New Journal of Physics
The open-access journal for physics

Practical long-distance quantum key distribution system using decoy levels

D Rosenberg[1,4], C G Peterson[1], J W Harrington[1], P R Rice[1], N Dallmann[1], K T Tyagi[1], K P McCabe[1], S Nam[2], B Baek[2], R H Hadfield[3], R J Hughes[1] and J E Nordholt[1]

[1] Los Alamos National Laboratory, Los Alamos, NM, USA
[2] National Institute of Standards and Technology, Boulder, CO, USA
[3] Heriot-Watt University, Edinburgh, UK
E-mail: rosenberg@lanl.gov

New Journal of Physics **11** (2009) 045009 (10pp)
Received 29 May 2008
Published 30 April 2009
Online at http://www.njp.org/
doi:10.1088/1367-2630/11/4/045009

Abstract. Quantum key distribution (QKD) has the potential for widespread real-world applications, but no secure long-distance experiment has demonstrated the truly practical operation needed to move QKD from the laboratory to the real world due largely to limitations in synchronization and poor detector performance. Here, we report results obtained using a fully automated, robust QKD system based on the Bennett Brassard 1984 (BB84) protocol with low-noise superconducting nanowire single-photon detectors (SNSPDs) and decoy levels to produce a secret key with unconditional security over a record 140.6 km of optical fibre, an increase of more than a factor of five compared with the previous record for unconditionally secure key generation in a practical QKD system.

Contents

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

1. Introduction

Quantum key distribution (QKD) holds the promise of communication with security resting firmly on the foundation of quantum mechanics rather than unproven assumptions regarding current and future computational resources. In the Bennett Brassard 1984 (BB84) protocol [1], the most common prepare and measure protocol, the sender (Alice) ideally encodes a single photon with a bit value of either 0 or 1 in one of two conjugate bases and sends it to the receiver (Bob). When Bob receives a photon, he measures it in one of the two bases. Alice and Bob then publicly share their basis choices and only keep the bits where the bases match. Because the information is encoded in a single photon, any tampering by an eavesdropper (Eve) results in an increased error ratio detectable by the legitimate users of the system. After performing error correction [2] to remove any errors that may have arisen from the operations of an eavesdropper or from imperfections in the experimental apparatus, Alice and Bob perform a privacy amplification step [3] to erase any partial information Eve might have obtained about the transmission. The final result is a string of 0s and 1s that Alice and Bob share but about which Eve has negligibly small information.

Although it is straightforward to see how QKD with ideal sources and detectors is secure, real-world QKD systems must contend with imperfect experimental components. In 2000, it was pointed out that the use of attenuated lasers (which emit photons in a Poissonian distribution) drastically limits the secure range of laser-based QKD systems [4]. Eve could perform a photon number splitting (PNS) attack in which she selectively changes the channel transmittance based on photon number but still maintains the expected rate of detections at Bob. If the rate of multi-photon pulses at Alice is larger than the rate of photon detections at Bob, then Eve could block all the laser pulses containing single photons, and only allow transmission of the multi-photon pulses, which are inherently insecure. In this case, the entire string of 'secure' bits could, in fact, be known to Eve.

Several methods have been proposed to mitigate the effects of PNS attacks. The most straightforward is to simply use a very low mean photon number μ, on the order of the channel transmittance, to guarantee that at least some of the detections at Bob originated from single photons at Alice [4]. Unfortunately, this results in very low secret bit rates as well as greatly limiting the possible transmission length due to dark counts in the detectors. The Scarani, Acin, Ribordy, Gisin (SARG) protocol [5], which allows for secure bits to be formed from both one- and two-photon signals, outperforms standard BB84, but it offers no performance advantage compared with BB84 with 'decoy states' as described below [6]. Differential phase shift QKD (DPS-QKD) is another method of protecting against PNS attacks [7], but a security proof against all attacks for the DPS-QKD protocol does not currently exist, so it does not provide the unconditional security needed for QKD.

