1310 nm differential phase shift QKD system using superconducting single photon detectors*

Lijun Ma[1], S Nam[2], Hai Xu[1], B Baek[2], Tiejun Chang[1], O Slattery[1], A Mink[1] and Xiao Tang[1]

[1]Information technology laboratory and [2]Electronics & Electrical Engineering Laboratory
National Institute of Standards and Technology, 100 Bureau Dr., Gaithersburg, MD 20899
xiao.tang@nist.gov

Abstract

We have implemented a differential-phase-shift (DPS) quantum key distribution (QKD) system at 1310 nm with superconducting single photon detectors (SSPD). The timing jitter of the SSPDs is very small (~60 ps) and its dark counts rate is low (< 200/s). 1310 nm is an ideal quantum signal wavelength for a QKD system, where quantum signals coexist with classical communication signals at 1550 nm in one fiber. As the key element in the DPS QKD, a Michelson interferometer was designed and built using Faraday mirrors that can automatically compensate for the polarization evolution in the fiber. As the result, our DPS QKD system can be steadily operated at 2.5 Ghz clock rate with a low quantum error rate of less than 4%.

Keywords: Quantum key distribution, Differential phase shift, Superconducting single photon detector, Optical fiber communication.

1. Introduction

A quantum key distribution (QKD) system can create a shared, secret cryptographic key over unsecured communication links between users. Its security is ensured by fundamental quantum principles instead of mathematical complexity. The most popular QKD protocol is the BB84 [1], which was proposed by Bennett and Brassard in 1984. However, when attenuated laser light is used as a photon source, a BB84 system may be susceptible to a photon number splitting (PNS) attack [2]. While this attack can be defeated using decoy states, differential phase shift (DPS) protocol [3] offers another PNS tolerant QKD protocol, and it provides higher sifted-key rate since it does not lose any key due to incompatible measurement bases.

For QKD optical signal transmission over a fiber longer than 10 km, the wavelength needs to be in the 1310 nm or 1550 nm bands, where the optical loss in the commercial telecom fiber is the lowest. As wavelength-division multiplexing (WDM) and erbium-doped fiber amplifier (EDFA) technology are widely used in optical networks, the 1550 nm band is very noisy because of the Raman scattering of strong optical communication signals and the amplified spontaneous emission of EDFA. It is not practical for a very weak quantum signal to be transmitted in such noisy band. In contrast, the 1310-nm band is very quiet and a much more suitable wavelength for QKD systems [4,5]. For a standard telecom fiber, zero dispersion occurs at 1310

* The identification of any commercial product or trade name does not imply endorsement or recommendation by the National Institute of Standards and Technology.

nm, which is an advantage for a high speed communication system even though its attenuation is a little higher than 1550 nm.

Among these single photon detectors available for the 1310 nm band, InGaAs avalanche photodiode (APD) [6], up-conversion detector using silicon APDs[7] and superconducting single-photon detector (SSPD) [8] are used to implement high-speed QKD system . Recently, a self-different technique was developed for InGaAs APD to suppress the afterpulse noise, and it has been successfully applied into a QKD system over GHz [9]. The InGaAs APD has about 10% detection efficiency, but it still has about 6% afterpulse probability which would contribute an extra 3% to the quantum bit error rate (QBER) of a QKD system. Up-conversion detectors use nonlinear optical devices, such as a periodically poled lithium niobate (PPLN) waveguide, to convert 1310-nm photons into the wavelengths that silicon-based APDs (Si-APD) can detect. Up-conversion detectors can operate in free-running mode and their detection efficiency is relatively high (20~40%). We have previously implemented a DPS QKD system at 2.5 GHz with up-conversion detectors [10], but the QBER was high due to its high dark counts from up-conversion elements and the large timing jitter caused by the Si-APDs used. SSPDs can be operated in free-running mode in telecom wavelengths (1310 and 1550 nm) with a small response timing jitter (~60ps) and a low dark count rate (< 200/s). SSPDs are the most suitable photon detectors for achieving low error rate in high-speed QKD systems.

Since the DPS protocol was proposed in 2002, several DPS QKD systems have been successfully demonstrated [11], including a 1550-nm DPS QKD system using SSPDs implemented in 2007 [12]. In this paper, we report a 1310-nm DPS QKD system with SSPDs and a Michelson interferometer using Faraday mirrors. We also report the system performance operating over 10~50 km of optical fiber.

