# Entanglement Based Quantum Key Distribution Using a Bright Sagnac Entangled Photon Source

C. Erven[1], D. Hamel[1], K. Resch[1], R. Laflamme[1,2], and G. Weihs[1,3]

[1] Institute for Quantum Computing, University of Waterloo, Waterloo, ON, N2L 3G1, Canada
cerven@iqc.ca
http://www.iqc.ca/∼cerven/
[2] Perimeter Institute, 31 Caroline Street North, Waterloo, ON, N2L 2Y5, Canada
[3] Institut für Experimentalphysik, Universität Innsbruck, Technikerstrasse 25, 6020 Innsbruck, Austria

**Abstract.** We report on improvements in an entangled free-space quantum key distribution (QKD) system by replacing the original non-collinear type-II spontaneous parametric down-conversion (SPDC) polarization entangled photon source with a new brighter Sagnac interferometric entangled photon source. While the SPDC source was integral to the initial setup of the system, it was limited in photon pair production rate and entanglement quality. Initial experiments with the new Sagnac source have already yielded substantially higher entangled photon rates and improved visibilities. In order to examine the integration of the new source with the QKD system, a local QKD experiment is performed where the source is pumped with 5 mW of power yielding an average raw key rate of 9,423 bits/s and an average final secret key rate of 2,695 bits/s, with an observed average QBER of 2.48%. Initial experiments distributing entangled photons over a single 1,305 m free-space link have seen entangled photon pair coincident detection rates as high as 3,000 cps. Extrapolating based on these initial numbers and previous experiments, we hope to obtain an average secret key rate of 715 bits/s for a two free-space link QKD experiment running the source at full power which will represent an order of magnitude increase over our previous experiments. An additional benefit of the new source is that it has a much narrower bandwidth which will aid in making the system compatible with daylight experiments. However, one drawback of the source is an appreciable double pair emission rate which initial experiments indicate.

**Keywords:** Quantum Cryptography, Free-Space Quantum Key Distribution, QKD, Entangled Photons, Sagnac Interferometric Source.

## 1 Introduction

Free-space quantum key distribution (QKD) has seen many experiments validate the possibility of its implementation in various real world scenarios; for example, see the more recent experiments performed by Marcikic *et al.* [1], Ursin *et al.* [2],

A. Sergienko, S. Pascazio, and P. Villoresi (Eds.): QuantumCom 2009, LNICST 36, pp. 108–116, 2010.

and Erven *et al.* [3]. Now that the feasibility of the basic idea has been demonstrated, experiments have shifted to improving the practical use of such systems. Some groups have started working on performing quantum key distribution with an orbiting satellite, such as the International Space Station, in order to achieve world wide quantum communication [4,5,6]. While other groups have focused on operating a free-space QKD system during daylight hours where high background light can make communication difficult [7]. Towards the same goal of improving free-space QKD for practical applications, we focus on improving the key generation rate of our system from previous experiments [3] through the use of a new brighter source of entangled photon pairs.

## 2 Experimental Setup

Our system performs the BBM92 entanglement based QKD protocol developed by Bennett *et. al.* [8] in 1992. Entangled photon pairs are distributed from a source to Alice and Bob who randomly measure a photon from each pair in one of two complementary bases. These measurement results become their generated secret key while the laws of quantum mechanics guarantee the security of the key. Precise integrity for the system is assured with the security proof by Ma *et. al.* [9] neglecting the need for authenticated classical communication, the loopholes opened from detector efficiency mismatch and double clicks, finite key statistics, and some simplifying assumptions made in the proof such as bit and phase errors being equal. We also require the squashing model [10,11,12] and the knowledge that the requirement for active polarization detection can be relaxed to include the passive scheme [13] in order to apply the security proof.

In previous experiments [3], entangled photon pairs were generated using a non-collinear type-II spontaneous parametric down-conversion (SPDC) source first reported by Kwiat *et al.* [14]. In this setup, a BBO non-linear optical crystal in a non-collinear configuration was used to produce entangled photon pairs. While the SPDC source was one of the first stable, high-intensity sources of polarization-entangled photon pairs developed and was integral in the initial setup of the experiment; it was limited to a local coincident entangled photon detection rate of 18,000 counts/sec(cps) with observed visibilities of 99.5% and 92% in the rectilinear (H/V) and diagonal (+45°/-45°) bases respectively. These visibilities corresponded to a baseline error rate for the system of 2.1% which increased the amount of error correction and privacy amplification needed, even without an eavesdropper present, and thus reduced the final secret key rate of the system significantly.

