Experimental demonstration of the DPTS QKD protocol over a 170 km fiber link

da Lio, Beatrice; Bacco, Davide; Cozzolino, Daniele; Ding, Y.; Dalgaard, K.; Rottwitt, Karsten; Oxenløwe, Leif Katsuo

Published in:
Applied Physics Letters

Link to article, DOI:
10.1063/1.5049659

Publication date:
2019

Document Version
Publisher's PDF, also known as Version of record

Experimental demonstration of the DPTS QKD protocol over a 170 km fiber link

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

Citation: Appl. Phys. Lett. **114**, 011101 (2019); doi: 10.1063/1.5049659
View online: https://doi.org/10.1063/1.5049659
View Table of Contents: http://aip.scitation.org/toc/apl/114/1
Published by the American Institute of Physics

Applied Physics Letters ARTICLE scitation.org/journal/apl

Experimental demonstration of the DPTS QKD protocol over a 170 km fiber link

Cite as: Appl. Phys. Lett. **114**, 011101 (2019); doi: 10.1063/1.5049659
Submitted: 24 July 2018 · Accepted: 14 December 2018 · Published Online: 02 January 2019

B. Da Lio,[a] D. Bacco,[b] D. Cozzolino, Y. Ding, K. Dalgaard, K. Rottwitt, and L. K. Oxenløwe

AFFILIATIONS

CoE SPOC, DTU Fotonik, Department of Photonics Engineering, Technical University of Denmark, Ørsteds Plads 340, Kgs. Lyngby 2800, Denmark

[a] Electronic mail: bdali@fotonik.dtu.dk
[b] Electronic mail: dabac@fotonik.dtu.dk

ABSTRACT

Quantum key distribution (QKD) is a promising technology that aims to solve the security problem arising from the advent of quantum computers. While the main theoretical aspects are well developed today, limited performances, in terms of the achievable link distance and the secret key rate, are preventing the deployment of this technology on a large scale. More recent QKD protocols, which use multiple degrees of freedom for encoding of the quantum states, allow enhancement of the system performances. Here, we present the experimental demonstration of the differential phase-time shifting protocol up to 170 km of the fiber link. We compare its performance with the well-known coherent one-way and differential phase shifting protocols, demonstrating a higher secret key rate up to 100 km. Moreover, we propagate a classical signal in the same fiber, proving the compatibility of quantum and classical light.

The security of digital data is extremely important in our society, due to the continuous exchange of sensitive information. Classical cryptography is based on mathematical assumptions which do not guarantee information-theoretic security,[1] i.e., a security that cannot be broken with unlimited computational power. However, quantum key distribution (QKD), a branch of quantum communication (QC), provides unconditional security based on the laws of quantum physics.[2,3] In the last 30 years, free-space, underwater, and fiber based experiments have demonstrated the exploitation of different physical degrees of freedom for QC protocols.[4–7] Among these, the differential phase reference (DPR) schemes were proposed as a step towards easier implementation of fiber transmission schemes. They make use of the time of arrival of pulses, the phase difference between them, or, more recently, both dimensions to encode secure key bits.[8–11] Furthermore, several quantum networks have already been implemented.[12–15] During the last few decades, the efforts of the scientific community were focused on enhancing the quantum communication performance in terms of the key rate, the transmission distance, and security aspects.[8,16–24] Here, we present a practical implementation of the differential phase-time shifting (DPTS) protocol over 170 km of a single mode fiber, proving a higher secure key rate compared with other protocols of the DPR family, such as coherent one-way (COW) and differential phase shifting (DPS).[8,10,11] Furthermore, we also prove that a classical signal at a different wavelength can coexist on the same optical fiber up to 90 km distance.

