Quantum key distribution at 1550 nm with twin superconducting single-photon detectors

Robert H. Hadfield[a)]
National Institute of Standards and Technology, 325 Broadway, Boulder, Colorado 80305

Jonathan L. Habif and John Schlafer
BBN Technologies, 10 Moulton Street, Cambridge, Massachusetts 02138

Robert E. Schwall and Sae Woo Nam
National Institute of Standards and Technology, 325 Broadway, Boulder, Colorado 80305

(Received 11 July 2006; accepted 9 November 2006; published online 15 December 2006)

The authors report on the full implementation of a superconducting detector technology in a fiber-based quantum key distribution (QKD) link. Nanowire-based superconducting single-photon detectors (SSPDs) offer infrared single-photon detection with low dark counts, low jitter, and short recovery times. These detectors are highly promising candidates for future high key rate QKD links operating at 1550 nm. The authors use twin SSPDs to perform the BB84 protocol in a 1550 nm fiber-based QKD link clocked at 3.3 MHz. They exchange secure key over a distance of 42.5 km in telecom fiber and demonstrate that secure key can be transmitted over a total link loss exceeding 12 dB. © *2006 American Institute of Physics*. [DOI: 10.1063/1.2405870]

Quantum key distribution (QKD) offers the ultimate in secure communications by encoding information on the states of individual photons.[1] Single-photon detectors are a key enabling technology for this field; the ideal detector for QKD would have high speed, low jitter, negligible dark counts, and high detection efficiency (η) at the wavelength of interest.[2] The best commercial single-photon detectors at 1550 nm, where fiber has lowest transmission loss [0.19 dB/km (Ref. 3)], are InGaAs avalanche photodiodes (APDs).[4] These operate at 200 K and typically offer $\eta \sim 10\%-30\%$. High dark count rates make bias gating essential and to avoid afterpulsing, the detector duty cycle must be reduced, leading to dead times ~ 10 μs. The maximum range for QKD using InGaAs APDs is 122 km (24.4 dB), at mean photon number $\mu=0.1$ with 5 dB receiver transmission loss (η_{Bob}).[5]

Emerging superconducting detector technologies offer notable advantages over conventional single-photon detectors. Transition edge sensors (TESs) inside optical structures[6] offer very high η (up to 89% at 1550 nm) and zero dark counts, but are slow (recovery time $\sim 4\mu s$), with 90 ns jitter (full width at half maximum), and operate at 100 mK. Recent QKD demonstrations have achieved record distances[7–9]—the maximum link loss at $\mu=0.1$ is 29 dB with $\eta_{\mathrm{Bob}}=8$ dB.[8] Nanowire-based superconducting single photon detectors[9–13] (SSPDs) offer an alternative with 4 K operation. The current generation of SSPDs has lower η (10% at 1550 nm—excluding coupling losses).[13] Significant improvements in η are anticipated (optical cavity designs yield intrinsic η up to 57%,[14] but these detectors are not yet widely available). SSPDs have finite dark counts, but are extremely fast (clock rates ~ 1 GHz) with low jitter.[13] In this letter we report a proof of principle demonstration of QKD using SSPDs.

Each SSPD used in this work consists of a narrow (100 nm wide, 4 nm thick) NbN superconducting track embedded in a 50 Ω transmission line. The superconducting track is current biased below its critical current I_C. When a photon strikes the track a resistive hot spot is momentarily formed, causing a voltage pulse. The SSPDs used in this work cover a 10×10 μm^2 area with a 100 nm width meander line with 200 nm pitch, (total length 500 μm). The kinetic inductance-limited recovery time of this detector is ~ 10 ns.[15,16]

We have fiber coupled these detectors and integrated them into a multichannel system based on a cryogen-free refrigerator, allowing continuous detector operation at 2.9 K.[17] In this study we use two of the four available channels in our system. Voltage pulses from the detectors are amplified and converted into logic signals by room temperature electronics. Each SSPD channel is biased such that η