In order to improve the key rate of the system and make it more practical in a real-world scenario, we built a brighter Sagnac entangled photon source originally developed by Kim *et al.* [15] and optimized by Fedrizzi *et al.* [16] to replace the previous SPDC source. The Sagnac entangled photon source, shown in Fig. 1, utilizes a periodically poled KTP (PPKTP) non-linear optical crystal in a collinear configuration placed in an interferometer loop to generate photon pairs. Entangled photons are produced by sending 45° polarized light onto a dual

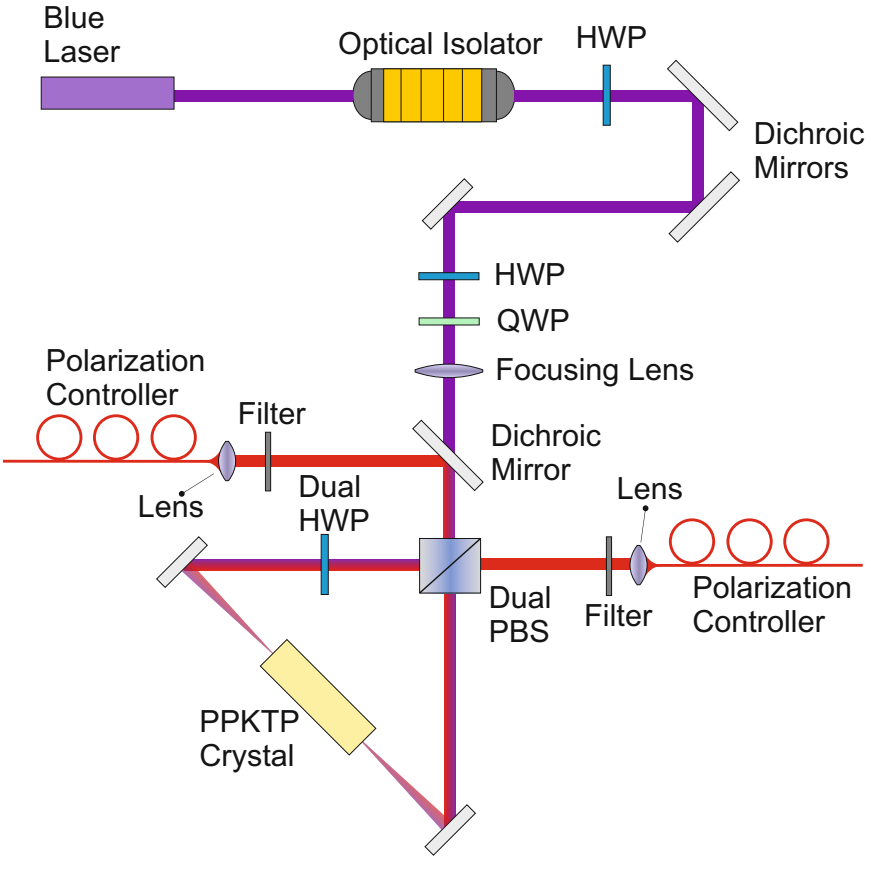


**Fig. 1.** Experimental schematic of the Sagnac interferometric entangled photon source. Entangled photon pairs are produced by bi-directionally pumping a PPKTP non-linear optical crystal which produces down-converted correlated photon pairs. The dual wavelength HWP and PBS are responsible for removing the path information of the photons, thus producing entangled photons, and for separating the pairs of photons into two paths to be sent to Alice and Bob.

wavelength polarizing beamsplitter (PBS) which has the effect of bi-directionally pumping the PPKTP crystal sitting in the middle of the interferometer loop. A dual wavelength half-waveplate (HWP) rotates the light in one arm by 90° and ensures that the blue laser light is properly polarized so that the crystal produces down-converted polarization correlated photon pairs in both directions around the loop. The dual wavelength HWP also rotates the polarization of the down-converted photons traveling counter-clockwise around the loop, this has the effect that after the down-converted photons are split on the dual wavelength PBS the path information has been erased. Thus, after the PBS, polarization entangled photons have been generated. The two beams of entangled photon pairs are

collected directly from one port of the PBS and via a dichroic mirror responsible for splitting the down-converted photons from the blue pump laser at the second exit port.