2. System Configuration

The configuration of our DPS QKD system is shown in figure 1(a). On Alice's side, a continuous wave 1310-nm laser beam is modulated into a 2.5-GHz pulse train with a FWHM of 100 ps by an amplitude modulator (AM), whose extinction ratio is 20dB. In the phase modulator (PM_1), the phase of each optical pulse is modulated to 0 or π following the phase modulation signal, which was produced electronically by a pattern generator (Tektronix DTG5274) according to a digital random pattern via a Matlab program. The phase-encoded pulse trains are attenuated by a variable optical attenuator (VOA) to single photon level, and then are launched into a standard telecom single mode fiber (SMF28).

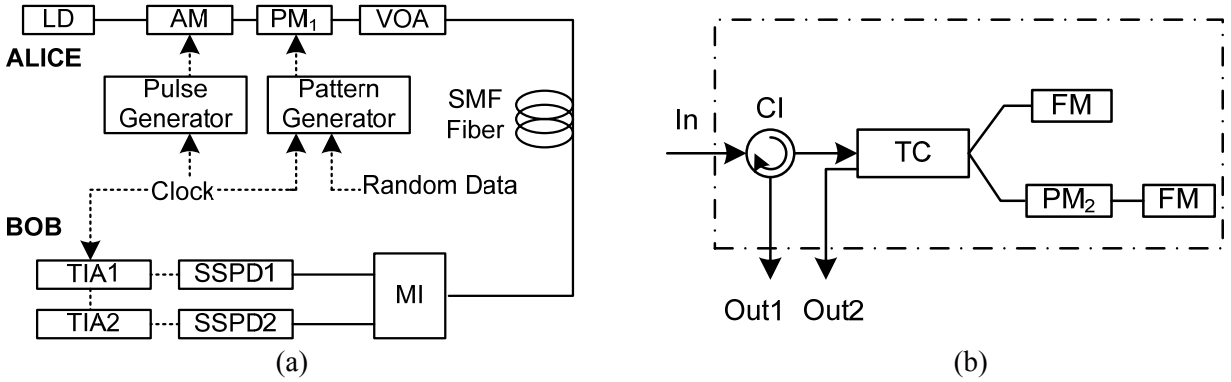


Figure 1. (a) Schematic diagram of the DPS-QKD system; (b) Schematic diagram of Michelson interferometer. LD: CW laser diode; AM: amplitude modulator; PM: phase modulator; VOA: variable optical attenuator; MI: Michelson interferometer, see (b); SSPD: superconducting single photon detector; TIA: time-interval analyzer; TC: tunable coupler; FM: Faraday mirror; CI: circulator; Dotted line: electric cable; Solid Line: optical fiber.

On Bob's side, the quantum signal passes through a 1-bit delay Michelson interferometer, which is polarization-insensitive and its outputs are dependent on the phase difference of consecutive pulses. The qubits of photon pulses encoded at Alice are passively decoded in the Michelson interferometer. The scheme using a Michelson interferometer configuration with two Faraday mirrors (shown in figure 1(b)) helps us minimize the polarization sensitivity, which is important for fiber-based QKD systems in field applications. To achieve the maximal extinction ratio, a tunable coupler is tuned to around 50/50 to equalize the power in the two arms of the Michelson interferometer; and an in-line piezo phase modulator (PM_2) is used to compensate the static phase difference.

Two SSPDs [8,12] are installed at the two outputs of the Michelson interferometer to detect the differentially phase-shifted photons. Each SSPD consists of a 100 nm wide, 4 nm thick NbN superconducting wire and is coupled to a 9 μm core single mode fiber. The packaged detector is housed in a closed-cycle cryogen-free refrigerator operating at a temperature of 3 K for convenient use in quantum information experiments. The photon detection signals are then sent to one of two precisely synchronized time interval analyzers (TIAs), which record the detection time relative to the sync pulses that provide the time slot information for the qubits.

Inter-symbol interference caused by the laser pulse width and timing jitter of detectors is one of main sources of the error bits in QKD system [13]. To reduce inter-symbol interference, we assigned a time slot to each detection event by setting a time window around the center of a slot. The largest bit error rate occurs when we chose a time window with a width as long as the clock period, due to inter-symbol interference, dark counts, incomplete extinction of the photon pulse by the AM, and imperfect interference. Using narrower time windows, we can improve the relative signal (correctly identified photon clicks) to noise ratio and reduce the error rate. At the same time, however, the secret key rate is somewhat reduced. Therefore, there is a compromise to choose the optimal time window in order to maximize the secret key rate and minimize the

error rate. A quantitative estimation of the secret key rate as a function of the error rate and the sifted-key rate indicates that a time window of around 200 ps is optimal for all our measured data [14].

