Two-dimensional quantum key distribution (QKD) protocol for increased key rate fiber-based quantum communications

da Lio, Beatrice; Bacco, Davide; Ding, Yunhong; Cozzolino, Daniele; Dalgaard, Kjeld; Rottwitt, Karsten; Oxenløwe, Leif Katsuo

Published in:
2017 European Conference on Optical Communication (ECOC)

Link to article, DOI:
10.1109/ECOC.2017.8346242

Publication date:
2017

Document Version
Peer reviewed version

Two-dimensional quantum key distribution (QKD) protocol for increased key rate fiber-based quantum communications

B. Da Lio , D. Bacco *, Y. Ding , D. Cozzolino , K. Dalgaard , K. Rottwitt , L. K. Oxenløwe

Department of Photonics Engineering, Technical University of Denmark, 2800 Kgs. Lyngby, Denmark.,
* dabac@fotonik.dtu.dk

Abstract *We experimentally prove a novel two-dimensional QKD scheme, relying on differential phase-time shifting (DPTS) of strongly attenuated weak coherent pulses. We demonstrate QKD transmission up to* 170 *km standard fiber, and even include a classical channel up to* 90 *km.*

Introduction

Security of public and personal data is becoming increasingly important. Classical cryptography, based on mathematical assumptions, cannot guarantee unconditional security[1]. In contrast, Quantum Cryptography based on fundamental laws of quantum physics holds the promise to do just that[2]. Although commercial QKD systems are available today, a complete deployment of this technology is far from being achieved. Limitations in terms of reachable link distance, secret key rate and tolerable bit error rate, are some essential factors which restrict the performance of quantum communication systems[3–5]. Increasing the modulation dimensionality for QKD systems allows for increased secure key rates and potentially longer transmission distances. High-dimensional (HD) quantum communication protocols essentially imprints more than a single bit per photon (or attenuated pulse), much like classical higher-order modulation formats do on classical pulses. As already demonstrated HD-QKD protocols enable higher quantum bit error rate (QBER) threshold compared to conventional ones[6,7]. This feature can be directly translated into a better noise resistance (lower level of OSNR can be tolerated) and thus in longer transmission links. Here, we experimentally realize a new two-dimensional distributed phase-time reference QKD protocol, in which the information is encoded in the time-position within a subslot and the relative phase of weak coherent pulses (WCPs) in adjacent subslots[8]. We demonstrate the robustness of this scheme by transmitting the quantum signal over 170 km single-mode fiber with tolerable QBER, and also show that a classical channel (CC) (carrying synchronization information) can be transmitted simultaneously through the same fiber up to 90 km. This is the first HD-QKD fiber demonstration with simultaneous transmission of a CC.

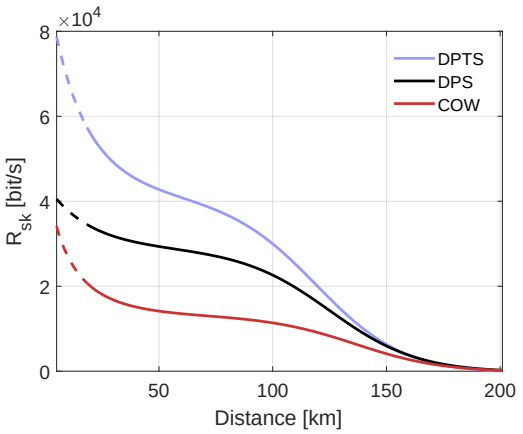

Fig. 1: Simulation of achievable secret key rates for DPTS, DPS and COW as a function of the transmission distance. Detectors dark counts $d_c = 100$ Hz, dead time $t_d = 20$ μs, efficiency $\eta_d = 20$ %, visibility $V = 0.97$, and $p_{decoy} = 0.1$. Optimal mean photon number per pulse μ: $\mu_{DPTS} = 0.26$, $\mu_{DPS} = 0.19$, $\mu_{COW} = 0.52$, with $\nu = 1.19$ GHz, $\langle N \rangle = 6$.