For our source, we pump the PPKTP crystal with a 404 nm grating stabilized, power tuneable, laser with a maximum power of 50 mW from Toptica Photonics. We use a 10 mm × 1 mm × 1 mm PPKTP crystal made by Raicol. Local experiments with the new source yield single photon detection rates of 400,000 cps in either output path and coincident entangled photon detection rates of 40,000 cps at only 5 mW of pump power. This is currently the maximal detection rate which the data acquisition system can handle. For comparison, the previous source was pumped with 50 mW of power; thus, we have already doubled the number of entangled photon pairs produced at one-tenth the power level of the previous source. In order to get more entangled photon pairs from the source to counteract losses experienced in the polarization detection units and eventually over the free-space link we can still increase the pump power to 50 mW and also use a longer crystal.

Another advantage of the Sagnac source over the previous SPDC source is that it is extremely narrowband, with a bandwidth of 0.36 nm, which allows us to filter much narrower at the receiver stations and reduce the number of errors due to the detection of background light. In the experiment detailed in this paper we use 5 nm interference filters as well as 635 nm long pass filters (responsible for filtering the blue laser light). In previous experiments with the old SPDC source we were forced to use 10 nm filters in order to maintain appreciable detection rates.

Lastly, for the experiment detailed in this paper, we observed local visibilities of 99.2% and 96.1% in the rectilinear and diagonal bases respectively. These represent much improved visibilities over the ones observed with the previous source. Additionally, the visibilities seem to degrade less when they pass through the polarization detection optics which is most likely due to the improved polarization compensation accomplished with manual polarization controllers. The compensation is better since the bandwidth of the photons is much narrower than before allowing the polarization controllers to correct the random rotation of the fibres accurately for more photon pairs. While visibilities for a Sagnac source as high as 99.5% were observed by Fedrizzi *et al.* [16] in the diagonal basis, these were measured at very low power levels which greatly reduced the effects of accidental coincidences. Even so, our observed visibilities lead to a lower baseline error rate of 1.18% which coupled with the fact that the polarization compensation is more accurate means less error correction and privacy amplification are required thus producing a higher final key rate.

We implemented a local QKD system due to polarization stability issues with our free-space link which we are currently still debugging. Thus, Alice and Bob locally measured each half of their photon pairs while sitting next to the source connected to it with short optical fibres. They measured the photons with passive polarization detector boxes consisting of: a filter to reject background light, a 50/50 non-polarizing beamsplitter (BS) to perform the basis choice, a polarizing

beamsplitter in the reflected arm of the BS to separate horizontally and vertically polarized photons, and a half waveplate and PBS in the transmitted arm of the BS to separate photons polarized at $+45°$ and $-45°$. Avalanche photodiode single photon detectors converted the photons into an electronic signal which was stamped with the polarization measured and a highly accurate time of arrival (accurate to 156.25 ps). This information was then transferred to Alice's and Bob's laptops and custom written software then performed the rest of the BBM92 protocol including entangled photon pair identification, sifting, error correction with an optimized Cascade algorithm [17,18], and privacy amplification with a 2-universal hash function [19].

## 3 Results

For the experiment detailed below, the source was operated at a power of 5 mW producing an average of 134,311 cps in Alice's detectors, 182,047 cps in Bob's detectors, and an average coincident entangled photon detection rate of 9,423 cps. As was mentioned before, this is the maximal detection rate which the current data acquisition system can handle. However, once we move to free-space experiments and link losses are taken into account this should still be adequate for detection while pumping the source with 50 mW of power.