The use of decoy states [8]–[11] with the BB84 protocol has provided a method for achieving high bit rates while protecting against PNS attacks and maintaining the underlying security of BB84. In a decoy state protocol, Alice transmits signals randomly picked from several different mean photon levels μ_j rather than just one. If Eve, who is ignorant of the μ_j value for each specific signal, were to attempt to perform a PNS attack, she would not be able to simultaneously modify the channel transmission for all the μ_j values to reproduce the expected statistics at Bob. By comparing the number of photon detections at each mean photon level, Alice and Bob can determine a rigorous bound on the number of single photons that have been received by Bob and incorporate this bound into the privacy amplification step.

Decoy state protocols have been demonstrated over a free-space link [12] and in several different fibre systems [13]–[21]. However, many of the demonstrations, although they are important proof-of-principle experiments, employ bi-directional systems [13, 14, 20] that are susceptible to Trojan horse attacks, or do not perform the full QKD protocol, including error correction and privacy amplification, but instead only estimate the secret bit rate and range of the system [19]. Furthermore, most fibre systems have employed either local synchronization (transmitter and receiver share the same clock) [15, 16, 21] or synchronization over a separate fibre [19], methods that pose a significant barrier for deployment. Although a practical uni-directional fibre system with remote synchronization has been demonstrated over short distances of 25 km with high bit rates [17, 18], the detectors used in these experiments were not sufficiently quiet to enable long-distance fibre QKD. Here we describe the first practical fibre QKD system capable of secure operation over distances greater than 100 km. The system uses a three-level decoy-state protocol in a fibre phase-encoding QKD system with independent clocks at the transmitter and receiver and low-noise superconducting nanowire single-photon detectors (SNSPDs). In addition to being secure against PNS attacks, our data are secure against Trojan horse attacks that afflict bi-directional systems and attacks based on differing timing responses between detectors [22].

2. Finite statistics decoy state protocol

The security of our protocol rests on knowing the number of sifted bits arising from single photons produced by Alice, and the disturbance, or bit error ratio, on those bits. Our approach has been to develop a finite statistics version of Koashi's security proof based on the uncertainty principle [23, 24]. The resulting secret bit yield has a form that is similar to that of Gottesman *et al* [25], with the addition of finite efficiency factors. The number of secret bits distilled from each basis is calculated as

$$N_{\text{secret}} = N_{\text{sifted}} \left[y_1^- \mu e^{-\mu} \left(1 - f_{\text{PA}} H_2(b_1^+)\right) - f_{\text{EC}} H_2(B) - \left(1 - \frac{1}{f_{\text{DS}}} H_2(z)\right) \right], \tag{1}$$

where N_{sifted} is the number of sifted bits in the selected basis, B is the observed bit error ratio in this basis, y_1^- is a lower bound on the transmittance of single photons, b_1^+ is an upper bound on the single-photon bit error ratio in the conjugate basis, z is the fraction of zeroes among the sifted bits in this basis, $H_2(\cdot)$ is the Shannon binary entropy function, and f_{PA}, f_{EC} and f_{DS} are privacy amplification, error correction and deskewing efficiency factors needed to accommodate the finite statistics of the data.

The decoy state protocol allows us to determine a lower bound on the single-photon transmittance y_1^- and an upper bound on the single-photon error ratio b_1^+. The value of y_1^- is the minimal value of y_1 satisfying the following inequalities:

$$Y_j^- \leqslant e^{-\mu_j} \sum_{n=0}^{\infty} \frac{(\mu_j)^n}{n!} y_n \leqslant Y_j^+,$$

where y_n is the transmittance of an n-photon signal and Y_j^+ (Y_j^-) is the upper (lower) bound on the yield of detection events when mean photon number μ_j is used for transmission. In contrast to other work where $Y_j^\pm$ are calculated assuming that the underlying detection statistics are Gaussian, we make no such assumption and use the full binomial distribution to calculate the bounds within a user-defined confidence level, ϵ, chosen to be 1×10^{-7} for this experiment. Our

protocol implements key distribution in a universally composable manner [26]–[28], resulting in a key that is ϵ'-secure, with $\epsilon' \leqslant 10\epsilon$ [24].