Protocol introduction

The DPTS protocol[8] belongs to the family of differential phase reference (DPR) protocols, where the information is encoded onto pulses in adjacent subslots. Compared to other protocols of the DPR family, the DPTS protocol allows a higher secret key rate (R_{sk}) as shown in Figure 1 and based on equation 1. The combination of pulse-position modulation and relative phase, enables the encoding of four different quantum states $\{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$ as described in Figure 2.

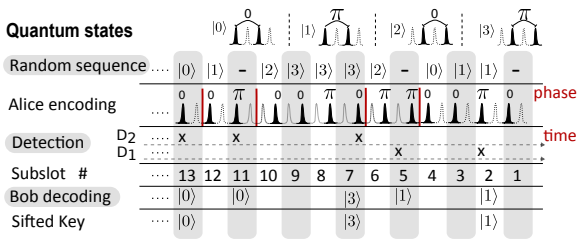

Fig. 2: DPTS distillation procedure. A *sifted* key is established between Alice and Bob.

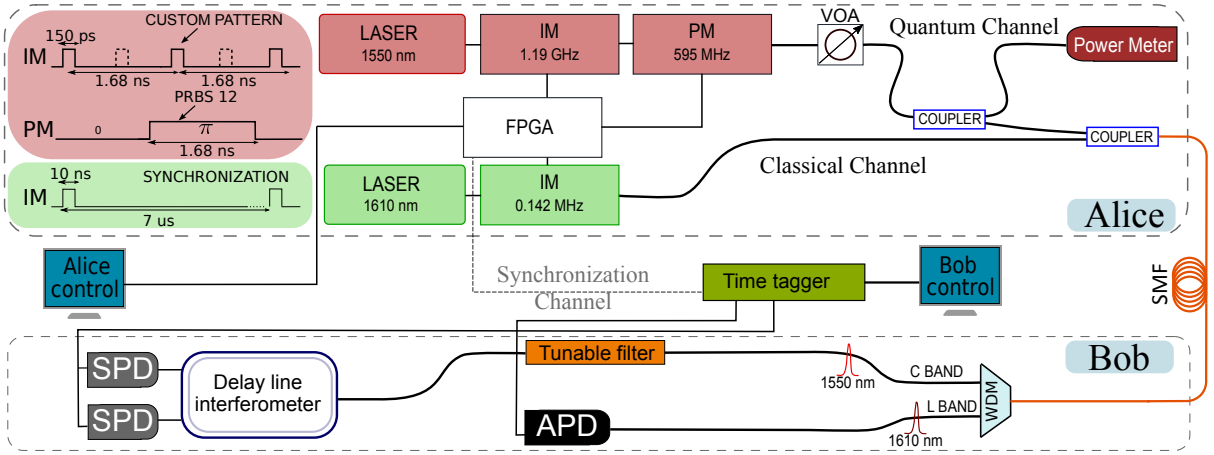

Fig. 3: Setup used in the current experiment. Up to 170 km LEAF single-mode transmission fiber is used.

Each state can carry two bits of classical information $(00, 01, 10, 11)$. Alice randomly chooses one of the quantum states and sends it through the quantum channel (QC) as reported in Figure 3. In order to increase the probability of "good" detection, Alice defines blocks of length N where the pulse-position is fixed (vertical red line defines block separation in Figure 2). An average block size is determined by Alice and the length of each block is randomly chosen $(N \geq 4)$. To measure the quantum state Bob uses a delay line Mach-Zehnder interferometer (DLI) making interference between adjacent subslots. So for a pulse repetition rate of ν, Bob's interferometer is set for $\nu/2$, consistent with the phase encoding rate. It is noted that by using a single measurement process, Bob can determine which quantum state was prepared by Alice. At this point after a distillation process, where Alice and Bob discard the transition sequence (see subslots 5 and 11 of Figure 2) and agree on the sifted key positions, a secure key rate can be extracted by the following equation:

