

Decoy-state quantum key distribution with heralded single photon source

Q. Wang^{1,2}, W. Chen², G. Xavier¹, M. Swillo¹, S. Sauge¹, M. Tengner¹,
T. Zhang², Z. F. Han², G. C. Guo², A. Karlsson¹

¹Department of Microelectronics and Applied physics, the Royal Institute of Technology, KTH, Sweden

²Department of Physics, Key Laboratory of Quantum Information, CAS, USTC, 230026, Hefei, China

Abstract: We have experimentally demonstrated a decoy-state quantum key distribution scheme with a heralded single-photon source based on parametric down-conversion. We used a one-way BB84 protocol with a four states and one-detector phase-coding scheme, which is immune to recently proposed time-shift attacks, photon-number splitting attacks, and can also be proven to be secure against Trojan horse attacks and any other standard individual or coherent attacks.

Since the Bennett-Brassard 1984 (BB84) protocol [1] was put forward, quantum key distribution (QKD) has been widely investigated in recent years because of its unconditional security compared with conventional cryptography. In current practice, an attenuated laser (*i.e.*, emitting a weak coherent state WCS) or a parametric down-conversion source (PDCS) are mostly employed in quantum cryptosystems. An HSPS has a sub-Poissonian photon number distribution, and it has already been proven that a source with sub-Poissonian distribution can substantially improve the performance of QKD compared with those with Poissonian distribution (e.g. WCS) [2]. Here, we apply both HSPS and the decoy-state method [3-5] in our QKD experiment.

In our experiment, we use a three-intensity decoy state method and our source is a HSPS with sub-Poissonian distribution emitting from a PDC process. By applying the same characterization method as in [6], we can get a substantial sub-Poissonian distribution (with about 40 percent single photon probability). Using the same method as in [6], and taking statistical fluctuation into account, we can derive a lower bound of the counting rate of single-photon states (Y_1^L) and an upper bound of the quantum bit-error rate of single-photon

$$\text{states } (e_1^U) \text{ as: } Y_1^L = \frac{p_2'(\mathbf{m}')Q_m^L - p_2(\mathbf{m})Q_{m'} - Y_0^U(p_0(\mathbf{m})p_2'(\mathbf{m}') - p_0'(\mathbf{m}')p_2(\mathbf{m}))}{p_1(\mathbf{m})p_2(\mathbf{m}') - p_1'(\mathbf{m}')p_2(\mathbf{m})}; e_1^U = \frac{Q_m E_m - e_0 Y_0^L p_0'(\mathbf{m}')}{Y_1^L p_1'(\mathbf{m}')}$$

Where e_0 and Y_0 are the quantum bit-error rate and counting rate of vacuum state; \mathbf{m} (\mathbf{m}') is the mean photon number per time slot (what we used is 2.5 ns in our experiment); Q_m ($Q_{m'}$) and E_m ($E_{m'}$) are the overall counting rate and the quantum bit-error rate for signal \mathbf{m} (\mathbf{m}') individually.

Furthermore, after error correction and privacy amplification, we can get the final key generation rate from the signal (\mathbf{m}') as [7]: $R \geq q \cdot \left\{ -Q_m f(E_{m'}) H_2(E_{m'}) + Q_0 + Q_1^L (1 - H_2(e_1^U)) \right\}$

As shown in Fig. 1, using the BB84 protocol and under the same experimental conditions, we compare our HSPS with decoy state scheme to several other schemes, including HSPS without decoy states, WCS with or without decoy states, and also the ideal single-photon source case. As can be seen, our scheme (red solid line) gets the maximum tolerable losses or the highest key generation rate under fixed losses among all these practical schemes. Moreover, if a better HSPS (blue dashed line with 70% correlated photon pairs [8]) is used, its performance comes close to the ideal single-photon source.

Our experimental setup is shown in Fig. 2. We use a 532 nm continuous wave (CW) laser to pump a periodically-poled LiNbO3 (PPLN) crystal of 50 mm length, to generate non-degenerate entangled photon pairs (with 809 nm and 1555 nm wavelengths); After triggering one photon at 809nm, with gating time at 2.5 ns and gating frequency at 650 kHz, we can get a HSPS with a narrow bandwidth (0.8 nm FWHM), which has about 40% single-photon probability. The heralded photon is transmitted from Alice to Bob through 25 km of spooled SMF-28 fiber, incorporating a one-way Faraday-Michelson (F-M) QKD system [9]. In order to avoid the large insertion loss of presently available optical amplitude modulators (AM, > 3 dB), we use a fiber pig-tailed optical switch (OS, 0.6 dB loss) at the arm of signal (1555nm), and place an acousto-optic-modulator (AOM) before the pump light, by controlling both of them in our program, we can randomly generate signals at 1555nm wavelength among the three intensities: $[\mathbf{m}', \mathbf{m}, \mathbf{m}_0] = [5.532 \times 10^{-3}$,

