Differential phase-time quantum key distribution protocol

D. Bacco*, J. B. Christensen, M. A. Usuga, Y. Ding, K. Rottwitt, L. K. Oxenløwe

Department of Photonics, Technical University of Denmark, 2800 Kgs. Lyngby, Denmark.,

Abstract.

We present a novel two-dimensional quantum key distribution protocol based on differential phase and time position modulation (DPTS). We study the performance of the protocol defining a bound against collective attacks. We also show preliminary experimental results implementing a proof of concept demonstration.

Motivation

Encryption of public and personal data is becoming increasingly important. Classical cryptography, based on the mathematical assumption of the encryption algorithm, can not guarantee data security of the the current century. In fact, classical cryptography is predicted to be rendered insecure when quantum computers become available [1]. Quantum cryptography, on the other hand, is guaranteed secure, as described by Bennett and Brassard more than 30 years ago [2]. Since then, big efforts from the research community and some industrial pioneers has made quantum key distribution (QKD) the first commercial quantum technology. However, a large-scale commercial breakthrough for quantum systems is far from realization. The main limitations are related to the lack of high-rate single photon sources, reliable quantum repeaters, expensive bulk apparatus systems and also on the intrinsic losses of the transmission channel. By increasing the quantum key rate, it becomes possible also to increment the transmission reach. This may be achieved by increasing the quantum symbol rate, or by using more degrees of freedom for modulation of the key information. Here, we introduce a new two-dimensional distributed phase reference (DPR) QKD protocol, in which the information is encoded in the time and relative phase of weak coherent pulses. The proposed protocol is highly practical and simple in its implementation, and thus paves the way for fully integrated quantum devices based on a minimum requirement of miniaturized components.

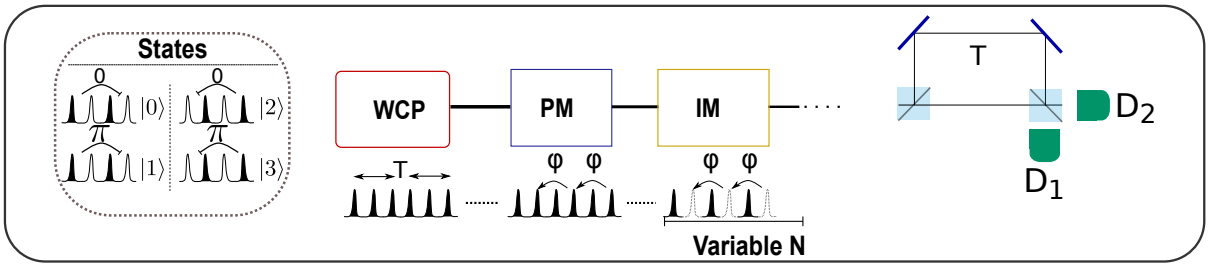


Fig. 1. *Base scheme of DPTS protocol.* A train of weak coherent pulses (WCP) is emitted by a laser with a repetition rate equal to v $(2/T)$, and attenuated to a single photon level ($\mu < 1$). A phase modulator (PM) encodes the first key bit in non adjacent pulses, choosing a random phase of either 0 or π. Then, an intensity modulator (IM), encodes the second key bit by randomly choosing between the time instances $|\pm\sqrt{\mu}, \text{vac}\rangle$ or $|\text{vac}, \pm\sqrt{\mu}\rangle$. The length of the block (N), in which is used the same time instance, is defined by Alice that randomly decide between different block duration ($N \geq 4$). In this way Alice prepares a sequence of different states, chosen by $|0\rangle$, $|1\rangle$, $|2\rangle$, $|3\rangle$. A random decoy sequence is implemented in order to check the coherence between pulses ($|\pm\sqrt{\mu}, \pm\sqrt{\mu}, \pm\sqrt{\mu}, \pm\sqrt{\mu} \cdots \leq N\rangle$). The receiver Bob, use a delay line interferometer (T delay between arms) and can measure simultaneously the phase and the time of arrivals of the photons.

