Experimental 11-Dimensional Secret Sharing with Perfect Vortex Beams

Jonathan Pinnell,1 Isaac Nape,1 Michael De Oliveira,1 Najmeh Tabebordbar,1 and Andrew Forbes1,2

1School of Physics, University of the Witwatersrand, Johannesburg 2000, South Africa
2Corresponding author: andrew.forbes@wits.ac.za

Secret sharing is the art of securely sharing information between more than two people in such a way that its reconstruction requires the collaboration of a certain number of parties. Entanglement-based secret sharing schemes which utilise multi-particle entanglement are limited by their scalability. Recently, a high-dimensional single photon secret sharing protocol was proposed which has impressive advantages in scalability. However, the experimental realisation of this protocol remains elusive. Here, by taking advantage of the high-dimensional Hilbert space for orbital angular momentum and using Perfect Vortex beams as their carriers, we present a proof-of-principle implementation of a high-dimensional single photon quantum secret sharing scheme. We experimentally implemented this scheme for 10 participants in $d = 11$ dimensions and show how it can be easily scaled to higher dimensions and any number of participants.

Quantum cryptography has paved the way in the development of many encryption schemes which utilise features that are unique to quantum mechanics, for example, the no-cloning theorem [1], non-locality [2] and the uncertainty-principle [3] to name a few. These features have fostered the evolution of quantum key distribution (QKD) schemes that are provably secure in the presence of an arbitrarily powerful eavesdropper. In typical QKD schemes, a key is shared between (and is thus restricted to) two parties [4]. In the past decade, schemes for generating correlated keys shared among multiple parties were developed, namely quantum secret sharing (QSS) protocols [5, 6].

Traditional QSS schemes were developed with multipartite entangled quantum states in mind, such as the Greenburg-Horne-Zeilinger (GHZ) state for three parties [5]. Later, many other schemes emerged including circular QSS [7], dynamic QSS [8, 9], graph state QSS [10, 11], verifiable QSS [12] and QSS based on error correcting QSS [13]. Many of the aforementioned schemes rely on non-local correlations between multiple particles which are difficult to generate and control and cannot yet be transported over appreciable distances.

Interestingly, a new class of QSS schemes involving single photon states has been developed [14] and implemented [15]. Here, the participants each apply a cascade of local unitaries whilst noting the phases they individually impart on the encoded photon. At the end, based on their choice of imparted phase, the validity of the round is checked after which a subset of the participants can distill the secret. This scheme was initially designed for two dimensional states but was shown to be insecure [16, 17]. Recently, a high dimensional variation of the single photon QSS protocol was formalised, where the security loop-holes were addressed [18]. In this protocol, $d$ mutually unbiased bases (MUBs) [19] are used in the generation and detection of the single photon states, making high dimensional photon encoding and the ability to control each dimension separately of vital importance.

The most common candidate for experimental implementation of single photon QSS schemes is based on the polarization of light [20]. However, since polarisation is limited to two dimensions, this implementation restricts scalability. Alternatively, the orbital angular momentum (OAM) degree of freedom of light [21] is an infinite-dimensional Hilbert space and is thus a promising candidate for scalable high dimensional photon encoding processes such as high-dimensional single photon QSS. The OAM of light has also been used to demonstrate the feasibility of high dimensional quantum cryptography [22].

Since, high-dimensional single photon secret sharing has only been demonstrated with at most three dimensions using spatial modes of light [23], here, we outline a proof-of-principle implementation of this scheme with a larger encoding alphabet, utilizing OAM for the basis states and Perfect Vortex (PV) beams as the OAM carriers [24, 25]. Since a toolbox for deterministic measurement in $d$ dimensions of OAM does not (yet) exist, we utilise a probabilistic OAM measurement based on modal decomposition to project the state. We successfully implement 1 round of this scheme for 10 parties in 11 dimensions. This implementation is easily scalable to higher dimensions and an unlimited number of parties.

