Article

High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres

STUCKI, Damien, *et al*.

Abstract

We present a fully automated quantum key distribution prototype running at 625MHz clock rate. Taking advantage of ultra low loss (ULL) fibres and low-noise superconducting detectors, we can distribute 6000 secretbits s?1 over 100 km and 15 bits s?1 over 250 km.

New Journal of Physics
The open-access journal for physics

High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres

D Stucki[1], N Walenta[1], F Vannel[1], R T Thew[1], N Gisin[1], H Zbinden[1,3], S Gray[2], C R Towery[2] and S Ten[2]

[1] Group of Applied Physics, University of Geneva, 1211 Geneva 4, Switzerland
[2] Corning Incorporated, Corning, NY 14831, USA
E-mail: hugo.zbinden@unige.ch and GrayS@Corning.com

New Journal of Physics **11** (2009) 075003 (9pp)
Received 8 December 2008
Published 2 July 2009
Online at http://www.njp.org/
doi:10.1088/1367-2630/11/7/075003

Abstract. We present a fully automated quantum key distribution prototype running at 625 MHz clock rate. Taking advantage of ultra low loss (ULL) fibres and low-noise superconducting detectors, we can distribute 6000 secret bits s^{-1} over 100 km and 15 bits s^{-1} over 250 km.

Contents

[3] Author to whom any correspondence should be addressed.

1. Introduction

Quantum key distribution (QKD) [1] could well be the second commercial success of quantum physics at the individual quanta level after that of quantum random number generators [2] (QRNGs). The goal of QKD is to distribute a secret key between two remote locations with security relying on the laws of quantum physics. Since the initial proposal for QKD in 1984 [3], a lot of theoretical and experimental progress has been done, leading to the first commercial products [2, 4, 5]. For example, the separation between the remote locations was 32 cm in the first experimental demonstration [6] and now reaches tens of kilometres [7]–[12] with a record distance of 200 km in the lab [10] and more importantly, up to 150 km just recently in field trials [8]. However, despite these significant advances over recent years QKD's primary challenge is still to achieve higher bit rates over longer distances. In practice, these should be averaged secret bit rates after distillation and not peak raw rates.

In order to progress towards this challenge one needs:

- to develop new QKD protocols that go beyond the historical BB84 protocol and are especially designed for quantum communication over optical fibre networks,
- to optimize the single-photon detectors, as this is a major limiting factor,
- to use low loss fibres, as the channel loss will ultimately limit the achievable rate of future point-to-point quantum communication.

Protocols optimized for quantum communication over optical networks need to be robust against all sorts of decoherence mechanisms in the quantum channel—the optical fibre. For example, it should be intrinsically robust against fluctuations of the polarization even if it is possible to actively compensate theses fluctuations [13, 14]. A limiting factor for long-distance QKD is the dark counts of the detectors. Effectively, the probability of detection decreasing at long distance because of the high losses and the detector noise rate being constant lead to a too high error rate above a certain distance. Above this limit it is no longer possible to exchange a secret key. Therefore low-noise detectors are essential for long-distance QKD. Finally, limiting the losses in the fibre also allow us to extend the range of QKD.

In this paper, we present an experiment fulfilling these three requirements. Firstly, we implement the coherent one way (COW) protocol, which is well tailored for QKD at high speed and over long distances [8, 15, 16] (see also section 2). We also used low-noise superconducting single-photon detectors. Finally, we used ultra low loss (ULL) fibres from Corning®. These different elements allow us to distribute a key over 250 km. We can still add one important point: we developed a prototype running for hours without human intervention.

2. QKD protocol and prototype

As an efficient QKD protocol well suited for fibre-based quantum communication, we use the COW protocol [8, 15, 16]. The system, inspired by classical fibre optical communication, is functional and features inherently low loss: Alice, the transmitter, sends full and empty pulses, and Bob, the receiver, temporally distinguishes them with the help of his detector. There are,

