High speed prototype quantum key distribution system and long term field trial

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*

Abstract: Securing information in communication networks is an important challenge in today's world. Quantum Key Distribution (QKD) can provide unique capabilities towards achieving this security, allowing intrusions to be detected and information leakage avoided. We report here a record high bit rate prototype QKD system providing a total of 878 Gbit of secure key data over a 34 day period corresponding to a sustained key rate of around 300 kbit/s. The system was deployed over a standard 45 km link of an installed metropolitan telecommunication fibre network in central Tokyo. The prototype QKD system is compact, robust and automatically stabilised, enabling key distribution during diverse weather conditions. The security analysis includes an efficient protocol, finite key size effects and decoy states, with a quantified key failure probability of $\varepsilon = 10^{-10}$.

OCIS codes: (060.5565) Quantum communications; (060.2330) Fiber optics communications; (270.5568) Quantum cryptography; (270.5565) Quantum communications; (060.4785) Optical security and encryption.

References and links

1. C. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Proc. IEEE Int. Conf. Comput. Syst. Signal Process. **175**, 175–179 (2014).
2. A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, "Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate," Opt. Express **16**(23), 18790–18797 (2008).
3. Q. Zhang, H. Takesue, T. Honjo, K. Wen, T. Hirohata, M. Suyama, Y. Takiguchi, H. Kamada, Y. Tokura, O. Tadanaga, Y. Nishida, M. Asobe, and Y. Yamamoto, "Megabits secure key rate quantum key distribution," New J. Phys. **11**(4), 045010 (2009).
4. S. Wang, W. Chen, J.-F. Guo, Z.-Q. Yin, H.-W. Li, Z. Zhou, G.-C. Guo, and Z.-F. Han, "2 GHz clock quantum key distribution over 260 km of standard telecom fiber," Opt. Lett. **37**(6), 1008–1010 (2012).
5. H. Xu, L. Ma, A. Mink, B. Hershman, and X. Tang, "1310-nm Quantum key distribution system with up-conversion pump wavelength at 1550 nm," Opt. Express **15**(12), 7247–7260 (2007).
6. K. Patel, J. Dynes, I. Choi, A. Sharpe, A. R. Dixon, Z. Yuan, R. Penty, and A. Shields, "Coexistence of high-bit-rate quantum key distribution and data on optical fiber," Phys. Rev. X **2**, 041010 (2012).
7. J. Mora, W. Amaya, A. Ruiz-Alba, A. Martinez, D. Calvo, V. G. Muñoz, and J. Capmany, "Simultaneous transmission of 20x2 WDM/SCM-QKD and 4 bidirectional classical channels over a PON," Opt. Express **20**(15), 16358 (2012).
8. N. Walenta, A. Burg, D. Caselunghe, J. Constantin, N. Gisin, O. Guinnard, R. Houlmann, P. Junod, B. Korzh, N. Kulesza, M. Legré, C. W. Lim, T. Lunghi, L. Monat, C. Portmann, M. Soucarros, R. T. Thew, P. Trinkler, G. Trolliet, F. Vannel, and H. Zbinden, "A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing," New J. Phys. **16**(1), 013047 (2014).
9. M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A.

#226822 - $15.00 USD Received 28 Nov 2014; revised 20 Jan 2015; accepted 20 Jan 2015; published 16 Mar 2015

Zeilinger, "Field test of quantum key distribution in the Tokyo QKD Network," Opt. Express **19**(11), 10387–10409 (2011).