3. Results and discussion

The sifted-key rate and quantum bit error rate (QBER) are widely used as the performance criteria of QKD systems. In this section we describe the measurement results from our DPS QKD system and discuss the important parameters in the experiments over different fiber lengths.

The sifted-key rate of a QKD system is determined by the system clock rate, its mean photon number μ at Alice, the loss in the transmission fiber, the insertion loss of the interferometer, and the detection efficiency of SSPDs. The sifted key rate can be estimated by the following equation:

$$R = \mu \cdot L_f \cdot L_i \cdot L_t \cdot Pd \cdot \nu \tag{1}$$

where R is the sifted key rate. The system clock is set to 2.5 GHz (actual clock rate is 2.499 GHz to meet the 1-bit delay of the interferometer). In all of our experimental set-ups, the mean photon number is set to 0.1. In this case, 9% of the pulses contain a single photon, less than 1% contains more than one photon, and the rest is empty according to the Poisson statistics. The attenuation of SMF28 fiber at 1310 nm is 0.35 dB/km. The insertion loss of the interferometer is about 4.5 dB. The detection efficiency of our SSPDs at 1310 nm is measured to be 1%. Applying the time window on the detection events imposes a 1 dB loss. An additional 1.5 dB loss is from fiber connectors and due to fiber bending. Figure 2 shows the measured data as a function of the fiber length (0-50 km), along with the calculated sifted-key rate, and we see that the measured data agrees well with the calculated results. The system generates more than 150 Kbps over 10 km and 8.5Kbps over 50 km.

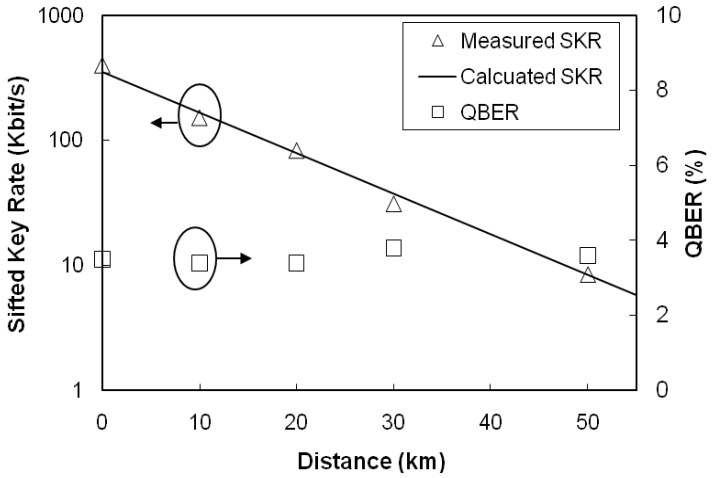


Figure 2. The system performance of the DPS- QKD system using SSPDs. To the left, solid line: the calculated sifted-key rate; triangles: the sifted-key rates measured in the experiment; To the right, squares: the error rate measured in the experiment.

QBER is another important metric for QKD systems. QBER is mainly caused by the limited extinction ratio of the modulators (e_{ext}), inter-symbol interference (e_{isi}), dark counts of the photon detectors (e_{dar}), visibility of interferometer (e_{vis}) and the limited performance of the pattern generator (e_{gen}). The QBER can be estimated with the following equation:

$$QBER = \frac{Counts_{incorrect}}{Counts_{total}} \approx e_{ext} + e_{isi} + e_{dar} + e_{vis} + e_{gen} \tag{2}$$

In our case, the extinction ratio of the amplitude modulator is 20 dB, so e_{ext} is about 1%. Due to the remarkable small timing jitter of SSPD (~ 60 ps), the detection events have a Gaussian distribution with a FWHM ~150 ps. Figure 3 shows the histogram of the output counts in the DPS QKD system with SSPD and the up-conversion detectors [10], in which the green line denotes the histogram of counts with SSPDs and the blue line is with the up-conversion detector. Although the SSPD has the similar timing jitter (FWHM value) with the low jitter silicon based APD [14] used in the up-conversion detector, the response of SSPD fits well with the Gaussian distribution and does not have a long tail. Using SSPD detectors and properly assigning a detection window can significantly reduce inter-symbol interference, and therefore, the inter-symbol interference does not contribute much to bit error rate and e_{isi} is negligible in the experiments. In addition, the SSPDs have very low dark count rate (< 200/s) compared to the up-conversion detectors. The sifted key rate reduces as the transmission fiber is longer but the dark count rate of detectors does not change, so the contribution of dark counts to QBER is fiber length dependent and significant for long distance. In these experiments, e_{dar} varies according to the distance, from 0.1% to 0.5%.