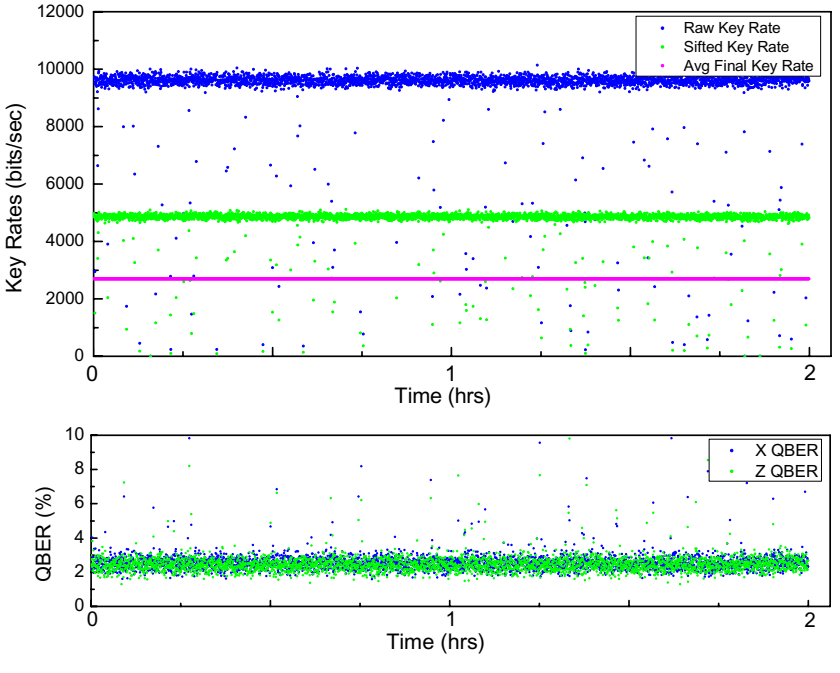


**Fig. 2.** Top Graph: Observed raw (top series, in blue), sifted (middle series, in green), and average final (bottom series, in magenta) key rates during the experiment. Bottom Graph: Observed X (in blue) and Z (in green) QBER's throughout the experiment.

**Table 1.** Reconstructed coincidence matrix for Alice and Bob from the experiment

| | | Alice | | | | |
|---|---|---|---|---|---|---|
| | | H | V | + | - | Total |
| | H | 72,545 | 3,992,143 | 1,436,747 | 2,041,365 | 7,542,800 |
| Bob | V | 3,053,610 | 103,283 | 2,675,152 | 2,629,527 | 8,461,572 |
| | + | 1,049,401 | 2,246,669 | 88,197 | 3,986,896 | 7,371,163 |
| | - | 1,503,492 | 1,783,033 | 4,296,481 | 126,318 | 7,709,324 |
| | Total | 5,679,048 | 8,125,128 | 8,496,577 | 8,784,106 | |

The lower panel of Fig. 2 shows the observed QBER over the course of the experiment. As was discussed earlier, we see a lower average total QBER of 2.48% over the course of the experiment compared to previous experiments with the old SPDC source. The top panel of Fig. 2, shows the observed raw key rate (top series, in blue), sifted key rate (middle series, in green), and average final key rate (bottom series, in magenta) throughout the experiment. We observed an average raw key rate of 9,423 bits/s, an average sifted key rate of 4,765 bits/s, and an average final key rate of 2,695 bits/s. Table 1 shows the reconstructed coincidence matrix from Alice's and Bob's measurement data recorded during the experiment. The table also allows one to calculate the average visibilities of 95.13% and 94.95% in the rectilinear and diagonal bases from the experiment.

## 4 Discussion

As can be seen from the local experiment detailed above, the new Sagnac source shows much promise for producing entangled photon pairs with a lower error rate than before. Experiments with the source over one 1,305 m free-space link have yielded coincident detection rates for entangled photons of between 1,500 cps and 3,000 cps at 10 mW of pump power. While polarization stability issues in the 30 m singlemode fibre, which transports the entangled photons to rooftop sending telescopes, and the free-space link have so far made experiments with the full free-space link impossible; the initial numbers from free-space experiments make us very optimistic for good rates in a two free-space link experiment. Extrapolating from results in our previous experiment [3] where the transmission of one free-space link was ∼20% and the transmission of two free-space links was ∼9%, we are expecting to get coincident detection rates of approximately 850 cps at 10 mW of pump power and 2,500 cps at 50 mW of pump power for a two free-space link experiment. With an efficiency of ∼0.2860 secret key bits per raw key bit after sifting, error correction, and privacy amplification; we are hoping to get final key rates of ∼243 bits/s at 10 mW and ∼715 bit/s at 50 mW of pump power. This would represent an order of magnitude increase in our secret key rate over our previous experiments and would almost put the system in the kbits/s range, making it much more practical for real world applications.