The DPTS protocol encodes the information in relative properties of consecutive weak coherent pulses (WCPs). However, as opposed to the other DPR protocols, the DPTS exploits more than one degree of freedom at once, namely, the position in time and the phase difference among consecutive pulses. This allows the DPTS to improve the secret key rate in an intra-city network scenario (in terms of reachable distances and channel loss), while at the same time being more robust against channel noise as shown in Fig. 1(a).[8]

In the DPTS protocol, the information is encoded in four possible symbols in the alphabet $\{0,1,2,3\}$, which are

$$\begin{aligned} |0\rangle &= |\pm\alpha\rangle|vac\rangle|\pm\alpha\rangle|vac\rangle, \\ |1\rangle &= |\pm\alpha\rangle|vac\rangle|\mp\alpha\rangle|vac\rangle, \\ |2\rangle &= |vac\rangle|\pm\alpha\rangle|vac\rangle|\pm\alpha\rangle, \\ |3\rangle &= |vac\rangle|\pm\alpha\rangle|vac\rangle|\mp\alpha\rangle. \end{aligned} \tag{1}$$

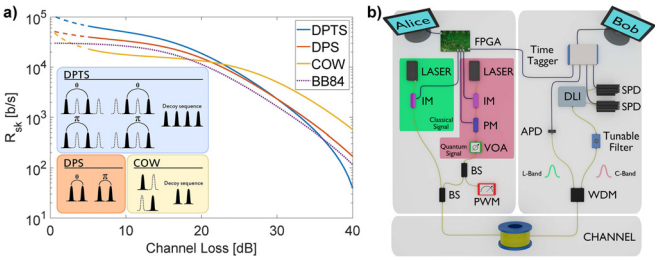

FIG. 1. (a) Theoretical secret key rates R_{sk} as a function of channel loss. DPTS (blue), DPS (orange), and COW (yellow) secret key rates under the condition of beam splitting attack and BB84 with a decoy state method (dotted violet) secret key rate against collective attacks. Parameters: $\nu = 1.19$ GHz, $r_{dc} = 100$ Hz, $\eta = 20\%$, $t_d = 20$ μs, $\mu_{DPTS} = 0.26$, $\mu_{DPS} = 0.13$, $\mu_{COW} = 0.52$, $\mu_{BB84} = 0.25$ (signal), $\nu_{BB84} = 0.08$ and $\omega_{BB84} = 10^{-10}$ (decoy) photon/pulse; $V = 0.98$ and $l_{int} = 8$ dB (DPTS, DPS, and BB84); probability of the decoy sequence $p_d = 0.1$ (DPTS and COW); $N = 6$ pulses/block (DPTS). The inset shows the encoding symbols in DPR protocols: filled pulses are WCPs, dotted pulses are vacuum states. (b) Schematics of the experimental setup. FPGA: field programmable gate array board; continuous wave lasers: 1550 nm for the quantum signal (C-band) and 1610 nm for the classical signal (L-band); IM: intensity modulator; PM: phase modulator; VOA: variable optical attenuator; BS: beam splitter; PWM: power meter; WDM: wavelength division multiplexer filter; APD: avalanche photodiode; DLI: delay line interferometer; SPD: single photon detector.

The terms $|\pm\alpha\rangle$ and $|vac\rangle$ in Eq. (1) represent a coherent state of intensity α and a vacuum state, respectively. The $\pm$ sign represents the phase of the state. When the two coherent states have the same (opposite) sign, their phase difference is 0 (π), see Fig. 1(a). When the transmitter, usually called Alice, has prepared the quantum states, she sends them through a quantum channel towards the receiver, called Bob. To measure them, Bob uses a delay line interferometer (DLI), with a delay $T = 2/\nu$ (ν is the repetition rate), to sort among the 0 or π phase difference. At the same time, Bob measures on each output of the interferometer the time of arrival of the pulses. After the quantum communication process, the sifting procedure takes place. Hence, Alice and Bob share a sifted key, and the following steps in the protocol are given by the classical error correction and privacy amplification. The equations for the final achievable secret key rate, under the assumption of beam splitting attacks, are reported in the supplementary material.[3,8] Figure 1(a) shows a comparison of the achievable secret key rate using DPTS, DPS, and COW from the DPR family and the secret key generated with the standard BB84 protocol with a decoy state method. It is to be noted that the BB84 protocol offers unconditional security,[25] i.e., it is secure against collective attacks (the most comprehensive kind of attacks), while the DPR protocols are secure against collective beam splitting attacks. Even though a fair comparison is not possible, it is also important to highlight that the experimental implementation of the BB84 with decoy states requires more equipment, a more advanced control unit to generate all the states in the mutually unbiased bases and also a more complicated receiver.