We use two methods to determine the single-photon error ratio b_1. The first, referred to as the 'worst-case' scenario, makes the conservative assumption that all observed errors occur on single photons. In this case, b_1^+ is simply equal to the number of observed errors divided by the number of sifted bits that arose from single photons prepared by Alice, which can be computed from the lower bound y_1^-. However, we can obtain a tighter bound on b_1 by utilizing the information contained in the differing error ratios at each μ_j and constructing a set of inequalities involving the bounds on the observed bit error ratios B_j and the n-photon bit error ratios b_n:

$$B_j^- \leqslant e^{-\mu_j} \sum_{n=0}^{\infty} \frac{(\mu_j)^n}{n!} y_n b_n \leqslant B_j^+.$$

Analogous to the method for finding y_1^-, b_1^+ is found by determining the maximal value of b_1 that satisfies these inequalities. Computing this tighter bound on b_1 can be carried out by linear programming, as for y_1^-, but here it is subject to quadratic constraints, so the analysis is computationally more intensive, although still tractable. In either case, the bounds on y_1 and b_1 are valid even if the quantum channel is time varying [29].

Equation (1) involves three efficiency factors (f_{EC}, f_{PA} and f_{DS}) that quantify finite statistics effects during the stages of QKD. Asymptotically, all three factors approach unity, but for a finite session length they are strictly greater than one. Reconciliation via practical error-correcting algorithms does not achieve the Shannon capacity of the binary symmetric channel, and the extra overhead in parity checks that needs to be communicated between Alice and Bob is expressed by the factor f_{EC}. Privacy amplification involves removing any partial information Eve may have gained by disturbing the single-photon signals that comprise the sifted bits. Following Koashi [23], we numerically compute the logarithm (base two) of the number of typical strings that are needed to describe with high confidence the output of a binary symmetric channel with a given bit flip probability, using the bit error ratio in one basis to determine the amount of privacy amplification required in the other basis. The factor f_{PA} denotes how much the size of this output differs from the Shannon entropy of the single-photon signals. The last finite statistics effect we consider is due to the imbalance between the two detector efficiencies, which leads to a bias between the 0s and 1s for the sifted bits in each basis. This bias can reduce Eve's search space of guessing over likely reconciled keys prior to privacy amplification. Asymptotically, Shannon entropy again gives the required reduction in secret information, but any practical algorithm for removing the bias, or *deskewing*, is likely to have inefficiencies, which is encompassed by the factor f_{DS}. We followed Peres [30] in iterating von Neumann's algorithm for generating unbiased bits out of the reconciled keys to determine the value of f_{DS}.

3. Automated QKD system

A diagram of the automated, reconfigurable QKD system used [31] is shown in figure 1. A 1550 nm distributed feedback laser emits photons with a 100 ps pulse width (full width half maximum (FWHM)) at a clock rate of 10 MHz, and the resulting photons are sent to Alice's phase encoder. The photon wavepacket is split into a 'short' and a 'long' path, and the portion of the wavepacket that traversed the long path is modulated by the electro-optic phase

