High-dimensional fiber based quantum key distribution with twisted photons

Bacco, Davide; Cozzolino, Daniele; da Lio, Beatrice; Ingerslev, Kasper; Ding, Yunhong; Dalgaard, Kjeld; Kristensen, Poul; Galili, Michael; Rottwitt, Karsten; Ramachandran, Siddharth

Published in:
Proceedings of 8th International Conference on Quantum Cryptography

Publication date:
2018

Document Version
Peer reviewed version

Citation (APA):
High-dimensional fiber based quantum key distribution with twisted photons

Davide Bacco, Daniele Cozzolino, Beatrice Da Lio, Kasper Ingerslev, Yunhong Ding, Kjeld Dalgaard, Poul Kristensen, Michael Galili, Karsten Rottwitt, Siddharth Ramachandran, Leif Katsuo Oxenløwe

1 CoE SPOC, DTU Fotonik, Dep. Photonics Eng., Technical University of Denmark, Orsted Plads 340, Kgs. Lyngby, 2800 Denmark
2 OFS-Fitel, Priorparken 680, DK-2605, Broendby, Denmark
3 Electrical and Computer Engineering Department, Boston University, 8 St Mary’s St, Boston, MA, USA

Emails: †dabac@fotonik.dtu.dk; *dacoz@fotonik.dtu.dk

Introduction
Quantum key distribution (QKD), a branch of Quantum Communications (QCs), provides ultimate security based on quantum mechanics laws [1, 2]. Essential challenges of most QKD systems are the relatively short propagation distances and the low transmittable bit rates. A fundamental way to overcome these issues is represented by high-dimensional (HiD) quantum states, which allow increased information capacity and higher robustness against channel noise. This higher information efficiency has the benefit of increasing the robustness to channel noise, resulting in an increased error threshold [3–5]. The generation, transmission and detection of high-dimensional quantum states is very challenging and only a few experimental realizations have been achieved for Hi-D QC protocols [6, 12]. Using the orbital angular momentum (OAM) of light is promising, as it provides a natural discrete Hi-D basis for quantum states [13]. However, OAM fiber transmission with more than two modes has only been used for classical communication so far [14]. We experimentally demonstrate the first transmission of Hi-D quantum states, encoded in four OAM modes and their superposition, over a 1.2 km long OAM fiber, by implementing a real-time decoy-state Hi-D QKD protocol, demonstrating the highest secret key rate and the longest transmission distance presented to date [15].

Generation, transmission and detection of the OAM quantum states
High-dimensional quantum states are suitable for longer transmission distance and higher secret key rate transmission, being more robust to noise level and allowing a higher channel capacity [3]. In Figure[1](a) we report the setup of the Hi-D decoy-state quantum communication protocol based on the spatial degree of freedom (OAM modes). Weak coherent pulses are polarization modulated through a phase modulator (PM) and subsequently vortex plates allow for the spin-orbit coupling. The quantum states are coupled to the fiber that enables conservation of orbital angular momentum modes (about 1dB/km losses). Due to different mode group velocities in the air-core fiber, a free-space delay (about 4.5 m) is implemented before coupling the weak pulses to the fiber. This delay is required in order to pre-compensate the different time-of-arrivals of the modes with \( \ell = 6 \) and \( \ell = 7 \). To detect the OAM quantum states the receiver (Bob) implements projective measurements to recover the encoded information. An OAM mode sorter is used to separate even and odd modes, in our case \( \ell = 6 \) and \( \ell = 7 \). The implemented mode sorter is a free-space MZI with two Dove prisms with a relative angle of 90° [16]. After the sorting process, the photons are converted back to the fundamental Gaussian mode with two other vortex plates and then conveniently separated according to their polarization. In particular, to measure the basis \( \mathcal{M}_0 \), half-waveplates (HWPs), quarter-waveplates (QWPs) and two polarization beam-splitters (PBSs) are adopted in the two arms of the sorter. In the case of \( \mathcal{M}_1 \), a free-space MZI is required to measure the relative phase difference between the OAM modes. The photons are then detected by four InGaAs single photon detectors and registered by a time-tagger unit. The insertion loss attributed to Bob’s detection system is measured to be 9 dB in receiver \(|\psi_i\rangle\) and 10 dB in receiver \(|\phi_j\rangle\) (from the output of the OAM fiber to the input of the detectors).

Results
In order to characterize the system, a quantum state tomography technique is implemented for dimension \( D = 2 \) and \( D = 4 \). Figure[2] shows the two matrices for the two cases, measured with weak laser pulses and mean photon number \( \mu = (9.9 \pm 0.2) \times 10^{-3} \) for 1.2 km. Using the definition of fidelity \( F(p, q) = \sum_i (p_i q_i)^{1/2} \), where \( p \) (q) is a
Fig. 1 a) Setup of the experiment. Fast Mach-Zehnder Interferometer (MZI) switches, controlled by a field programmable gate array (FPGA), allow the real-time preparation of the MUBs $\mathcal{M}_0$ and $\mathcal{M}_1$. Only a single MZI is required to separately generate the two bases (dashed edges MZI). Note that, within each basis, the states are prepared in real-time mode. At the input of the MZI, we inject attenuated pulses, carved out of a continuous wave (CW) laser beam at 1550 nm by an intensity modulator (IM). A second IM is used to implement a three-intensities decoy-state technique for the QKD protocols. A variable optical attenuator (VOA) allows for reaching the quantum regime. The polarization of the modulator (IM) driven by the same FPGA. A second IM is used to implement a three-intensities decoy-state technique for the QKD protocols. A variable optical attenuator (VOA) allows for reaching the quantum regime. The polarization of the modulator (IM) driven by the same FPGA.