The $d$-dimensional secret sharing protocol that we use is based on sequential single qudit communication between $N + 1$ participants [18]. Each participant operates locally on the single qudit, mapping it to one of the $d$ vectors in one of the $d$ MUBs:

$$|e_k^{(j)}⟩ = \frac{1}{\sqrt{d}} \sum_{\ell=0}^{d-1} \omega^{(k+j)\ell} |\ell⟩,$$  \hspace{1cm} (1)$$

where $|e_k^{(j)}⟩$ is the $k^{th}$ vector in the $j^{th}$ MUB, $\omega = e^{2\pi i/d}$ and $|\ell⟩$ represents a vector in the computational basis. The possible values of $\ell, j$ and $k$ are integers which lie in the range $[0, d-1]$. It is possible to start with any of the $d^2$ vectors and span the whole $d$-dimensional MUB space.
FIG. 1. Concept behind our proposed $d$-dimensional secret sharing scheme with Perfect Vortex beams. The distributor generates an attenuated field corresponding to $|e_0^{(0)}\rangle$ which comprises $d$ number of PV rings each containing different OAM values. Each participant applies their unitary in the form of ring apertures encoded on phase-only spatial light modulators (or an equivalent optical device). The final participant transmits the qudit state back to the distributor who deterministically measures in the randomly chosen $J^{th}$ MUB, obtaining outcome $a$. If the round is valid, the distributor’s secret can be determined through the collaboration of the remaining participants.

by applying the operators

$$X_d = d \sum_{\ell=0}^{d-1} \omega^\ell |\ell\rangle \langle \ell| ,$$

(2)

$$Y_d = \sum_{\ell=0}^{d-1} \omega^\ell 2 |\ell\rangle \langle \ell| .$$

(3)

In words, $X_d$ maps between vectors inside the same MUB while $Y_d$ maps between corresponding vectors in different MUBs. Mathematically,

$$X_d |e_k^{(j)}\rangle = |e_{k+1}^{(j)}\rangle ,$$

(4)

$$Y_d |e_k^{(j)}\rangle = |e_{k+1}^{(j+1)}\rangle .$$

(5)

Therefore, by repeatedly and sequentially applying both of these operators, we can span the whole $d$-dimensional MUB space,

$$X_d^{x} Y_d^{y} |e_k^{(j)}\rangle = |e_{k+x}^{(j+y)}\rangle ,$$

(6)

where $x, y \in [0, d-1]$ and the indices are modulo $d$.

How does the $d$-dimensional secret sharing scheme work? Suppose that there are $N + 1$ participants and a distributor $R_1$ who desires to share a secret between the $N$ other parties. Firstly, the distributor generates the initial state $|e_0^{(0)}\rangle$ and uniformly samples two random integers $(x_1, y_1)$ from $[0, d-1]$. He/she then locally operates on this qudit state by applying the operator $X_d^{x_1} Y_d^{y_1}$. The distributor then sends this new state $|\psi_{R_1}^d\rangle$ to the next party $R_2$. Similarly, this participant also generates two random integers $(x_2, y_2)$ from $[0, d-1]$ and locally applies $X_d^{x_2} Y_d^{y_2}$ to the received qudit. The resulting state $|\psi_{R_2}^d\rangle$ is sent to the next participant and so on. Once the qudit has been sequentially communicated between all $N$ parties who each apply $X_d^{x_n} Y_d^{y_n}$, the final participant $R_{N+1}$ then sends the qudit back to $R_1$ (the distributor), whereupon the final qudit state is given by,

$$|\psi_{\text{final}}\rangle = X_d^{x_{N+1}} Y_d^{y_{N+1}} \ldots X_d^{x_1} Y_d^{y_1} |e_0^{(0)}\rangle = \frac{1}{\sqrt{d}} (|0\rangle + \sum_{\ell=1}^{d-1} \omega^{\sum_{n=1}^{N+1}(x_n + \ell y_n)} |\ell\rangle) ,$$

(7)

(8)

Now, $R_1$ chooses a random integer $J \in [0, d-1]$ and deterministically measures the qudit in the $J^{th}$ MUB with measurement outcome labelled $a \in \{0,1,\ldots,d-1\}$. In random order, parties $R_2, \ldots, R_{N+1}$ announce their choice of $y_n$ whereupon the distributor announces the validity of the round by checking the criterion:

$$\sum_{n=1}^{N+1} y_n = J \mod d .$$

(9)

This is effectively verifying whether the distributor measured the qudit in the correct MUB. If the round is valid,
of this implementation and give experimental results for measurement. In what follows, we outline the details we instead utilise a probabilistic mode projection-based form of the well-studied Bessel modes and are described as the OAM that they carry [25]. These "special" modes turn out to be the Fourier transform in the field. However, PVs are a set of modes whose field is independent of the OAM that they carry [25].