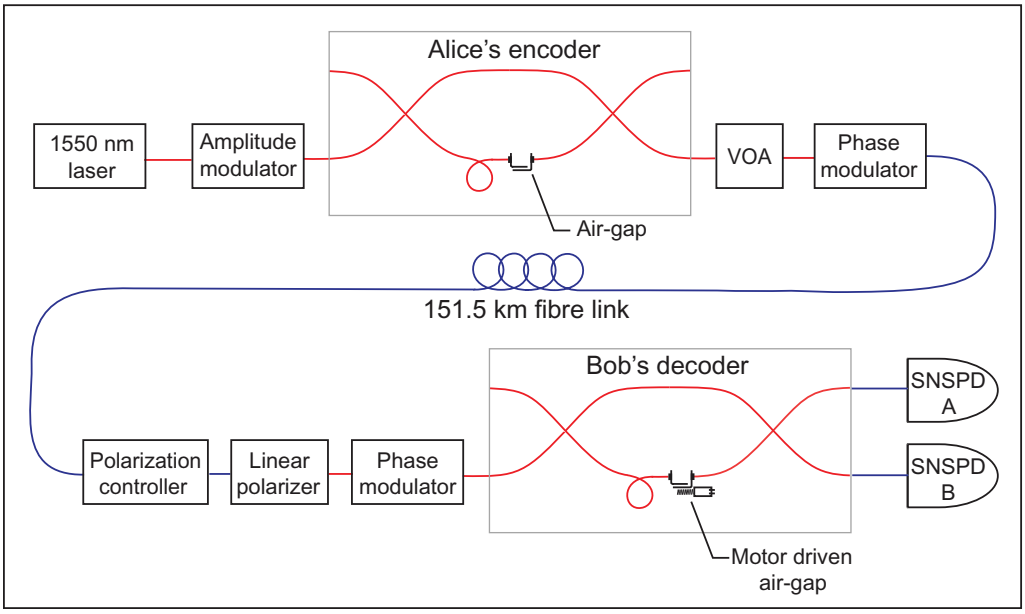

Figure 1. Optical train of the phase-encoding QKD system used in this work. The variable optical attenuator (VOA) provides attenuation to the single-photon level, from which the amplitude modulator provides the different μ_j levels needed for the decoy level protocol. Red lines indicate polarization maintaining fibre, and blue lines represent single-mode fibre. Photons are detected by two SNSPDs biased to yield matching detection efficiencies.

modulator, located outside the interferometer for stability. Likewise, the wavepacket is again split in Bob's decoder, and only the part of the wavepacket that travelled through Alice's long path is modulated. Interference ultimately occurs between the Alice-long-Bob-short and Alice-short-Bob-long amplitudes. Polarization maintaining fibre is used within the interferometers to ensure that these two paths are indistinguishable.

The quantum channel consists of 151.5 km of spooled dark optical fibre in an isolated container. The measured fibre attenuation was 0.206 dB km^{-1}, and shorter distances are obtained by redefining Alice's enclave to include a portion of the fibre. The bit and basis selections at Alice and Bob are determined by the outputs of physical random number generators, and a high-speed optical switch, driven by a pseudo-random pattern, provides the three intensity levels needed for our decoy state protocol. (In a deployed system, the pseudo-random pattern generator would simply be replaced by a physical random number generator.) We tested various combinations of sending probabilities and attenuation levels to determine the accuracy of the mean photon numbers. Including long-term drifts, the overall accuracy of the μ levels was $\sim$0.1 dB, which is in good agreement with the number of photons detected at Bob.

The SNSPDs [32] used for these measurements are cooled to 3 K in a closed-cycle refrigeration system and coupled to single-mode telecom fibre. They operate in ungated mode with a measured timing jitter of 69 ps and a recovery time of $<$10 ns. The detectors were individually current biased to a matching detection efficiency of 0.5%, resulting in a summed average dark count rate over the entire acquisition period of 78.1 counts s^{-1}.

The system is fully automated and able to run for many hours without user intervention. Independent rubidium oscillators are employed as frequency references at Alice and Bob and