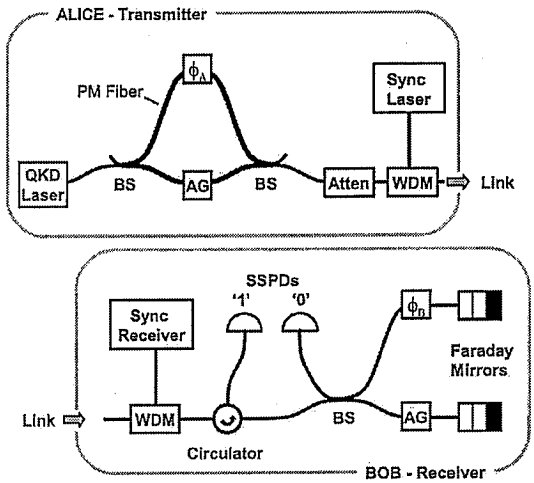

FIG. 1. Schematic of the one-way phase-modulated QKD link. The system is clocked at 3.3 MHz. The QKD laser emits polarized light at 1550.12 nm; the synchronization laser emits 1550.90 nm (time delay 75 ns). Alice's Mach-Zehnder interferometer is composed of polarization maintaining (PM) fiber (thick lines). The attenuator is set such that $\mu=0.1$ out of Alice. The link is composed of SMF28 fiber with/without additional digital attenuation. Other notations: SSPD—superconducting single photon detector; BS—beam splitter; WDM—wavelength division multiplexer; ϕ_A, ϕ_B—respective phase modulators; AG—adjustable air gap delay.

a)Electronic mail: hadfield@boulder.nist.gov

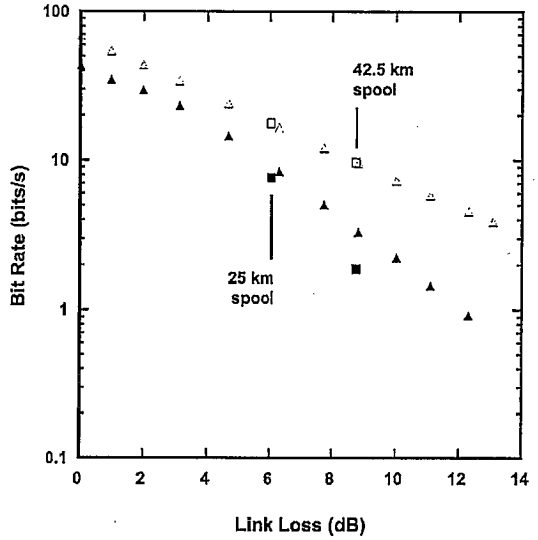

FIG. 2. QKD with twin SSPD receiver. Sifted (hollow triangles) and secure (solid triangles) key rates vs link loss via a digital attenuator. Sifted (hollow squares) and secure key rates (solid squares) via real fiber spools (25 and 42.5 km fiber length) are also shown. A duty cycle of 0.5 was used to allow for adequate interferometer training. Each data point represents the uncompensated bit rate averaged over 30 min of stable operation.

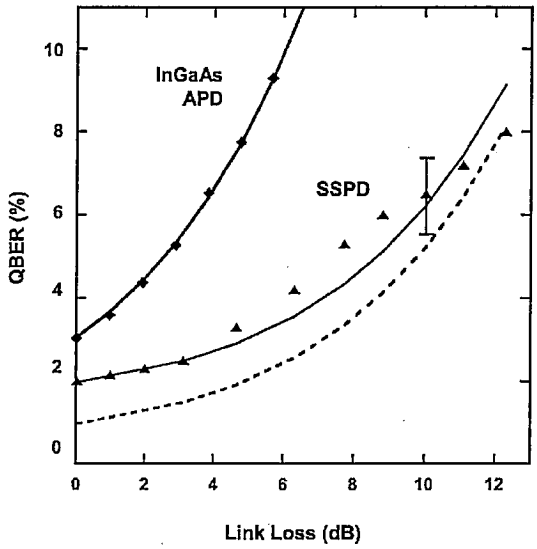

FIG. 3. Measured quantum bit error rate (QBER) vs link loss for InGaAs APD (diamonds) and SSPD (triangles) receivers. A 2σ error bar is given for the SSPD at ~10 dB link loss, indicating the large uncertainty in the measurement at low bit rate (ten sifted bits per second). The calculated QBER is shown for InGaAs APD and SSPD receivers (solid lines). The InGaAs APD is simulated with a detection efficiency (η) of 13.2%%, dark count probability P_{dark} of 3.5×10^{-5} per clock cycle, and a fixed interferometer modulation error of 0.45%. The SSPD is simulated using η=0.9%, P_{dark}=4.5×10^{-7}, and modulation error=1.5%. The dashed line is a fit for the SSPD assuming the same P_{dark} and modulation error=0.45%—the scenario expected for higher bit rates.

