A high-speed multi-protocol quantum key distribution transmitter based on a dual-drive modulator

Boris Korzh, Nino Walenta, Raphael Houlmann, Hugo Zbinden

GAP-Optics, University of Geneva, CH-1211 Geneva 4, Switzerland

1 July 2013

Abstract

We propose a novel source based on a dual-drive modulator that is adaptable and allows Alice to choose between various practical quantum key distribution (QKD) protocols depending on what receiver she is communicating with. Experimental results show that the proposed transmitter is suitable for implementation of the Bennett and Brassard 1984 (BB84), coherent one-way (COW) and differential phase shift (DPS) protocols with stable and low quantum bit error rate. This could become a useful component in network QKD, where multi-protocol capability is highly desirable.

Introduction

Quantum key distribution enables the distribution of provably secure shared bit strings, which is an important fundamental primitive for many cryptographic tasks such as one-time pad encrypted secure communication [1] or message authentication [2]. Since the first theoretical conception [3], a wide variety of different QKD protocols have emerged and have been demonstrated in numerous real-world scenarios [4, 5, 6, 7].

For implementations in optical fiber telecommunication infrastructures, many QKD systems rely on quantum states in the time-phase domain to benefit from their inherent robustness against depolarization during propagation through the fiber. Moreover, the receiver of such systems can be rendered completely passive, without the need for active components which would introduce losses in the quantum channel and require the use of a fast random-number generator. Among the most prominent of such QKD protocols are the BB84 [3] time-phase coding scheme [8, 9], the COW protocol [10] and the DPS protocol [11].

Although many interesting approaches of distributing secret keys between different users have been demonstrated, independent of the physical connections in a fiber network [4, 6, 7], the physical layer of QKD systems is so far restricted to specialized transmitters and receivers running the same QKD protocol. However, in reconfigurable network environments there is a potential interest in the possibility of interconnecting systems that are not necessarily restricted to a single QKD protocol but that can adapt. In this way, one single transmitter station could perform QKD with receivers dedicated to different protocols, or a transmitter and receiver could choose the most efficient protocol for a given quantum channel without the need of a hardware change, providing a reduction in system complexity, management and cost.

In [12] it was shown that any arbitrary time-bin qubit state can be generated using a pulsed laser source, an imbalanced Mach-Zehnder Interferometer (MZI) and a dual-drive modulator (DMM). In this work we apply and extend this result to implement a simplified DMM based QKD transmitter which does not require a stabilized interferometer. Crucially, the lack of an interferometer at the transmitter allows for flexible time-bin period adjustment achieved by simply changing the DDM clock frequency. Such flexibility is essential when switching between receivers who may have a different interferometer path difference. This transmitter is especially suited for compact implementations of distributed phase reference protocols, namely COW and DPS, as well as BB84 schemes based on non phase randomized coherent states [13]. We present experimental results obtained with a GHz clocked QKD multi-protocol platform, which is based on a DDM transmitter, a reconfigurable receiver with free-running avalanche photodiode (APD) single photon detectors and a hardware-based key distillation engine. Our transmitter exhibits stable low quantum bit error rates (QBER) in both the time and phase bases, suitable for multi-protocol QKD in optical fiber infrastructures.

A DDM consists of two electro-optic phase modulators, one in each arm of an integrated MZI. The ability to control the phase shift in the individual interferometer arms using the electrical radio-frequency (RF) input ports, enables the generation of any arbitrary qubit state, limited only by the capability of the driving electronics. We implement a simple and robust way of generating the Z-basis (time-bin) and X-basis (phase encoded) states with the DDM as illustrated in Fig. 1, which allows the use of the three protocols mentioned previously.

