Practical Quantum Cryptography

Alexei Trifonov[a], Anton Zavriyev[a], Darius Subacius[a], Romain Alléaume[b], Jean-François Roch[b]
[a]MagiQ Technologies, Inc. 11 Ward Street 300 Somerville MA 02215
[b]Laboratoire de Photonique Quantique et Moléculaire, UMR 8537 du CNRS, ENS Cachan,
61 avenue du Président Wilson, 94235 Cachan Cedex France

ABSTRACT

We report our recent results in development of the secure fiber-optics communication system based upon quantum key distribution. Emphasize is made on the limitation imposed by the state-of-the-art components crucial for the system performance. We discuss the problem of the interferometer design and highlight the possible security loopholes known. Together with single photon counting performance it places the main restriction on the distance range and the secure key rate of the QKD system based upon the week coherent pulses. Finally we describe the result of the first test of the system using single photons produced by non-degenerate parametric down-conversion as a source.

Keywords: Quantum cryptography, quantum communication, single photon detection

INTRODUCTION

Quantum cryptography [1] is coming out from research labs and entering the real world of applications[2]. In the next few years we will observe the OKD impact on the secure communication industry infrastructure as well as the security market and the final user feedback that in turn will affect the future development of the QKD and quantum communication. This paper highlights the possibilities and limitations imposed on QKD performance by the current state-of-the-art technology. It is restricted to the fiber-optic implementation, which seems to be the closest to the deployment stage and the most promising from the commercial point of view. It is very likely that some of the limitations discussed in this paper will be overcome with time; some others, while not being fundamental seem to represent the long-lasting problems. As an example we can mention an issue of the fiber loss. The solution to this problem found in classical fiber optics communication (optical amplification) does not work for secure quantum communication and the search for leveraging attenuation of the optical line is a real challenge. It seems unlikely that the whole fiber-optics infrastructure will be replaced in foreseeable future even if a lower loss fiber (compared to the current 0.2dB/km) will be developed.

Sometimes QKD is referred as “unconditionally secure” key distribution technique. It must be stressed that the term “unconditional” can mean “unconditional computational resources used by eavesdropper” and does not fully reflect the restrictions of the measuring apparatus of an eavesdropper. A reasonable assumption is to provide an eavesdropper with unlimited resources to tap the optical fiber and perform any quantum measurement allowed by the physics laws. An eavesdropper’s ability to look inside the QKD apparatus, on the other hand, can be assumed to be very limited. These factors are common for all cryptographic systems – quantum or classical and thus lye outside the scope of the QKD security analysis. This is the approach we adapted in this publication.

The use of the week coherent pulses (WCP) as an approximation of the single photon source greatly simplifies the QKD apparatus. However, WCPs can contain more than one photon so the average mean photon number must be kept low enough to guarantee the security[3]. Vulnerability of the system utilizing WCP increases with the loss of the channel. To assure the necessary level of security one must decrease the mean photon number as the link distance (loss) increase. This situation seems to be paradoxical: to leverage the loss imposed by the channel one must not *increase* but *decrease* the signal. This is the main drawback of the quantum cryptography based upon the WCP approach. Despite the attempts

made to figure out the solution around this problem[4, 5] the ultimate performance can be searched only by using the true single photon source.

2. Fiber-optics QKD: how to transmit qubits over the optical fiber

Polarization usually used for encoding in free-space QKD systems is not a good degree of freedom in a case of fiber-optics QKD[2]. Alternative methods of sending a qubit over the optical fiber were suggested. The most known schemes are time-domain double Mach-Zehnder interferometer originally brought into consideration by Bennett[6], and a so-called Plug-and-Play (autocompensating) system developed by Geneva group[7]. We will refer to these schemes as one- and two-way systems correspondingly, the nomenclature derived from to the number of directions of photon travel through the fiber. Both schemes have advantages and disadvantages; let us briefly overview the most crucial ones.

