidence curves $R(n, q, \beta)$ for four q plates with $\beta \neq 0$ shown in Fig. 2, and $R(n, q, 0)$ with $\beta = 0$ in Fig. 3, respectively. Taking $q = 1$, it is shown in Fig. 2d that the coincidence curve $R(n, 1, \beta)$ keeps unchanged regardless of the rotation angular β due to the fact that it does not alter the OAM analyzer under the circular symmetry. Taking $q \in \{0, 1/2, 1/4\}$ for the rotation angular $\beta \neq 0$, the coincidence curves $R(n, q, \beta)$ are respectively illustrated in Fig. 2a–c, which indicates the coincidence of the OAM Bell-states in the combined multi-dimensional OAM Hilbert space $\mathcal{H}$.

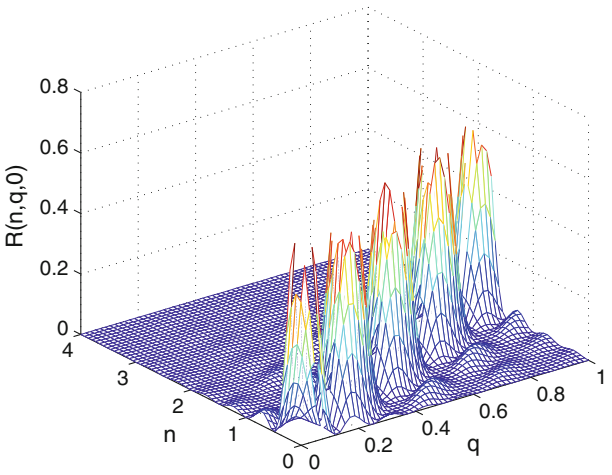

Fig. 3 Coincidence curves with any q plates in $q \in [0, 1]$ with the rotation angle $\beta = 0$

6 Conclusion

We have reported a creation of the CRT-based QSS on finite field via the OAM entanglement analysis in multi-dimensional OAM Hilbert space. It shows how to transfer the secret among legal participants based on the generation of the multi-qudit entanglement OAM state with the corresponding OAM analyzers. It provides an alternative technique for the QSS with the high-rate and large-capacity in the combined multi-dimensions OAM Hilbert spaces, where SAM and OAM entanglement swapping serve as two critical constituents in the SAM-based OAM hybrid entanglement quantum system.

Acknowledgements This work has been supported by the National Natural Science Foundation of China (60902044, 61172184), the New Century Excellent Talents in University, China (NCET-11-0510), and partly by the World Class University R32-2010-000-20014-0 NRF, and Fundamental Research 2010-0020942 NRF, Korea.

References

1. Goldenberg, L., Vaidman, L.: Quantum cryptography based on orthogonal states. Phys. Rev. Lett. **75**, 1239–1243 (1995)
2. Guo, Y., Lee, M., Zeng, G.: Large-capability quantum key distribution with entangled qutrits. Optics Commun. **281**(14), 3938–3942 (2008)
3. Zhang, J., He, G., Zeng, G.: Equivalence of continuous-variable stabilizer states under local clifford operations. Phys. Rev. A **80**, 052333 (2009)
4. Xu, X.-Y., Xu, J.-S., Li, C.-F., Zou, Y., Guo, G.-C.: Experimental demonstration of nonlocal effects in the partial-collapse measurement and reversal process. Phys. Rev. A **83**, 010101 (2011)