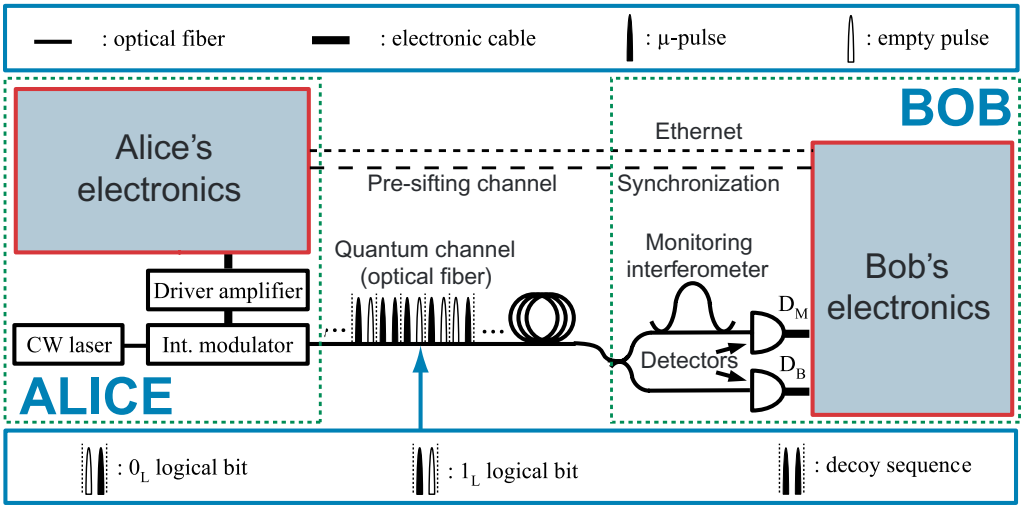

Figure 1. Schematic of the COW QKD protocol and its implementation.

however, three important differences with classical systems:

1. Alice's non-empty pulses are very weak, they contain a mean photon number of 0.5. Consequently, the two kinds of pulses have a common vacuum component and thus do not correspond to orthogonal quantum states.
2. As most of Alice's non-empty pulses cannot be detected by Bob, the bits are encoded in pairs of pulses, one empty and one non-empty; the bit value is defined by the position of the non-empty pulse: first = 0 and second = 1.
3. For true quantum communication, Alice and Bob have to verify the coherence (i.e. perform measurements in a basis conjugate to the data basis); this is done by Alice sending all pulses with a common phase reference, and Bob randomly selecting a small fraction of pulses, not used as data, to send to an interferometer. This coherence is measured between adjacent qubits. This means that an eavesdropper may not individually act on qubits by either removing one photon out of pulses with multiple photons, or by blocking pulses with only 1 photon, without disturbing the system and being detected. Therefore, the system is resistant to photon number splitting attacks. To avoid coherent attacks on two pulses across the bit separation, we also send decoy sequences [8, 15, 16].

Figure 1 shows a schematic of the COW protocol. The QKD prototype is built around field programmable gate arrays (FPGAs) (Virtex II Pro) and embedded computers for Alice and Bob. The Alice–Bob system controls: an intensity modulator shaping 300 ps pulses out of a cw beam emitted by a DFB laser, all communication between Alice and Bob, Bob's detectors, the secret key distillation, Alice's random number generator (4 Mb s^{-1} of QRNG, expanded to >312.5 Mb s^{-1}) and the fast electronics. The initialization and auto-alignment procedures involve synchronization of Alice and Bob's local clocks, optimal timing of the detection window for the detectors and adjustment of the phase between adjacent pulses to the passively stabilized interferometer by tuning the laser wavelength. The final secret bits are then stored, ready to be used, e.g. as in the SECOQC demonstration [17]. More system details can be found in [8].

(a) (b)

Figure 2. (a) Detector contact pad design and SEM image of the superconducting meander covering a $10\,\mu\text{m} \times 10\,\text{m}$ area. The strip widths are generally 100–120 nm with spacings of 80–100 nm, respectively. (b) Closed cycle pulse tube cryostat.

3. Superconducting single-photon detectors (SSPD)

In order to maximize the potential of the COW prototype, we employed two fibre-coupled superconducting SSPDs based on meandered NbN nanowires (figure 2(a)) [18]. Despite normally being cooled in liquid helium, SSPDs show great promise for long-distance QKD as they have a very low dark noise and the potential for high quantum efficiency. As part of the EU project SINPHONIA [19] we took a step towards their more practical integration and implemented these detectors in a cryogen-free, closed cycle, cryostat system (figure 2(b)).

