Experimental demonstration of the differential quadrature phase shift protocol

G. L. Roberts[1,2], M. Lucamarini[1], J. F. Dynes[1], S. J. Savory[2], Z. L. Yuan[1], A. J. Shields[1]
[1]Toshiba Research Europe Ltd, 208 Cambridge Science Park, Milton Road, Cambridge, CB4 0GZ, UK
[2]Cambridge University Engineering Department, 9 J J Thomson Ave., Cambridge, CB3 0FA, UK

Quantum key distribution (QKD) [1] is a technology that allows two parties to share a completely secure key. Whilst the technique has proven itself inside and outside laboratories [2], there is still potential for refinements, both in theory and implementation. The differential quadrature phase shift (DQPS) protocol has recently been proposed as an improvement to the well-established phase-encoded BB84 protocol [1]. Here we show the first proof-of-principle demonstration of this protocol, achieving megabit per second secure key rates, which are higher than those possible with phase-encoded BB84. We use a directly phase-modulated laser system based on optical injection locking to control the phase of the pulses within the same block and simultaneously randomize the phase of different blocks of pulses, as required by the DQPS protocol [3]. This development would enable high-rate QKD over metropolitan distances with a simple, stable and power efficient transmitter.

Distributed phase reference QKD protocols rely on maintaining a coherent phase between different optical pulses to guarantee security [1]. They were initially put forward by experimental groups to reduce the complexity of QKD systems. One example is the differential phase shift (DPS) protocol [4], which encodes information on the phase shift between two consecutive pulses. It can provide high key rates over long distances under the assumption of individual attacks [5, 6], however when full security is taken into account, its performance is seriously degraded [7, 8]. The DQPS protocol, on the other hand, maintains its superiority against the phase-encoded BB84 even in the presence of a full security proof [9].

DQPS splits a DPS signal into blocks of length L, each with a global phase that varies randomly between blocks. Each block is randomly assigned to the data basis $\{0, \pi\}$ or the check basis $\{\pi/2, 3\pi/2\}$, with L-1 bits in each block. The phase-encoded BB84 is thus a special case of the DQPS protocol, with L=2. The signal is then attenuated so that the probability of having more than one photon per block is relatively small. Bob measures the phase of his received pulses, telling Alice when he made a successful measurement, which is represented by having at least one click in his detectors. The users communicate their basis choice to sift the measurement results and then perform error correction and privacy amplification to obtain a secure key.

Figure 1(a) shows a schematic of Alice's transmitter and Bob's receiver. Alice's master laser prepares the phase that is inherited by the slave laser pulses. Small perturbations to the master laser within blocks give the phase shifts without affecting the coherence of the pulses. Deep modulations below the lasing threshold, however, ensure the cavity is depleted, breaking the phase continuity of the master laser between two successive blocks of pulses. This is an improvement over the current situation, where QKD transmitters require a separate component in order to randomize the phase, increasing the system complexity.

The slave laser is gain-switched at 2 GHz to produce a train of phase-modulated 70 ps pulses under optical injection from the master laser. A 512-bit pseudorandom pattern is input to the transmitter. A simulation is used to calculate the optimum block size and mean photon number for each channel attenuation, based on realistic experimental parameters. In Bob, a single photon detector is placed on one output port of an unbalanced Mach-Zehnder interferometer with a 500 ps time delay in one arm to interfere consecutive pulses. The heater is used to select a basis, and the number of counts and quantum bit error rate (QBER) are measured for both

bases until at least 4×10^5 counts are detected at each channel attenuation.

Figure 1(b) shows the results from our experimental demonstrations of DQPS and phase-encoded BB84 as well as their numerical simulations, which are in excellent agreement. An estimated secure key rate of 2.37 Mbit/s is achieved at an equivalent distance of 9 km, and positive key rates are achieved up to equivalent distances of 110 km using DQPS. We also conducted the experiment with three lengths of standard optical fiber, with the results showing close alignment to the data measured using an optical attenuator as the quantum channel. The average increase in key rate of DQPS over BB84 is 2.71 times, which is very close to the 8/3 increase predicted by the theory [9]. Figure 1(c) shows the resultant secure key rate over three days of acquisition with no active feedback. This outstanding stability removes the need for complicated stabilization routines.