In this Letter, we propose an experimental implementation of this protocol based on the OAM states of light. The key steps for an experimental implementation lie in the ability to generate the initial qudit state $|e^{(0)}_0\rangle$, sequentially apply the operators $X_d^n Y_d^m$ on the qudit and then deterministically measure the qudit in any of the $d$ MUBs. We’ll show, using Perfect Vortex beams as the OAM carriers, how the initial qudit state can be generated, how the unitaries $X_d, Y_d$ can be created and applied and also how the qudit state transforms after each participant. Since a toolbox for deterministic OAM measurement in $d$ dimensions has yet to be developed, we instead utilise a probabilistic mode projection-based measurement. In what follows, we outline the details of this implementation and give experimental results for $d = 11$ and $N = 9$.

We begin with an overview of Perfect Vortex (PV) beams. Typical vortex modes have a characteristic doughnut shape whose width scales with OAM content; for example, Laguerre-Gaussian modes have a width which scales as $\sqrt{\ell}$ where $\ell$ is the OAM of a single photon in the field. However, PVs are a set of modes whose field is independent of the OAM that they carry [25]. These "special" modes turn out to be the Fourier transform of the well-studied Bessel modes and are described by [24],

$$PV^\ell_R(r, \phi) \propto \exp\left(-\frac{r^2 + R^2}{2T^2}\right) I_\ell\left(\frac{2Rr}{T^2}\right) \exp(i\ell\phi),$$

where $R, T$ is the radius and thickness of the PV ring and $I_\ell(\cdot)$ is the modified Bessel function.

So, why use PVs for secret sharing? The main aspect is that one can generate a field which is a superposition of PVs that all have different radii,

$$U(r, \phi) \propto \sum_{\ell=0}^{d-1} PV^\ell_{R_\ell} \equiv \sum_{\ell=0}^{d-1} |\ell\rangle,$$

where $R_\ell$ is the radius of the $\ell$th PV and the thickness of each PV is effectively constant. Since PV fields are independent of OAM, one can then structure the OAM modes in the superposition in a very convenient way (something which cannot be done with any other set of vortex modes). In particular, the PVs in the superposition can be organised so that each ring is spatially separated from the others. It turns out that if the rings are structured such that the radii of adjacent rings $\Delta R$ satisfies $\Delta R \geq 2T$, then the PVs are sufficiently separated from one another that the OAM modes they carry can be manipulated independently [26]. This is key, since it grants one the ability to apply any unitary operation to the qudit OAM state.

From Eq. [3], it’s apparent that applying the unitary $X_d^n Y_d^m$ is equivalent to applying specific phase shifts to particular OAM modes in the superposition field. As outlined in [26], these inter-modal phase shifts can be applied in a single step through the use of binary ring apertures encoded on phase-only spatial light modulators (SLMs). Hence, by appropriately choosing the phase within each ring aperture, each participant is able to apply the unitary $X_d^n Y_d^m$.