The experimental setup used in the current experiment is shown in Fig. 1(b). To prepare the train of time-encoded WCPs, Alice carves with an intensity modulator a continuous wave laser at 1550 nm. The obtained signal has an average block length of $N = 6$ pulse/block (in a block, there are only symbols with the same time encoding[8]). The optical signal is then sent through a phase modulator, which imprints the required phase difference among consecutive WCPs. Hence, Alice uses an optical variable attenuator to reach the quantum regime of $|\alpha|^2 = \mu \approx 0.26$ photon/pulse. With this value, the secret key generation rate of the DPTS is maximized.[8] The WCPs are then sent to Bob through a single mode fiber link of variable length, from 10 km to 170 km. The loss per unit distance of the fiber is 0.22 dB/km. At the receiver side, Bob uses a free-space delay line interferometer with an overall insertion loss of approximately $l_{int} \approx 8$ dB and visibility $V \approx 0.98$ to infer the quantum states. A phase difference of 0 is routed towards one output of the interferometer, while a phase difference of π constructively interferes on the other output. The two outputs are then linked to two IDQ230 InGaAs single photon detectors (SPDs), which have the following parameters: efficiency $\eta_{det} = 20\%$, dark count rate $r_{dc} \approx 100$ Hz, dead time $t_d = 20$ μs, and jitter $t_j \approx 300$ ps. Both detectors are connected to a time tagging unit. The electrical control at Alice's side is given by a field programmable gate array (FPGA) board whose three electrical outputs are for the intensity modulator, the phase modulator, and the synchronization signal. The repetition frequency is $\nu = 1.19$ GHz, the electrical pulse width is of approximately 100 ps, whereas the obtained optical pulse width is around 150 ps. The synchronization signal is either sent electrically to Bob's time-tagger unit directly from the FPGA or converted into a classical optical signal which co-propagates with the quantum channel. More details are reported in the supplementary material. To implement the DPS and COW protocols, the setup is easily adapted. We changed the delay of the optical interferometer in order to have a fair comparison between the protocols, i.e., all the protocols are implemented at the same transmitter speed. Moreover, for the COW protocol, at Bob's side, an unbalanced beam splitter is required so that most of the time the pulses are directly received using one single photon detector but sometimes, with a low probability, they are used to check coherence and are therefore sent to the delay line interferometer. For both protocols, the optimal mean photon number per pulse is used in the implementation.[8,26]

Figure 2 shows the performance comparison of the three protocols in terms of the quantum bit error rate (QBER) and the secret key rate under the condition of beam splitting attacks (when the synchronization signal is electrically sent to Bob). The triangles represent data collected for each protocol when the link between Alice and Bob is made by fiber spools (with distances ranging from 10 to 170 km with steps of 40 km), whereas the squares are measurements taken when an optical attenuator constitutes the channel, thus emulating only the fiber loss (from 5 to 40 dB losses with steps of 5 dB). Solid curves represent simulations taking setup imperfections into account. An intrinsic error of $e_t = 1.5\%$ is estimated in the time domain, due to the finite extinction ratio of the intensity modulator during the carving procedure (for COW and DPTS protocols), and an intrinsic error of $e_p = 0.5\%$ affects the phase domain, due to an imperfect modulation in the phase modulator (for DPTS and DPS protocols). Note that the bounds used in this work to compute

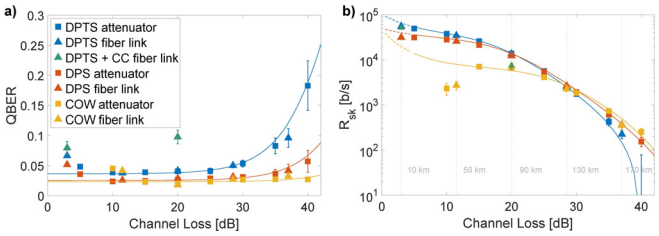

FIG. 2. (a) Measured QBER and (b) experimental secret key rate. The color scheme used is DPTS without a co-propagating classical channel (blue), DPTS with optical classical synchronization (green), DPS (orange), and COW (yellow). Triangles report data collected using fiber spools as the channel link and squares show data obtained emulating channel loss with a VOA. Solid lines show the simulated results taking into account setup imperfections as intrinsic errors.