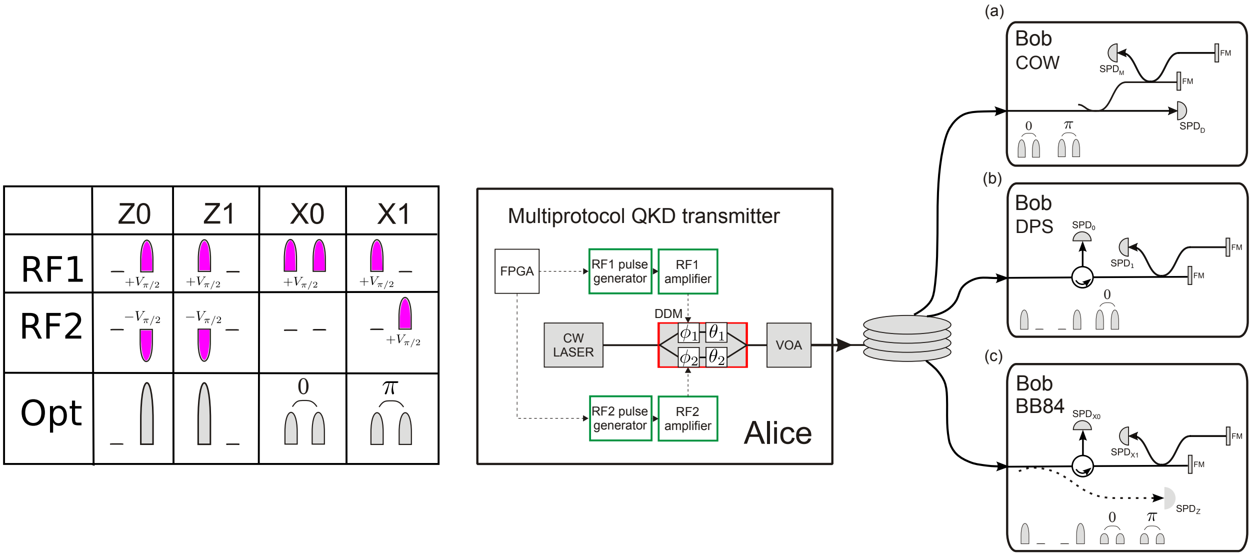

Figure 1: *Left:* Coding scheme for phase-time quantum state preparation enabling the use of BB84, COW and DPS protocols; Positive and negative electrical pulses (push-pull operation) in the two arms of the DDM produce the time basis states, whilst two consecutive positive pulses either in the same arm or alternate arms produce the phase basis states. *Right:* Sketch of the multi-protocol QKD transmitter and of three potential QKD receivers running the (a) COW, (b) DPS or (c) BB84 protocols. The transmitter is composed of a dual drive modulator which transforms the output of a continuous wave (CW) DFB diode laser, followed by a variable optical attenuator (VOA). A field-programmable gate array (FPGA) drives two radio frequency (RF) pulse generators by pulse sequences required for the relevant protocols. The receiver is implemented using an imbalanced Michelson interferometer and a free-running avalanche photodiode (APD) detection scheme.

Summary of results

It is important that the pulses generated by the transmitter are indistinguishable, i.e. the shape is independent of the bit value or the history of previous bit values. Mismatch in pulse shape for states encoded in the phase basis leads to errors due to imperfect interference. Moreover, a high extinction ratio is desirable, i.e. a good suppression of light in empty time bins, since this limits the QBER in the time basis. In Fig. 2 we show that the pulse shapes of phase encoded states are very similar and that the extinction ratio of the time basis states is >27 dB which should result in a QBER due to imperfect amplitude modulation in the region of only 0.2 %.

Running the multi-protocol QKD platform clocked at a time-bin frequency of 1.25 GHz we were able to test the performance of the DDM transmitter in a key exchange scenario. When testing the COW and BB84 protocols the encoding states were chosen randomly and transmitted at a qubit frequency of 625 MHz (each qubit has 2 time-bins). The DPS protocol allows the use of every time-bin to encode bit values, hence the qubit frequency in this case was 1.25 GHz. All of the detections on Bob's side were analyzed in real-time over a service channel of the hardware distillation engine.

Fig. 3 shows the QBER and sifted rate obtained for the BB84 and COW protocols for different losses in the quantum channel. For both low and high average photon numbers the errors are dominated by detector noise since the free-running APD detectors used are susceptible to significant dark counts and have a large deadtime (20 μs), which also limits the sifted rate drastically. For the BB84 protocol a minimum time basis QBER of 0.8% was obtained, 0.2% of which is attributed to detector dark counts whilst the remaining 0.6% is expected to stem from detector timing jitter and non-zero modulator extinction ratio. In the phase basis the minimum QBER was found to be 1.9% of which 0.4% is due to dark counts. We have also demonstrated stable operation of the DDM transmitter over 40 hours.

Conclusion

To summarize, we have demonstrated a novel optical quantum communication transmitter that can be applied to a large variety of QKD protocols. Moreover, the transmitter is constructed with off-the-shelf components, i.e. a commercial dual-drive modulator running at a frequency of 1.25 GHz, a continuous wave laser and a variable optical attenuator (VOA). It is possible to switch between different coding schemes by changing the electrical pulse sequences, attenuation of the VOA and the sifting procedure. Switching between receivers with different interferometer path differences is also possible by changing the electronic