* dabac@fotonik.dtu.dk

Principle of DPTS

A simple setup of the DPTS protocol is reported in Fig. 1. Alice uses an intensity modulator (IM) to encode one bit in two different time instances. For every pair of pulses, one pulse is transmitted with mean photon number μ, and one is blocked completely [3]. Then, using a phase modulator (PM), it is possible to encode a random phase $\{0\}$, or $\{\pi\}$ between non-empty pulses [4]. By combining the effect of the IM and the PM, Alice may prepare four different states: $|0\rangle = |\pm\sqrt{\mu}\rangle\,|\text{vac}\rangle\,|\pm\sqrt{\mu}\rangle\,|\text{vac}\rangle\,, |1\rangle = |\pm\sqrt{\mu}\rangle\,|\text{vac}\rangle\,|\mp\sqrt{\mu}\rangle\,|\text{vac}\rangle\,, |2\rangle = |\text{vac}\rangle\,|\pm\sqrt{\mu}\rangle\,|\text{vac}\rangle\,|\pm\sqrt{\mu}\rangle\,, |3\rangle = |\text{vac}\rangle\,|\pm\sqrt{\mu}\rangle\,|\text{vac}\rangle\,|\mp\sqrt{\mu}\rangle$. As reported in Fig. 1, Alice prepares blocks of length N, within which the temporal sequence is the same. The value of N for each block is chosen randomly in a uniform distribution: $N \in \{4, 6, ...N_{max}\}$. Bob, at the receiving end of the channel, unambiguously distinguish between the four stats by interfering adjacent non-empty pulses in an unbalanced interferometer with a T time-delay between its arms, and performing photodetection at the output ports. The security of DPTS relies on the same principle as other DPR protocols: the coherence between non-empty pulses [5, 6]. Eve can not perform a measurement on any finite number of states without at some time breaking coherence between successive pulses. This is specifically true for the DPTS protocol, since Eve is completely ignorant about the start and the end of blocks. A variable decoy sequence length, formed by a train of non-empty weak pulses, is used to prevent the attacks inside sub-blocks which are not detectable during an attack just in that instance. The secret key rate is defined as:

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

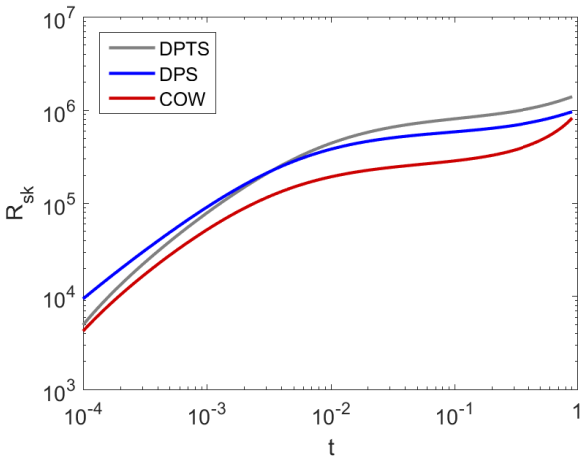
where $R_B = R + 4p_d(1-R)$ is the total detection rate with $R = [1 - \exp(-\mu t \eta_d)]/2$. μ is the mean photon number of non-empty pulses, t represents the quantum channel transmission coefficient, η_d is the (common) detector efficiency, and p_d is the dark count probability. The pre-factor $f = (1 - p_{decoy})\,(\langle N\rangle - 1)\,/\,\langle N\rangle$, where $\langle N\rangle$ is the average block length and p_{decoy} is the probability of the decoy sequence, take into account the fraction of Bob's detection events that is assigned to the key string. Considering the case of collective attacks, or more specifically the beam-splitter attack (BSA), the maximum information for Eve is given by the Holevo quantity [7, 8] $\chi_{AE} = S(\rho_E) - \sum_j p_j S(\rho_{E|j})$, where S is the von Neumann entropy, $\rho_E = \sum_j p_j \rho_{E|j}$, p_j is the probability of Alice preparing the four states $j \in \{0, 1, 2, 3\}$, and $\rho_{E|j}$ is Eve's state conditioned on preparation of state j. $\chi^{(0)}_{AE} = S_4\left(\frac{\left(1+\gamma^2\right)^2+(2\gamma)^2}{8}\right) + 4S_4\left(\frac{1-\gamma^4}{8}\right) + 3\,S_4\left(\frac{\left(1-\gamma^2\right)^2}{8}\right) - h_4\left(\frac{1-\gamma^4}{2}\right)$, where $S_4(x) \equiv -x\log_4 x$, and $h_4(x) = S_4(x) + S_4(1-x)$. $\chi^{(0)}_{AE}$ represents an upper bound on the information that Eve can obtain trying to distinguish between the four different states. A complete description of the security analysis will be presented at the conference.

