Quantum-key distribution with vector modes

Ndagano, B., Nape, I., Perez-Garcia, B., Scholes, S., Hernandez-Aranda, R., et al.

B. Ndagano, I. Nape, B. Perez-Garcia, S. Scholes, R. I. Hernandez-Aranda, F. S. Roux, T. Konrad, A. Forbes, "Quantum-key distribution with vector modes," Proc. SPIE 10120, Complex Light and Optical Forces XI, 101200X (27 February 2017); doi: 10.1117/12.2251465

SPIE.

Event: SPIE OPTO, 2017, San Francisco, California, United States

Quantum-key distribution with vector modes

Ndagano B.[a], Nape I.[a], Perez-Garcia B.[a,b], Scholes S.[a], Hernandez-Aranda R.I.[b], Roux F.S.[c], Konrad T.[d], and Forbes A.[a]

[a]School of Physics, University of the Witwatersrand, Private Bag 3, Wits 2050, South Africa
[b]Photonics and Mathematical Optics Group, Tecnológico de Monterrey, Monterrey 64849, Mexico
[c]National Metrology Institute of South Africa, Meiring Naude Road, Pretoria, South Africa
[d]College of Chemistry and Physics, University of KwaZulu-Natal, Private Bag X54001, Durban 4000, South Africa

ABSTRACT

High-dimensional encoding using higher degrees of freedom has become topical in quantum communication protocols. When taking advantage of entanglement correlations, the state space can be made even larger. Here, we exploit the entanglement between two dimensional space and polarization qubits, to realize a four-dimensional quantum key distribution protocol. This is achieved by using entangled states as a basis, analogous to the Bell basis, rather than typically encoding information on individual qubits. The encoding and decoding in the required complementary bases is achieved by manipulating the Pancharatnam-Berry phase with a single optical element: a q-plate. Our scheme shows a transmission fidelity of 0.98 and secret key rate of 0.9 bits per photon. While the use of only static elements is preferable, we show that the low secret key rate is a consequence of the filter based detection of the modes, rather than our choice of encoding modes.

Keywords: quantum key distribution, vector modes, entanglement

1. INTRODUCTION

Unlike traditional (classical) cryptography based on numerical acrobatics, quantum cryptography relies solely on the counter-intuitive properties of quantum particles. Quantum key distribution (QKD) is a realization of quantum cryptography[1,2] , whereby a secret key is generated between two parties (Alice and Bob), and subsequently used to encrypt data. In the optical world, QKD is traditionally implemented with quantum bits (qubits), encoded onto the polarization of photons[3–5] ; that is because polarization is well understood, can easily be manipulated with standard optics, and is immune to atmospheric turbulence, making ideal for fiber and free-space communication. However, the two-dimensional polarization DoF fundamental limits the secret key rate in QKD protocol; the upper bound, imposed by the Shannon limit[6] in such protocols is only $\log_2 d = 1$ bit per-photon, where $d = 2$ is the dimension. The next step in terms of secret key rate and security requires a different approach that employs higher-dimensional photonic DoFs[7,8] .

Spatial modes of light, particularly those carrying orbital angular momentum (OAM) have emerged as the candidate of choice to realize high-dimensional QKD[9–11] : The OAM space is infinite dimensional, it is quantized at the single photon level[12] , and can easily be measured with digital holograms[13] . Alternatively, it is possible to construct a higher dimensional space by combining the internal degrees of freedom of the photons. Recently, we have considered non-separable states known as vector modes for classical and quantum studies.[14–18] For example, in vector OAM modes[19] , the OAM and polarization DoFs are couple in a manner reminiscent of entanglement in quantum mechanics: a measurement on the polarization determines the observed spatial field and vice versa. Classically, it has been shown that by exploiting this non-separability, it is possible to realize high-dimensional encoding with vector modes[20,21] .