To make the concept concrete, we now outline the steps of this implementation scheme for $d = 3$, which is also shown visually in Fig. 1. The initial state/field is given by,

$$|e^{(0)}_0\rangle = \frac{1}{\sqrt{3}} (|0\rangle + |1\rangle + |2\rangle),$$

$$\propto PV^{R_0}_{R_0} + PV^{R_1}_{R_1} + PV^{R_2}_{R_2},$$

where $R_\ell = R_0 + 3\ell T$. This superposition means that the OAM modes are ordered sequentially in an increasing
FIG. 3. Results for 10 participant, $d = 11$ dimensional secret sharing with PV beams. Vectors in each MUB are mutually orthogonal which allows one to immediately discern the qudit’s state. Vectors in different MUBs have an overlap of $1/\sqrt{d}$. The inter-modal phases are shown below the projection matrices; the dark lines represent the theoretical phases corresponding to the qudit state in $|e_i\rangle$. 

manner from the innermost ring and the ring spacing is $\Delta R = 3\ell$. One can arrange the modes in any desired order, but this choice is the most convenient. The unitary operations $X_3$ and $Y_3$ correspond to,

$$X_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^{-1} \end{pmatrix},$$  \hspace{1cm} (15)$$

$$Y_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega \end{pmatrix}.$$  \hspace{1cm} (16)$$

where $\omega = \exp(2\pi i/3)$. For randomly drawn integers $(x_n, y_n)$, the unitary $X_3^{x_n}Y_3^{y_n}$ corresponds to the phase map (modulo $2\pi$),

$$\Phi = \omega(x_n + y_n)B_{\Delta R}(R_1) + \omega(y_n - x_n)B_{\Delta R}(R_2),$$  \hspace{1cm} (17)$$

where $B_{\Delta R}(R_i)$ is the boxcar function centred at $R_i$ and having width $\Delta R$. This phase map is displayed directly onto a SLM to implement the desired unitary, as shown in Fig. 1.

The qudit state is transmitted from participant to participant, who each apply their unitary. Finally, the distributor performs a deterministic measurement in a randomly chosen MUB using some (as yet undeveloped) OAM-MUB mode sorter optic. Once the measurement is performed, shown in Fig. 1 as a projection matrix where each element is a state in the $d^2$ MUB state space, the classical post processing steps then follow as usual.

The PV field, states, MUBs and unitaries extend analogously for $d = 11$. A schematic of the experimental setup used to implement the scheme for 10 participants is shown in Fig. 2. The first SLM was used to generate the field corresponding to the $|e_0\rangle$ state from an expanded and collimated He-Ne laser beam. The unitaries (phase maps) of each participant were applied in sequence, whereupon the final state was measured using an optical inner product. To ensure consistency, we use two different methods of measuring the state: a projection matrix approach and a modal decomposition approach. We resorted to probabilistic/statistical measurements since there does not yet exist a toolbox for deterministic measurement of OAM-MUBs for arbitrary dimension $d$. Each element of the projection matrices corresponds to performing the optical overlap between the MUB vector $|e_i\rangle$ and the shared qudit state. The modal decomposition corresponds to the overlap between the qudit state and the two superposition states $|0\rangle + |\ell\rangle$ and $|0\rangle + i|\ell\rangle$. Performing these two optical overlaps is known to be sufficient for determining the inter-modal phase between $|0\rangle$ and $|\ell\rangle$ [27] and is now also known to be effective for PV beams [28]. The projection matrix route of reconstructing the state requires $d^2$ measurements, whilst the modal decomposition route requires $2d - 1$ measurements. The experimental results for 1 round of QSS are summarised in Fig. 3; we performed a state measurement after each participant to show the evolution of the qudit state. We can read off the final state from the final projection matrix, whereupon we see that the round is valid provided $J = 3$. In this case, the distributor’s measurement outcome is $a = 6$ and so the shared secret is $x_1 - a = 4$.

Extending the scheme to any dimension is straightforward: add more rings. In principle, the limitation when utilising SLMs is the number of PV rings that can fit onto the screen. Making the rings thinner would allow one to pack more rings onto the SLM. However, it turns out that
the optical system’s numerical aperture limits how thin the PV rings can be made. Since PVs are the Fourier transform of Bessel beams, these fields are not propagation invariant. This means that PVs have to be relayed from plane to plane using an imaging system. The thickness of the PV is inversely related to the width of the Bessel beam since
\[ T = \frac{2f}{kw_0} \]
where \( w_0 \) is the Gaussian width of the Bessel-Gaussian beam. Hence, making the rings thinner causes the corresponding Bessel beam to be larger and there will come a point where the optical system will not be able to collect all the necessary light.