$$R_{sk} = f R_B [I_{AB} - \min(I_{AE}, I_{BE})] \qquad (1)$$

where I_{AB} is the mutual information between Alice and Bob, I_{AE}, I_{BE} are the corresponding mutual information between Alice and Eve, or Bob and Eve. $R_B = R + 4p_d(1 - R)$ is defined as the total detection rate and $R = [1 - \exp(-\mu\, t\, \eta_d)]/2$ with t the channel transmission coefficient. The first term f is a predefined value, which includes the length of blocks and the probability of a decoy sequence (we used $f = 0.83$ with $\langle N \rangle = 6$ and $p_{decoy} = 0.1$)[8].

Experiment

The DPTS experiment was carried out using only standard off-the-shelf lab equipment. A CoBrite DX1 continuous wave laser at 1550 nm (C band) was used to prepare the quantum states. The train of weak coherent pulses (WCPs) was generated by using an Altera FPGA (Stratix V), which controls a pulse carver generating a pulse width of 150 ps with a repetition rate of 1.19 GHz. By using a custom pattern (see Figure 3) in combination with an intensity modulator (IM), the bit information related to the pulse-position was encoded. The IM was followed by a phase modulator (PM) and controlled by the same FPGA. For the PM we used a $2^{12} - 1$ PRBS sequence with a repetition rate of 595 MHz, i.e. at half the pulse rate and matching the DLI. Two different trials were realized: 1. only the quantum signal was sent into the fiber link, and 2. a CC was combined with the QC. In the first one we transmitted up to 170 km of LEAF single-mode fiber (0.22 dB/km loss at 1550 nm). Bob was synchronized directly to the transmitter using an electrical pulse train at a repetition rate of 0.145 MHz, and with pulse widths of 10 ns. Before entering into the QC, μ was monitored using a very sensitive photodiode. Following the theoretical evaluation, this number was set to 0.26 photon/pulse. In the second trial, in order to be as close as possible to a complete QKD system, a CC at 1610 nm (L band), i.e. an optical copy of the aforementioned electrical clock signal, was co-propagated with the QC. In this case, after 90 km, the two signals were separated using a WDM filter (C and L band). After a polarization controller, the quantum signal is injected into the free-space DLI (10 dB loss) and measured with two ID-230 single photon detectors (SPDs, $\eta_d = 0.2$ and $d_c = 100$ Hz). The outputs are connected to the ID-801 time tagger unit (TT). The CC is measured by a fiber coupled photo-diode and directly connected to the TT unit, after being separated by the WDM filter. In this way a synchronization signal permits a perfect time match,

and easily allows synchronization between Alice and Bob. Note that a narrow filter at 1550 nm (0.8 nm 3dB-BW, 6 dB losses, 80 dB extinction ratio) was used to remove the leakage of the CC before the DLI. In this way the noise level introduced into the QC is comparable to the dark counts of the detectors. An extra measurement was performed with a $2^7 - 1$ PRBS for the purpose of studying the behavior of the system with a higher repetition rate (4.7 MHz) of the CC. Negligible counts were measured in the QC showing that the filtering method is adequate for this QKD system.

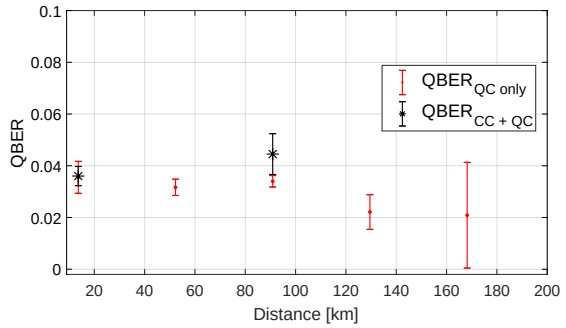

Fig. 4: Experimental QBER for different link distances. μ is set to 0.26. The black stars are acquired with the CC combined with QC into the same fiber.