The quantum efficiency of the SSPDs depends considerably on the cryostat temperature, on the bias current applied and, because of their meander-structure, on the polarization state of the incident photons [20]. It increases linearly with the applied bias current, while the corresponding dark count noise increases exponentially. Figure 3 shows the dark count rate as a function of the quantum efficiency of the better detector at 2.5 K, when the bias current is scanned. In our experiment, over 250 km, we used this detector for the data line, with a bias current of 26.5 μA (88% of the critical current), leading to quantum efficiency of 2.65% at a very low noise rate of 5 Hz. For all measurements we optimized the input polarization at the beginning of the key exchange. As changes in the environment temperature can affect the input polarization state, we also have to accept variations in the detection efficiency during long-term key exchanges (up to a factor 2). For the monitoring line we used an SSPD, which had a slightly lower detection efficiency at comparable dark count rates.

4. The ultra low loss fibres

A major limitation for all quantum communication is fibre loss. To this end, for this QKD experiment we have used a special low-attenuation ITU-T G.652 standard compliant fibre: Corning® SMF-28® ULL fibre [21]. This fibre has a Ge-free silica core (sometimes referred to as pure silica core fibres) with a low Rayleigh scattering coefficient [22]. The effective area and dispersion at 1550 nm are also comparable with standard installed fibre with about 85 μm^2 and 16.1 ps (nm-km)$^{-1}$, respectively. Typically, these low attenuation pure silica core fibres comply

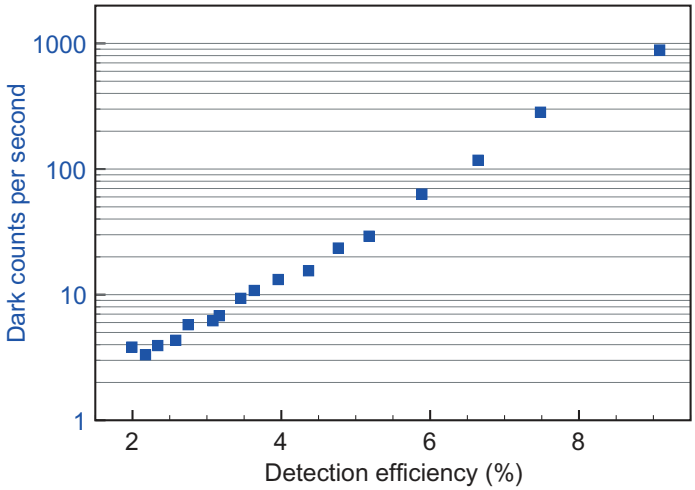

Figure 3. Dark count rate versus detection efficiency at 1550 nm for a cryogen-free SSPD at 2.5 K.

with the ITU-T G.654 standard, and are used in repeater-less submarine transmission systems where the lowest possible attenuation is highly desirable. For terrestrial applications where backwards compatibility with existing fibre plant can be an issue, the SMF-28® ULL fibre offers the advantage of a more straightforward integration into the installed network. However, it is the potential for very low attenuation fibres in terrestrial links that is interesting for QKD. The average fibre attenuation (without splices) is 0.164 dB km^{-1} at 1550 nm. Our 250 km link has a total loss 42.6 dB. This is equivalent to 213 km of standard fibre with attenuation of 0.2 dB km^{-1}.

5. Security

The proof of the security of the COW protocol is still a work in progress. The standard methods, developed to prove the security of QKD protocols, were designed for protocols in which the quantum symbols are sent one-by-one. As the COW protocol does not use a symbol-per-symbol coding, standard security proofs are not applicable in a straightforward manner. As is the case for the DPS protocol [10], the COW protocol is a so-called distributed-phase-reference protocol and its security relies on the coherence between successive non-empty pulses. To date, the COW protocol has been proven robust against some zero-error attacks, among which beam-splitting attacks [15, 16], [23]–[25] and a certain class of unambiguous state discrimination attack [23]. The security of the COW protocol against some intercept resend attacks has been shown in [15, 16, 23]. Finally, the security against a large class of collective attacks, under the assumption that Bob receives at most one photon per bit, has been proved in [24, 25]. In this instance, for the information of Eve, we take the estimate derived in [16]:

$$I_{\mathrm{AE}}(\mu) = \mu(1-t) + (1-V)\frac{1+\mathrm{e}^{-\mu t}}{2\mathrm{e}^{-\mu t}},$$

where the first term is due to the individual beam-splitting attacks and the second to the intercept–resend attacks. μ is the mean number of photons per pulse, t the transmission between Alice and Bob and V is the visibility of the interferometer.

