Technical University of Denmark

DTU

Differential phase-time shifting protocol for QKD (DPTS)

Usuga Castaneda, Mario A.; Bacco, Davide; Christensen, Jesper Bjerge; Ding, Yunhong; Rottwitt, Karsten; Oxenløwe, Leif Katsuo

Published in:
Proceedings of QCMC 2016

Publication date:
2016

Document Version
Peer reviewed version

Citation (APA):
Usuga Castaneda, M. A., Bacco, D., Christensen, J. B., Ding, Y., Rottwitt, K., & Oxenløwe, L. K. (2016). Differential phase-time shifting protocol for QKD (DPTS). In Proceedings of QCMC 2016

Differential phase-time shifting protocol for QKD (DPTS)

Mario A. Usuga*, Davide Bacco, Jesper B. Christensen, Yunhong Ding, Karsten Rottwitt and Leif K. Oxenløwe

Department of Photonics, Technical University of Denmark, 2800 Kgs. Lyngby, Denmark.
**Corresponding author: mauc@fotonik.dtu.dk*

Dated: February 29, 2016

Abstract

We explore the implementation of a novel protocol for fiber-based high-dimensional quantum key distribution (QKD) which improves over the traditional DPS-QKD and COW protocols.

The emergence of distributed-phase-reference protocols such as differential-phase shift (DPS) [1] and coherent one-way (COW) [2, 3], have had a great influence on the field of practical QKD. Naturally, this impact has lead to the proposal of related protocols [4, 5]. We here propose a novel combination of the DPS and COW protocols, which we refer to as the DPTS protocol.

To explain the principle of the DPTS protocol we refer to Fig. 1 which shows a simplified setup. Alice prepares a pulse train consisting of weak coherent pulses, which are phase modulated at a frequency of half the laser repetition rate. As in the DPS protocol relative phases only assume the values $\{0, \pi\}$. At this point, the pulses appear in pairs, so that any single pulse has a neighbor with 0 relative phase and another neighbour with 0 *or* π relative phase. We denote pairs of pulses, which with certainty share the same phase as a *sub-block*. After phase-modulation, the pulse train is intensity modulated in a similar manner to how it is done in the COW protocol. However, in this situation each COW sequence is repeated three times as illustrated in Fig. 1. We denote a six-pulse sequence, of common COW sequence, as a *block*. Note that the COW sequence is therefore always the same within a block, but changes randomly across a block separation. To interpret the stream of weak coherent pulses sent by Alice, Bob employs a Mach-Zehnder interferometer with a delay, T, corresponding to twice the temporal difference between pulses. Using this setup, Alice and Bob establish a key from utilizing intra-block interference, and monitor the channel using the inter-block interference in cases of identical consecutive COW sequences. The protocol in summary:

- Alice prepares six-pulse sequences (defined as blocks) containing three empty and three non-empty pulses so that they appear in pairs (sub-blocks).
- The sub-blocks are phase-modulated so that the relative phase within a sub-block is 0, but the relative phase across each sub-block separation is $\{0, \pi\}$.
- Bob reveals the sub-blocks that resulted in detection events.
- For detection events in sub-block 'A', Alice reveals for which of the detections, the two corresponding COW sequences were identical. Bob, in these cases, reports whether D_1 or D_2 resulted in the click, enabling Alice to estimate the interferometer visibility. In cases where the COW sequences were not identical, they both discard their related bits.
- From the remaining detection events (sub-blocks 'B' and 'C'), Alice immediately knows the temporal time-slot of the detections, and may realize which detector clicked by considering her phase-modulation data. Thus, Alice and Bob establishes two bits of sifted key.