2.1. Two-ways system

The beauty of the PnP system is the absence of necessity for active stabilization of the interferometer. The scheme is well known and the detailed can be found elsewhere[2, 7, 8]; we just want to bring readers attention to the fact that there are some issues originating from the fact the photons travel in both directions in this system:

2.1.1. Pulse collision problem

Double pass of the signal through the Bob's phase modulator lead to the problem of pulse collision. In combination with the fiber distance temperature drifts it results in a lower repetition rates as compared to a one-way system. This limitation is not severe for the repetition rate typically reached in most QKD experiments, but it can represent a bigger problem if higher rates are searched to increase the key rate.

2.1.2. Trojan horse attack

In agreement with the conservation of problems law, canceling the problem of interferometric stability opens a loophole in physical security. This problem is known as a Trojan horse attack [2]. Alice is reflecting the signal sent by Bob and thus might be open for Eve's probing as well. Eve can send a strong signal and learn the phase setting of the Alice modulator, thus getting direct access to the value of the bit. Eve can also take an advantage of the channel loss. She can create a duplicate of the Alice system near the Bob station (fake Alice); as soon as she successfully reads out the setting of the Alice phase modulator she sends this information over the classical channel to the fake Alice. To reject this attack, Alice at least should monitor the light coming through the fiber to be sure no signal is added and no eavesdropping is taking place.

It was previously suggested using a photodiode to monitor the average intensity of the light to detect this attack [2]: The reasonable assumptions are: Eve can change (amplify or attenuate) the signal send to Alice by Bob. She can even completely block the signal and substitute it with her probe. She is not restricted in her ability of constructing the probe; any quantum state can be used for this purpose. Her main task is to resolve four different Alice's phase settings. In agreement with the phase estimation theory (see [9] for a review) the maximum state resolution is given by the Heisenberg limit

$$\phi = \frac{\pi}{2N} \tag{1.1}$$

where N is the number of photons used by Eve. It seems like two-photon state is sufficient for Eve to read out the phase. Unlucky for her and lucky for Alice and Bob this state does not tell which of the four states was used but rather discriminates between the two orthogonal states sets used by Alice to encode the bit. A three-photon state must be used by Eve to fully discriminate the phase. Such states are known as equipartition states

$$\left|\Psi\right\rangle = \frac{1}{\sqrt{N+1}} \sum_{n=0}^{N} \exp(i\theta_n) \left| N-n, n \right\rangle \tag{1.2}$$

They not only possess the phase sensitivity at the Heisenberg limit

$$\phi = \frac{2\pi}{N+1} \tag{1.3}$$

but are capable of resolving which of the phases

$$\phi_k = k\frac{2\pi}{N+1} \tag{1.4}$$

was used for encoding. Hence, the lowest photon number that gives Eve necessary phase resolution is three. The states like (1.2) are entangled states. They are fragile to loss and decoherence; it looks like the best solution that helps Alice to reject this attack is to apply attenuation to the incoming signal. The probability of detecting the state scales as η_A^3 (we denote the transparency of the Alice box as η_A). The loss inserted by Alice must be sufficient to guarantee than the number of successful measurements that Eve can make is much less than she needs to send to the fake Alice. Detailed analysis of this attack will be given elsewhere.

Usually it is assumed that the statistics of the signal sent to Bob by Alice is Poissonian. This assumption is used in the estimation of the number of pulses that contain more then one photon and affects the security. If Alice controls the state preparation completely it is not an issue: she creates a state by applying strong attenuation to the laser pulse that guarantees the Poinssonian statistics. In a two-way system Alice uses the signal sent by Bob through the optical fiber - a signal that runs through Eve's territory. Eve can change the statistics by modulating Bob's signal and increase the probability of a two-photon event without changing the mean photon number. To detect this attack Alice must monitor not only the mean photon number but the statistics as well.