Further author information: (Send correspondence to A.F.)
A.F.: E-mail: andrew.forbes@wits.ac.za, Telephone: +27 11 717 6885

Complex Light and Optical Forces XI, edited by David L. Andrews, Enrique J. Galvez, Jesper Glückstad, Proc. of SPIE Vol. 10120, 101200X · © 2017 SPIE
CCC code: 0277-786X/17/$18 · doi: 10.1117/12.2251465

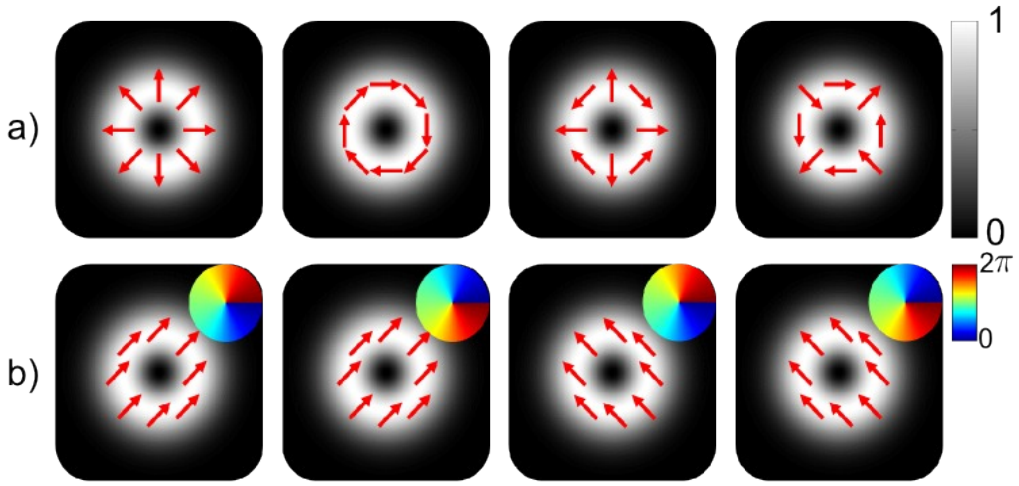

Figure 1. Alice randomly prepares her photon in one of two complementary bases: (a) the vector basis or (b) the scalar basis. The insets in (b) show the phase profile of the scalar OAM modes

Here, we use the non-separability of vector OAM modes to realize a four dimensional QKD protocol. By manipulating the Panchanratnam-Berry phase with a single optical element, we demonstrate a high-dimensional encoding/decoding in the vector mode basis and a complementary scalar basis (modes with uniform polarization). Using our scheme, we realized a detection fidelity of as high as 98% and an error rate of 2%. We however acknowledge that our filter-based detection scheme does not allow us to take full advantage of the high-dimensional space. This is reflected in a reduction of the secret key rate for a two-basis protocol by a factor of 2 to 0.9 bits per photon.

2. RESULTS

Consider a quantum link in which Alice transmits information to Bob using single photons, randomly prepared, on one hand, in a given state $|\psi\rangle_\ell^\theta$ in the vector mode basis, defined as follows

$$|\psi\rangle_\ell^\theta = \frac{1}{\sqrt{2}}(|R\rangle\,|\ell\rangle + \exp(i\theta)\,|L\rangle\,|-\ell\rangle), \tag{1}$$

where $\ell\hbar$ is the quantized OAM carried by the photons, $|R\rangle$ and $|L\rangle$ are the right and left circular polarization eigenstates and $\theta = [0, \pi]$ is the intra-modal phase. For a given $|\ell|$ OAM subspace, there exist four orthogonal vector modes, defined as in Eq. 1, that form a basis for the subspace. Instead of using vector modes as carriers because of their rotation invariance[22,23] , here, we use the full vector mode space to achieve higher-dimensional encoding. As an example, we use vector modes from the $|\ell| = 1$ OAM subspace, shown in Fig. 1(a). Analogous to the Bell basis, each state in the vector basis can be produced by transforming any given vector mode with single qubit unitary operations, acting on either the polarization or the spatial degree of freedom.

On the other hand, Alice prepares her photon in a complementary basis $\{|\phi\rangle_\ell^\theta\}$, represented as follows

$$|\phi\rangle_\ell^\theta = \frac{1}{\sqrt{2}}\left[|R\rangle + \exp\left(i\left(\theta - \frac{\pi}{2}\right)\right)|L\rangle\right]|\ell\rangle\,, \tag{2}$$

such that $|\langle\phi|\psi\rangle| = 1/\sqrt{d}$, where d is the dimension of the two bases. The elements of this complementary basis, shown in Fig. 1(b) for the $|\ell| = 1$ OAM subspace, are scalar modes; that is, the electric field is uniformly polarized across the transverse plane.

