77 day field trial of high speed quantum key distribution with implementation security

A. R. Dixon[2*], J. F. Dynes[1, 2], M. Lucamarini[1, 2], B. Fröhlich[1], A. W. Sharpe[1], A. Plews[1, 2], S. Tam[1, 2], Z. L. Yuan[1, 2], Y. Tanizawa[2], H. Sato[2], S. Kawamura[2], M. Fujiwara[3], M. Sasaki[3] and A. J. Shields[1, 2]

[1]*Toshiba Research Europe Ltd, 208 Cambridge Science Park, Cambridge CB4 0GZ, UK*
[2]*Toshiba Corporate Research & Development Center, 1 Komukai-Toshiba-Cho, Saiwai-ku, Kawasaki 212-8582, Japan*
[3]*Quantum ICT Laboratory, National Institute of Information and Communications Technology, 4-2-1 Koganei-city, Tokyo 184-8795, Japan*
alexander.dixon@toshiba.co.jp

Quantum key distribution's central and unique claim is information theoretic security. However there is an increasing awareness that the security of real QKD systems relies not only on theoretical security proofs, but also on how closely the system matches the theoretical models and resists known attacks. These hacking or side channel attacks exploit physical devices which do not necessarily behave precisely as the theory expects. As a result there is a need to demonstrate QKD systems providing both theoretical and implementation based security. We report here a QKD system which has been designed to provide these features of resistance to real security issues, component monitoring and failure detection – important not only from a security point of view but also for reliable and robust operation. Alongside the increased security confidence level the system operates with a high and stable secure key rate due to newly developed active stabilisation, averaging 210kbps and producing 1.33Tbits of secure key data over 77 days in a telecom network.

1. Introduction

Quantum Key Distribution is well known for its unique information theoretic security, as represented for example in the BB84 protocol[1]. As the experimental maturity of QKD has advanced so too has the understanding of important differences between the assumptions of the theory behind this security and the physical implementation. These differences could potentially be exploited by an eavesdropper, allowing attacks which bypass the presumed information theoretic security. This is a problem facing all cryptographic devices – classical cryptography hardware implementations have been demonstrated to be vulnerable to hacking targeting unexpected physical behaviour such as power usage[2] or computation timing[3] instead of the underlying mathematical algorithms.

While quantum key distribution theory guarantees information theoretic security, practical QKD systems must be carefully designed to adhere to the theory and avoid security loopholes which are outside of the theoretical models – so-called side channel or hacking attacks. Invariably reports of breaking the security of QKD refer to breaking a particular hardware implementation rather than attacks on the theory. A number of different hacking attacks have been proposed; some of the more well-known include photon number splitting attacks[4] (which can be mitigated using the decoy state protocol[5,6]), Trojan horse attacks[7,8] and detector control attacks[9–12]. Many of these attacks have also been demonstrated experimentally[13–17].

We focus on providing security against side-channel and hacking attacks for conventional QKD, which is practical and reliable with long term operation, high key rates, and integration on fibres with existing telecom infrastructure possible. While efforts are underway towards the standardisation of QKD[18], there is currently no consensus on security countermeasures against side-channel attacks, and as such we aim to develop and explore possible solutions.

In this article we report a QKD prototype system which has been designed to provide not only theoretical but also practical security against implementation flaws. Furthermore the system implements critical component monitoring for security and reliability, as well as refined stabilisation subsystems to provide consistent operation under harsh operating conditions such as those experienced during transmission through aerial fibre cables. We subject the QKD prototype to rigorous field testing by installing the system in a telecom fibre network located in metropolitan Tokyo. Over a 77 day period the system operated continuously and autonomously, with a secure key rate in excess of 200 kbps.

2. Prototype QKD System

The prototype QKD system consists of rack mount server sized (19" wide and 3U high) units, as shown in Figure 1. A compact size is made possible by using FPGAs and integrated electronics. One unit is the transmitter ("Alice"), and the second unit a receiver ("Bob"). The system is based around the BB84 protocol with decoy states, and uses phase encoded optical pulses with sub single photon intensities to transmit the quantum information. The QKD system implements an automated initialisation and alignment routine to allow single button start-up.