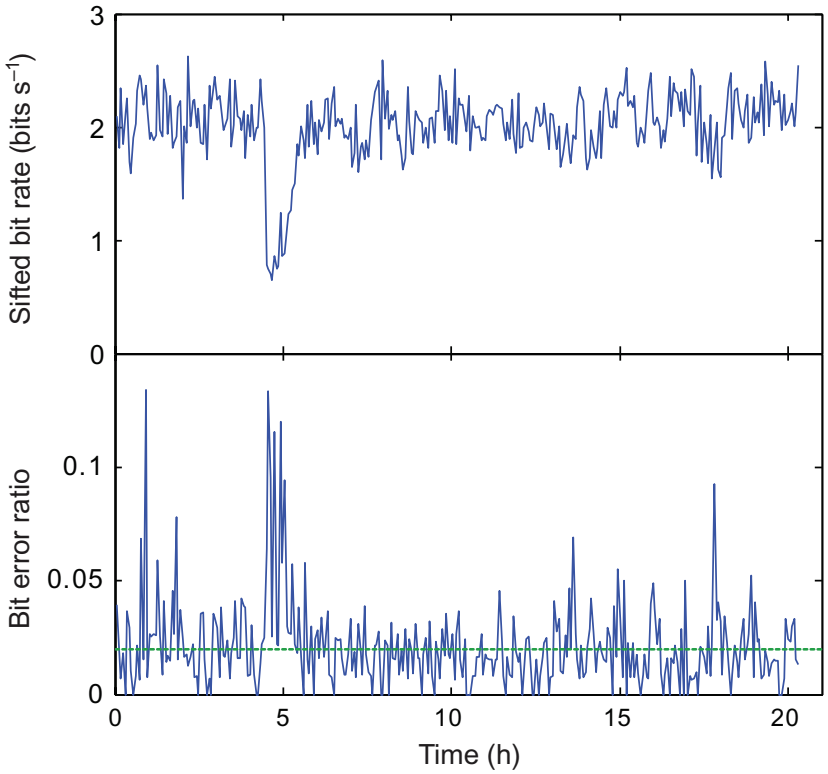

Figure 2. Sifted bit rate and bit error ratio for entire data run. Bit rate and error ratio are for data at μ_2, and each point is an average over 60 s of acquisition time. The dashed green line shows the average error ratio of 2.01%. Approximately 4.5 h into the data run, the bit rate fell and the error ratio increased, probably indicating a polarization misalignment. The system was able to recover from this error without any user intervention. Data from the entire run period were used to make secret bits.

are synchronized prior to each QKD run. To synchronize the clocks, the mean photon number is set to a very high value (corresponding to several thousand detection events per second at Bob), and the received detection events are used to create a photon arrival time histogram that is used to determine the current average frequency offset between the two oscillators, which is corrected by adjusting one of the clocks' frequencies. After the synchronization step but before the QKD session, a tuning step is performed to keep the interferometer balanced. Tuning runs are insecure sessions executed at a high photon number to quickly obtain the statistics needed for interferometer adjustments, while QKD runs adhere to the requirements for secure key generation. To minimize the effects of system de-tuning, tuning runs are promptly followed by QKD runs. The use of ungated detectors and post-selection of detection timestamps in software relaxes the system timing requirements to the phase modulator voltage pulse width, 2–3 ns, rather than being constrained to the sub-nanosecond electrical detector gate width required for avalanche photodiodes. However, we observed that the width of the peaks in the arrival time histograms was typically only a few hundred picoseconds, indicating that our synchronization scheme should work at clock rates up to 1 GHz under these conditions. Periodically, the polarization controller is automatically adjusted to compensate for any polarization drifts within the fibre by maximizing transmission through the linear polarizer.

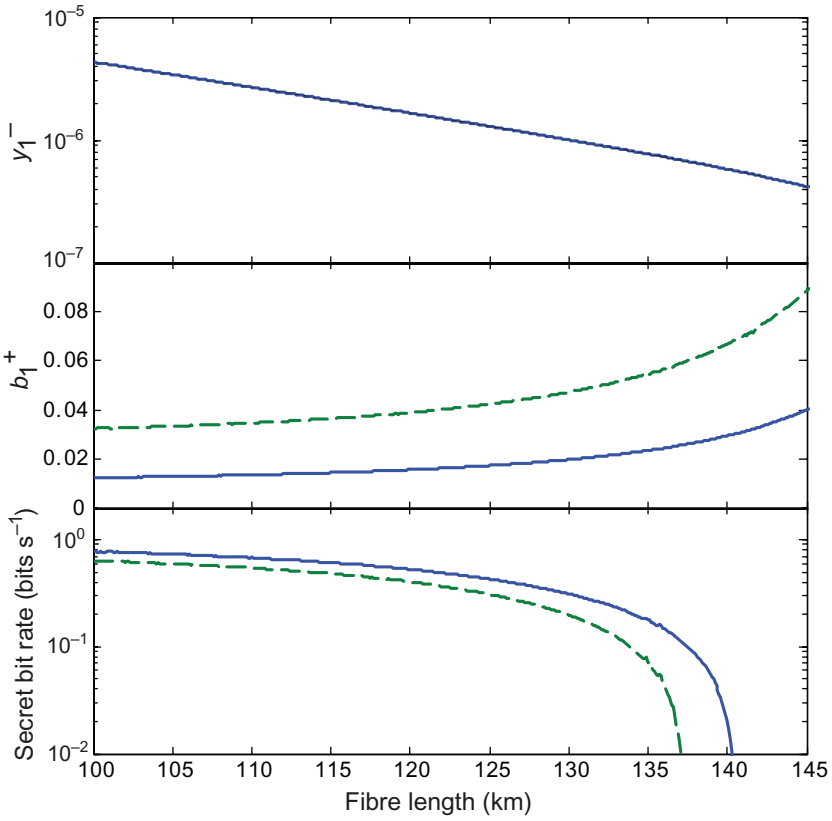

Figure 3. (a) Bound on single-photon transmittance y_1^-; (b) bounds on the single-photon error ratio b_1^+ assuming either the 'worst case' (dashed green line) or by finding a tighter bound (solid blue line); and (c) secret bit rate using forward error correction as a function of distance. Data were acquired over a 151.5 km link, and the decoy levels and sending probabilities were chosen to maximize the secret bit rate at 135 km.