One potential problem with the higher entangled photon rates generated with the new Sagnac source is the possibility of double pair emission events where two

entangled photon pairs are created in the crystal within one coincidence window. Alice's and Bob's resulting measurements will no longer agree if they happen to measure photons from different pairs. Worse than this, the assumption that double clicks are negligible, needed to apply the security proof, will no longer be reasonable as the number of double pair emissions becomes appreciable. Indeed, preliminary experiments by one of us (D.H.) indicate that the visibilities degrade from 98.6% and 98.3% (H/V and +/-) to 85.0% and 84.4% (H/V and +/-) when increasing the laser power from 0.6 mW to 31.5 mW (measured after the optical isolator). This will be the subject of a forthcoming publication by some of the authors. In order to re-apply the security proof for the system, special care will be required to detect double clicks and assign each of them a random outcome. This will have the unfortunate consequence of increasing the error rate and shrinking the final key rate.

The narrow bandwidth of the new Sagnac source also leads to the additional benefit of helping towards daylight compatibility for the system. As was mentioned earlier, there are a number of groups [7] focused on operating a free-space QKD system during daylight hours. The main problem encountered with operating a free-space system during daylight hours is the extremely high background light levels. To combat this, there are really only 3 possible filtering techniques one can use: spatial, spectral, and temporal. Having a much narrower bandwidth than the previous source allows us to greatly improve the spectral filtering of the photons at the receiver stations. With a bandwidth of 0.36 nm we should be able to move from 10 nm to 1 nm filters to greatly reduce the background light without seeing a significant drop in the entangled photon detection rates. With slightly improved spatial and temporal filtering, the hope is that we shall be able to run the system in daylight conditions.

## 5 Conclusions

In conclusion, in order to improve on our previous experiments with an entangled free-space QKD system and make the system viable for real-world practical applications we have focused on improving the key generation rate of our system. In order to do this, we replaced the type-II SPDC entangled photon source, which was limited to an entangled photon pair detection rate of 18,000 cps with 50 mW of pump power detected locally, with a new brighter Sagnac entangled photon pair source, capable of producing local coincidence rates of 40,000 cps with just 5 mW of pump power. The narrow bandwidth of the source will also allow us to better filter out background light, thus helping to further reduce errors and the additional error correction and privacy amplification required. The narrow bandwidth will furthermore be useful in implementing daylight compatibility for the system. The one observed drawback of the source is a non-negligible double pair emission rate which will have to be carefully handled by the system so as not to expose a security loophole.

A local experiment examining the integration of the new source with the QKD system was detailed using 5 mW of pump power, which yielded a raw key rate

of 9,423 bits/s and a final secret key rate of 2,695 bits/s. While issues with our free-space link prevented a fully distributed QKD experiment from being run, initial results with distributing entangled photon pairs over a single 1,305 m free-space link have seen entangled photon detection rates between 1,500 cps and 3,000 cps at 10 mW of pump power. Extrapolating from these numbers and our previous experiments with the old source, we expect to see a final secret key rate of ∼715 bits/s running the source at the full 50 mW of pump power during a two-free space link experiment. This will represent an order of magnitude increase in our secret key rate over our previous experiments.

*Acknowledgements.* Support for this work by NSERC, QuantumWorks, CIFAR, CFI, CIPI, ORF, OCE, ERA, and the Bell family fund is gratefully acknowledged.