(measured from the fiber input) is 0.9% at 1550 nm, with an ungated dark count rate under 100 Hz. The jitter (limited by the readout) is 68 ps full width at half maximum.[18]

The detector system was installed in a receiver node of the DARPA Quantum Network, a metroscale QKD network in Boston/Cambridge, MA.[19] Figure 1 shows the link between two nodes (Alice—transmitter; Bob—receiver). A one-way phase-modulated configuration is used (clocked at 3.3 MHz) to implement the BB84 protocol.[1,20] The Mach-Zehnder interferometer in Alice is composed of polarization maintaining (PM) fiber (bold) in order to avoid polarization rotation differences between paths. A Faraday mirror is used at Bob to mitigate polarization changes in the link fiber. This system is very stable, but has high receiver transmission loss (η_{Bob}=−10.4 dB). Alice and Bob perform random basis selection via electro-optic phase modulators (ϕ_A, ϕ_B) driven by a microwave A/D hardware random number generator. The encoding pulse (λ=1550.12 nm) is generated by an attenuated gain-switched diode laser. The encoding pulse splits into two time-separated wave packets traversing the long and short paths of Alice's interferometer (time difference 18 ns). The mean photon number μ (per encoding pulse pair leaving Alice) is set to 0.1. A bright optical (synchronization) pulse at 1550.9 nm, separated in time from the encoding signal, maintains synchronization. Wavelength division multiplexers (WDMs) exclude the synchronization pulse from Bob's interferometer. A feedback signal added to the phase modulation at Bob maintains phase stability within the transmitter and receiver interferometers as fiber path lengths fluctuate. This feedback signal is derived from training frames sent from the transmitter, which are not used to distill key. The fraction of training frames must be increased to maintain phase stability with increasing link loss and falling raw bit rate. After sifting, secret key is distilled by CASCADE error correction[21] and BBBSS92 privacy amplification.[22,23]

Figure 2 shows the results of a QKD experiment using two SSPDs at μ=0.1. The η per channel is 0.9%. The dark count probability P_{dark} is 4.5×10^{-7} per clock cycle with a 4 ns gate. The sifted key rate (hollow triangles) and generated secure key rate (solid triangles) are shown versus link loss. A digital attenuator controlled the link loss. The interferometer training rate, i.e., the duty cycle, is 0.5, ensuring phase stability at low bit rates. The key rates are averaged over 30 min of continuous operation (without compensation for the duty cycle). The secure key rate falls to zero beyond 12.2 dB link loss. This corresponds to ~63 km distance of ideal fiber.[3] Real fiber spools [25 and 42.5 km—corresponding to total link loss (including insertion) of 6 and 8.8 dB respectively] were also substituted into the link. This yielded similar sifted key rates (hollow squares) with slightly increased quantum bit error rate (QBER) and reduced secure key rate (solid squares).

Figures 3 and 4 compare the SSPD and InGaAs APD receivers in the same QKD link. Figure 3 shows QBER versus link loss and Fig. 4 shows secure key rate versus link loss. QBER is the ratio of errors (dark counts) to sifted bits per time interval, plus a contribution from interferometer phase modulation errors. Each InGaAs APD has a η of 13.2%. The InGaAs APD QBER is dominated by the P_{dark} (3.5×10^{-5} per clock cycle with a 1 ns gate), with a modulation error contribution of 0.45%. The SSPD receiver in contrast has low P_{dark} (4.5×10^{-7} per clock cycle with a 4 ns gate) leading to a slower rise in QBER with link loss. The fit (solid line) is for a constant modulation error of 1.5%. In practice we see scatter in the SSPD QBER data (30 min per data point) because of drift in the modulation error from inadequate sampling of the drift in the path lengths in Alice and Bob and because of the low measurement statistics at high attenuation. The second fit (dashed line) shows the expected QBER versus link loss of the SSPD at 0.45% modulation error—representing the lower bound for the QBER