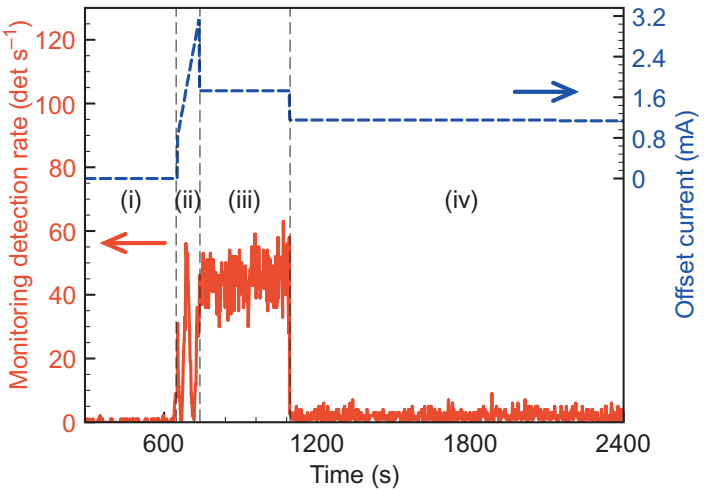

Figure 4. Detection rates at the monitor detector (red solid line) as a function of time and depending on the wavelength of the laser offset current (blue dashed line). From left to the right, we see the noise measurement (i), scanning of the laser wavelength leading to interference fringes (ii), constant wavelength in order to determine the maximum value (constructive interference) (iii), and wavelength tuned for the minimum (destructive interference) during the key exchange (iv). From (iii) and (iv) we calculate the visibility. In this measurement, the visibility was always higher than 92% over 2 h.

As such an upper bound on the secret key rate K can be given by

$$K = R(\mu)[1 - h(\mathrm{QBER}) - I_{\mathrm{AE}}(\mu)],$$

where $R(\mu)$ is sifted key rate and h(QBER) is the Shannon entropy for a given quantum bit error rate (QBER) that only depends on imperfect optical modulation and detection noise.

6. Results

We performed key exchanges in the laboratory over fibre lengths ranging from 100 to 250 km with secret bit rates from 6 kbits s^{-1} to 15 bits s^{-1} and QBERs from 0.85 to 1.9%, respectively. Figure 4 illustrates the operation of the monitoring line for a 100 km run. In an initial step, the laser wavelength is scanned in order to determine the visibility of the interference fringes and the optimal point of operation. After the exchange is started, the counts on the monitor detector are maintained at a minimum value by adjusting the wavelength. The registered counts and the corresponding fringe visibility give us Eve's potential information, which has to be taken into account during privacy amplification. The privacy amplification is implemented using hashing functions based on Toeplitz matrices [26]. Note, that the fibres used for synchronization/presifting and for classical communications were fixed at 100 and 25 km, respectively, in order to avoid the need for amplification of the classical signals.

Figure 5 presents the results obtained over 250 km of SMF-28® ULL fibre with our SSPDs. The horizontal scale denotes the time; at time 0 the prototype starts with an automatic adjustment of the electronic delays and initial alignment of the interferometer. The secret bit

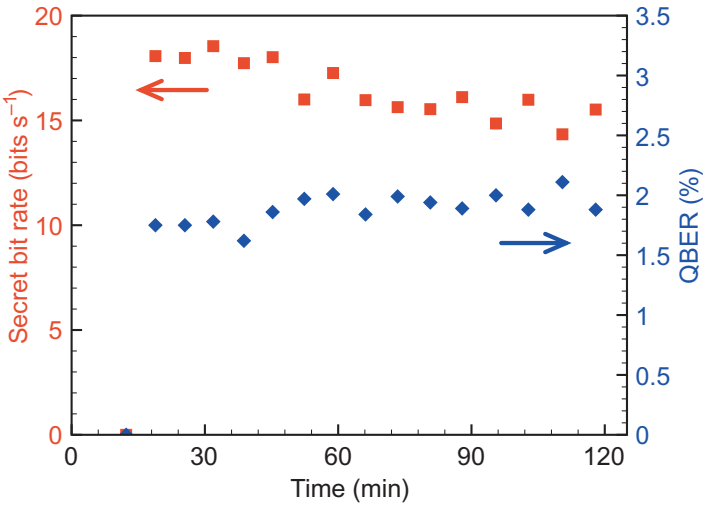

Figure 5. Mean secret bit rate per second over 250 km of ULL fibre (red squares) and corresponding QBER (blue diamonds) as a function of time from the start of the key exchange. Each point is the result of the distillation from 2^{15} bits of raw key leading to approximately 7000 secret bits per block.