## References

1. Marcikic, I., Lamas-Linares, A., Kurtsiefer, C.: Free-Space Quantum Key Distribution with Entangled Photons. Appl. Phys. Lett. 89, 101122 (2006)
2. Ursin, R., Tiefenbacher, F., Schmitt-Manderbach, T., Weier, H., Scheidl, T., Lindenthal, M., Blauensteiner, B., Jennewein, T., Perdigues, J., Trojek, P., Ömer, B., Fürst, M., Meyenburg, M., Rarity, J., Sodnik, Z., Barbieri, C., Weinfurter, H., Zeilinger, A.: Entanglement-Based Quantum Communication Over 144 km. Nature Physics 3, 481–486 (2007)
3. Erven, C., Couteau, C., Laflamme, R., Weihs, G.: Entangled Quantum Key Distribution Over Two Free-Space Optical Links. Opt. Exp. 16, 16840–16853 (2008)
4. Rarity, J.G., Tapster, P.R., Gorman, P.M., Knight, P.: Ground to Satellite Secure Key Exchange Using Quantum Cryptography. New J. Phys. 4, 82 (2002)
5. Aspelmeyer, M., Jennewein, T., Pfennigbauer, M., Leeb, W., Zeilinger, A.: Long-Distance Quantum Communication With Entangled Photons Using Satellites. IEEE J. of Selected Topics in Quantum Electronics 9, 1541 (2003)
6. Perdigues, J., Furch, B., de Matos, C., Minster, O., Cacciapuoti, L., Pfennigbauer, M., Aspelmeyer, M., Jennewein, T., Ursin, R., Schmitt-Manderbach, T., Baister, G., Rarity, J., Leeb, W., Barbieri, C., Weinfurter, H., Zeilinger, A.: Quantum Communications at ESA - Towards a Space Experiment on the ISS. In: 58th International Astronautical Congress, Hyderabad, India (2007)
7. Peloso, M.P., Gerhardt, I., Ho, C., Lamas-Linares, A., Kurtsiefer, C.: Daylight Operation of a Free Space, Entanglement-Based Quantum Key Distribution System (2008), eprint, quant-ph/0812.1880
8. Bennett, C.H., Brassard, G., Mermin, N.D.: Quantum Cryptography without Bell's Theorem. Phys. Rev. Lett. 68, 557 (1992)
9. Ma, X., Fung, C.H., Lo, H.K.: Quantum Key Distribution With Entangled Photon Sources. Phys. Rev. A 76, 012307 (2007)
10. Beaudry, N.J., Moroder, T., Lütkenhaus, N.: Squashing Models for Optical Measurements in Quantum Communication. Phys. Rev. Lett. 101, 093601 (2008)
11. Tsurumaru, T., Tamaki, K.: Security Proof for QKD Systems with Threshold Detectors (2008), `http://arxiv.org/abs/0803.4226`
12. Koashi, M., Adachi, Y., Yamamoto, T., Imoto, N.: Security of Entanglement-Based Quantum Key Distribution with Practical Detectors (2008), `http://arxiv.org/abs/0804.0891`

13. Lütkenhaus, N.: Institute for Quantum Computing, University of Waterloo, 200 University Avenue West, Waterloo, ON, N2L 3G1, Canada (personal communication, 2008)
14. Kwiat, P.G., Mattle, K., Weinfurter, H., Zeilinger, A., Sergienko, A., Shih, Y.: New High-Intensity Source of Polarization-Entangled Photon Pairs. Phys. Rev. Lett. 75, 4337 (1995)
15. Kim, T., Fiorentino, M., Wong, F.N.C.: Phase-Stable Source of Polarization-Entangled Photons using a Polarization Sagnac Interferometer. Phys. Rev. A 73, 012316 (2006)
16. Fedrizzi, A., Herbst, T., Poppe, A., Jennewein, T., Zeilinger, A.: A Wavelength-Tunable Fiber-Coupled Source of Narrowband Entangled Photons. Opt. Exp. 15, 15377 (2007)
17. Brassard, G., Salvail, L.: Secret-Key Reconciliation by Public Discussion. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 410–423. Springer, Heidelberg (1994)
18. Sugimoto, T., Yamazaki, K.: A Study on Secret Key Reconciliation Protocol "Cascade". IEICE Trans. Fundamentals E83A(10), 1987 (2000)
19. Carter, J.L., Wegman, M.N.: Universal Classes of Hash Functions. Journal of Computer and System Sciences 18, 143 (1979)