

MIT Open Access Articles

*High-Rate Quantum Key Distribution with
Superconducting Nanowire Single Photon Detectors*

The MIT Faculty has made this article openly available. **Please share**
how this access benefits you. Your story matters.

Citation: Dauler, Eric A. et al. "High-Rate quantum key distribution with superconducting nanowire single photon detectors." Lasers and Electro-Optics (CLEO) and Quantum Electronics and Laser Science Conference (QELS), 2010 Conference on. 2010. 1-2. ©2010 IEEE

As Published: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5500759

Publisher: Institute of Electrical and Electronics Engineers (IEEE)

Persistent URL: <http://hdl.handle.net/1721.1/74219>

Version: Final published version: final published article, as it appeared in a journal, conference proceedings, or other formally published context

Terms of Use: Article is made available in accordance with the publisher's policy and may be subject to US copyright law. Please refer to the publisher's site for terms of use.



High-Rate Quantum Key Distribution with Superconducting Nanowire Single Photon Detectors

Eric A. Dauler¹, Neal W. Spellmeyer¹, Andrew J. Kerman¹, Richard J. Molnar¹, Karl K. Berggren², John D. Moores¹, Scott A. Hamilton¹

¹Lincoln Laboratory, Massachusetts Institute of Technology, Lexington, MA 02420

²Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, MA 02139
edauler@ll.mit.edu

Abstract: We demonstrate the potential for 1.85 Mbit/s secure key rates over 101 km of fiber, >100 times faster than previously demonstrated, using the differential phase shift quantum key distribution protocol and superconducting nanowire single-photon detectors.

©2010 Optical Society of America

OCIS codes: (270.5568) Quantum cryptography; (270.5570) Quantum detectors;

1. Introduction

Quantum key distribution provides a means to secure communication channels without relying on methods that are vulnerable to future algorithmic or information processing advances. To fully realize this potential, however, one-time-pad encryption should be utilized and fast key generation rates are necessary. Increasing the key generation rate requires increasing the speed of electronics, random number generators, and high-efficiency single photon detectors. In this work, we demonstrate that a pair of superconducting nanowire single photon detectors (SNSPDs) [1-3] with 31% system detection efficiency and 40 ps timing jitter can be used to implement the differential phase shift quantum key distribution (DPS-QKD) protocol [4-7] at a 10.7 GHz clock rate. Based on the measured 4.0 Mbit/s sifted key rate and 0.77% quantum bit error rate (QBER), keys secure against general individual attacks [5] and sequential attacks described in [6, 7] could be generated over 101 km of fiber at rates as high as 1.85 Mbit/s.

2. Results

The DPS-QKD experimental setup shown in Fig. 1(a) was used to measure the sifted key rate and QBER with a 1550 nm operating wavelength and 0.2 average photons per pulse at the transmitter output. The electroabsorption (EA) modulator generated a return-to-zero signal with short pulses and the dual-drive Mach-Zehnder modulator was driven with a 2^7 -1 pseudo-random bit sequence (PRBS) to set the phase of each pulse. A low-loss (0.3 dB), all-fiber interferometer and SNSPD detectors described below were used to form a high-efficiency receiver. Data from the photon counters was post-processed from 50 μ s sequences recorded on a real-time oscilloscope. Dispersion compensating fiber was used in the transmitter to pre-compensate for chromatic dispersion in a 101 km spool of LEAF fiber (20.19 dB loss) used to simulate the channel. The clock frequency and phase were recovered by post-processing the photon count data recorded on the oscilloscope without an electrical or an intense optical clock signal.

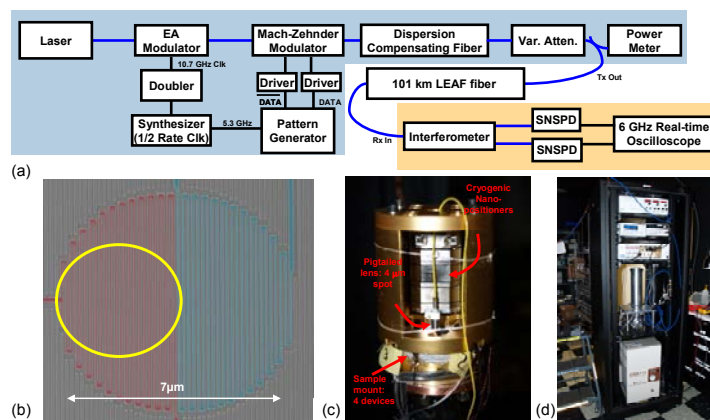


Fig. 1. (a) DPS-QKD experimental setup with transmitter (receiver) components on a blue (orange) background and electrical (fiber) connections indicated by black (blue) lines. (b) A scanning electron micrograph of the dual-element SNSPD, before integration with an optical cavity. Red and blue shading indicate the two independent elements and a yellow outline encircles $\sim 80\%$ of the optical power focused on one of the elements. (c,d) Two dual-element SNSPDs, the fiber-coupling assemblies and the required electronics packaged in rack-mounted cryocooler.