10. B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, "A quantum access network," Nature **501**(7465), 69–72 (2013).
11. A. Mirza and F. Petruccione, "Realizing long-term quantum cryptography," JOSA B **27**(6), 185–188 (2010).
12. D. Stucki, M. Legré, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, L. Monat, J.-B. Page, D. Perroud, G. Ribordy, A. Rochas, S. Robyr, J. Tavares, R. Thew, P. Trinkler, S. Ventura, R. Voirol, N. Walenta, and H. Zbinden, "Long-term performance of the SwissQuantum quantum key distribution network in a field environment," New J. Phys. **13**(12), 123001 (2011).
13. P. Jouguet, S. Kunz-Jacques, T. Debuisschert, S. Fossier, E. Diamanti, R. Alléaume, R. Tualle-Brouri, P. Grangier, A. Leverrier, P. Pache, and P. Painchault, "Field test of classical symmetric encryption with continuous variables quantum key distribution," Opt. Express **20**(13), 14030–14041 (2012).
14. K. Yoshino, T. Ochi, M. Fujiwara, M. Sasaki, and A. Tajima, "Maintenance-free operation of WDM quantum key distribution system through a field fiber over 30 days," Opt. Express **21**(25), 31395–31401 (2013).
15. K. Shimizu, T. Honjo, M. Fujiwara, T. Ito, K. Tamaki, S. Miki, T. Yamashita, H. Terai, Z. Wang, and M. Sasaki, "Performance of long-distance quantum key distribution over 90-km optical links installed in a field environment of tokyo metropolitan area," J. Lightwave Technol. **32**(1), 141–151 (2014).
16. S. Wang, W. Chen, Z.-Q. Yin, H.-W. Li, D.-Y. He, Y.-H. Li, Z. Zhou, X.-T. Song, F.-Y. Li, D. Wang, H. Chen, Y.-G. Han, J.-Z. Huang, J.-F. Guo, P.-L. Hao, M. Li, C.-M. Zhang, D. Liu, W.-Y. Liang, C.-H. Miao, P. Wu, G.-C. Guo, and Z.-F. Han, "Field and long-term demonstration of a wide area quantum key distribution network," Opt. Express **22**(18), 21739–21756 (2014).
17. T. E. Chapuran, P. Toliver, N. A. Peters, J. Jackel, M. S. Goodman, R. J. Runser, S. R. McNown, N. Dallmann, R. J. Hughes, K. P. McCabe, J. E. Nordholt, C. G. Peterson, K. T. Tyagi, L. Mercer, and H. Dardy, "Optical networking for quantum key distribution and quantum communications," New J. Phys. **11**(10), 105001 (2009).
18. D. Lancho, J. Martinez, D. Elkouss, M. Soto, and V. Martin, "QKD in standard optical telecommunications networks," Quantum Commun. **19**, 142–149 (2010).
19. T.-Y. Chen, J. Wang, H. Liang, W.-Y. Liu, Y. Liu, X. Jiang, Y. Wang, X. Wan, W.-Q. Cai, L. Ju, L.-K. Chen, L.-J. Wang, Y. Gao, K. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, "Metropolitan all-pass and inter-city quantum communication network," Opt. Express **18**(26), 27217–27225 (2010).
20. I. Choi, R. J. Young, and P. D. Townsend, "Quantum information to the home," New J. Phys. **13**(6), 063039 (2011).
21. C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, "Current status of the DARPA quantum network," Proc. SPIE 5815, Quantum Inf. Comput. III **138**, 138–149 (2005).
22. M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J. D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J. B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, "The SECOQC quantum key distribution network in Vienna," New J. Phys. **11**(7), 075001 (2009).
23. A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, "Continuous operation of high bit rate quantum key distribution," Appl. Phys. Lett. **96**(16), 161102 (2010).
24. J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, M. Fujiwara, M. Sasaki, and A. J. Shields, "Stability of high bit rate quantum key distribution on installed fiber," Opt. Express **20**(15), 16339 (2012).
25. H.-K. Lo, H. F. Chau, and M. Ardehali, "Efficient quantum key distribution scheme and a proof of its unconditional security," J. Cryptol. **18**(2), 1–46 (2005).
26. V. Scarani and R. Renner, "Quantum cryptography with finite resources: unconditional security bound for discrete-variable protocols with one-way postprocessing," Phys. Rev. Lett. **100**(20), 200501 (2008).
27. M. Lucamarini, K. A. Patel, J. F. Dynes, B. Fröhlich, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Efficient decoy-state quantum key distribution with quantified security," Opt. Express **21**(21), 24550–24565 (2013).
28. W.-Y. Hwang, "Quantum key distribution with high loss: toward global secure communication," Phys. Rev. Lett. **91**(5), 057901 (2003).
29. H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," Phys. Rev. Lett. **94**(23), 230504 (2005).
30. Z. L. Yuan, B. Kardynal, A. W. Sharpe, and A. J. Shields, "High speed single photon detection in the near infrared," Appl. Phys. Lett. **91**(4), 041114 (2007).
31. G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," Adv. Cryptology EUROCRYPT **93**, 410–423 (1994).

1. Introduction

Communication over fibre optic networks underpins a significant part of contemporary society. Economic, public and social activities all increasingly depend upon globe spanning fibre optic cables. As the importance of these networks has grown so too has the need to secure the

#226822 - $15.00 USD Received 28 Nov 2014; revised 20 Jan 2015; accepted 20 Jan 2015; published 16 Mar 2015

information crossing them, ensuring that users can identify each other and that their data is safe from interception and eavesdropping.