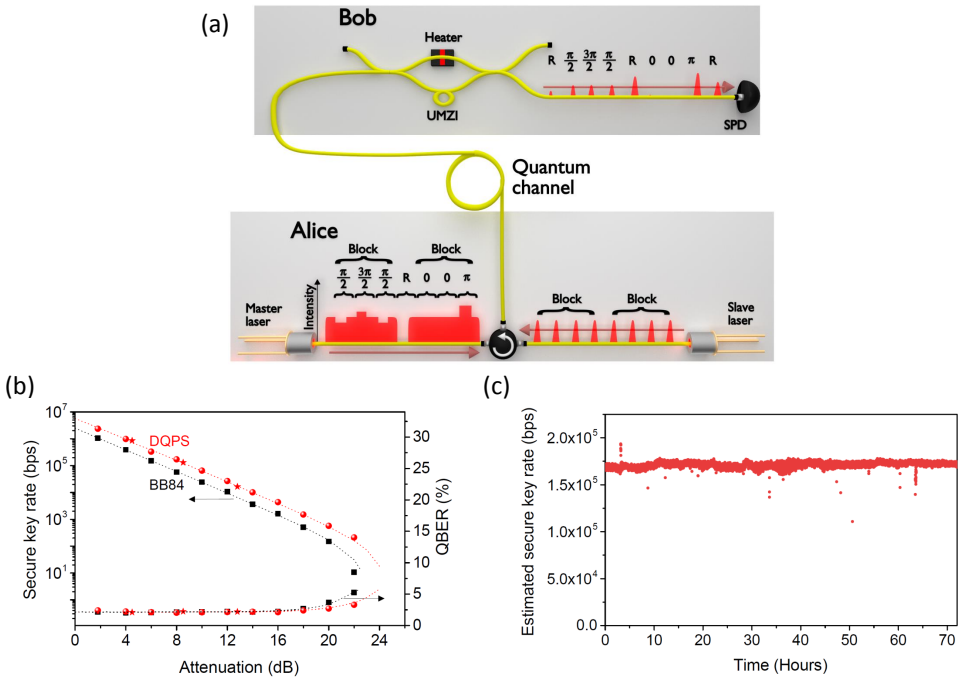

Figure 1: (a) Alice's directly phase-modulated transmitter and Bob's receiver for the DQPS protocol with a block size L=4. Light from the master laser is injected to the slave laser via a circulator to provide phase modulation. Each block has a globally random phase because of the cavity depletion between blocks. The slave laser is gain-switched to produce ultra-short pulses. UMZI: Unbalanced Mach-Zehnder interferometer; SPD: Single photon detector. (b) Estimated secure key rates and error rates for DQPS (red circles) and BB84 (black squares), alongside simulated rates (lines) and real fibre DQPS points (stars) (c) Estimated secure key rate over three days for a system with no active feedback over 8 dB of channel attenuation.

In summary, we have used a directly phase-modulated transmitter to realize the first experimental demonstration of the DQPS protocol. It has provided higher secure key rates than the standard BB84 protocol, whilst requiring no extra components for implementation. This could be added to a standard library of protocols in the future, specifically for providing high key rates over metropolitan distances. The low error rates of the source, its excellent stability with no active feedback and its versatility also highlight its potential to become the standard transmitter for quantum networks.

[1] V. Scarani *et al.* Rev. Mod. Phys. **81**, 1301 (2009)
[2] J. Qiu, Nature **508**, 441 (2014)
[3] Z. L. Yuan *et al.* Phys. Rev. X. **6**, 031044 (2016)
[4] K. Inoue *et al.* Phys. Rev. Lett. **89**, 037902 (2002)
[5] H. Takesue *et al.* Nat. Photon. **1**, 343 (2007)
[6] T. Honjo *et al.* Opt. Commun. **284**, 5856 (2011)
[7] T. Moroder *et al.* Phys. Rev. Lett. **109**, 260501 (2012)
[8] K. Tamaki *et al.* preprint arXiv:1208.1995 [quant-ph] (2012)
[9] S. Kawakami *et al.* Phys. Rev. A. **94**, 022332 (2016)