distillation then starts only when the raw key buffer is full (2^{15} bits). Hence, for some initial time no key is generated. The error correction is realized with the Cascade algorithm [27]. A Wegman–Carter-type scheme, implementing universal hashing functions [28], is used for authentification. Albeit for some minor fluctuations, the system is then stable over hours, producing, on average, more than 15 secret bits s^{-1}.

Note that at this distance the count rate on the monitor detector is too low to correctly determine the visibility and to allow continuous alignment of the laser wavelength. Therefore the security for the key exchange at this extreme distance is questionable. The low detection efficiencies and high channel losses are the main limitations at these long distances and needs to be compensated by long acquisition times to obtain sufficient statistics. In the case of this COW system, this is not a problem up to distances of 150 km. For distances up to 200 km the software used for the alignment of the interferometer with the laser should be improved. Around 250 km, we estimate an accumulation time around 90 min to measure a visibility of 95% with a sigma of 2%. This would require active and independent stabilization of the interferometer and/or the laser wavelength. N.b. that the proof of the security over such long distances is particularly challenging for all QKD protocols [29].

Figure 6 summarizes several QKDs over distances ranging from 100 to 250 km. The secret bit rate over 100 km (6 kbit s^{-1}) is close to the actual record rate, which was obtained with a laboratory system without synchronization between distributed Alice–Bob systems [30]. For the last run at 250 km, the temperature of the detector's cryostat was particularly low and as such the data detector was operating with a lower noise and higher quantum efficiency for the same bias current. For this reason, the QBER did not continue to increase with respect to the other measurements and as a consequence the secret bit rate did not show the characteristic drop at the end of the range. Note that each point corresponds to the bit rate averaged over 10 min or more.

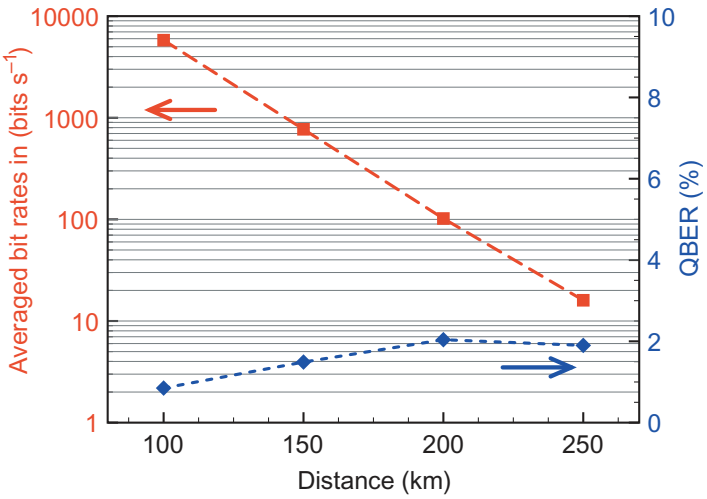

Figure 6. Averaged secret bit rates (red squares) and QBER (blue diamonds) for a range of SMF-28® ULL fibre lengths.

7. Conclusions

The performance of this COW QKD prototype is the product of a large mix of competencies, from theoretical physics (for the security analysis of protocols) to experimental physicists, telecom engineers and electronic and software specialists. Moreover, taking advantage of recent progress for SSPDs and optical fibre technology, we have demonstrated a quantum key exchange over a record distance of 250 km of optical fibre with over 15 bits s^{-1}. The target of distributing quantum keys over intercity distances of up to 300 km with meaningful secret key rates is in sight.

Acknowledgments

The Geneva group's work was supported, in part, by the EU projects SECOQC and SINPHONIA as well as the ERC-AG QORE and by the Swiss NCCR Quantum Photonics. We would like to thank C Barreiro and P Eraerds for technical assistance and helpful discussions.