4. Results and conclusions

We chose μ_j values with associated sending probabilities that were near-optimal for a fibre length of 135 km based on the results of simulations. The selected mean photon numbers were ($\mu_0 = 0.0025$, $\mu_1 = 0.13$ and $\mu_2 = 0.57$) (μ_0, ideally the vacuum state, was constrained to be 23.5 dB below the high μ_2 level by the extinction ratio of the switch) with associated sending probabilities (0.1, 0.2, 0.7). Before each 10 s QKD run, a 1 s clock synchronization step and two 500 ms tuning runs were performed. The system was allowed to run for 20.3 h before being stopped manually. Not including the overhead time for classical communication, synchronization and tuning, QKD data were acquired for 5.6 h. Figure 2 displays the stability of the sifted bit rate and bit error ratio of the system over the entire data run.

In 5.6 h of acquisition time and using a timing window of 184 ps, the number of detection events recorded at μ_2, μ_1 and μ_0 was 80 776, 5729 and 341, respectively, and a total of 40 538 sifted bits with a bias (fraction of zeros in one basis) of 0.494 were created. The sifted bits and the basis choices both passed the FIPS 140–2 cryptographic randomness tests [33]. After data were collected, the bits were sifted and error corrected using either a regular (3,14)

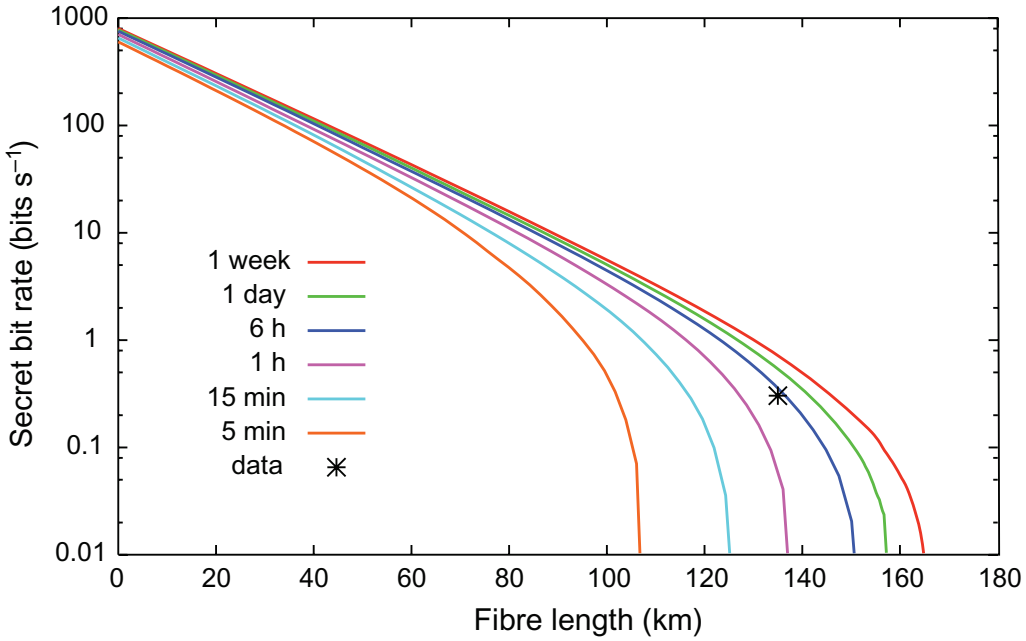

Figure 4. Simulated performance of system used in this work for different acquisition times and distances. The optimal mean photon number and sending probabilities are found for each distance and acquisition time. The data point at 135 km matches the prediction of the simulation. Even with an efficiency of 0.5%, the SNSPDs enable the creation of secret bits out to 166.1 km.

low-density parity check forward error correction code, or the modified CASCADE protocol for interactive error correction [34]. Using interactive error-correcting codes yields more secret bits than forward error correction, but the security of a protocol using two-way error correction has not yet been conclusively proven. The error-corrected bits were then privacy amplified as described in equation (1) after determining the bounds on the single-photon transmittance and error ratio. The efficiency factors due to the finite data size were determined to be $f_{\mathrm{EC}} \approx 1.06$ for the modified CASCADE protocol and $f_{\mathrm{EC}} \approx 1.51$ for forward error correction, $f_{\mathrm{PA}} \approx 1.09$ and $f_{\mathrm{DS}} \approx 1.05$. As a final step, Wegman–Carter authentication [35] was performed on the secret bits and all the messages between Alice and Bob.