the achievable secret key rate are valid in the long distance regime,[8,26] which is ensured after approximately 5 dB of channel loss (corresponding to ∼23 km link). This is also shown in Fig. 2(b), where the simulation curves are dashed before reaching this regime. Finally, as a preliminary demonstration of our system used in real communication networks, we co-propagate a classical channel, carrying the optical synchronization used for the QKD system, with the DPTS signal. This is obtained by modulating a CW laser at 1610 nm. At the receiver side, a wavelength division multiplexing filter (extinction ratio, 60 dB) separates the two signals directing the synchronization to a photodetector. The quantum channel is further filtered with a narrow bandpass filter with a 3-dB bandwidth of 0.8 nm around 1550 nm and an extinction ratio of 40 dB. The second filtering step is needed to further reduce the leakage from the classical channel into the quantum channel. The results are reported in Figs. 2(a) and 2(b) with green triangle markers. The input power of the classical channel was set to −27 dBm, minimizing the impact on the quantum channel, but ensuring enough power for successful detection with the photodiode.

The comparison of the three protocols shows that for short-range links, i.e., up to 21 dB channel loss, the achievable secret key rate is indeed higher when using the DPTS compared to DPS and COW performances. Note that the experimental values up to 5 dB attenuation, for the DPTS and the DPS protocol, exhibit a higher QBER than expected. This is mainly due to the detectors' saturation regime. For the COW protocol, which does not rely on an interferometer with insertion loss at Bob's side, the detectors saturate up to 11 dB (50 km) of channel loss. An interesting channel distance to consider is thus 50 km, where the bound conditions are valid. Here, the DPTS reaches a secure rate of 34 kb/s with a system that is stable for over 1 h, as reported in Fig. 3. The DPS protocol is able to produce 25 kb/s of the secret key rate and the COW protocol produces only 2.7 kb/s in the experimental implementation, while the simulation curve reaches up to 7.8 kb/s (saturation regime). The DPTS protocol indeed shows an improved performance in the secret key rate and a better robustness against noise for applications in an intra-city scenario. On the other hand, on longer distances, the secret key rate drops more rapidly than the other protocols, even though a positive secret key rate can still be experimentally

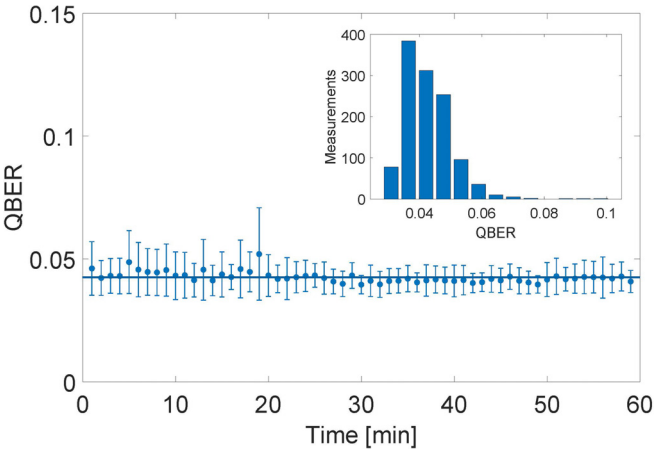

FIG. 3. Stability of the DPTS protocol. Experimental QBER of the DPTS protocol at 50 km distance for over 1 h of continuous measurements. The inset shows the QBER distribution.

obtained for a distance of 170 km. An intuitive explanation to this is given by the fact that any error can affect both the time and phase domains: when the random dark count clicks are comparable in number to the actual photon clicks, then this effect starts having a more severe impact on the protocol performance. In the case of co-propagation of classical and quantum signals, the higher QBER and the respective decrease in the secret key rate result from leakage from the classical channel and the detectability of the classical channel itself. Indeed, the information the classical signal is carrying is crucially needed for synchronizing the quantum channel. The maximum distance we could achieve was 90 km with a secret key rate of 7.3 kb/s. To increase the transmission distance, it appears necessary to introduce a more sophisticated filtering scheme, which would allow higher classical input power, and/or amplification schemes for the classical channel.