References

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Quantum cryptography *Rev. Mod. Phys.* **74** 145–95
[2] http://www.idquantique.com
[3] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing* pp 175–9
[4] http://www.magiqtech.com
[5] http://www.smartquantum.com
[6] Bennett C, Bessette F, Brassard G, Salvail L and Smolin J 1992 Experimental quantum cryptography *J. Cryptol.* **5** 3–28
[7] Stucki D, Gisin N, Guinnard O, Ribordy G and Zbinden H 2002 Quantum key distribution over 67 km with a plug&play system *New J. Phys.* **4** 41

[8] Stucki D *et al* 2008 High speed coherent one-way quantum key distribution prototype arXiv:0809.5264 [quant-ph]
[9] Gobby C, Yuan Z L and Shields A J 2004 Quantum key distribution over 122 km of standard telecom fiber *Appl. Phys. Lett.* **84** 3762–4
[10] Takesue H, Nam S W, Zhang Q, Hadfield R H, Honjo T, Tamaki K and Yamamoto Y 2007 Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors *Nat. Photonics* **1** 343–8
[11] Tanaka A *et al* 2008 Ultra fast quantum key distribution over a 97 km installed telecom fiber with wavelength division multiplexing clock synchronization *Opt. Express* **16** 11354–60
[12] Rosenberg D *et al* 2009 Practical long-distance quantum key distribution system using decoy levels *New J. Phys.* **11** 045009
[13] Xavier G B, Walenta N, De Faria G V, Temporao G P, Gisin N, Zbinden H and Von der Weid J 2009 Experimental polarization encoded quantum key distribution over optical fibres with real-time continuous birefringence compensation *New J. Phys.* **11** 045015
[14] Hübel H, Vanner M R, Lederer T, Blauensteiner B, Lorünser T, Poppe A and Zeilinger A 2007 High-fidelity transmission of polarization encoded qubits from an entangled source over 100 km of fiber *Opt. Express* **15** 7853
[15] Gisin N, Ribordy G, Zbinden H, Stucki D, Brunner N and Scarani V 2004 Towards practical and fast quantum cryptography arXiv:quant-ph/0411022
[16] Stucki D, Brunner N, Gisin N, Scarani V and Zbinden H 2005 Fast and simple one-way quantum key distribution *Appl. Phys. Lett.* **87** 194108
[17] http://www.secoqc.net
[18] Korneev A *et al* 2007 Single-photon detection system for quantum optics applications *IEEE J. Quantum Electron.* **13** 944–51
[19] http://www.sinphonia.org
[20] Dorenbos S N, Reiger E M, Akopian N, Perinetti U, Zwiller V, Zijlstra T and Klapwijk T M 2008 Superconducting single photon detectors with minimized polarization dependence *Appl. Phys. Lett.* **93** 161102
[21] http://www.corning.com
[22] Ohashi M, Shiraki K and Tajima K 1992 Optical loss property of silica-based single-mode fibers *J. Lightw. Technol.* **10** 539–43
[23] Branciard C, Gisin N, Lütkenhaus N and Scarani V 2007 Zero-error attacks and detection statistics in the coherent one-way protocol for quantum cryptography *Quantum Inf. Comput.* **7** 639–64
[24] Branciard C, Gisin N and Scarani V 2008 Upper bounds for the security of two distributed-phase reference protocols of quantum cryptography *New J. Phys.* **10** 013031
[25] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dusek M, Lütkenhaus N and Peev M 2008 The security of practical quantum key distribution *Rev. Mod. Phys.* at press (arXiv:0802.4155 [quant-ph])
[26] Wegman M N and Carter J L 1981 New hash functions and their use in authentication and set equality *J. Comput. Syst. Sci.* **22** 265–79
[27] Brassard G and Salvail L 1994 Secret-key reconciliation by public discussion *Proc. on Advances in Cryptology—EUROCRYPT '93* (*Lect. Notes Comput. Sci.* vol 765) pp 410–23
[28] Wegman M N and Carter J L 1979 Universal classes of hash functions *J. Comput. Syst. Sci.* **18** 143–54
[29] Cai R Y Q and Scarani V 2009 Finite-key analysis for practical implementations of quantum key distribution *New J. Phys.* **11** 045024
[30] Dixon A R, Yuan Z L, Dynes J F, Sharpe A W and Shield A J 2008 Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate *Opt. Express* **16** 18790