Quantum Key Distribution (QKD) [1] offers new and unique possibilities for securing this information, including detection of attempted interception and forward security free from assumptions about an adversary's abilities. QKD is now well studied in the laboratory, with high key rates [2–4] achieved simultaneously with wavelength division multiplexing [5–8] and network architectures [9,10]. The focus of much recent research has been directed towards the practicality of QKD – long term operation [11–16], deployment in real telecom networks [17–20] and linking together multiple different QKD systems [9,21,22].

Our initial high speed QKD system [2] occupied an entire laboratory and operated at its maximum 1 Mbit/s rate only for a few seconds. The next generation system implemented active stabilisation techniques to allow high speed operation over much longer times of more than one day [23]. From this laboratory bound system a compact and transportable system constructed from off-the-shelf electronics and optics was developed [24], and this was installed and operated in a field environment over 60 hours [9].

There are several challenges to developing a practical QKD system from a laboratory to the real world. Installed fibre optics are invariably subject to much stronger perturbations due to changing environmental conditions and physical stress, which in turn causes disturbance of the quantum states transmitted. Installed fibres also suffer from higher losses due to splices, sharp bends and inter-fibre coupling. The software and hardware of the QKD units must not only be designed to cope with all the conditions affecting the transmission fibre but also must be robustly engineered to operate in premises designed for standard telecom equipment. Furthermore, as the systems should run continuously and without frequent attention, they should also be designed to automatically recover from any errors and shield the end users from service interruptions.

With these challenges in mind, we build upon the previous work to report the design of a new prototype high speed QKD system intended for stable, long term operation. The optical subsystem is broadly the same as described in [9], while the controlling electronics are of an entirely new design and the corresponding control software has also been updated. The major advances include the integration of the dedicated commercial electronics and devices onto a custom field programmable gate array (FPGA) based printed circuit board (PCB) along with much improved software stability. This ground up design simplifies the electronic scheme and reduces the occurrence of unwanted glitches, allowing for unattended and reliable operation compared to the previous experimental type QKD systems. Integration of all electronics onto a PCB also has several advantages in terms of reduced electrical noise, size and power requirements as well as streamlined assembly and production.

The prototype system also implements an efficient version of the BB84 protocol [25] with finite-size composable security [26,27]. Composable security is a vital property for QKD keys as it ensures that the generated keys can be used in any required application without further security considerations. Keys are produced with a quantified failure probability of $\varepsilon = 10^{-10}$. The epsilon parameter is the deviation of the produced key from an ideal key, and can be interpreted as the maximum probability a key is produced which is not perfectly secure [26]. To put this number into context; for the chosen failure probability ($\varepsilon = 10^{-10}$) and typical key rate this equates to one key failure on the order of every 100,000 years.

One prototype system was installed into a 45 km link of a metropolitan telecom fibre network in Tokyo and we report data from its continuous operation over a period of 34 days. During this time the system ran unattended with no periods of down time or user interaction required. A total of 878 Gbit of key data was distributed, an average rate of 300 kbit/s over the 34 days. At the time of ending the 34 day trial the system was continuing to operate as normal, indicating that longer term operation than this would also be possible.

#226822 - $15.00 USD Received 28 Nov 2014; revised 20 Jan 2015; accepted 20 Jan 2015; published 16 Mar 2015

2. Methods – Prototype QKD system

2.1. FPGA based system

The prototype system (shown in Fig. 1) is based on a one-way, decoy-state [28,29] BB84 protocol [1]. In the transmitter (Alice) is a distributed feedback (DFB) laser pulsed at 1 GHz produces 1550 nm photon pulses with a 50 ps pulse width. These pulses pass through an intensity modulator from which three different pulse intensities for the decoy state scheme are created. Signal pulses of ~0.4 photons/pulse are sent with > 98% probability and two different decoy pulses of ~0.04 and ~0.0007 photons/pulse are sent with ≈1.5% and < 0.5% probability respectively. The bit and basis information is encoded in the photon's phase using a phase modulator (PM) in an asymmetric Mach-Zehnder interferometer (AMZI). In the efficient BB84 protocol [25], an unequal basis choice (97% majority, 3% minority) is used to minimise the sifting loss and maximise the secure key rate.