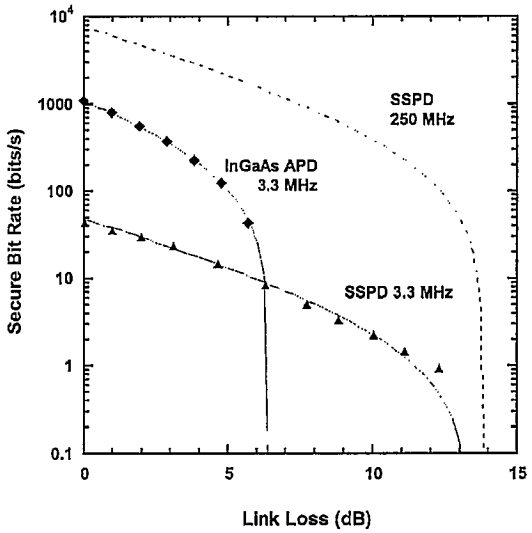

FIG. 4. Secure key rate vs link loss for SSPDs (triangles—0.5 duty cycle) and InGaAs APDs (diamonds—0.9 duty cycle) at 3.3 MHz. The solid lines are generated from the QBER fits in Fig. 3. The projected performance for SSPDs at 250 MHz with a 0.9 duty cycle is also shown (dotted line)—derived from the calculated high bit rate QBER dependence in Fig. 3.

expected in practice at given link loss, when high bit rates allow full feedback control.

In Fig. 4 we see that, despite lower η, the SSPD receiver permits key distribution over longer distance due to lower P_{dark}. Significantly better transmission range has been achieved elsewhere using InGaAs APDs[5] and TES detectors.[8] However, if we were to use the current SSPDs in the link described in (Ref. 8) with η_{Bob}=5 dB and implement a 1 ns gate ($P_{\text{dark}}=1.1\times10^{-7}$) we would obtain a range of 23.6 dB, close to the recorded result of Ref. 5. Improvement in η would lead to significant improvements in range (up to 40 dB if the result of Ref. 14 is practical). Moreover, due to the short SSPD recovery time (10 ns) it is worthwhile considering boosting the system clock rate.[25] The third calculated curve on Fig. 4 is the projected performance of the SSPDs at a clock rate of 250 MHz (derived from the fitted QBER in Fig. 3 assuming 0.45% modulation error and a 0.9 duty cycle—using the model of Ref. 21). The construction of a phase-encoding QKD system at 250 MHz (4 ns period) is challenging but technologically feasible; using a 1 ns width pulse, the time delay between short and long paths can be tuned to 6 ns preventing the redundant side pulses from interfering with the encoding pulse. Indeed, a phase-encoding QKD scheme at 1550 nm clocked at 1 GHz has been recently been demonstrated using upconversion detectors.[25] In our 250 MHz projection the secure bit rate increases dramatically but the only improvement in range is due to the reduced modulation error (secure key rate vanishes at 13.88 dB)—unless the gating time can be reduced. In the gigahertz-clocked regime, the SSPD jitter (68 ps) will limit the maximum clock rate; as the SSPD count rate approaches 100 MHz a limit will be reached due to the ~10 ns recovery time.[24]

To conclude, we have integrated a cryogen-free SSPD detector system as a receiver into a fiber-based QKD link. We have demonstrated that secure key can be exchanged over a link loss of 12.2 dB via the BB84 protocol with twin SSPDs. There is scope for considerable improvement on this result, both in terms of transmission range and secret bit rate.

The DARPA QuIST program and the NIST Quantum Information program sponsored this work. The authors thank N. Bergren (NIST), C. Elliott, H. Yeh, A. Colvin, D. Pearson, and O. Pikalo (BBN) for support, technical assistance, and helpful discussions. They also thank G. Gol'tsman (Moscow) for providing the original detectors.