Both vector and scalar modes were generated using geometric phase manipulation with wave-plates and a q-plate that couples the polarization and the OAM DoFs[24,25] . The q-plate transformation are summarized as

follows:

$$|\ell, L\rangle \rightarrow |\ell + 2q, R\rangle\,, \tag{3}$$
$$|\ell, R\rangle \rightarrow |\ell - 2q, L\rangle\,, \tag{4}$$

where q is the charge of the q-plate, and is such that $2q = \ell'$. A summary of the generation process is shown in Table 1.

Table 1. Generation of vector and scalar modes using q-plates and wave plates. The angles quoted are that of the fast axis of the wave plate with respect to the horizintally polarized input Gaussian beam.

Vector	$\lambda/2(\theta_1)$	q-plate	$\lambda/2(\theta_2)$
$\|\psi\rangle_{\ell}^{0}$	0	$\|q\|$	–
$\|\psi\rangle_{\ell}^{\pi}$	$\pi/4$	$\|q\|$	–
$\|\psi\rangle_{-\ell}^{0}$	–	$\|q\|$	0
$\|\psi\rangle_{-\ell}^{\pi}$	–	$\|q\|$	$\pi/4$

Scalar	$\lambda/4(\alpha_1)$	q-plate	$\lambda/4(\alpha_2)$	$\lambda/2(\theta_2)$
$\|\phi\rangle_{\ell,0}$	$-\pi/4$	$\|q\|$	$-\pi/4$	$\pi/4$
$\|\phi\rangle_{\ell,\pi}$	$-\pi/4$	$\|q\|$	$-\pi/4$	$-\pi/4$
$\|\phi\rangle_{-\ell,0}$	$\pi/4$	$\|q\|$	$\pi/4$	$\pi/4$
$\|\phi\rangle_{-\ell,\pi}$	$\pi/4$	$\|q\|$	$\pi/4$	$-\pi/4$

At the receiver's end, Bob randomly makes a measurement in either the scalar of vector basis as shown in Fig.2. The randomness of the choice is implemented using a beam splitter, ensuring that the probability of the photon exiting on either port of the beam splitter is 1/2. To implement the filter based detection, we used the generation process depicted in Table 1 in reverse. However, with this approach, it is not possible to measure simultaneously all the basis elements. We thus implement an additional randomization to detect two modes at the time within each basis. This however comes at the cost of having a null detection half the time.