To summarize: the following conditions are necessary (not obviously sufficient) for rejecting the Trojan horse attack:
1. Alice apparatus should have a certain amount of loss to make sure that Eve cannot use a quantum probe;
2. Alice should control the mode structure of the signal coming through the box;
3. Alice should continuously monitor *both,* mean photon number and the statistics of the signal passing through her apparatus

2.1.3. Scattering problem

Long distance secure quantum communication requires that the detector dark current noise stays low to maintain high signal-to-noise ratio. In combination with interferometer visibility, this is the only parameter one should worry constructing a one-way system. For the two-way system another problem occurs: the Rayleigh backscattering from the fiber can cause the false detector clicks and increase the noise level. This effect scales as $1-\exp(-2\alpha L)$ with the length of the fiber reaching equilibrium for the long ($\alpha L >> 1$) fibers. The backscattering is proportional to the system repetition rate and depends on the type of the fiber used. In order to optimize the performance, the system designer must find a compromise between the channel attenuation (including the attenuation of the Alice part of the interferometer necessary to prevent the Trojan horse attack), repetition rate and the error rate. Methods of reducing the backscattering are proposed: IBM Almadein group suggest using a frequency shift introduced by Alice to filter the backscattering light from the signal at Bob side[10] and Geneva group uses additional fiber spool as storage for pulses to give the backscattered light to decay[2]. The use of the storage spool reduces the key generation rate and the frequency shift causes the degradation of the interferometer visibility of the because of the dispersion. It is obvious that some compromise is possible but the scattering problem remains one of the limitations of the performance of the two-way system.

2.2. One-way system

One-way system is free from most of the problems discussed above but instead the system designer faces a need for active stabilization of the interferometer. Most reasonable scenario can be found if the bit is encoded in a relative phase between two pulses of the same polarization. The two pulses are traveling the same path and accumulating the same phase retardation thus keeping the relative phase (and polarization) constant. As they arrive at the Bob's side, the pulses

pass through a scrambler that randomizes their electric field orientation and then sent to a polarizer connected to two different loops of Bob's interferometer (see Figure 1). The scrambler should be made quick enough to react to the transmission fiber changes, but slow enough to keep both pulse polarized the same way. As the pulses are randomly directed to one of the two loops, depending on the initial phase supplied by Alice, they will end up in one of the four detectors. An inherent shortcoming of this scheme is the doubled number of detectors required; its advantages, on the other hand, involve lack of necessity of having expensive (and lossy) phase modulators.

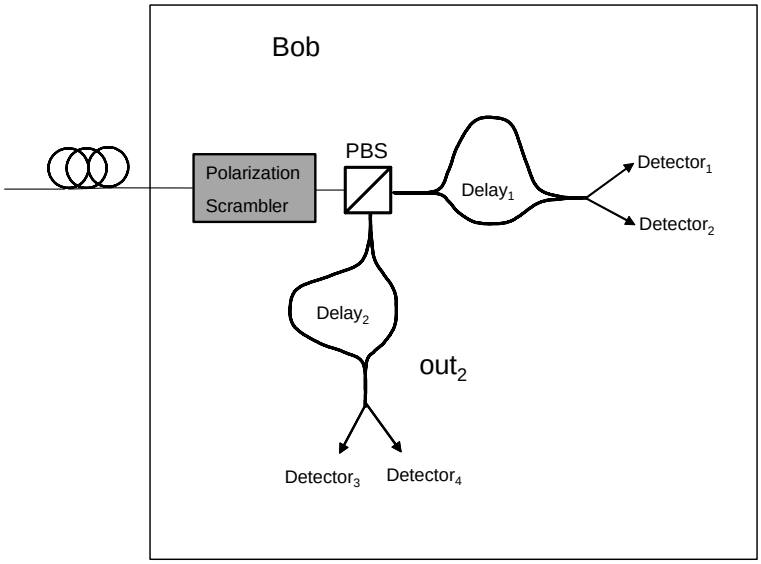

Figure 1. Bob with two different interferometer loops.

The main problem left is to keep the initial relative phase of the interferometer formed by Alice and Bob delay line constant. It requires precise temperature control of the Alice and Bob parts of interferometer. In our design we relax the requirement for the temperature stabilization using auxiliary strong pulses of different wavelength multiplexed with the quantum signal.