Simulation and experimental results

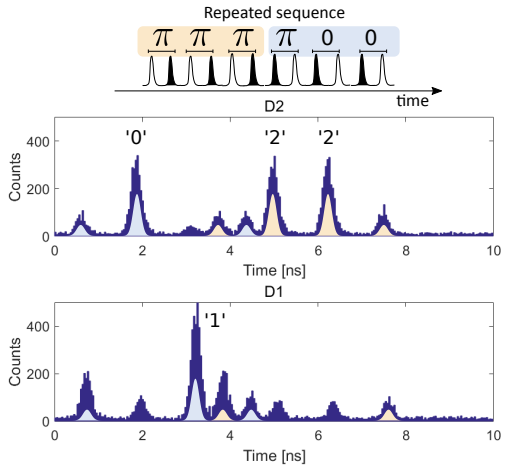
Using Eq.(1) it is possible to compare the performance of the DPTS protocol with the other protocols of the DPR family. In a realistic scenario, we must include all the parameters regarding the devices used in the QKD systems in the expected secret key rate. One of the most important parameter is the detector dead time. In fact, this number limits the maximum achievable key rate to the inverse of the dead time. In this case, the DPTS protocol, as reported in Fig. 2(a), permits us to extract twice of the information as compared to the classical DPR family. This advantage can be used in the case of a short/middle distance scenario and with a dead time value close to μs. We further present a proof of concept (PoC) demonstration of the DPTS protocol. A train of weak coherent pulses ($\mu < 1$) with a fixed phase-time pattern was sent from Alice to Bob. Bob uses a free-space delay Mach-Zehnder interferometer (delay corresponds to $T = 2/\nu$.) to register the incoming photons. The optical link established between Alice and Bob currently spans over 10 km of single mode fiber. Fig. 2(b) 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 with $N = 6$. The shadows above each detector in Fig. 2(b) represent the expected behavior of the photon counts when the reported sequence is continuously repeated by Alice. The 2-block bit sequence shown was chosen to demonstrate the effect of changing bits both for the differential phase and the time sequence, as well as to evaluate the system in the demanding scenario when two consecutive blocks are close to each other.

Conclusion

We have proposed and experimentally demonstrated a novel two-dimensional phase reference protocol for fiber based QKD link. The hardware requirements of DPTS are very similar to the other DPR protocols, however the



(a) *Simulated secret key rate versus transmittivity of the channel.* Different secret key rates achievable in a medium-length link scenario, where the dead time of the detectors plays a crucial role. The optimal μ value was chosen for the three protocols: $\mu_{DPTS} = 0.23$, $\mu_{DPS} = 0.19$, $\mu_{COW} = 0.52$, $p_d = 3.5 \cdot 10^{-9}$, dead time of the detectors ($t_d = 1 \cdot 10^{-6}$ s), efficiency 10%, $\nu = 10 \cdot 10^9$ Hz, $V = 1$ and fixed dimension of the block $N = 4$. Probability of decoy sequence 2% for COW and DPTS.



(b) *Histogram of fixed phase-time pattern* Alice send to Bob a fixed sequence in order to show the experimental feasibility of the protocol. Bob records photons with two Id-230 single-photon detectors with 20% of quantum efficiency, average dark counts rate 200/300 Hz and jitter about 300 ps. The repetition rate of the laser source is $\nu = 1.6$ GHz and the pulse train is phase modulated at 0.8 GHz.

Fig. 2. *Simulation of the secret key rate and PoC experiment.*

performance in terms of secret rate is significantly higher. In fact, the final secret key rate for DPTS is twice in the case of a short/middle link scenario, while in the long distance links, DPTS performance is comparable with the other protocols of the DPR family. We defined a bound on the security in the case of collective-attacks (BSA), which represents one of the most critical scenarios for QKD. Moreover, the security of the channel is continuously guaranteed by the random variation of the block length and by the random relative phase difference between empty and non-empty pulses. In conclusion, introducing this coherent two-dimensional DPR protocol, we provide a significant step towards fast, reliable, useful, integrated quantum communication. A complete experimental analysis will be presented at the conference.

References

[1] P. W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. en. *SIAM Journal on Computing* 26.5 (1997).

[2] C. H. Bennett and G. Brassard. Quantum Cryptography: public key distribution and coin tossing (1984).

[3] D. Stucki et al. Fast and simple one-way quantum key distribution. *Applied Physics Letters* 87.19 (2005).

[4] K. Inoue et al. Differential phase shift quantum key distribution. *Physical review letters* 89.3 (2002).

[5] N. Gisin et al. Towards practical and fast Quantum Cryptography. *arXiv:quant-ph/0411022* 0100.2 (2004).

[6] K. Inoue and T. Honjo. Robustness of differential-phase-shift quantum key distribution against photon-number-splitting attack. *Physical Review A - Atomic, Molecular, and Optical Physics* 71.4 (2005).

[7] V. Scarani et al. The security of practical quantum key distribution. *Reviews of Modern Physics* 81.3 (2009).

[8] I. Devetak and A. Winter. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences* 461.2053 (2005).