As shown in figure 3, b_1^+, the bound on the single-photon error ratio, is significantly higher when the worst-case assumption that all the errors occur on single photons is made. The tighter b_1 bound not only yields more secret bits at any given distance, but it also extends the distance over which secret bits can be exchanged. In the case where forward error correction is performed, use of the 'worst-case' b_1 results in 1412 secret bits at 135 km and a maximum range of 137.4 km. When the tighter bound on b_1 is used, 3549 secret bits are produced at 135 km and the range of the system is extended to 140.6 km, a new record for key distribution secure against general attacks [25], including PNS attacks. Using the modified CASCADE protocol for error correction extends the distance even further to 144.3 km.

By choosing different mean photon numbers and sending probabilities and acquiring data for longer times, it would be possible to extend the range even further in this system. Figure 4 shows the results of simulations based on the system properties to determine the maximum

range of the system. With the same detectors used in this work, this system could achieve a range of 166.1 km. Although the detection efficiency of these detectors is currently quite low, by embedding the detectors in a stack of optical elements designed to increase absorption at the target wavelength [36] and improving the optical coupling to the detector, it should be possible to increase the system detection efficiency considerably. An increase to 50% (assuming the same dark count and background photon rates) would result in bit rates higher by approximately two orders of magnitude at any given distance in the asymptotic limit, and an increase in the tolerable link loss to over 50 dB. From our results, which are the first demonstration of assured security over long distances in a practical system, we can infer that reasonable improvements in component technology will result in several hundred bits per second over distances of 100 km, more than an order of magnitude higher than what is presently available.

Acknowledgments

The authors thank Joe Dempsey and Corning, Inc. for the optical fibre, Thomas Chapuran and Nicholas Peters for helpful discussions and G Gol'tsman for providing the original detectors used in this work. The authors acknowledge support from IARPA, the Department of Commerce, the NIST quantum information science initiative and the Royal Society of London.

References

[1] 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 (Bangalore, India)* p 175

[2] Brassard G and Salvail L 1994 Secret-key reconciliation by public discussion *Lect. Notes Comput. Sci.* **765** 410

[3] Bennett C H, Brassard G, Crepeau C and Maurer U M 1995 Generalized privacy amplification *IEEE Trans. Inf. Theory* **41** 1915

[4] Brassard G, Lutkenhaus N, Mor T and Sanders B C 2000 Limitations on practical quantum cryptography *Phys. Rev. Lett.* **85** 1330

[5] Scarani V, Acin A, Ribordy G and Gisin N 2004 Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations *Phys. Rev. Lett.* **92** 057901

[6] Fung C-H F, Tamaki K and Lo H-K 2006 Performance of two quantum-key-distribution protocols *Phys. Rev.* A **73** 012337

[7] Takesue H, Nam S, 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] Hwang W-Y 2003 Quantum key distribution with high loss: toward global secure communication *Phys. Rev. Lett.* **91** 057901

[9] Lo H-K, Ma X and Chen K 2005 Decoy state quantum key distribution *Phys. Rev. Lett.* **94** 230504

[10] Wang X-B 2005 Beating the photon-number-splitting attack in practical quantum crytography *Phys. Rev. Lett.* **94** 230503

[11] Harrington J W, Ettinger J M, Hughes R J and Nordholt J E 2005 Enhancing practical security of quantum key distribution with a few decoy states arXiv:quant-ph/0503002

[12] Schmitt-Manderbach T *et al* 2007 Experimental demonstration of free-space decoy-state quantum key distribution over 144 km *Phys. Rev. Lett.* **98** 010504