The simplest way of preparing a superposition of two pulses of the same polarization is to divide and combine the initial pulse by 50/50 non-polarizing beam splitter. The use of the beam splitter introduces additional 3 dB loss at Alice and Bob side of interferometer. This results in 3 dB extra loss for the one-way system with WCP and in 6 dB loss for the one way system with single photon source (still better than sending a single photon through the two-way system though). Currently this should be considered as a main disadvantage of the one-way system. It was suggested to use the superposition of pulses of different polarization [11, 12]. In our view, that method does not differ much from simply sending a polarized photons. The two pulsed undergo different phase perturbation and interferometer must be stabilized with respect to internal and external perturbation - a very difficult task for the realistic experimental environment (this fact was mentioned already by [8]).

2.3. Summary

As we have seen there are pros and contras for using one-way and two-way systems. One may conclude that there is no unique answer which system is the best without specifying the experimental condition it is supposed to be used and the architecture of the whole system. The loss budget is currently better for the two-way implementation but it does not mean automatically the distance span is going to be necessary longer because of the backscattering problem and security loophole. One-way system seems to be the solution if one is looking for a high pulse repetition and correspondingly high key generation rate.

3. Performance of the WCP QKD

The most dramatic situation occurs if Alice and Bob are not capable of detecting the presence of the eavesdropping. It is known that quantum cryptography using one-photon states can be absolutely secure: Eve has no means to get information without introducing errors. Certain amount of errors can be leveraged by procedures known as error correction and privacy amplification. The situation with two-(many-) photons pulses is not so obvious. The difficulty comes from the fact that Alice and Bob needs to communicate over the public channel and there is no known bound on the information that can be obtained by Eve having unlimited measurement and calculation resources. Following [13, 14] we can assume that Eve gets full information about the bits represented by two-photon pulses and above. This seems to be a severe restriction but this assumption provides us with the security which does not depend on the resources allocated to Eve. We use this approach as a main benchmark for the system performance.

Performance of a WCP QKD depends on the detector efficiency and dark current noise as well as on the interferometer insertion loss and the security model used (through the choice of the mean photon number). The most practical way of single photon counting is the use of an avalanche photodiode in a so-called Geiger mode. At telecom wavelength the best performance is shown by cooled InGaAs APDs. For commercial applications it is reasonable to restrict the temperature range to the limit reached by TEC cooling. As it was reported by several research groups the best performance can be achieved currently by Epitaxx 239BA detector [15, 16]. Our results of Epitaxx 239BA detector performance as well as the security model used for system performance estimation can be found in [17]. Currently we reached quantum efficiency of 10% keeping the dark current per pulse probability as low as $5 \cdot 10^{-7}$ at -90C^0.

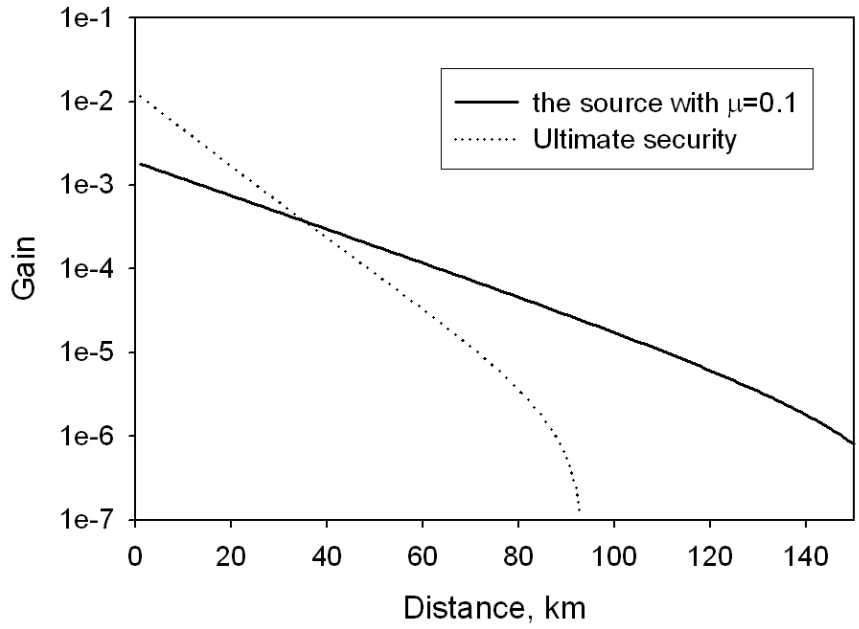

Figure 2 Expected WCP QKD system performance plot based upon the physical parameters used.