In the receiver (Bob) an electronic polarization controller (EPC) is used to correct for polarisation drifts which occur in the installed fibre. A PM located in the lower arm of Bob's AMZI is used for phase decoding and a fibre stretcher located in the upper arm for optical path length compensation. The photons from Bob's AMZI are then detected by single photon detectors composed of Peltier cooled InGaAs avalanche photodiodes (APDs) gated in Geiger mode at 1 GHz. This high gating speed is achieved with low avalanche current (which gives rise to low afterpulsing noise) by using a self-differencing technique to process the APD's output [30].

The FPGAs in Alice and Bob communicate directly to perform low level protocol functions such as photon time tagging and initial sifting, with key data passed to server computers which perform higher level post-processing and store the final secure key. The system is housed in three 19-inch rack mount units – one unit at Alice (transmitter) and two units at Bob (receiver and detector). All classical communication (protocol data, clock synchronisation, control signals) between the two units is carried out over one fibre optic cable, with a second fibre optic cable used for quantum communication. The use of separate fibres removes all noise, principally Raman scattering induced, on the very weak quantum signals caused by multiplexing with strong data signals. Although the focus of this paper is on long term stability of QKD in the field rather than single fibre QKD, we note that with suitable adjustments all signals can be combined on a single fibre, with a small penalty to the secure key rate [6].

Fig. 1. Photograph of the prototype high speed QKD system. The transmitter (Alice) is connected to the receiver (Bob, which includes a separate detector unit) by a pair of telecom fibres (not shown); the first fibre is used for quantum signals and the second fibre for classical communication.

2.2. Active stabilisation

The effects of environmental changes both in the transmission fibre and the installed unit locations can cause disturbances in the transmission of quantum states, and so for reliable continuous operation these effects should be counteracted. Several active stabilisation mechanisms are employed for this purpose. Changes in the overall length of the transmission fibre, mostly due to temperature variation causing expansion and contraction, are controlled by modifying an adjustable clock delay parameter at Bob such that the active time of the APD gating signal aligns with the photon arrival time. The timescale of this variation is typically on the order of 0.1 ps/s, increasing or decreasing depending on the rate of environmental temperature change, for example due to solar radiation. As such if uncorrected this would lead to a noticeable decrease in count rate after several hundred seconds. This clock delay adjustment also ensures correct temporal alignment of Bob's phase modulator.

The photon's polarisation state is used to increase the efficiency of the interferometer pair configuration through the use of polarising beam splitters, which ensure that transmission through non-interfering short-short and long-long paths are minimised. This ideally leads to 100% of photons interfering at the final beam splitter of Bob's interferometer. Only orthogonal polarisation states are used, so any arbitrary polarisation rotation occurring in the transmission fibre between the two interferometers can be reversed at the receiver using a multi-axis electrically controlled polarisation controller. This is driven from the FPGA card using the photon count rate as a feedback signal. The long-long and short-short path photons will arrive outside of the detector's active gate and so will not be included in this count rate. The timescale of the variation in polarisation rotation in the fibre again varies with environmental temperature, but is typically on the order of 1°/s. This would result in a noticeable count rate change in tens of seconds if uncorrected. This active compensation, together with the detector gate compensation, runs concurrently with QKD operation and does not introduce any loss in duty cycle or reduction on the secure key rate.