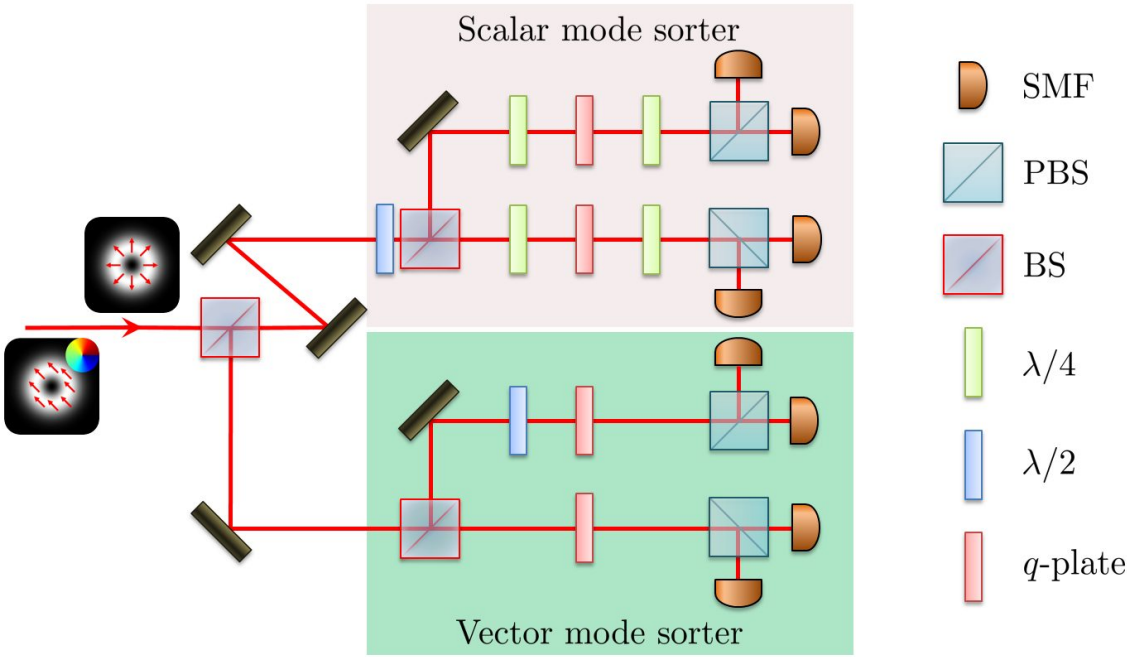

Figure 2. Measurement of vector and scalar modes. The input mode is directed to either a scalar or a vector mode sorterm using a 50:50 beam splitter (BS). Within each sorter, the input mode is again sent through 2 different paths with an additional BS, in which the projections on two scalar or vector modes at the time is performed using quarter- ($\lambda/4$) and half-wave ($\lambda/2$) plates, a q-plate, a polarizing beam splitter (PBS) and a single mode fiber (SMF).

Using the setup in Fig. 2, we measured a detection fidelity $F = 0.98$, and computed the error rate $Q = 1 - F = 0.02$ and the secret key rate as follows[8] :

$$R = \frac{1}{2}\left[\log_2(d) + 2F\log_2(F) + 2(1-F)\log_2\left(\frac{1-F}{d-1}\right)\right]. \quad (5)$$

Note that the factor of 1/2 arise due to the photon loss that is inherent to the detection scheme. We thus obtained a secret key rate of 0.9 bits per photon. To implement this approach, one would have to add additional step to the sifting process. For example, consider the BB84 protocol[1] where Alice sends random sequences of bits (modes) to Bob, who randomly measures in the scalar or the vector basis. If Bob uses the filter based method, he would need to record which bases he used, as well as which two modes were probed within a given basis. During the sifting process, Alice and Bob would discard, on one hand, data for which the encoding and decoding basis do not match (as is normally done), and, on the other hand, the data for which the wrong two modes were probed within a basis. If Alice prepares vector mode "1" and Bob measures in the scalar basis, the measurement is discarded. Similarly, suppose Bob can only measure vector modes "1"&"2" and "3"&"4" simultaneously. If Bob measures vector modes "3"&"4", the measurement is also discarded. Bob thus makes a valid measurement 25% of the time as opposed to 50% of the time, doubling the time it takes to generate a key.

3. DISCUSSION AND CONCLUSION

We have demonstrated a high dimensional QKD scheme that uses both scalar and vector OAM modes. We have shown that through geometric phase manipulation using wave plates and q-plates, it is possible to generate and detect all vector and scalar modes within a given OAM subspace. However, there are limitations to the method; of the four vector and scalar modes that exist within a given OAM space, one can only measure two modes simultaneously. This filter based methods has major consequences on the efficiency of the protocol; namely, it reduces the key rate by a factor of 2. We thus conclude that using a filter based detection to probe high dimensional spaces in QKD protocols is a hindrance to the benefits of increased dimensionality. A way forward is to devise a detection scheme based on mappings rather than projection as in Ref[11] , where OAM modes are mapped to positions using a mode sorter, allowing Mirhosseini *et al.* to realise a 7-dimensional QKD protocol.

REFERENCES

[1] Bennett, C. H. and Brassard, G., "Quantum cryptography: Public key distribution and coin tossing," *Proc. IEEE Int. Conf. on Computers Systems, and Signal Processing (Bangalore)* **1**, 175–179 (1984).

[2] Ekert, A., "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.* **67**, 661–663 (1991).

[3] Jennewein, T., Simon, C., Weihs, G., Weinfurter, H., and Zeilinger, A., "Quantum cryptography with entangled photons thomas," *Phys. Rev. Lett.* **84**, 4729–4732 (1991).

[4] Peng, C. Z., Zhang, J., Yang, D., Gao, W. B., Ma, H. X., Yin, H., Zeng, H. P., Yang, T., Wang, X. B., and Pan, J. W., "Experimental long-distance decoy-state quantum key distribution based on polarization encoding," *Phys. Rev. Lett.* **98**, 010505 (2007).

[5] Poppe, A., Fedrizzi, A., Ursin, R., Böhm, H. R., Lörunser, T., Maurhardt, O., Peev, M., Suda, M., Kurtsiefer, C., Weinfurter, H., Jennewein, T., and Zeilinger, A., "Practical quantum key distribution with polarization entangled photons," *Opt. Express* **12**, 3865–3871 (2004).

[6] Shannon, C. E., "Experimental long-distance decoy-state quantum key distribution based on polarization encoding," *ACM SIGMOBILE Mobile Computing and Communications Review* **5**, 3–55 (2001).