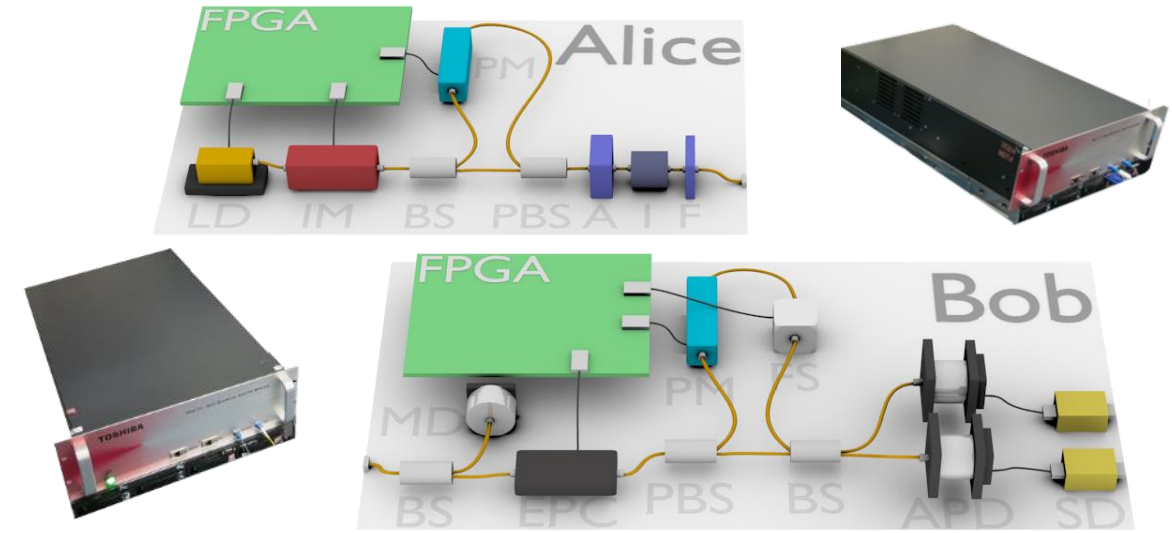

Figure 1: Photographs and schematic diagram of main components of the prototype QKD system, showing the transmitter (Alice) and receiver (Bob). LD: Laser diode, IM: Intensity modulator, BS: Beam splitter, PBS: Polarising beam splitter, A: Variable optical attenuator, I: Optical isolator, F: Narrow band pass optical filter, MD: Monitoring detector, EPC: Electronic polarisation controller, FS: Fibre stretcher, APD: Avalanche photodiode detector, SD: self-differencing circuit.

Figure 1 also shows an outline schematic of the major components in the QKD transmitter ("Alice") and receiver ("Bob"). The system operates at a 1 GHz transmission clock rate, with photon detection using self differenced[19] InGaAs/InP avalanche photodiodes (APDs).

Optical countermeasures consisting of attenuators (A), isolators (I) and spectral filters (F) are placed after the interferometer to provide a quantitatively analysed[20] resistance to the Trojan-horse attack[7]. In outline a bound is placed on how much light an eavesdropper can input before fibre damage occurs, and based on the characterised system reflectivity this places a bound on the reflected light intensity. This can then be used in a modified security proof to remove any information gained by the eavesdropper in this way. Approximately 170 dB of isolation is provided by the optical countermeasures.

The transmitter's laser diode temperature and output power is continuously monitored to ensure it is in the correct operating regime, and the system output power is constantly monitored and kept stable using the automated variable optical attenuator (A).