[1]C. H. Bennett, G. Brassard, *Proceedings of IEEE International Conference on Computer, Systems and Signal Processing* (IEEE, New York, 1984), p. 175.
[2]N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[3]www.corning.com; SMF-28e optical fiber.
[4]F. Zappa, A. Lacaita, S. Cova, and P. Webb, Opt. Lett. **19**, 846 (1994).
[5]C. Gobby, Z. L. Yuan, and A. J. Shields, Appl. Phys. Lett. **84**, 3762 (2004).
[6]D. Rosenberg, A. E. Lita, A. J. Miller, and S. W. Nam, Phys. Rev. A **71**, 061803R (2005).
[7]D. Rosenberg, S. Nam, P. A. Hiskett, C. G. Peterson, R. J. Hughes, J. E. Nordholt, A. E. Lita, and A. J. Miller, Appl. Phys. Lett. **88**, 021108 (2006).
[8]P. Hiskett, D. Rosenberg, C. G. Peterson, R. J. Hughes, S. Nam, A. E. Lita, A. J. Miller, and J. E. Nordholt, New J. Phys. **8**, 193 (2006).
[9]D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, and J. E. Nordholt, Phys. Rev. Lett. (to be published), e-print quant-ph/0607186.
[10]G. N. Gol'tsman, O. Okunev, G. Chulkova, A. Lipatov, A. Semenov, K. Smirnov, B. Voronov, A. Dzardanov, C. Williams, and R. Sobolewski, Appl. Phys. Lett. **79**, 705 (2001).
[11]A. Verevkin, J. Zhang, R. Sobolewski, A. Lipatov, O. Okunev, G. Chulkova, A. Korneev, K. Smirov, G. N. Gol'tsman, and A. Semenov, Appl. Phys. Lett. **80**, 4687 (2002).
[12]A. Korneev, P. Kouminov, V. Matvienko, G. Chulkova, K. Smirnov, B. Voronov, G. N. Golt'sman, M. Currie, W. Lo, K. Wilsher, J. Zhang, W. Slysz, A. Pearlman, A. Verevkin, and R. Sobolewski, Appl. Phys. Lett. **84**, 5338 (2004).
[13]A. Verevkin, A. Pearlman, W. Slysz, J. Zhang, M. Currie, A. Korneev, G. Chulkova, O. Okunev, P. Kouminov, K. Smirnov, B. Voronov, G. N. Gol'tsman, and R. Sobolewski, J. Mod. Opt. **51**, 1447 (2004).
[14]K. M. Rosfjord, J. K. W. Yang, E. A. Dauler, A. J. Kerman, V. Anant, B. M. Voronov, G. N. Gol'tsman, and K. K. Berggren, Opt. Express **14**, 527 (2006).
[15]R. H. Hadfield, A. J. Miller, S. W. Nam, R. L. Kautz, and R. E. Schwall, Appl. Phys. Lett. **87**, 203505 (2005).
[16]A. J. Kerman, E. A. Dauler, W. E. Keicher, J. K. W. Yang, K. K. Berggren, G. Gol'tsman, and B. Voronov, Appl. Phys. Lett. **88**, 111116 (2006).
[17]R. H. Hadfield, M. J. Stevens, S. S. Gruber, A. J. Miller, R. E. Schwall, R. P. Mirin, and S. W. Nam, Opt. Express **13**, 10846 (2005).
[18]M. J. Stevens, R. H. Hadfield, R. E. Schwall, S. W. Nam, R. P. Mirin, and J. A. Gupta, Appl. Phys. Lett. **89**, 031109 (2006).
[19]C. Elliott, D. Pearson, and G. Troxel, Comput. Commun. Rev. **3**, 227 (2003).
[20]O. Pikalo, J. Schlafer, A. Colvin, and C. Elliott, Proc. SPIE **5436**, 21 (2004).
[21]G. Brassard and L. Salvail, Lect. Notes Comput. Sci. **765**, 410 (1994).
[22]C. H. Bennett, F. Bessette, G. Brassard, L. Savail, and J. Smolin, J. Cryptology **5**, 3 (1992).
[23]D. S. Pearson and C. Elliot, e-print quant-ph/0403065.
[24]J. Habif, D. Pearson, R. H. Hadfield, R. Schwall, S. W. Nam, and A. Miller, Proceedings of SPIE Workshop on Advanced Photon Counting, 2006 (unpublished).
[25]R. T. Thew, S. Tanzilli, L. Krainer, S. C. Zeller, A. Rochas, I. Rech, S. Cova, H. Zbinden, and N. Gisin, New J. Phys. **8**, 32 (2006).