5. Modlawska, J., Grudka, A.: Nonmaximally entangled states can be better for multiple linear optical teleportation. Phys. Rev. Lett **100**, 110503 (2008)
6. Bouwmeester, D., Pan, J.-W., Mattle, K., Eibl, M., Weinfurter, H., Zeilinger, A.: Experimental quantum teleportation. Nature **390**, 575–579 (1997)
7. Jennewein, T., Weihs, G., Pan, J.-W., Zeilinger, A.: Experimental nonlocality proof of quantum teleportation and entanglement swapping. Phys. Rev. Lett **88**, 017903 (2001)
8. Halder M., Halder A., Beveratos A., Gisin N., Scarani V., Simon C., Zbinden, H.: Entangling independent photons by time measurement. Nat. Phys. **3**, 692–695 (2007)
9. Lu, C.-Y., Yang, T., Pan, J.-W.: Experimental multiparticle entanglement swapping for quantum networking. Phys. Rev. Lett. **103**, 020501 (2009)
10. Zhao, Z., Yang, T., Chen, Y.-A., Zhang, A.-N., Pan, J.-W.: Experimental realization of entanglement concentration and a quantum repeater. Phys. Rev. Lett. **90**, 207901 (2003)
11. Allen, L., Beijersbergen, M.W., Spreeuw, R.J.C., Woerdman, J.P.: Orbital angular momentum of light and the transformation of laguerre-gaussian laser modes. Phys. Rev. A **45**, 8185–8189 (1992)
12. Franke-Arnold, S., Allen, L., Padgett, M.: Advances in optical angular momentum. Laser Photon. Rev. **2**, 299–313 (2008)
13. Molina-Terriza, G., Torres, J.P., Torner, L.: Twisted photons. Nat. Phys. **3**, 305–310 (2007)
14. Chen, L., She, W.: Hybrid entanglement swapping of photons: creating the orbital angular momentum bell states and greenberger-horne-zeilinger states. Phys. Rev. A **83**, 012306 (2011)
15. Chen, L., She, W.: Spin-orbit-path hybrid greenberger-horne-zeilinger entanglement and open-destination teleportation with multiple degrees of freedom. Phys. Rev. A **83**, 032305 (2011)
16. Leach, J., Jack, B., Romero, J., Ritsch-Marte, M., Boyd, R.W., Jha, A.K., Barnett, S.M., Franke-Arnold, S., Padgett, M.J.: Violation of a bell inequality in two-dimensional orbital angular momentum state-spaces. Opt. Exp **17**, 8287 (2009)
17. Ding, C., Pei, D., Salomaa, A.: Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography. World Scientific Publishing, Singapore (1996)
18. Asmuth, C., Bloom, J.: A modular approach to key safeguarding. IEEE Trans. Inform. Theory **29**(2), 208–210 (1983)
19. Cormen, T.H., Rivest, R.L., Leiserson, C.E., Stein, C.: Introduction to Algorithms, Second Edition. MIT Press and McGraw-Hill, New York (2001)
20. Cleve, R., Gottesman, D., Lo, H.-K.: How to share a quantum secret. Phys. Rev. Lett. **83**, 648–651 (1999)
21. Guo, Y., Huang, D., Zeng, G., Lee, M.H.: Multiparty quantum secret sharing of quantum states using entanglement states. Chin. Phys. Lett. **25**(1), 16–19 (2008)
22. Guo, Y., Zeng, G., Chen, Z.: Multiparty quantum secret sharing of quantum states with quantum registers. Chin. Phys. Lett. **24**(4), 863–866 (2007)
23. Shi, R., Su, Q., Guo, Y., Lee, M.H.: Quantum secretsharing based on chinese remainder theorem. Commun. Theor. Phys. **55**, 573 (2011)
24. Hillery, M., BuzekV. Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**, 1829–1834 (1999)
25. Zhang, Z.-J., Man, Z.-X.: Multiparty quantum secret sharing of classical messages based on entanglement swapping. Phys. Rev. A **72**, 022303 (2005)
26. Chen, Y.-A., Zhang, A., Zhao, Z., Zhou, X.-Q., Lu, C.-Y., Peng, C.-Z., Yang, T., Pan, J.-W.: Experimental quantum secret sharing and third-man quantum cryptography. Phys. Rev. Lett. **95**, 200502 (2005)
27. Jan Bogdanski, J., Rafiei, N., Bourennane, M.: Experimental quantum secret sharing using telecommunication fiber. Phys. Rev. A **78**, 062307 (2008)
28. Han, L.F., Liu, Y.M., Liu, J., Zhang, Z.J.: Multiparty quantum secret sharing of secure direct communication using single photons. Opt. Commun. **281**, 2690 (2008)
29. Markham, D., Sanders, C.: Graph states for quantum secret sharing. Phys. Rev. A **78**, 042309 (2008)
30. Sarvepalli, P.K., Klappenecker, A.: Sharing classical secrets with Calderbank-Shor-Steane codes. Phys. Rev. A **80**, 022321 (2009)
31. Sarvepalli, P.: Entropic inequalities for a class of quantum secret-sharing states. Phys. Rev. A **83**, 042303 (2011)
32. Sarvepalli, P.: Bounds on the information rate of quantum-secret-sharing schemes. Phys. Rev. A **83**, 042324 (2011)
33. Scherpelz, P., Resch, R., Berryrieser, D., Lynn, T.W.: Entanglement-secured single-qubit quantum secret sharing. Phys. Rev. A **84**, 032303 (2011)
34. Oemrawsingh, S.S.R., Aiello, A., Eliel, E.R., Nienhuis, G., Woerdman, J.P.: How to observe high-dimensional two-photon entanglement with only two detectors. Phys. Rev. Lett. **92**, 217901 (2004)

35. Oemrawsingh, S.S.R., Ma, X., Voigt, D., Aiello, A., Eliel, E.R., Hooft, G.W., Woerdman, J.P.: Experimental demonstration of fractional orbitalangular momentum entanglement of two photons. Phys. Rev. Lett. **95**, 240501 (2005)
36. Nagali, E., Sciarrino, F., De Martini, F., Marrucci, L., Piccirillo, B., Karimi, E., Santamato, E.: Quantum information transfer from spin to orbital angular momentum of photons. Phys. Rev. Lett. **103**, 013601 (2009)
37. Chen, L., She, W.: Single-photon spin-orbit entanglement violating a Bell-like inequality. JOSA B **27**(6), 7–10 (2010)
38. Marrucci, L., Manzo, C., Paparo, D.: Optical spin-to-orbital angular momentumconversion in inhomogeneous anisotropic media. Phys. Rev. Lett. **96**, 163905 (2006)
39. Marrucci, L., Karimi, E., Slussarenko, S., Piccirillo, B., Santamato, E., Nagali, E., Sciarrino, E.: Spin-to-orbital conversion of the angular momentum of light and its classical and quantum applications. J. Opt. **13**, 064001 (2011)
40. Chen, L., She, W.: Increasing shannon dimensionality by hyperentanglement of spin and fractional orbital angular momentum. Opt. Lett. **34**(12), 1855–1857 (2009)
41. Allen, L., Beijersbergen, M.W., Spreeuw, R.J.C., Woerdman, J.P.: Orbital angular momentum of light and the transformation of Laguerre-Gaussian laser modes. Phys. Rev. A **45**(11), 8185–8189 (1992)
42. Molina, G., Torres, J.P., Torner, L.: Management of the angular momentum of light: preparation of photons in multidimensional vector states of angular momentum. Phys. Rev. Lett. **88**, 013601 (2002)
43. Law, C.K., Eberly, J.H.: Analysis and interpretation of high transverse entanglement in optical parametric down conversion. Phys. Rev. Lett. **92**, 127903 (2004)