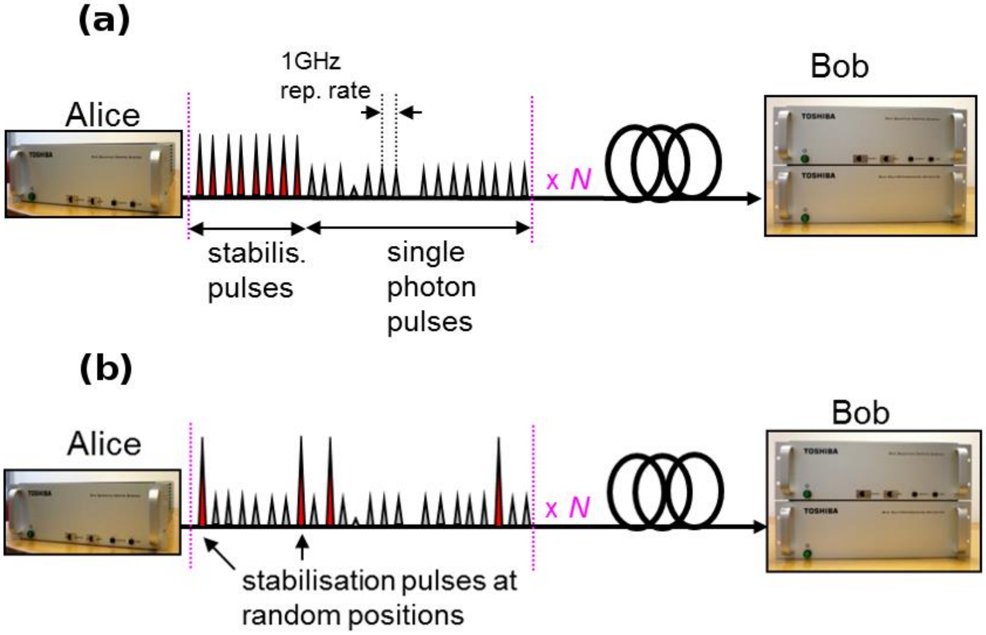

Fig. 2. Interferometer stabilisation pulse schemes. (a) Intense stabilisation pulses, sent in a known phase state and used to provide a feedback signal for the interferometer path length adjustment in Bob, are sent in a group after N single photon pulses. (b) The stabilisation pulses are placed at pseudo-random positions within the single photon pulses.

For high interference visibility it is necessary for the photon's phase from the two interferometer paths (short-long and long-short) to be exactly matched. We achieve this through the use of a fibre stretcher in one arm of Bob's interferometer to continually adjust this path's length and so maintain the phase alignment. Continual adjustment is necessary as the interferometers are constructed from fibre optics and are thus sensitive to temperature induced fibre expansion and contraction. As the transmitter and receiver are installed at remote locations

#226822 - $15.00 USD Received 28 Nov 2014; revised 20 Jan 2015; accepted 20 Jan 2015; published 16 Mar 2015

the difference in temperature variation can be significant necessitating an automated adjustment system. The phase of the interferometer drifts by around 4°/s if uncorrected, resulting in increases in QBER on a timescale of seconds if un-stabilised. This is implemented using stabilisation pulses; these are light pulses sent in a known phase state which are not used for generating key material and which can therefore be made more intense than the signal pulses. As these pulses are not used for key distribution their intensity can be greater than the normal signal pulses and as such only a small number are needed to generate a sufficient signal to noise ratio for feedback control of the fibre stretcher. The QKD system is capable of implementing two different stabilization schemes, as shown in Fig. 2. The first groups the stabilisation pulses together and the second uses sparse positioning. Sparse pulses reduce device artefacts caused by sending long trains of pulses into the phase and intensity modulators. Both schemes however enabled the interferometer path length to be stabilised correctly resulting in a low and consistent QBER.

2.3. Post processing

Post processing is performed in software using server computers, with all communication via 1 Gbps Ethernet routed over the dedicated classical communication fibre. Error correction is carried out using a multi-threaded implementation of the Cascade algorithm [24,31], which was measured to have an efficiency f_{EC} of 15–20% information leakage above the theoretical minimum. Privacy amplification is carried out using Toeplitz matrix multiplication. The secure key rate is calculated using a security analysis [27] which includes decoy states, finite key size effects, efficient BB84 basis choice and composable security with a failure probability of $\boldsymbol{\varepsilon} = 10^{-10}$.

3. Results

3.1. Lab results of detector stability

An often limiting factor for long term stable operation in QKD is the single photon detection system. Stable detector operation is important not only from a reliability perspective but also to avoid introducing bias in keys due to unbalanced detector efficiencies. Initially equalised detector efficiencies can drift over time to become unbalanced, resulting in a biased sifted key.

The detector unit contains two InGaAs APDs thermoelectrically cooled to −30°C. Thermoelectric cooling provides precise and reliable temperature control with no mechanical parts or coolants as failure points. The APDs are DC biased at a point below their breakdown voltage and activated using a square wave AC gating signal to periodically take them above the breakdown voltage. These voltages are applied using a custom PCB providing a high level of stability. The detectors' output is processed using an electrical self-differencing circuit [30] which subtracts the background signal from the previous gate, cancelling out the current gate's background and leaving only the detection signal. This enables much smaller detection signals to be discriminated against the background. This circuit is also implemented on a custom PCB and, combined with the precise temperature control and stable voltages, results in very stable detector efficiency as shown in Fig. 3. Over a 24 hour period the efficiency remains stable, approximately following a normal distribution with a 1% standard deviation.

