Directly intensity-modulated quantum key distribution

George L. Roberts[1,2,*], Marco Lucamarini[1], James F. Dynes[1], Seb J. Savory[2], Zhiliang Yuan[1], Andrew J. Shields[1]

[1]*Toshiba Research Europe Limited, 208 Cambridge Science Park, Milton Road, Cambridge, CB4 0GZ, United Kingdom*

[2]*Cambridge University Engineering Department, 9 J J Thomson Avenue, Cambridge, CB3 0FA, United Kingdom*

[*]*george.roberts@crl.toshiba.co.uk*

Abstract: The coherent one-way (COW) protocol is implemented using direct laser modulation, with security enabled by optical injection locking. This method generates secure keys at rates above 1 Mbit/s with interference visibilities over 98 %.

OCIS codes: (060.5565) Quantum communications; (270.5568) Quantum cryptography.

1. Introduction

Data confidentiality is fast becoming one of society's most pressing issues. High-profile attacks are now commonplace and can expose millions of people's private details [1]. Quantum key distribution (QKD) provides us with a method of circumventing these issues using the fundamental laws of physics [2]. QKD encodes a secure key onto single photons, so two communicating parties can infer the presence of an adversary listening to the communication. In a real system, it is desirable to have a photon source that is stable, power efficient and has a small footprint. Direct laser modulation achieves this in classical communications, where the current through the laser is varied to modulate the light. This is commonly used for on-off keying communication [3]. This is not directly transferable to quantum communication protocols, however, because the frequency and phase of the laser change alongside the intensity. These simultaneous changes provide a side channel that an eavesdropper can use to obtain information about the key. This work aims to solve this problem for the COW protocol by providing a secure method of intensity modulation.

2. Experimental setup

We have recently demonstrated a QKD transmitter based on direct phase modulation of a laser diode which can be reconfigured to accommodate different QKD protocols [4]. The main concept behind this transmitter is the transfer of coherence from a master laser to a slave laser through optical injection, shown in Figure 1a. In the absence of optical injection, the system is operating as a gain-switched laser, so the interference between pulses produces random intensity outputs [5] and the overall interference contrast is zero. With optical injection, the coherence of the master laser is transferred onto the slave laser pulses. The coherence level of the slave laser increases with the injected power, until saturating at that of the master laser at a seeding power of 200 μW.

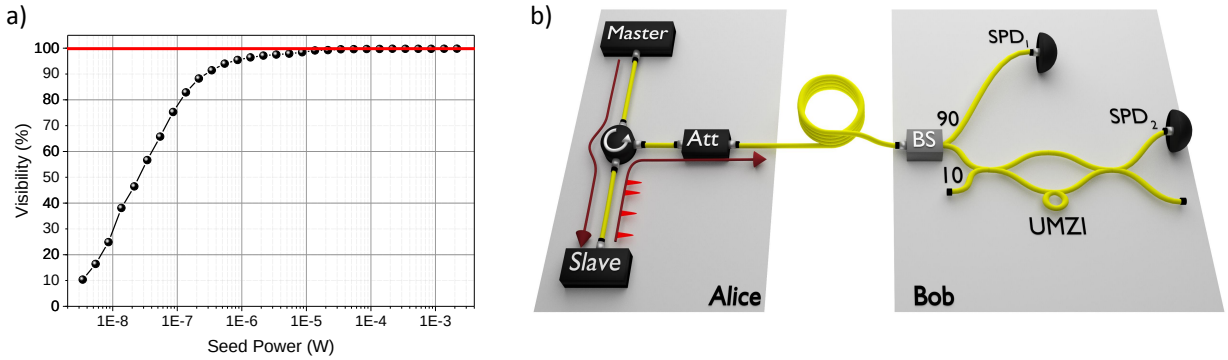

Fig. 1: (a) *Coherence transfer from a CW master laser to a 2 GHz gain-switched slave laser. The interference contrast is measured using a Mach-Zehnder interferometer (MZI) with a one-bit (500 ps) time delay. The red line shows the coherence of the master laser. The seed power is varied using an optical attenuator* (b) *Setup for the COW experiment. Att=attenuator, BS=beamsplitter and SPD=single photon detector.*