To provide an initial guard against potential APD blinding attacks[14] the input optical power is monitored at the receiver. In addition the APD module's temperature is also continuously monitored for any anomalies, which will further constrain possible hacking attacks[12]. The receiver unit is protected from Trojan horse attacks against the phase modulator through the internal fibre length and the propagation delay it introduces combined with the GHz modulation clock rate. This removes the possibility for Eve to receive any reflected light from the phase modulator before the modulated photon has been detected by Bob due to the photon time of flight[7].

3. Field Trial

The prototype system described in the previous section has been installed into a metropolitan area fibre telecom network[21] as shown in Figure 2. A fibre optic cable of 45 km length connects two sites, one an office building in central Tokyo and one a building in the western suburb of the city. The transmitter is installed in a server rack at the central location and connected to the receiver in the western location by two fibres from the cable; one is used for quantum signals and the second for all other communication data, such that no external network connection is required for the QKD system to operate. The fibre is of standard SMF-28 type with a total characterised loss of 14.5 dB, equivalent to 0.33 dB/km – this is increased compared to the typical laboratory fibre loss of 0.2 dB/km mainly due to splice and other connector losses. Approximately half of the fibre is located in underground ducts and half suspended above ground on aerial poles. Aerial fibre is in general much more exposed to environmental changes such as temperature and wind induced movement, which can affect the transmission characteristics (for example transit time and birefringence).

The system operated continuously for several extended periods of time during which the system was entirely automated, with no user control or adjustment of the system performed. Results from a typical 77 days of continuous operation are shown in Figure 3.

Over the period shown in Figure 3 the sifted key rate (94% of the raw rate) averaged 1.11 Mbit/s and QBER 3.47% and both remained stable, with approximately 5% standard deviation over the 77 days. This resulted in a secure key rate averaging 210 kbit/s and a total of 1.4 terabits of secure key data distributed. Despite several security enhancements to

Figure 2: Approximate location of the field trial of the QKD system, with the transmitter in central Tokyo and the receiver towards the western edge of the city. The two locations are connected by an installed telecom fibre pair with a length of 45 km (14.5 dB loss). [Map data: Google, SIO, NOAA, U.S. Navy, NGA, GEBCO, Image Landsat and Japan Hydrographic Association.]

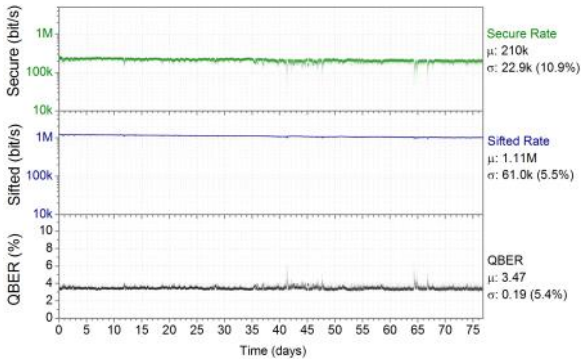

Figure 3: Field trial performance metrics of the prototype QKD system installed in a 45 km telecom fibre link over a 77 day period. From upper to lower the secure key rate, sifted key rate and QBER are shown along with their mean value (μ) and standard deviation (σ).

the current system the secure key rate is similar to the rate during a shorter field trial of a previous system[22] while the variation of all parameters is reduced. This is mainly due to the newly developed active stabilisation feedback subsystems which are based on PID feedback control and are able to cope with variable weather conditions.

The secure key rate is calculated with composable security (failure probability $\varepsilon = 10^{-10}$) on finite key block sizes (50 Mbit) and secure against collective attacks[23], with error correction and privacy amplification performed in real time.

4. Conclusion

We have reported the development and field trial performance of a high speed QKD prototype system. The system implements security counter-measures to prevent against side-channel hacking attacks, in particular providing a quantitative security against Trojan horse attacks and security against detector blinding attacks. Additionally components of the system including the laser diode and APDs are monitored continuously.

The system is contained within rack mountable units and can be automatically set-up and controlled using a graphical user interface. It was deployed between a telecom server room in central Tokyo and a remote location connected by 45 km of installed fibre. The system operated continuously, with the longest period of operation recorded as 77 days, the operation time limited by external power supply maintenance.