#226822 - $15.00 USD Received 28 Nov 2014; revised 20 Jan 2015; accepted 20 Jan 2015; published 16 Mar 2015

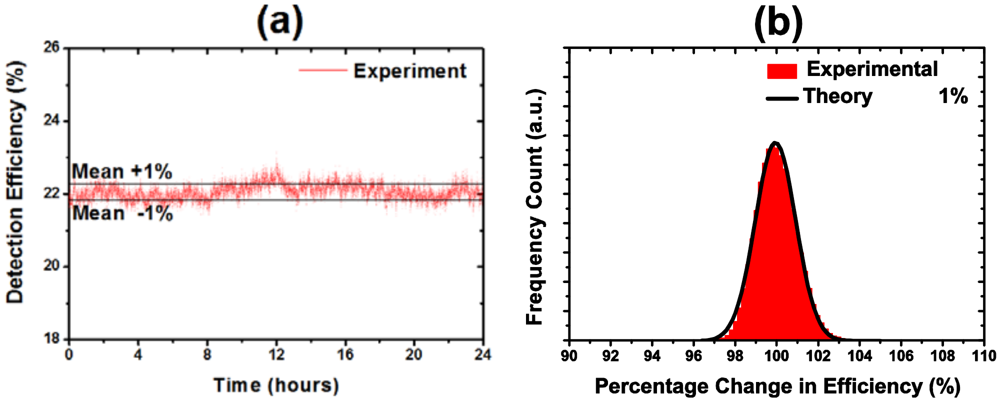

Fig. 3. (a) APD detector efficiency measured over 24 hours in laboratory conditions, along with bands indicating ± 1% of the mean value over this period. (b) Histogram of relative change in detector efficiency along with a distribution with 1% standard deviation.

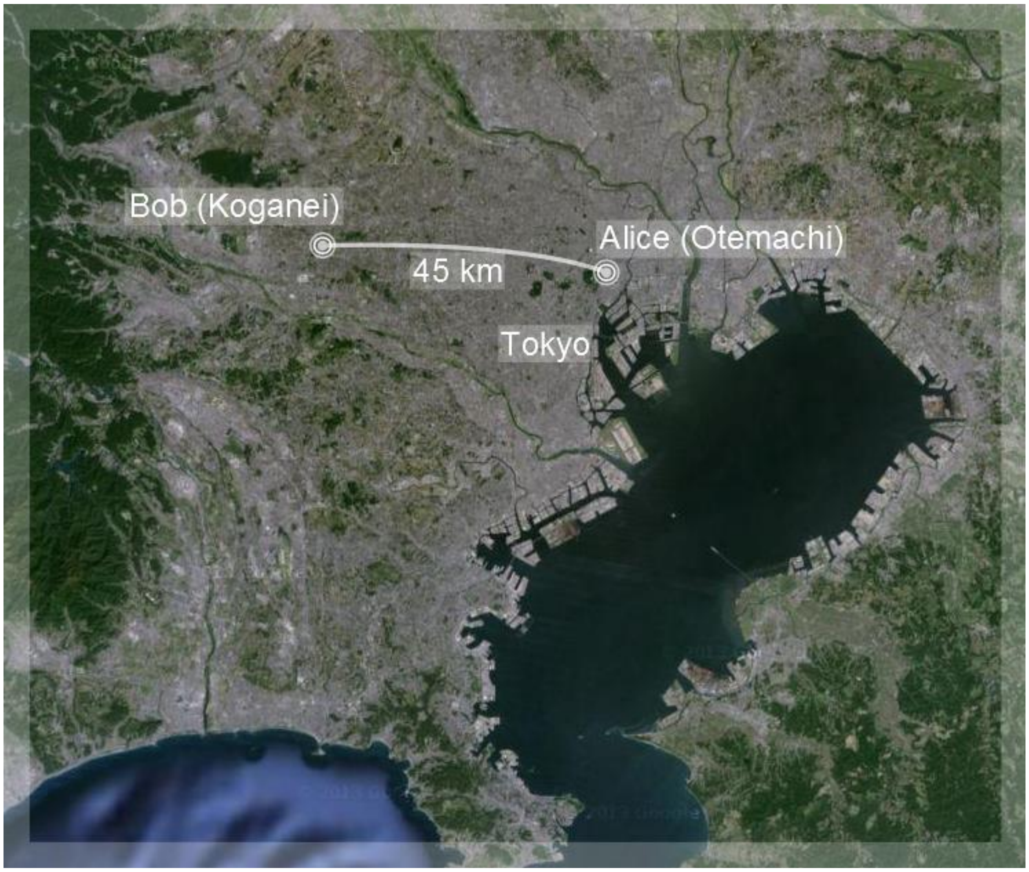

Fig. 4. Location of the field trial of the prototype QKD system. The two locations are connected by an installed telecom fibre pair with a length of 45 km and loss of 14.5 dB. (Map Imagery ©2014 TerraMetrics, Map data ©2014 Google, ZENRIN).