In summary, we proposed a scalable implementation of a high dimensional quantum secret sharing protocol which utilises MUB states of single photons carrying OAM. We confirmed the efficacy of our scheme in a proof-of-principle experiment in 11-dimensions with 10 participants using probabilistic state measurement. Since the protocol relies on a deterministic measurement of the photon’s qudit state, future work should investigate the development of a toolbox to achieve this with MUBs of OAM.

---

[1] W. K. Wootters and W. H. Zurek, Nature 299, 802 (1982).
[2] M. Redhead and L. E. Ballentine, American Journal of Physics 57 (1987).
[3] W. Heisenberg, in Original Scientific Papers Wissenschaftliche Originalarbeiten (Springer, 1985) pp. 478–504.
[4] C. H. Bennett and G. Brassard, Theor. Comput. Sci. 560, 7 (2014).
[5] M. Hillery, V. Bužek, and A. Berthiaume, Physical Review A 59, 1829 (1999).
[6] A. Karlsson, M. Koashi, and N. Imoto, Physical Review A 59, 162 (1999).
[7] F.-G. Deng, H.-Y. Zhou, and G. L. Long, Journal of Physics A: Mathematical and General 39, 14089 (2006).
[8] H.-Y. Jia, Q.-Y. Wen, F. Gao, S.-J. Qin, and F.-Z. Guo, Physics Letters A 376, 1035 (2012).
[9] J.-L. Hsu, S.-K. Chong, T. Hwang, and C.-W. Tsai, Quantum Information Processing 12, 331 (2013).
[10] D. Markham and B. C. Sanders, Physical Review A 78, 042309 (2008).
[11] B. Bell, D. Markham, D. Herrera-Martí, A. Marin, W. Wadsworth, J. Rarity, and M. Tame, Nature communications 5, 5480 (2014).
[12] Y.-G. Yang, Y.-W. Teng, H.-P. Chai, and Q.-Y. Wen, International Journal of Theoretical Physics 50, 792 (2011).
[13] Z. Zu-Rong, L. Wei-Tao, and L. Cheng-Zu, Chinese Physics B 20, 050309 (2011).
[14] G.-P. Guo and G.-C. Guo, Physics Letters A 310, 247 (2003).
[15] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Żukowski, and H. Weinfurter, Physical review letters 95, 230505 (2005).
[16] G. P. He, Physical review letters 98, 028901 (2007).
[17] S.-J. Qin, F. Gao, Q.-Y. Wen, and F.-C. Zhu, Optics Communications 281, 5472 (2008).
[18] A. Tavakoli, I. Herbauts, M. Żukowski, and M. Bourennane, Physical Review A 92, 030302 (2015).
[19] T. Durt, B.-G. Englert, I. Bengtsson, and K. Życzkowski, International journal of quantum information 8, 535 (2010).
[20] F.-G. Deng, H.-Y. Zhou, and G. L. Long, Physics Letters A 337, 329 (2005).
[21] A. M. Yao and M. J. Padgett, Advances in Optics and Photonics 3, 161 (2011).
[22] M. Mafu, A. Dudley, S. Goyal, D. Giovannini, M. McLaren, M. J. Padgett, T. Konrad, F. Petruccione, N. Lütkenhaus, and A. Forbes, Phys. Rev. A 88, 032305 (2013).
[23] M. Smiaia, A. M. Elhassan, A. Tavakoli, and M. Bourennane, Npj Quantum Information 2, 16010 (2016).
[24] P. Vaity and L. Rusch, Optics letters 40, 597 (2015).
[25] A. S. Ostrovsky, C. Rickenstorff-Parrao, and V. Arrizón, Optics letters 38, 534 (2013).
[26] J. Pinnell, V. Rodriguez-Fajardo, and A. Forbes, arXiv e-prints, arXiv:1907.08878 (2019), arXiv:1907.08878.
[27] A. Forbes, A. Dudley, and M. McLaren, Advances in Optics and Photonics 8, 200 (2016).
[28] J. Pinnell, V. Rodriguez-Fajardo, and A. Forbes, Opt. Lett. 44, 2736 (2019).