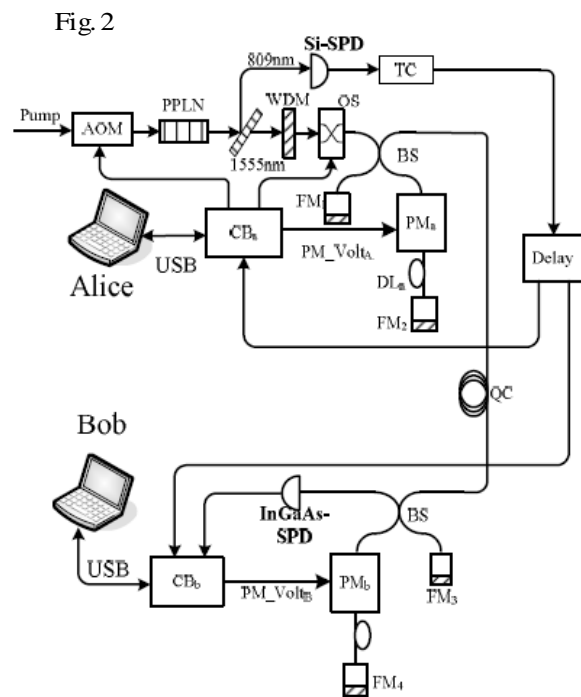
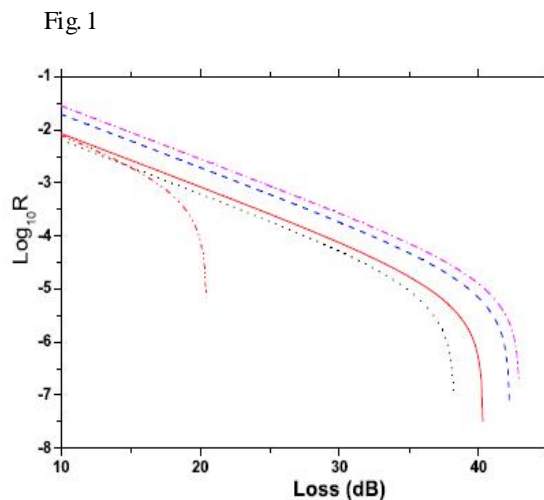
$0.588 \times 10^{-3}, 0.577 \times 10^{-5}]$, and the ratio between them is about 10 : 4 : 1. Meanwhile, we set a time chopper in the triggering signal, on one hand to easily synchronize the signals at 1555 nm, on the other hand to keep the dark count rate for the three intensities at almost the same level. In our QKD system, we adopted a scan

and transmission mode, which makes it quite stable for several hours of continuous measurements. For example, during a typical measurement of 200 mins, (with effective transmission time about 54 mins, the scan and responding time are considerably longer than the transmission time because of the low coincidence count rate), with a total of 1.5×10^9 triggering pulses, the detection efficiency is about 7.5%, the vacuum state counting rate is about 0.8×10^{-5} /gate, the counting rate and average quantum bit-error rate (QBER) are about 1.01×10^{-4} (1.06×10^{-4}) and 6.33% (5.44%) for m' (m) respectively. After a total loss of 36 dB, we get a key generation rate of about 5.065×10^{-6} . Finally, we obtain 5065 secure key bits from a total of 143176 coincidence counts, which agrees well with the theoretical value.

The final key rate is lower than in other systems, because there are large losses in our QKD system, including the insertion losses of the WDM filter and the optical switch, the inefficient InGaAs detector, and most importantly, the F-M interferometer, for the signal photons have to go through each phase modulator (PM) twice, and have to suffer losses from two beam-splitters. With present technology, it is realistic to decrease the loss by 15 - 18 dB in this QKD system, which is quite considerable for a long distance transmission (>100 km).

In summary, though our present setup still contains many deficiencies, our experimental results are sufficient to in principle demonstrate that our using the HSPS based decoy state scheme could overcome many practical schemes in loss tolerance, which also means it could give a highest key generation rate under fixed loss. Besides, our scheme does not evoke higher costs or other technological requirements than in any other schemes. Therefore, even when practical usability is taken into account, it is still a very promising candidate in the implementation of the quantum cryptography in the near future.

Figures:



References:

- [1] C. H. Bennett and G. Brassard, in Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India (IEEE, New York, 1984), p. 175.
- [2] E. Waks, C. Santori, and Y. Yamamoto, Phys. Rev. A 66 042315 (2002).
- [3] W. Y. Hwang, Phys. Rev. Lett. 91, 057901 (2003).
- [5] X. B. Wang, Phys. Rev. Lett. 94, 230503 (2005).
- [6] Q. Wang *et al.* ArXiv: quant-ph/0803.3643
- [7] H. K. Lo, e-print quant-ph/0503004v1.
- [8] A. Zavriyev and A. Trifonov, in Proceedings of single photon workshop 2007 (Turin, Italy, 2007).
- [9] X. F. Mo, B. Zhu, Z. F. Han, Y. Z. Gui, and G. C. Guo, Opt. Lett. 30, 2632 (2005).