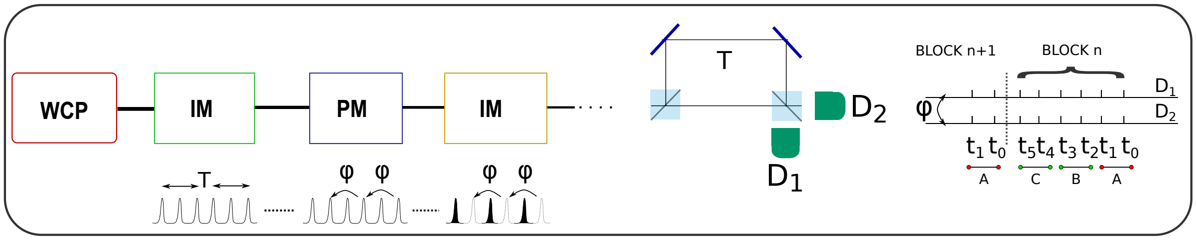

Figure 1: *Setup of the DPTS scheme.*

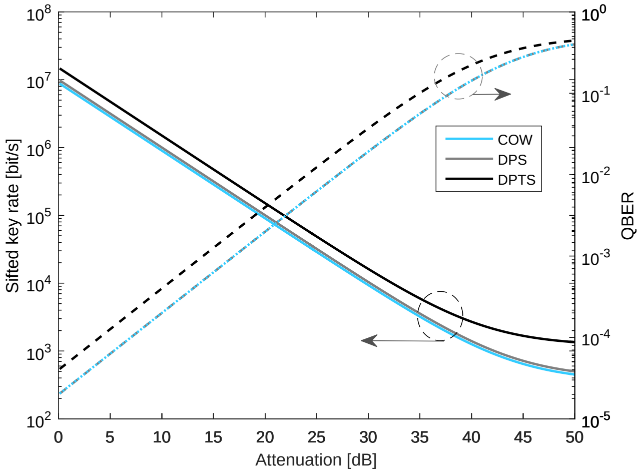

Figure 2: *Sifted key rate and QBER comparison.* In the simulation we used the following parameters: dark count rate of 200 Hz, detector efficiency of 10%, time detection window of 1 ns, a laser repetition rate of 1 GHz, and a mean photon number per pulse of 0.1. Moreover, for the COW protocol, we assumed a decoy-sequence probability of 0.1 and a negligible amount of monitoring.

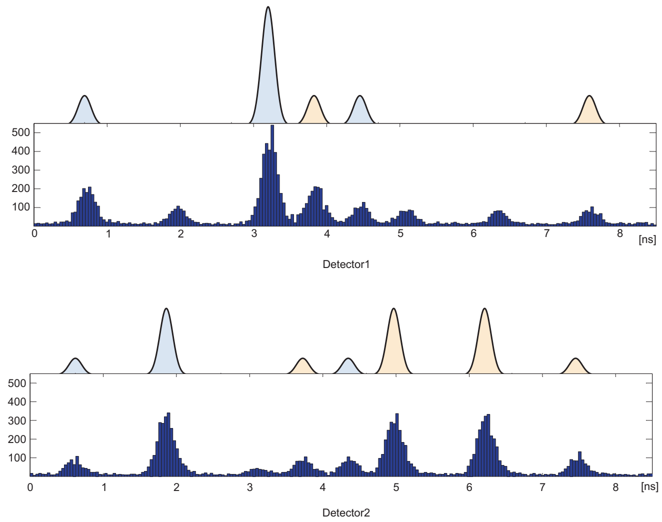

Figure 3: Accumulated photon counts for both detectors on Bob's side, with a 1.6 GHz laser repetition rate, propagated through 10 km of single mode fiber. The bit sequence presented is '1011_b' for the differential phase shift bits and '10_b' for the time shift bits. Above each detector's photon counts we plot the theoretical expectations for the selected detector settings, see text for details.

The sifted key rate and the QBER of the DPTS protocol are seen in Fig. 2 compared with the DPS and COW protocols under similar conditions. The DPTS protocol has superior performance at low levels of attenuation, ideally allowing for 33% higher key rate as compared to its two parent protocols in terms of key rate per average mean photon number. On the other hand, dark counts have greater influence due to their two-bit interpretation, and as a result the QBER is generally larger for the present protocol.

We have performed a proof of principle demonstration of the DPTS protocol, using two Id-230 single-photon detectors of quantum efficiency $\eta = 25\%$, average dark count rate of $p_{d1} = 200$ counts/s and $p_{d2} = 300$ counts/s for detectors D_1 and D_2 respectively which in our case presents a jitter of about 300 ps. The repetition rate of the laser source is ν_s=1.6 GHz and the pulse train is phase modulated at 0.8 GHz. At Bob's side, we used an unbalanced free-space Mach-Zehnder interferometer with a temporal delay that corresponds to $T = 2/\nu_s$. The optical link established between Alice and Bob currently spans over 10 km of single mode fiber.

Figure 3 shows the photon counts for both D_1 and D_2 when the system is run with a fixed bit sequence corresponding to two consecutive blocks. The shadows above each detector in Fig. 3 represent the expected behavior of the photon counts when considering the above mentioned detector configuration, where the two blocks are shown in different color. The light-blue (light-yellow) shadows show the first bit for the time shift, in this case: '1_b' ('0_b') along with 2 bits for the differential phase shift: '10_b' ('11_b'). The 2-block bit sequence shown was chosen to demonstrate the effect of changing bits both for the differential phase and time shift, as well as to evaluate the system in the demanding scenario when two consecutive blocks are closer to each other -due to a change in time shift bit- where D1 and D2 have to be able to distinguish between pulses separated by T/2 which would set a limit for the attainable key rate.

We have proposed and experimentally demonstrated a new protocol (DPTS) for high-dimensional QKD which is compatible with fiber optics links. We found that the sifted bit rate for DPTS is higher than both DPS and COW protocols when using the same mean photon number per block. An important feature of DPTS is that it does not, in contrast to COW, require extra monitoring detectors to check the coherence between pulses at Bob's side in order to reveal Eve's presence.

References

[1] K. Inoue, *et al.*, Phys. Rev. A **68**, 022317 (2003).

[2] N. Gisin, *et al.*, arXiv preprint quant-ph/0411022 (2004).

[3] D. Stucki, *et al.*, Appl. Phys. Lett. **87**, 194108 (2005).

[4] J.-Y. Guan, *et al.*, Phys. Rev. Lett **114**, 180502 (2015).

[5] T. Sasaki, *et al.*, Nature, **509**, 475 (2014).