#226822 - $15.00 USD Received 28 Nov 2014; revised 20 Jan 2015; accepted 20 Jan 2015; published 16 Mar 2015

3.2. Field trial operation

One prototype QKD system was installed into a metropolitan area telecom network, with the transmitter located in a server room in central Tokyo (Otemachi) and the receiver at Koganei in the western outskirts as shown in Fig. 4. The locations are linked by a 45 km installed fibre pair with a loss of 14.5 dB (0.33 dB/km), much higher than standard spool fibre loss of 0.2 dB/km due to the presence of splices and other joints. One fibre from the pair was used for quantum transmission and one for classical communication. Approximately 50% of the fibre is above ground and suspended by aerial poles. This type of fibre is especially susceptible to environmental factors affecting the transmission characteristics and thus the received quantum states. These effects can include temperature changes, both from ambient air temperature and direct solar radiation, causing expansion and contraction of the fibre length and wind and precipitation causing fibre motion. The result is constantly changing conditions for the photon transmission, with the most important factors for QKD including transit time and birefringence changes.

As described above in Section 2.2 active stabilisation of Bob's clock delay parameter based on the detector gate position enables variations in photon transit time to be counteracted. However, in the field trial the control in clock delay required was small. As a clock synchronisation signal is sent through the classical fibre, and this fibre follows the same path and is subject to similar fluctuations as the quantum fibre, the arrival time of the quantum pulse remains closely aligned to the clock signal even with fibre length variations. The detector gate and other systems in Bob are synchronised to this clock signal and this makes the system mostly immune to fibre length changes. The active stabilisation then compensates for any residual timing difference between the classical and quantum signals to ensure an optimally high photon count rate.

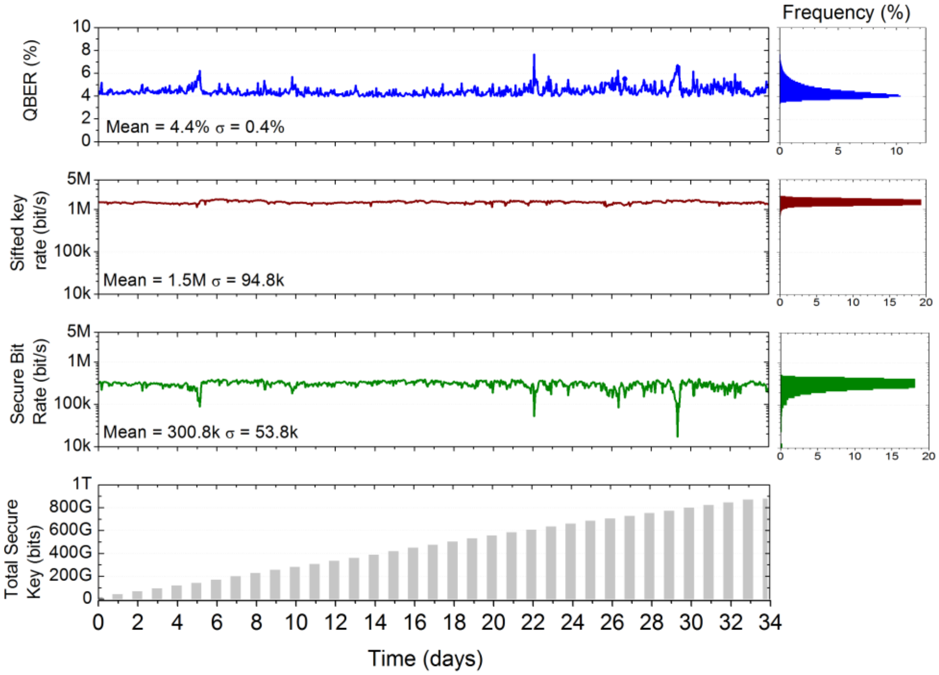

Fig. 5. Performance metrics of the prototype QKD system over a 34 day period while installed in the 45 km telecom fibre link shown in Fig. 4. From upper to lower the QBER, sifted key rate, secure key rate and total amount of secure key bits distributed are shown. For the first 3 parameters a frequency histogram is also shown to the right indicating the distribution of values.