We used our experimental results to predict the QKD system performance. Fig. 2 illustrates the degradation of the key rate as a function of link distance. The parameters used to make the plots are the following: the quantum efficiency of the SPD is 10%, dark current probability is 5.10^{-7} per gate pulse, and attenuation at Bob side of interferometer is 4 dB (currently it covers our one- and two-ways system). Fiber loss is assumed to be equal to $0.2dB/km$. If the fiber with higher loss is used the distance must be lowered correspondingly. We plot the gain as a probability of distilling a secure key from the every pulse send by Alice to Bob. To calculate the key rate one must multiply this number by the repetition rate. With these parameters the absolutely secure communication is possible up to the distance of 90 km. To compare our results with the results of the groups not interested in absolute security we plot the key generation rate for

the case of $\mu = 0.1$. This number still provides the user with the reasonable level of security, e.g. it is secure against unambiguous state discrimination attack and simple beam splitting attack but it cannot guarantee the absolute security compared to the single photon case.

SINGLE-PHOTON EXPERIMENTS

4. Experimental Setup.

We also did some precursory QKD measurements using a one-way system employing a true single-photon source and a high performance detector. Figure 3 depicts our experimental setup. All the light sources were located on Alice's side, while the quantum signal detectors were at Bob's. Bob and Alice were connected by a pair of 26.4-km long spools of SMF-28 fiber. One spool (the transmission fiber) was used to transmit both, QKD and interferometer stabilization signals; the other one (the synch fiber) carried strong laser pulses used to synchronize Alice and Bob.

Both, the QKD signal and synchronization pulses were initiated by a linearly polarized CW 532-nm pump light incident on a 20-mm-long Y-cut $LiNbO_3$ crystal. Inside the crystal, the pump photons were parametrically down converted into the time and energy entangled photon pairs. The crystal was situated inside an oven and its temperature was controlled to achieve the optimal conditions for non-critical phase matching (NCPM) of the pump, signal (810 nm) and idler (1550 nm) waves. The idler photons were directed to the interferometer and used for QKD measurements, while the 810 nm photons were used for initiating the timing sequence. A narrow-band (FWHM = 0.12 nm) interference filter was placed in the signal beam path in order to minimize the chromatic dispersion effects in the transmission fiber. After a room-temperature silicon APD detected a 810-nm photon, it would trigger a pulse generator that supplied an electrical pulse to a 1550-nm laser source providing a synchronizing signal. The output of this laser (~ 1 ns long pulse) was propagated to Bob through a synch fiber, where it gated the thermo electrically cooled InP/InGaAs APDs that we used as single photon detectors (SPDs) to measure the QKD signal.