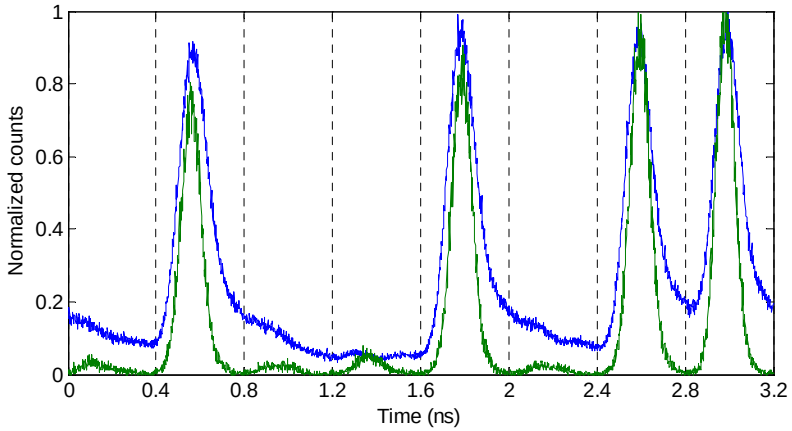


Figure 3. Histogram of the output counts with SSPD (green) and up-conversion detector (blue) at a fixed pattern 01001011.

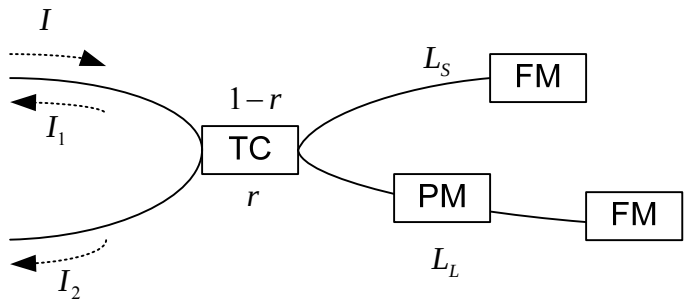


Figure 4.. Schematic diagram of the function of the Michelson interferometer. TC: tunable coupler; FM: Faraday mirror; PM: phase modulator. *I* is the optical intensity of input signal; I_1 and I_2 : the optical intensity of the two outputs; *r* is the coupling ratio into the long arm; L_L and *Ls* is the total loss in round trip through the long and short arms.

On the other hand, high visibility of the interferometer is the crucial factor for obtaining a low QBER. Figure 4 schematically shows the structure of 1-bit delay Michelson interferometer. The two outputs of the interferometer can be expressed as following:

$$\begin{aligned} I_1 &= I_{1S} + I_{1L} + 2\sqrt{I_{1S} \cdot I_{1L}}\cos(\delta).....(a) \\ I_2 &= I_{2S} + I_{2L} - 2\sqrt{I_{2S} \cdot I_{2L}}\cos(\delta).....(b) \end{aligned} \tag{3}$$

where I_1 and I_2 are the optical intensity of the two outputs of the interferometer, I_{1S} and I_{1L} are the optical intensity in output 1 from short and long arms respectively, and the I_{2S} and I_{2L} are the optical intensity in output 2 from short and long arms respectively. δ is the phase difference between the two pulses from the short and long arms. Because the time delay of the two arms is exactly 1-bit long, δ is actually the phase difference of consecutive pulses in the system. According to the equation, two factors are critical to obtain high visibility, which are optical intensity balance from the two arms in the interferometer and the phase difference for consecutive pulses.