The transmitter has been proven for two QKD protocols based on phase modulation: BB84 and DPS. A number of protocols also rely on intensity modulation, however. One example is the COW protocol [6], which uses three signals: '0', '1' and a decoy bit, represented by $|\beta_0\rangle=|\alpha\rangle|0\rangle$, $|\beta_1\rangle=|0\rangle|\alpha\rangle$ and $|\beta_2\rangle=|\alpha\rangle|\alpha\rangle$ respectively, where $\mu=|\alpha|^2$, μ is the average number of photons per pulse and '$|0\rangle$' is an empty time bin. Coherence is maintained across all pulses, allowing the key to be encoded in the time basis and an eavesdropper to be detected at Bob by monitoring a drop in coherence of the transmission.

The key ingredient of the technique proposed here is the injection of a CW laser into a patterned slave laser. This allows the realisation of intensity modulation, whilst maintaining a high coherence. The resultant gain-switched pulses have a low jitter and a short temporal width of 70 ps. This experimental design is detailed in Figure 1b. A circulator gives efficient injection of the master laser into the slave laser with a high extinction ratio for the return direction. The pulses are then attenuated to contain 0.1 photons per pulse, before being sent to Bob. Bob splits the pulses into two arms through a 90:10 beamsplitter: the key measuring arm (SPD_1) and the coherence measuring arm (SPD_2). Superconducting nanowire SPDs with a 50% efficiency and a dark count rate of 10 Hz are used.

3. Results and Discussion

A variable optical attenuator is used to simulate six quantum channel lengths. The protocol is continued for each attenuation until 2×10^7 bits are detected in SPD_1. A finite key size analysis is then carried out according to [7], with a security parameter $\varepsilon_{QKD} = 10^{-10}$ defining the probability that the key is insecure. Around 10 % of the sifted bits are used for error correction. The final key rates are shown alongside the visibilities in Figure 2. The visibility remains above 97.5 % at all attenuations. At an optical attenuation of 10 dB, equivalent to 50 km of standard optical fibre with a loss of 0.2 dB/km, the quantum bit error rate (QBER) is 0.74 %, which gives a secure key rate of over 300 kbit/s. This exceptionally low QBER is possible because of the laser modulation technique.

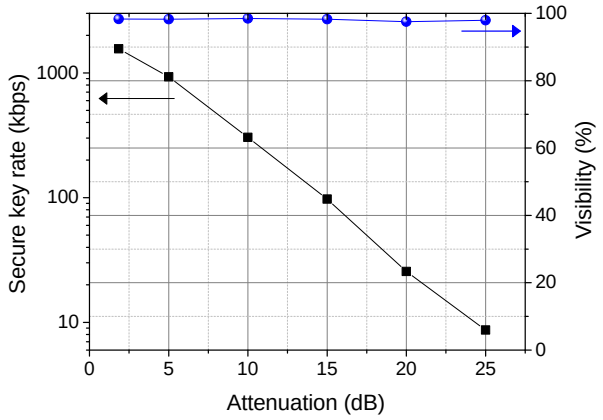

Fig. 2: *Secure key rates for a finite key size in the COW protocol, shown alongside the interference visibility.*

4. Conclusion

We have demonstrated the coherent one way protocol without any reliance on an external modulator. We achieve high secure key rates even at an attenuation equivalent to 125 km of optical fibre. This work opens the door to a stable, small-footprint, power-efficient transmitter that supports interoperability. The directly-modulated QKD transmitter would allow a central network hub to switch between different protocols as signals are sent to different clients, based on the clients' requirements.

References

1. Z. Durumeric *et al.*, Proc. of the Conf. on Internet Measurement Conf (ACM, 2014), pp. 475-488.
2. C. H. Bennett and G Brassard, Int. Conf. on Comput. Syst. and Signal Process., IEEE, (1984), pp. 175-179.
3. C. Xu *et al.*, IEEE Photonics Technol. Lett. **15**, 617-619 (2003).
4. Z. L. Yuan *et al.*, Phys. Rev. X **6**, 031044 (2016).
5. Z. L. Yuan *et al.*, Phys. Rev. Appl. **2**, 064006 (2014).
6. D. Stucki *et al.*, Appl. Phys. Lett. **87**, 194108 (2005).
7. B. Korzh *et al.*, Nat. Photon. **9**, 163-168 (2015).