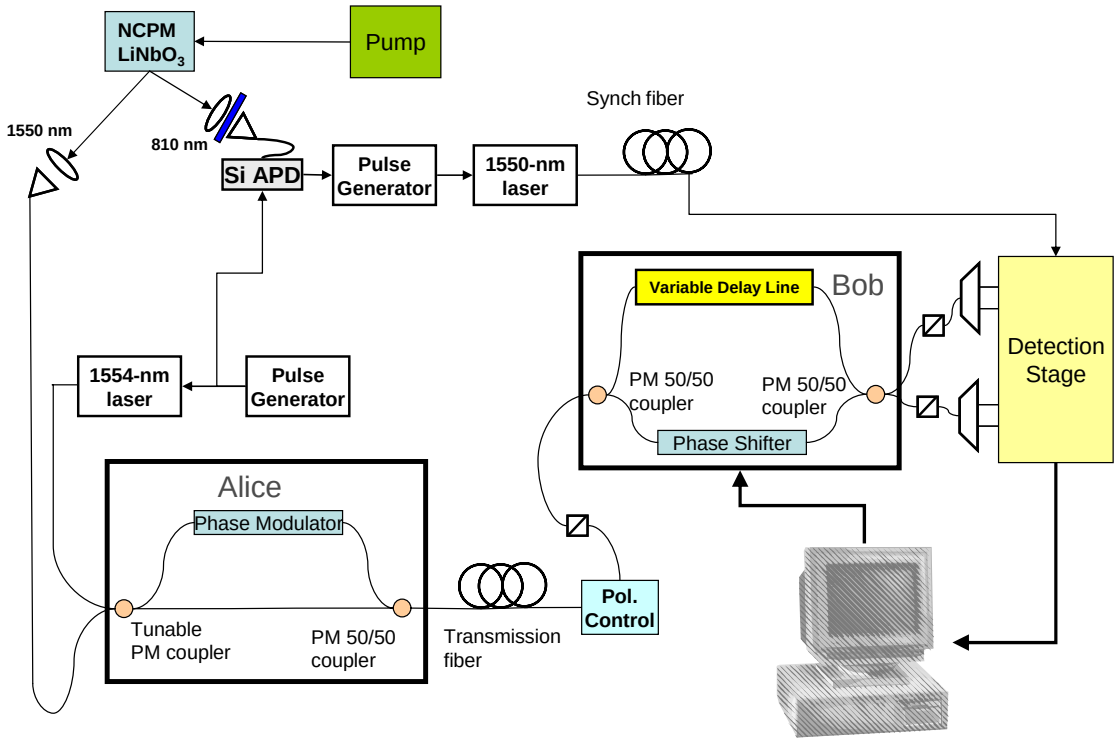

Figure 3. Experimental setup

Short laser pulses (~8 ns) from another 1554-nm source were used to stabilize the interferometer against thermal and mechanical drifts. This laser was fired at 1 kHz, which proved to be often enough for the laboratory conditions. Because of the spontaneous nature of the down conversion, the interferometer stabilizing pulses were not synchronized with the QKD signal and thus could have coincided with the InP/InGaAs APD gates. In order to minimize this effect we used both, time and wavelength de-multiplexing. In addition to the thin film DWDM filters directing the signals to the appropriate Bob's receivers, we also separated them in the time domain: Every time a stabilization pulse was generated, a 100-μs long voltage pulse was supplied to the silicon APD to prevent it from re-triggering. Since no synch pulses were generated during this time interval, the InP/InGaAs APDs were not gated and the QKD signal integrity was preserved.

4.1. Interferometer.

Alice and Bob shared a pair of unbalanced Mach-Zender interferometers, separated by the transmission fiber. There were four different paths that idler photons could have taken through the system; we will denote them as following: Long-Long path (LL) if a wave packet passed through the long arms of both interferometers, Short-Short (SS) – if it passed through both of the short arms, Long-Short (LS) – if it chose to go through a long arm of Alice's interferometer and a short arm of Bob's, and, finally, Short-Long (SL) – if a short arm of Alice's interferometer was combined with the long arm of Bob's. When the path differences in the interferometers were matched within the coherence length of the propagating light, one could observe interference of the LS and SL parts of the wave packet. By adjusting these path differences one could change photon's phase and encode the information this way.

We also used this phase change to balance the interferometers: As one of the interferometers started to drift, the relative path difference would change. This effect would manifest itself in varying differential phase shift between the LS and SL parts of the strong stabilizing signal. By comparing the signature of these interfering peaks appearing at the outputs, we could measure the relative path change. Signals from two classical detectors were feed into a PC with Labview used to analyze the ratio of the peaks and adjust Bob's interferometer accordingly. (No effort was put into compensating the Alice's drift; instead we chose to force both sides to drift in synch.)