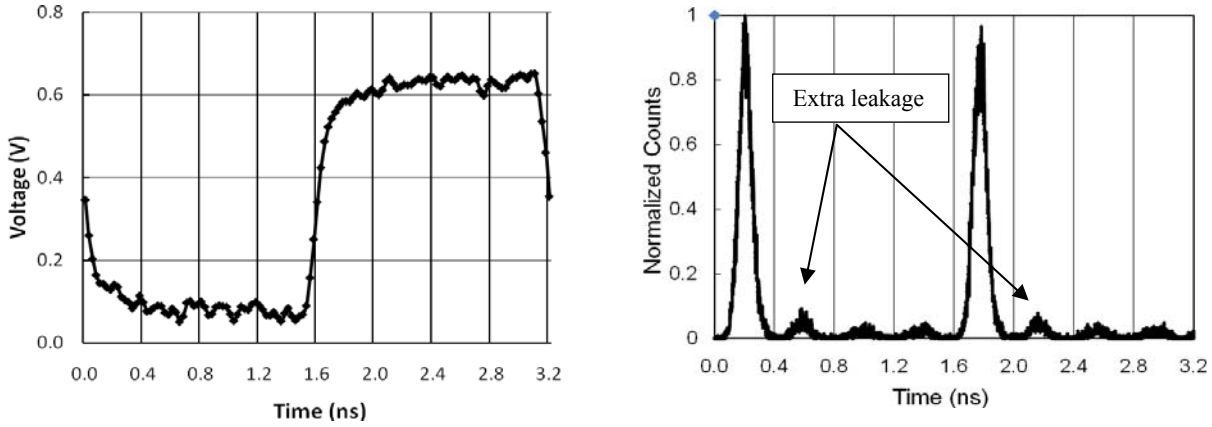
To get good interference, I_1 and I_2 should be zero when the δ is π and 0 respectively. In that case, the following condition should be satisfied:

$$\begin{aligned} r^{2\cdot}L_L^{\,2} + (1-r)^2 \cdot L_S^{\,2} - 2 \cdot r \cdot (1-r) \cdot L_L \cdot L_S = 0.....(a) \\ L_L^{\,2} + L_S^{\,2} - 2L_S \cdot L_L = 0.....(b) \end{aligned} \tag{4}$$

where *r* is the coupling ratio into the long arm, and (1-*r*) is the ratio to the short arm. L_L is the total loss in the round trip through the long arm (double insertion losses of the coupler, PM and FM), and *Ls* is the loss in the round trip through the short arm (double insertion losses of the coupler and FM). To satisfy Equ.(4), the loss of the two arms should be equal and the ratio should be 50% exactly. However, the long arm with the PM has more optical loss than the other due to the additional insertion loss in the piezo PM. We add a small loss in the short arm by winding the fiber in a small loop to balance the two losses. The coupling ratio of the

tunable coupler in the interferometer can be adjusted to be precisely 50/50 during the experiment. After optimizing the intensity balance, the visibility of the interferometer is measured to be about 19dB. Therefore, the contribution to QBER by the limited visibility of interferometer (e_{vis}) is estimated to be about 1.2% .

Another prerequisite for good interference visibility is that the phase difference (δ) of consecutive pulses must be 0 or π precisely, and the limited performance of the pattern generator degrades the condition and contributes more errors to QBER(e_{gen}). In the interferometer, a PM is installed in the long arm, and it can be adjusted to compensate the phase difference between the two arms, so the δ is only dependent on the phase difference of consecutive pulses of the original signal from Alice. At Alice, the phase of each pulse is set by a PM and the phase of pulses can be finely adjusted to 0 or π according to the data '0' and '1'. However, the limited bandwidth (2.7 Gbps) and signal rise/fall times (about 140 ps from 20 to 80%) of the pattern generator causes the actual signal phase not to change as quickly as an ideal square wave. A signal with a repetitive pattern 00001111 from the pattern generator is shown in figure 5(a). We can see that the voltage could not reach to a desired level if the previous adjacent time bin has a different value. Therefore, the interference of the signals is not perfect which results in an extra leakage as shown in figure 5(b). The extra leakage is one of the main factors contributing to the QBER. It is measured that the leakage counts in the time bin that has a different value than the previous one is about 3.2 times as that with same value as the previous one. In the QKD system, the data sequence sent from Alice is a random pattern and the probability that the two adjacent time bins have the different value is 0.5, which means half of the time-bins suffer from the extra leakage caused by the limited performance of the pattern generator. In that case, the limited performance of the generator causes about 1.1% error rates to QBER(e_{gen}). However, it is expected that e_{vis} can be significantly reduced by using a higher-bandwidth signal generator with faster rise/fall times, and therefore the QBER can be reduced also.



(a) (b)

Figure 5. (a) The signal to drive phase modulator for a repetitive pattern 00001111. (b) Histogram of the detected event of SSPD1 at the interferometer output 1. After differential-phase-shifting (passing the 1-bit delay interferometer), the output pattern is 10001000.