Results

In Figure 4, we report the experimental QBER for varying link distances. Low and stable QBER was measured. In particular, a value below 5% was achieved even for a transmission length of 170 km. Note that the two data points corresponding to 10 and 50 km were acquired in the saturation regime of the detectors, and therefore exhibit a higher QBER. In the case of QC and CC co-propagating into the same fiber, a slightly higher QBER was obtained, as expected. In Figure 5, the experimental secret key rate matches the simulated one (solid blue line). In particular, a positive key rate of 4000 bit/s was extracted after 90 km of fiber transmission (20 dB losses) in the case of combined signals, and a key rate of 3000 bit/s is maintained out to 170 km transmission for the QC alone. This shows that our proposed QKD scheme operates very successfully and is able to co-exist robustly with a CC. The CC could not be transmitted longer than the 90 km, but amplification of the CC could improve this, if a more sophisticated filtering scheme is introduced. Additionally, it is expected that the quantum key could be transmitted even further if more advanced detector systems were used, such as cryogenic superconducting detectors. In this experiment, the point was to only use off-the-shelf components, and with the relatively cheap SPDs, it is possible to transmit 170 km. Although state-of-the art experiments, which use advanced detection schemes, can go further, our demonstrated key rate is orders of magnitude higher for local area network distances[9].

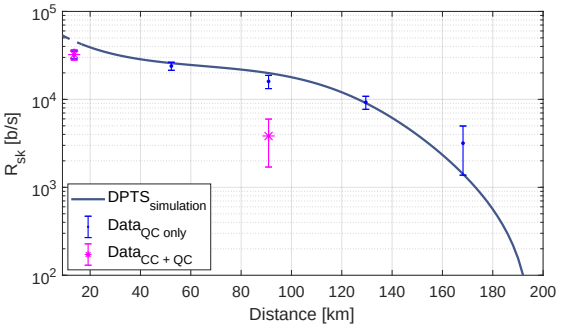

Fig. 5: Experimental secret key rate. Solid blue line is the simulation of DPTS.

Conclusions

We experimentally demonstrated the two-dimensional QKD based on differential phase-time shifting. For the first time, this is shown to operate over a fiber link and including a CC. The QC is transmitted 170 km alone, and 90 km together with a CC. Only commercially available off-the-shelf components were used in this demonstration, showing that it is practical and simple.

Acknowledgements

Work supported by Center of Excellence SPOC (ref DNRF123), the Danish Council for Independent Research (DFF-1337-00152; DFF-1335-00771), T.I.M.E. project of University of Padova, and from the People Programme (Marie Curie Actions FP7/2007-2013) n° 609405 (COFUNDPostdocDTU).

References

[1] P. Shor, 'Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,' SIAM J. Comput. 26 (1997)

[2] C. H. Bennett, G. Brassard, 'Quantum Cryptography: public key distribution and coin tossing,' Proceeding of IEEE International Conference on Computer, Systems & Signal Processing (1984).

[3] V. Scarani et al., 'The security of practical quantum key distribution,' Reviews of Modern Physics, 81(3) (2009)

[4] K. Inoue, et al., 'Differential-phase-shift quantum key distribution using coherent light', Phys. Rev. A 68 (2003).

[5] D. Stucki et al., 'Fast and simple one-way quantum key distribution', Appl. Phys. Lett. 87 (2005).

[6] N. J. Cerf et al., 'Security of Quantum Key Distribution Using d-level system,' Phys. Rev. Lett. 88 (2002)

[7] Y. Ding et al., 'High-Dimensional Quantum Key Distribution based on Multicore Fiber using Silicon Photonic Integrated Circuits,' arXiv:1610.01812 (2016)

[8] D. Bacco et al., 'Two-dimensional distributed-phase-reference protocol for quantum key distribution', Sci. Reports 6:36756 (2016)

[9] B. Korzh et al.,'Provably secure and practical quantum key distribution over 307 km of optical fibre', Nat. Photon. 9 (2015)