Both interferometers were constructed using polarization maintaining (PM) components and their path differences were matched to within a few micrometers. A low loss optical phase shifter was placed into Bob's interferometer to minimize the relative path difference resulting from the thermal and mechanical drifts in the system. It was also used to adjust the relative phase of the quantum signal. (A PM $LiNbO_3$ phase modulator was used for this purpose at Alice's end.) Because of the polarization mode dispersion (PMD) in the interferometer components, it was necessary to control the polarization state of the incoming 1550-nm light. A zero-order half-wave plate was used for this purpose at the entrance of Alice's interferometer, while a polarizer preceded by a polarization controller was placed at Bob's side. We periodically adjusted the controller to compensate for the polarization rotation in the transmission fiber. Additional polarizers were required at the detector's input to compensate for the PMD effects in Bob's interferometer. The performance of the interferometer in the classical regime (with a strong multi photon light pulses) is summarized in the table below.

Component	**Loss (dB)**	**Comments**
Polarizer	1.1	At Bob's Input
Polarizer	1	At Bob's Output #1
Polarizer	0.8	At Bob's Output #2
Polarization Controller	0.6	
DWDM filter	0.6	Quantum Channel Loss
DWDM filter	0.9	Quantum Channel Loss
Total Alice's Loss	3.6	
Total Bob's Loss	4.6	

Table 1a. Interferometer losses

Alice's Input	Bob's Output	Visibility (dB)
1	1	18
1	2	14
2	1	26
2	2	18

Table 1b. Interferometer classical visibility

We used the "better" input port (#2) to inject the quantum signal into the interferometer, while the input port # 1 was used for the stabilization.

Since we used two different wavelengths for QKD and interferometer stabilization, a few words should be said about the limitations of this approach: A perfectly stabilized interferometer (i.e. – when the path difference between the arms is exactly matched) is balanced for any wavelength. However, a finite coherence length of the photonic wave packet, relaxes the stabilization criteria. In general, many different variables, including temperature and mechanical stability of the interferometers, wavelength difference of the signals, etc. need to be balanced to find a solution.

4.2. Single photon visibility

We used this experimental setup to conduct a set of precursory quantum measurements: Figure 4 below illustrates interferometer performance in the single-photon regime. In order to collect the data below, we simply disconnected the feedback loop and ramped up voltage Bob's phase shifter. As the phase delay changed, we gated the SPDs and counted the number of photons appearing at the either end of Bob's output. Since we did not implement the interferometer stabilization for this preliminary experiment, we could not measure the minimum count very accurately; the rough estimate places the visibility at around 20 dB. This number is similar to the classical results shown in Table 2.

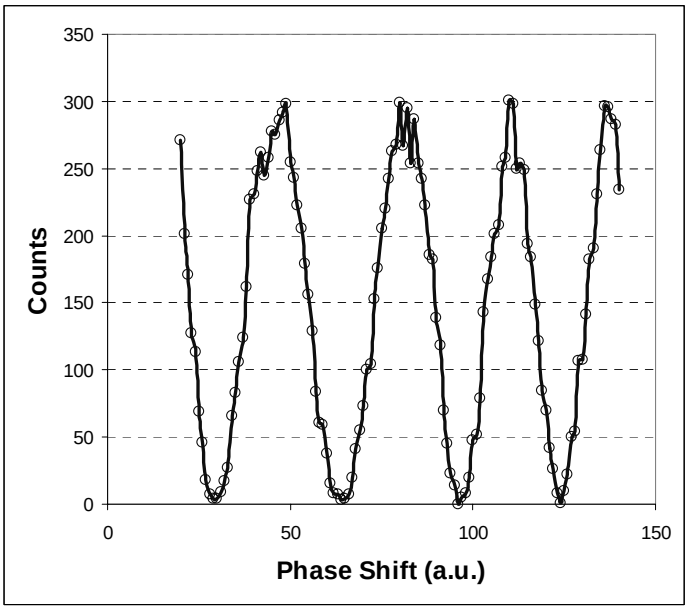

Figure 4. Visibility measurements in the single-photon regime corroborate results obtained with the classical laser pulses. Only one of the output counts is shown; the other one is delayed by π.