An alternative possible approach to avoid hacking attacks would be the use of "device independent" (DI) QKD[24,25], however even laboratory experimental demonstrations remain a challenge due to the requirement for a loophole free Bell test.

An intermediate proposal which provides some of the benefits of full DI QKD is measurement device independent (MDI) QKD[26,27]. However there remain significant challenges, not least the secure key rate which is several orders of magnitude below that of conventional QKD and the difficulty of accurately synchronising independent sources. However there has been recent progress in this area[28].

Furthermore while MDI-QKD is theoretically immune to attacks on the detectors, it will still require security counter-measures for the transmitter units – indeed in MDI-QKD the communicating parties (Alice and Bob) are both transmitter units. As such we believe the types of counter-measures reported here will be a useful tool for all future QKD systems, including those based on measurement device independent (MDI) QKD.

Acknowledgements

The work is partly supported by the Commissioned Research of National Institute of Information and Communications Technology (NICT), Japan.

References

[1] C. Bennett and G. Brassard, Proc. IEEE Int. Conf. Comput. Syst. Signal Process. **175**, 175 (1984).
[2] P.C. Kocher, J. Jaffe, et al., in *Adv. Cryptol. — CRYPTO '99* (1999), pp. 388–397.
[3] P.C. Kocher, in *Adv. Cryptol. — CRYPTO '96* (1996), pp. 104–113.
[4] G. Brassard, N. Lutkenhaus, et al., Phys. Rev. Lett. **85**, 1330 (2000).
[5] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[6] H.-K. Lo, X. Ma, et al., Phys. Rev. Lett. **94**, 15 (2005).
[7] A. Vakhitov, V. Makarov, et al., J. Mod. Opt. **48**, 2023 (2001).
[8] N. Gisin, S. Fasel, et al., Phys. Rev. A **73**, 022320 (2006).
[9] B. Qi, C.-H.F. Fung, et al., Quantum Inf. Comput. 9 (2005).
[10] V. Makarov, A. Anisimov, et al., Phys. Rev. A **78**, 019905 (2005).
[11] C. Wiechers, L. Lydersen, et al., New J. Phys. **13**, (2011).
[12] L. Lydersen, C. Wiechers, et al., Opt. Express **18**, 27938 (2010).
[13] N. Jain, E. Anisimova, et al., New J. Phys. **16**, (2014).
[14] I. Gerhardt, Q. Liu, et al., Nat. Commun. **2**, 349 (2011).
[15] L. Lydersen, C. Wiechers, et al., Nat. Phot. **4**, 5 (2010).
[16] Y. Zhao, C. Fung, et al., Phys. Rev. A 1 (2008).
[17] F. Xu, B. Qi, et al., New J. Phys. **12**, (2010).
[18] T. Länger and G. Lenhart, New J. Phys. **11**, 055051 (2009).
[19] Z.L. Yuan, B.E. Kardynal, et al., Appl. Phys. Lett. **91**, 41114 (2007).
[20] M. Lucamarini, I. Choi, et al., Phys. Rev. X **5**, (2015).
[21] JGNX Testbed (www.jgn.nict.go.jp) (2016).
[22] A.R. Dixon, J.F. Dynes, et al., Opt. Express **23**, 7583 (2015).
[23] M. Lucamarini, K.A. Patel, et al., Opt. Express **21**, 24550 (2013).
[24] D. Mayers and A.C. Yao, Proc. IEEE Symp. Found. Comp. Sc. 503 (1998).
[25] A. Acín, N. Brunner, et al., Phys. Rev. Lett. **98**, (2007).
[26] S.L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, (2012).
[27] H.-K. Lo, M. Curty, et al., Phys. Rev. Lett. **108**, 130503 (2012).
[28] L.C. Comandar, M. Lucamarini, et al., Nat. Photonics 1 (2016).