[13] Zhao Y, Qi B, Ma X, Lo H-K and Qian L 2006 Experimental quantum key distribution with decoy states *Phys. Rev. Lett.* **96** 070502

[14] Zhao Y, Qi B, Ma X, Lo H-K and Qian L 2006 Simulation and implementation of decoy state quantum key distribution over 60 km telecom fiber In *Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing* p 2094

[15] Rosenberg D, Harrington J W, Rice P R, Hiskett P A, Peterson C G, Hughes R J, Lita A E, Nam S and Nordholt J E 2007 Long-distance decoy-state quantum key distribution in optical fiber *Phys. Rev. Lett.* **98** 010503

[16] Peng C-Z, Zhang J, Yang D, Gao W-B, Ma H-X, Yin H, Zeng H-P, Yang T, Wang X-B and Pan J-W 2007 Experimental long-distance decoy-state quantum key distribution based on polarization encoding *Phys. Rev. Lett.* **98** 010505

[17] Yuan Z L, Sharpe A W and Shields A J 2007 Unconditionally secure one-way quantum key distribution using decoy pulses *Appl. Phys. Lett.* **90** 011118

[18] Dynes J F, Yuan Z L, Sharpe A W and Shields A J 2007 Practical quantum key distribution over 60 h at an optical fiber distance of 20 km using weak and vacuum decoy pulses for enhanced security *Opt. Express* **15** 8465

[19] Yin Z-Q, Han Z-F, Chen W, Xu F-X and Guo G-C 2008 Experimental decoy quantum key distribution up to 130 km fiber *Chin. Phys. Lett.* **25** 3547

[20] Hasegawa J, Hayashi M, Hiroshima T, Tanaka A and Tomita A 2007 Experimental decoy state quantum key distribution with unconditional security incorporating finite statistics arXiv:0705.3081 [quant-ph]

[21] Dixon A R, Yuan Z L, Dynes J F, Sharpe A W and Shields A J 2008 Gigahertz decoy quantum key distribution with 1 mbit s^{-1} secure key rate *Opt. Express* **16** 18790

[22] Lamas-Linares A and Kurtsiefer C 2007 Breaking a quantum key distribution system through a timing side channel *Opt. Express* **15** 9388

[23] Koashi M 2006 Unconditional security of quantum key distribution and the uncertainty principle *J. Phys.: Conf. Ser.* **36** 98–102

[24] Harrington J W, Rice P R and Hughes R J unpublished

[25] Gottesman D, Lo H-K, Lutkenhaus N and Preskill J 2004 Security of quantum key distribution with imperfect devices *Quantum Inf. Comput.* **4** 325

[26] Renner R 2005 Security of quantum key distribution arXiv:quant-ph/0512258

[27] Ben-Or M, Horodecki M, Leung D W, Mayers D and Oppenheim J 2005 The universal composable security of quantum key distribution *Lect. Notes Comput. Sci.* **3378** 386

[28] Lo H-K and Preskill J 2007 Security of quantum key distribution using weak coherent states with nonrandom phases *Quantum Inf. Comput.* **8** 431–58 (arXiv:quant-ph/0610203)

[29] Rice P and Harrington J W 2009 Numerical analysis of decoy state quantum key distribution protocols arXiv:0901.0013 [quant-ph]

[30] Peres Y 1992 Iterating von Neumann procedure for extracting random bits *Ann. Stat.* **20** 590–7

[31] Hughes R J *et al* 2005 A quantum key distribution system for optical fiber networks *Proc. SPIE* **5893** 1–10

[32] Hadfield R H, Stevens M J, Gruber S S, Miller A J, Schwall R E, Mirin R P and Nam S 2005 Single photon source characterization with a superconducting single photon detector *Opt. Express* **13** 10846

[33] NIST (ed) 2001 *2001 Security Requirements for Cryptographic Modules* vol 140–2 (Gaithersburg, MD: NIST)

[34] Sugimoto T and Yamazaki K 2000 Study on secret key reconciliation protocol 'cascade' *IEICE Trans. Fundamentals* E83-A:1987

[35] 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

[36] Rosfjord K M, Yang J K W, Dauler E A, Kerman A J, Anant V, Voronov B M, Gol'tsman G N and Berggren K K 2006 Nanowire single-photon detector with an integrated optical cavity and anti-reflection coating *Opt. Express* **14** 527