[7] Bechmann-Pasquinucci, H. and Tittel, W., "Quantum cryptography using larger alphabets," *Phys. Rev. A* **61**, 062308 (2000).

[8] Cerf, N. J., Bourennane, M., Karlsson, A., and Gisin, N., "Security of quantum key distribution using d-level systems," *Phys. Rev. Lett.* **88**, 127902 (2002).

[9] Gröblacher, S., Jennewein, T., Vaziri, A., Weihs, G., and Zeilinger, A., "Experimental quantum cryptography with qutrits," *New J. Phys* **8**, 75 (2006).

[10] Mafu, M., Dudley, A., Goyal, S., Giovannini, D., McLaren, M., Padgett, M. J., Konrad, T., Petruccione, F., Lütkenhaus, N., and Forbes, A., "Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases," *Phys. Rev. A* **88**, 032305 (2013).

[11] Mirhosseini, M., Magaña-Loaiza, O. S., O'Sullivan, M. N., Rodenburg, B., Malik, M., Lavery, M. P., Padgett, M. J., Gauthier, D. J., and Boyd, R. W., "High-dimensional quantum cryptography with twisted light," *New J. Phys.* **17**, 033033 (2015).

[12] Mair, A., Vaziri, A., Weihs, G., and Zeilinger, A., "Entanglement of the orbital angular momentum states of photons.," *Nat.* **412**, 313–316 (2001).

[13] Forbes, A., Dudley, A., and McLaren, M., "Creation and detection of optical modes with spatial light modulators," *Adv. Opt. Phot.* **8**, 200–227 (2016).

[14] McLaren, M., Konrad, T., and Forbes, A., "Measuring the nonseparability of vector vortex beams," *Phys. Rev. A* **92**, 023833 (2015).

[15] Ndagano, B., Brüning, R., McLaren, M., Duparré, M., and Forbes, A., "Fiber propagation of vector modes," *Opt. Express* **23**, 17330–17336 (2015).

[16] Ndagano, B., Perez-Garcia, B., Roux, F. S., McLaren, M., Rosales-Guzmán, C., Zhang, Y., Mouane, O., Hernandez-Aranda, R. I., Konrad, T., and Forbes, A., "Process tomography of quantum channels using classical light," *arXiv:1605.05144* (2016).

[17] Cox, M. A., Rosales-Guzman, C., Lavery, M. P. J., Versfeld, D. J., and Forbes, A., "On the resilience of scalar and vector vortex modes in turbulence," *Opt. Express* **24**, 18105–18113 (2016).

[18] Nape, I., Ndagano, B., Perez-Garcia, B., Scholes, S., Hernandez-Aranda, R. I., Konrad, T., and Forbes, A., "High-bit-rate quantum key distribution with entangled internal degrees of freedom of photons," *arXiv:1605.05144* (2016).

[19] Zhan, Q., "Cylindrical vector beams: from mathematical concepts to applications," *Adv. Opt. Phot.* **1**, 1–57 (2009).

[20] Milione, G., Nguyen, T. A., Leach, J., Nolan, D. A., and Alfano, R. R., "Using the nonseparability of vector beams to encode information for optical communication," *Opt. Lett.* **40**, 4887–4890 (2015).

[21] Li, P., Wang, B., and Zhang, X., "High-dimensional encoding based on classical nonseparability," *Opt. Express* **24**, 15143–15159 (2016).

[22] Souza, C., Borges, C., Khoury, A., Huguenin, J., Aolita, L., and Walborn, S., "Quantum key distribution without a shared reference frame," *Phys. Rev. A* **77**, 032345 (2008).

[23] Vallone, G., DAmbrosio, V., Sponselli, A., Slussarenko, S., Marrucci, L., Sciarrino, F., and Villoresi, P., "Free-space quantum key distribution by rotation-invariant twisted photons," *Phys. Rev. Lett.* **113**, 060503 (2014).

[24] Marrucci, L., Manzo, C., and Paparo, D., "Optical spin-to-orbital angular momentum conversion in inhomogeneous anisotropic media," *Phys. Rev. Lett.* **96**, 163905 (2006).

[25] Marrucci, L., Karimi, E., Slussarenko, S., Piccirillo, B., Santamato, E., Nagali, E., and Sciarrino, F., "Spin-to-orbital conversion of the angular momentum of light and its classical and quantum applications," *J. Opt.* **13**, 064001 (2011).