We also conducted a set of "simplified" QKD measurements with this system: By changing the voltage applied to the Alice's phase modulator, we changed the phase delay and switched the signal between two different outputs. We alternated between sending 0's and 1's every 10 seconds; 0's appeared mostly at one output, while 1's showed up at the other one. Averaging the data collected during 40 sets of 10 second long runs, we estimated the count rate for 1's to be ~4.5 per second, while that for 0's was around 0.22 s^{-1}. The initial data suggests that when used for QKD, the system should have a bit rate of approximately 2 Hz and quantum bit error rate (QBER) of around 9.1%.

CONCLUSIONS

We implemented a one-way stabilized QKD system using a true single-photon source and high-performance single-photon detectors. Results of the preliminary measurements suggest a possible secure link distance of 150 km (using true single-photon source), 150 km (using WCP with 0.1 photons per pulse on average – the industry benchmark), and 90 km (using unconditionally secure WCP QKD). While there is a definite improvement when a true single photon source is used, the gain is limited by the losses in the Alice's optics. By improving the idler photon collection efficiency and minimizing interferometer losses the single-photon source advantage can be leveraged further.

REFERENCE

1. Bennett, C.H. and G. Brassard. *Quantum Cryptohraphy: public key distribution and coin tossing.* in *International Coference on computers, Systems&Signal Processing.* 1984. Bangalore, India.
2. Gisin, N., et al., *Quantum Cryptography.* Reviews of Modern Physics, 2002. **74**(1): p. 145-195.
3. Brassard, G., et al., *Limitations on practical quantum cryptography.* Physical Review Letters, 2000. **85**(6): p. 1330-3.
4. Hwang, S.-W., *Quantum Key Distribution with High Loss: Toward Global Secure Communication.* Physical Review Letters, 2003. **91**(5): p. 057901/1-4.

5. Acin, A., N. Gisin, and V. Scarani, *Coherent pulse implementations of quantum cryptography protocols resistant to photon number splitting attacks*, in *arXiv:quant-ph/0302037 v1 5 Feb 2003*. 2003.
6. Bennett, C.H., *Quantum cryptography using any two nonorthogonal states.* Physical Review Letters, 1992. **68**(21): p. 3121-4.
7. Muller, A., et al., *"Plug and play" systems for quantum cryptography.* Applied Physics Letters, 1997. **70**(7): p. 793-5.
8. Zbinden, H., et al., *Practical aspects of quantum cryptographic key distribution.* Journal of Cryptology, 2000. **13**(2): p. 207-20.
9. Bjork, G., et al., *Quantum phase resolution and phase distribution.* Quantum Semiclass. Opt., 1998. **10**: p. 705-721.
10. Bethune, D.S., M. Navarro, and W.P. Risk, *Enhanced autocompensating quantum cryptography system.* Applied Optics, 2002. **41**(9): p. 1640-1648.
11. Marand, C. and P.D. Townsend, *Quantum key distribution over distances as long as 30 km.* Optics Letters, 1995. **20**(16): p. 1695-7.
12. Townsend, P.D., J.G. Rarity, and P.R. Tapster, *Enhanced single photon fringe visibility in a 10 km-long prototype quantum cryptography channel.* Electronics Letters, 1993. **29**(14): p. 1291-3.
13. Lutkenhaus, N., *Estimates for practical quantum cryptography.* Physical Review A, 1999. **59**(5): p. 3301-19.
14. Lutkenhaus, N., *Security against individual attacks for realistic quantum key distribution.* Physical Review A, 2000. **61**(5): p. 052304/1-10.
15. Stucki, D., et al., *Photon counting for quantum key distribution with Peltier cooled InGaAs/InP APD's.* Jour. Mod. Optics, 2001. **43**.
16. Hiskett, P.A., et al., *Low-noise single-photon detection at wavelength 1.55 mu m.* Electronics Letters, 2001. **37**(17): p. 1081-1083.
17. Trifonov, A., et al., *Single photon counting at telecom wavelength and quantum key distribution.* Jour. Mod. Optics, 2004: p. 1-17.