4. Discussion – Comparison with other recent QKD field trials

Recently several other long term QKD field trials have been reported [12–15]. Figure 6 and Table 1 provides an overview; the points are experimentally reported results for secure key rate while the lines are an approximate guide to secure key rate variation with fibre loss assuming constant error rate. This assumption will not be valid for longer distances with increased loss. The field trials however all use different protocols, implementations and security proofs, and as such the level of security and true secure key rate may not be directly comparable between the systems. The present work adopts an applicable security analysis [27] and we believe reports both the largest amount of continuously distributed key material by a QKD system and the highest average secure key rate for a system installed in a field trial environment.

Table 1. Comparison of parameters of recent long term QKD system field trials.

	ID Quantique (2011) [12]	**SeQureNet (2012)** [13]	**NEC-NICT (2013)** [14]	**NTT-NICT (2014)** [15]	**USTC (2014)** [16]	**This work (2014)**
Protocol	SARG	CV	BB84	DPS	BB84	**BB84**
Link type	Point-to-point	Point-to-point	Loop-back	Loop-back	Point-to-Point	**Point-to-point**
Fibre loss	2.5 dB	5.6 dB	12.6 dB	29 dB	18.4 dB	**14.5dB**
Continuous operation period	~300 days	55 days	30 days	25 days	212 days	**34 days**
Secure bit rate	2.5 kbps	0.6 kbps	110 kbps	1 kbps	0.8 kbps	**301 kbps**
Total secure key material	64.8 Gbit	2.85 Gbit	295 Gbit	2 Gbit	14.1 Gbit	**878 Gbit**
Secure bit rate normalised to 10dB	0.44 kbps	0.22 kbps	200 kbps	79 kbps	5.3 kbps	**848 kbps**

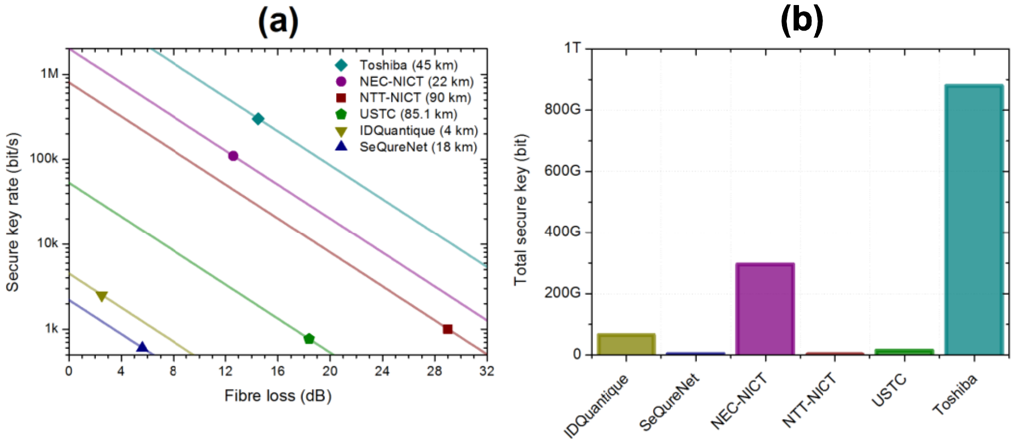

Fig. 6. (a) Secure key rate of recent QKD long term field trials shown as a function of fibre loss. Solid lines indicate secure key rates scaling with fibre loss. (b) Total amount of continuous secure key data distributed during the field trials.

5. Conclusion

We have reported a high speed QKD prototype based around FPGAs and custom PCB hardware. The system is robust, compact and easily installable in standard telecom environments.

#226822 - $15.00 USD Received 28 Nov 2014; revised 20 Jan 2015; accepted 20 Jan 2015; published 16 Mar 2015

The system was deployed in such an environment and operated over a 45 km fibre pair installed in Tokyo. Over a 34 day period the system operated continuously and without any user interaction, distributing 878 Gbit of secure key material in total at an average rate of ~300 kbit/s. The secure key rate is calculated using a security proof with composable security and a key failure probability of $\varepsilon = 10^{-10}$. The secure key rate was stable, and the system was able to continue operating uninterrupted throughout diverse weather conditions and continued to operate up until the termination of the trial.

Acknowledgments

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

#226822 - $15.00 USD Received 28 Nov 2014; revised 20 Jan 2015; accepted 20 Jan 2015; published 16 Mar 2015