Due to the above factors, the QBER of our DPS QKD system, which is shown in figure 2, is measured from 3.4-3.8% over 0-50 km fiber lengths. This QBER value is low enough to generate secure keys, though a lower QBER is preferred to obtain higher secure key rates. SSPDs have very small timing jitter and low dark counts, which mean the timing jitter and dark counts are not main factors of QBER. Therefore, to further reduce the QBER of the QKD system, we need to increase the extinction ratio of modulators and the bandwidth of the pattern generator, and to improve the visibility of the interferometer in the system.

4. Conclusion

We have experimentally implemented a fiber-based DPS QKD system with SSPDs at 1310 nm using a Michelson interferometer with Faraday mirrors. Operating at a 2.5-GHz clock rate, the QKD system generates sifted-key rates of more than 150 Kbps over 10 km and 8.5K bps over 50 km. Due to the limited performance of the modulator, pattern generator and interferometer, the system QBER is measured 3.4-3.8%. The QBER is expected to be reduced down to 2.2~2.7% at a distance less than 50 km once a higher-bandwidth signal generator with faster rise/fall times is used in the system, and the QBER can be further reduced by improving the extinction ratio of the modulators and the visibility of the interferometer. 1310 nm is a suitable wavelength for QKD systems for coexistence with the 1550-nm classical communication signals in one fiber. The configuration of Michelson interferometer with Faraday mirrors can automatically compensate for the polarization evolution in the fiber. This work paves the way for high-speed DPS QKD systems over the existing optical networks.

Acknowledgements

The authors are grateful for the support from the NIST quantum information initiative.

References

1. C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing” in Proc. of the IEEE Int. Conf. on Computers, Systems & Signal Processing, pp. 175-179, Bangalore, India, December 10-12, (1984).
2. G. Brassard, N. Lutkenhaus, T. Mor, and B. C. Sanders, “Limitations on practical quantum cryptography”. Phys. Rev. Lett. **85** 1330–1333 (2000).
3. K. Inoue, E. Woks and Y. Yamamoto, “Differential phase shift quantum key distribution” Phys. Rev. Lett. **89**, 037902, (2002).
4. P.D. Townsend, “Simultaneous quantum cryptographic key distribution andconventional data transmission over installed fibre usingwavelength-division multiplexing, ” Electronics Letters, **33**, 188-190 (1997)
5. N. Nweke, P. Toliver, R. Runser, S. McNown, T. Chapuran, M. Goodman, R. Hughes, C. Peterson, K. McCabe, J. Nordholt, K. Tyagi, P. Hiskett, and N. Dallmann, “Experimental characterization of wavelength separation for "QKD+WDM" co-existence,” CLEO05: 1503- 1505
6. Z. Yuan,a_ B. Kardynal, A. Sharpe, and A. Shields, “High speed single photon detection in the near infrared” Applied Physics Letters, **91** 041114 (2007).

7. 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", Optics Express, **15** 7247- 7260 (2007)
8. R. Hadfield, J. Schlafer, L. Ma, A. Mink, X. Tang, S. Nam, "Quantum key distribution with high-speed superconducting single-photon detectors, " CLEO 07 QML4, (2007)
9. Z. Yuan, A. Dixon, J. Dynes, A. Sharpe, and A. Shields, " Gigahertz quantum key distribution with InGaAs avalanche photodiodes", Applied Physics Letters, **92** 201104 (2008).
10. L. Ma, H. Xu, T. Chang, O. Slattery, X. Tang, "Experimental Implementation of 1310-nm Differential phase shift QKD system with up-conversion detectors," CLEO 08, JTuA105, (2008)
11. H. Takesue, E. Diamanti, T. Honjo, C. Langrock, M. Fejer, K. Inoue and Y. Yamamoto, " Differential phase shift quantum key distribution over 105 km fibre,' New Jour. Phys. **7**, 232, (2005)
12. H. Takesue, S. Nam, Q Zhang, R. Hadfield, T. Honjo, K. Tmaki, and Y. Yamamoto, " Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors," Nature Photonics, **1**, 343-348, (2007)
13. K. J. Gordon, V. Fernandez, P. D. Townsend, and G. S. Buller, "A Short Wavelength GigaHertz Clocked Fiber-Optic Quantum Key Distribution System," IEEE J. of Quantum Electron. **40**, 900-908 (2004).
14. B. Baek, L. Ma, A. Mink, X. Tang and S. Nam, "Time window optimization for a differential-phase-shift quantum key distribution system using superconducting single photon detectors," submitted to conference on quantum communication, measurement and computing (2008).