The superconducting nanowire single photon detectors used in this experiment are shown in Fig. 1(b-d). Two independent, 2-element SNSPDs with optical cavities [2,3] were operated at a temperature of $\sim 3\text{K}$ in a single cryocooler. Although higher speeds and limited photon-number-resolution can be obtained when both elements of each 2-element SNSPD are operated simultaneously [3], only a single element was required for the desired 2 Mcount/s counting rates based on the fast, $\sim 10\text{ ns}$, single-element reset time. Fiber focusers were positioned using cryogenic nanopositioners to couple light from single-mode fibers onto a single element from each of the 2-element SNSPDs. The system detection efficiency, from the fiber input outside the cryocooler to the single-element detector output signal, was $31\pm 3\%$ for each of the detectors operating at 93% of their respective critical currents.

Data from over 16,000 sifted bits was used to calculate the 4.0 Mbit/s sifted key rate and the 0.77% QBER, after temporally filtering the data in each time slot. The photon count timing, the frequency and phase of the clock and the PRBS pattern alignment were extracted from the oscilloscope traces. A single clock frequency was used in analyzing all of the data and the pattern alignment was consistent between the “0” and “1” detector channels for all of the data sets. The sifted key rate and QBER were both obtained by ignoring all photon count events outside the central 50 ps of the 94 ps time slots. This time windowing resulted in a 1.4 dB reduction in the total number of detection events and reduced the errors due to timing jitter as shown in Fig. 2 to maximize the potential secure key rate. The ratio between the secure and sifted key rates was calculated following the approach taken in [5] for general attacks on individual photons. Assuming an error correction overhead 16% above the Shannon limit, a maximum secure key rate of 1.85 Mbit/s was calculated. Based on the measured experimental parameters, the sequential attacks described in [6,7] would generate error rates well above the measured QBER.

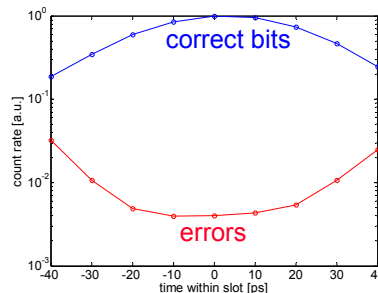


Fig. 2. Fraction of photon count events that correspond to the correct and incorrect bit as a function of time within the slot.

3. Summary

The potential for secure key rates of 1.85 Mbit/s over more than 100 km of fiber was experimentally demonstrated for the first time using the DPS-QKD protocol and SNSPDs. The low detector dark count rates, high speed and broadband detector response provided by these SNSPDs make them well-suited for QKD systems operating over a wide range of channel losses, background levels and operating wavelengths. The high key rate achieved in these experiments permitted fast data collection, real-time optimization of the system parameters and straightforward clock recovery at 10.7 GHz without the need for atomic clocks or dedicated clock signals. The demonstrated combination of high key rate and relatively large link loss raises the possibility of adding additional opto-electronic components for networking or operating over existing spans between amplifiers at $\sim 1300\text{ nm}$ wavelength [8].

This work was sponsored by the United States Air Force under Air Force Contract #FA8721-05-C-0002. Opinions, interpretations, recommendations and conclusions are those of the authors and are not necessarily endorsed by the United States Government.

4. References

- [1] G. Goltsman, et al., “Picosecond superconducting single-photon optical detector,” *Appl. Phys. Lett.* **79**, 705-707, (2001).
- [2] Rosfjord, K. M., et al. “Nanowire Single-Photon Detector with an Integrated Optical Cavity and Anti-Reflection Coating,” *Opt. Express* **14**, 527-534 (2006).
- [3] Dauler, E. A., et al., “Multi-Element Superconducting Nanowire Single-Photon Detector,” *IEEE Trans. Appl. Supercond.* **17**, 279-284 (2006).
- [4] Inoue, K. Waks, E., and Yamamoto, Y., “Differential Phase Shift Quantum Key Distribution,” *Phys. Rev. Lett.* **89**, 037902 (2002).
- [5] Waks, E., Takesue, H., and Yamamoto, Y., “Security of differential-phase-shift quantum key distribution against individual attacks,” *Phys. Rev. A* **73**, 012344 (2006).
- [6] Curty, M. et al., “Sequential attacks against differential-phase-shift quantum key distribution with weak coherent states,” arXiv.org :quant-ph/0609094v1 (2006).
- [7] Tsurumaru, T., “Sequential attack with intensity modulation on the differential-phase-shift quantum-key-distribution protocol,” *Phys. Rev. A* **75**, 062319 (2007).
- [8] Nweke, N. I. et al., “Experimental characterization of the separation between wavelength-multiplexed quantum and classical communication channels,” *Appl. Phys. Lett.* **87**, 174103 (2005).