Fig. 2 a) Tomography measurement for 2 D. Average fidelity measurement for 2 minutes is 0.980 ± 0.002. Here the quantum states are defined as $|\xi_1\rangle = |\psi_2\rangle + |\psi_4\rangle$ and $|\xi_2\rangle = |\psi_2\rangle - |\psi_4\rangle$. b) Tomography measurement for 4 D. The average fidelity measured over 5 minutes is 0.954 ± 0.004. The measurements were acquired with a mean photon number value of $\mu = (9.9 \pm 0.2) \times 10^{-3}$. c) Secret key rate as a function of the channel losses. The first blue circle represents the rate measured after transmission through the 1.2 km fiber (37.43 kbit/s for 4D and 21.81 kbit/s for 2D), while the others are obtained by adding further channel losses with a VOA.

Following the standard authentication process between Alice and Bob, Alice randomly switches between the two MUBs and modulates the secret key on the different states (two or four, depending on the dimension). Usually, one of the two bases provides the key and the other monitors the presence of an eavesdropper. After the transmission through the OAM-fiber, Bob decides in which of the two bases to project the quantum states. Photons measured in the wrong basis will be discarded during the sifting procedure. The protocol implemented can be considered as a BB84 with a three-intensities decoy-state method ($\mu, \nu, \omega$) with dimensions $D = 2$ and $D = 4$. In Figure 2c we show the experimental secret key rate for $D = 2$ and $D = 4$ as a function of the channel loss. The first blue and first red circles are the experimental data measured after the propagation through 1.2 km fiber for 4D and 2D respectively. The following red and blue circles are measured data obtained by adding further channel loss with discrete probability distribution with elements $p_i$ ($q_i$), we measure in average $F = 0.980 \pm 0.002$ for the qubit (D=2) and $F = 0.954 \pm 0.004$ in the ququart case. To demonstrate the usefulness of quantum communication through the air-core fiber using OAM states, we implement real-time 2D and 4D quantum key distribution protocols [2][17].

Mutually Unbiased Bases

$\mathcal{M}_0 = \begin{pmatrix} |R, +6\rangle & |L, -6\rangle \\ |R, +7\rangle & |L, -7\rangle \end{pmatrix}$

$\mathcal{M}_1 = \frac{1}{2} \begin{pmatrix} |R, +6\rangle + |L, -6\rangle + |R, +7\rangle - |L, -7\rangle \\ |R, +6\rangle - |L, -6\rangle - |R, +7\rangle + |L, -7\rangle \end{pmatrix}$

The first red circle represents the rate measured after transmission through the 1.2 km fiber (37.43 kbit/s for 4D and 21.81 kbit/s for 2D), while the others are obtained by adding further channel losses with a VOA.
a VOA. The experimental data fit the theoretical prediction (dashed lines), showing that the secret key extraction would be guaranteed by our protocol over a distance of \( \sim 14 \) km, with a secret key rate of 0.78 kbit/s and 0.40 kbit/s, for the 2D and 4D case respectively. We measure an average QBER of 6.7% for the states \( |\psi_2\rangle \) and \( |\psi_4\rangle \), and 7.9% for \( |\zeta_1\rangle \) and \( |\zeta_2\rangle \). Furthermore, in the case of high-dimensional encoding a QBER of 14.1% in the \( M_0 \) basis and 18.1% in \( M_1 \) is measured. The QBER values are obtained over \( \sim 7 \) minutes of measurement time and these values are below the individual and collective attack thresholds [15]. Positive secret key rates of 21.81 kbit/s (\( D = 2 \)) and 37.43 kbit/s (\( D = 4 \)) are obtained after the 1.2 km fiber. An enhancement of 71% in the final key rate is achieved by using high-dimensional encoding.

**Conclusion** In this work, we propose and demonstrate the use of twisted photons for fiber based high-dimensional quantum communication. We successfully prove the principle by sending two- and four-dimensional MUBs through 1.2 km of a special air-core fiber. These results represent a key point for the development of distributed quantum applications, proving that fiber based spatial modes protocols can be used for quantum communications.

**Funding** This work is supported by the Center of Excellence, SPOC-Silicon Photonics for Optical Communications (ref DNRF123), by the People Programme (Marie Curie Actions) of the European Union’s Seventh Framework Programme (FP7/2007-2013) under REA grant agreement n° 609405 (COFUNDPostdocDTU) and by the Office of Naval Research MURI program (N00014-13-1-0627) and the National Science Foundation (ECCS-1610190).

**References**