In this paper, we demonstrated the DPTS protocol over 170 km of single mode fiber and compared its performance with other DPR protocols. We showed that in an intra-city network scenario, the DPTS outperforms the other protocols for up to 21 dB channel loss (about 100 km) under the assumption of beam splitting attacks. We also demonstrated that our scheme can coexist on the same fiber with classical light, necessary for complete deployment of QKD systems.

See supplementary material for secret key rate formulas and further details on the experimental setup and the electronic design.

This work was supported by the Centre of Excellence, SPOC (Silicon Photonics for Optical Communications) (ref DNRF123) and by the People Programme (Marie Curie Actions) of the European Union's Seventh Framework Programme (FP7/2007-2013) under REA Grant Agreement No. 609405 (COFUNDPostdocDTU).

REFERENCES

[1]P. Shor, SIAM J. Comput. **26**, 1484–1509 (1997).
[2]C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computer, Systems and Signal Processing* (1984), pp. 175–179.
[3]V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**(3), 1301–1350 (2009).
[4]A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, Phys. Rev. Lett. **121**, 190502 (2018).
[5]L. Ji, J. Gao, A.-L. Yang, Z. Feng, X.-F. Lin, Z.-G. Li, and X.-M. Jin, Opt. Express **25**, 19795 (2017).
[6]F. Bouchard, A. Sit, F. Hufnagel, A. Abbas, Y. Zhang, K. Heshami, R. Fickler, C. Marquardt, G. Leuchs, R. W. Boyd, and E. Karim, Opt. Express **26**, 22563 (2018).
[7]G. Vallone, D. G. Marangon, M. Canale, I. Savorgnan, D. Bacco, M. Barbieri, S. Calimani, C. Barbieri, N. Laurenti, and P. Villoresi, Phys. Rev. A **91**, 042320 (2015).
[8]D. Bacco, J. B. Christensen, M. A. U. Castaneda, Y. Ding, S. Forchhammer, K. Rottwitt, and L. K. Oxenløwe, Sci. Rep. **6**, 36756 (2016).
[9]B. Da Lio, D. Bacco, Y. Ding, D. Cozzolino, K. Dalgaard, K. Rottwitt, and L. K. Oxenløwe, in *Proceedings of the 43rd European Conference on Optical Communication* (ECOC), W.3.E.6, Gothenburg, Sweden, September 2017.
[10]D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, Appl. Phys. Lett. **87**(19), 194108 (2005).
[11]K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. **89**(3), 037902 (2002).
[12]M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka *et al.*, Opt. Express **19**, 10387 (2011).
[13]T.-Y. Chen, H. Liang, Y. Liu, W.-Q. Cai, L. Ju, W.-Y. Liu, J. Wang, H. Yin, K. Chen, Z.-B. Chen *et al.*, Opt. Express **17**, 6540 (2009).
[14]M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, and J. F. Dynes, New J. Phys. **11**, 075001 (2009).
[15]S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li *et al.*, Nature **549**, 43 (2017).
[16]X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**(1), 012326 (2005).
[17]W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[18]T. Zhong, H. Zhou, R. D. Horansky, C. Lee, V. B. Verma, A. E. Lita, A. Restelli, J. C. Bienfang, R. P. Mirin, T. Gerrits *et al.*, New J. Phys. **17**, 022002 (2015).
[19]H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
[20]H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang *et al.*, Phys. Rev. Lett. **117**, 190501 (2016).
[21]N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, Sci. Adv. **3**, e1701491 (2017).
[22]M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Nature **557**, 400 (2018).
[23]G. L. Roberts, M. Lucamarini, J. F. Dynes, S. J. Savory, Z. Yuan, and A. J. Shields, Appl. Phys. Lett. **111**, 261106 (2017).
[24]J. F. Dynes, W. W.-S. Tam, A. Plews, B. Fröhlich, A. W. Sharpe, M. Lucamarini, Z. Yuan, C. Radig, A. Straw, T. Edwards, and A. J. Shields, Sci. Rep. **6**, 35149 (2016).
[25]H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[26]C. Branciard, N. Gisin, and V. Scarani, New J. Phys. **10**, 013031 (2008).