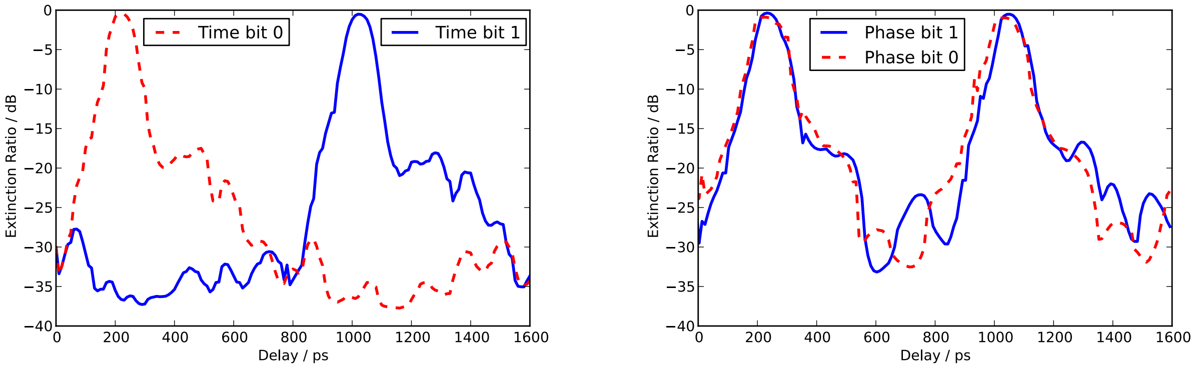

Figure 2: *Left:* Time basis extinction ratio for the two bit values encoded with light being sent in the early or late time-bins. *Right:* Phase basis extinction ratio with bits encoded in the relative phase of 0 or π between two pulses.

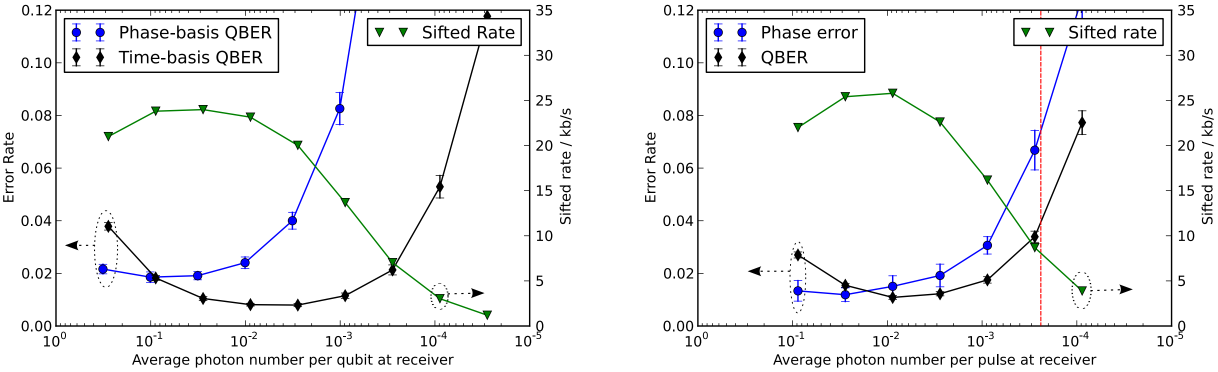

Figure 3: *Left:* Measured QBER in the time and phase bases along with the sifted rate for randomly prepared pulse sequences using the BB84 protocol for different losses in the quantum channel. *Right:* Measured QBER and visibility (converted into phase error rate for direct comparison) using the COW protocol. Dotted line indicates an estimated maximum transmission distance in this scenario, which is about 93 km (assuming fiber losses of 0.2 dB/km).

clock frequency. The preliminary experimental results show an extinction ratio of > 27 dB allowing time and phase coding with a stable QBER as low as 0.8 % and 1.9 % in the respective bases, even with non-ideal detectors. The source can simplify the extensions to network QKD environments where the use of a transmitter that can support different QKD protocols could be of interest in order to provide a reduction in system complexity, management and cost.

References

[1] Shannon. *Bell System Technical Journal*, 27:379–423 and 623–656, 1948.

[2] Portmann. *arXiv:1202.1229 [cs.IT]*, 2012.

[3] Bennett and Brassard. In *Int. Conference on Computers, Systems and Signal Processing*, pages 175–179, 1984.

[4] Peev et al. *New Journal of Physics*, 11(7):075001, 2009.

[5] Chen et al. *Opt. Express*, 18(26):27217–27225, Dec 2010.

[6] Stucki et al. *New Journal of Physics*, 13(12):123001, 2011.

[7] Sasaki et al. *Opt. Express*, 19(11):10387–10409, May 2011.

[8] Yoshino et al. *Optical Communication (ECOC), 2007 33rd European Conference and Ehxibition of*, pages 1–2, sept. 2007.

[9] Yoshino et al. *Opt. Lett.*, 37(2):223–225, Jan 2012.

[10] Stucki et al. *Applied Physics Letters*, 87:194108, 2005.

[11] Inoue et al. *Phys. Rev. Lett.*, 89:037902, Jun 2002.

[12] Tomita et al. *Optical Fiber Technology*, 16(1):55 – 62, 2010.

[13] Lo and Preskill. *Quantum Info. Comput.*, 7(5):431–458, July 2007.