Use of discrete modulation and a continuous wave local oscillator in a 24 km continuous variable quantum key distribution system

Quyen Dinh Xuan[1], **Zheshen Zhang**[1,2], **and Paul L. Voss**[1,2]

1. Georgia Tech Lorraine, Georgia Tech-C.N.R.S., UMI 2958,

2-3 rue Marconi, Metz, France

and

2. School of Electrical and Computer Engineering,

Georgia Institute of Technology,

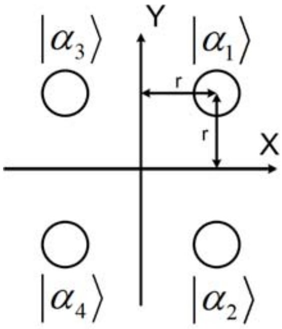
777 Atlantic Drive NW 30332-0250 Atlanta, USA

Abstract: We implement an experimental continuous variable quantum key distribution system over 24 km of optical fiber that uses discrete signaling and a continuous wave local oscillator. A secure key rate of 3.45 kb/s was achieved.

OCIS codes: (270.5568) Quantum cryptography; (270.5565) Quantum communications

As the most mature application of quantum communication, quantum key distribution (QKD) enables two users to build a secure key with unconditional security. As opposed to discrete QKD which uses single photon counters, continuous variable QKD [1] performs homodyne or heterodyne measurements. This provides benefits for implementation in metro optical networks, which include potential multi-GHz signaling with detection by standard PiN photodiodes and a high degree of immunity to out of band noise. However, the rate bottleneck for continuous variable based systems has occurred in the complexity of CVQKD error reconciliation process because extremely efficient error correction codes on Gaussian distributed signals have been required. The development of security proofs of protocols that use discrete signaling [2-4] has been motivated by the need to simplify the reconciliation process and to make CVQKD more compatible with binary-signaled optical networks. Our proposal [4] further improves on the situation by providing the first security proof against collective attacks for a discretely-signaled protocol that also uses post-selection. Post-selection provides a critical speed-up in error correction because the required error correcting code on a binary symmetric channel, while still required to be highly efficient, must correct far fewer errors and thus executes more quickly. In this conference paper, we present results from an experimental system over 24 km of optical fiber that is the first implementation of a discretely-signaled CVQKD system associated with a protocol with security proof. The system also provides several other novel features, compared to other experiments [5-9]. It is the first experiment that uses a continuous wave local oscillator, which we believe to be better suited to future higher-speed systems, and the first to use optical amplification in the receiver.

In the protocol Alice uses QPSK modulation, randomly sends one of four states as pictured in Fig. 1-left. Bob performs homodyne measurements. The key idea of the protocol [4] is the use of a tomographic measurement of Bob's quantum state on a random subset of data, which allows calculation of security when post-selection is used. It produces a relatively tight bound on an Eavesdropper’s obtainable information and results in a large secrecy capacity.



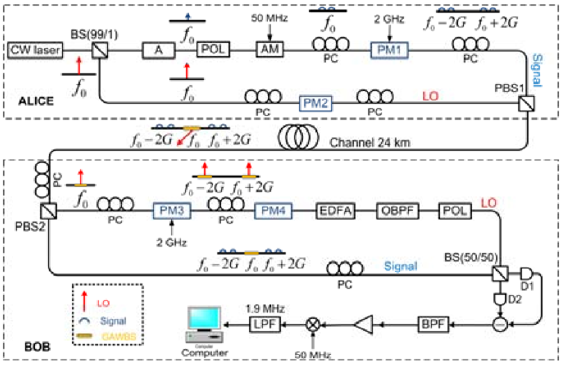


Fig. 1-left, The signaling scheme used in the protocol.   Fig. 1-right Experimental scheme.

The experimental setup is shown in Fig. 1-right. Alice first uses a beam splitter to split the continuous wave beam into signal and local oscillator paths. She then uses an amplitude modulator on the signal path to move the signal power to two 50MHz sidebands. The amplitude modulator is operating at the extinction point so that all signal power is completely moved into the sidebands. Alice then uses a phase modulator operating at very nearly 2GHz. The amplitude of the RF 2GHz signal is set at the first root of the Bessel function so that baseband of the signal is ideally completely moved to a set of sidebands separated by 2GHz. This is needed in order to avoid guided acoustic wave scattering (GAWBS) [10] from the LO into the signal band at 50 MHz. On the local oscillator path, Alice uses another phase modulator to randomly set the local oscillator into four phases as is described in the protocol. Alice then uses a polarization beam splitter to couple the signal and local oscillator into two orthogonal polarizations and sends them into 24km optical fiber. On the detection side, Bob first uses a polarization beam splitter to split the signal and local oscillator. On the local oscillator path, Bob first uses a polarization phase modulator operating at the same frequency and amplitude as Alice’s first phase modulator in order to ideally entirely move the local oscillator frequency into sidebands separated by 2GHz. Then he uses a second phase modulator to select the detection phase of the homodyne measurement. The local oscillator then undergoes optical amplification, which boosts the local oscillator power to 15.0dBm. The output of the local oscillator is filtered by an optical filter with bandwidth of 0.8nm. After a polarizer, the local oscillator and the signal interfere on a 50/50 beam splitter and are detected by two PiN detectors. The output RF signal of the two detectors is then subtracted by a 180 degree hybrid bridge. The electronic signal then passes through a 25 MHz high pass filter and an electronic amplifier with 50dB gain. The detector common mode noise rejection is 64 to 65 dB. The output of the electronic amplifier is then frequency shifted by a mixer operating at 50MHz. The base band signal is filtered by a 1.9MHz low pass filter and acquainted by National Instrument analog data acquisition card. The computer performs post-selection and error correction.

GAWBS noise cancellation must be very effective in order for the system to operate securely. This is because any GAWBS noise detected by Bob must be considered to be under the control of Eve, reducing the security of the system. We see in Fig. 2 the GAWBS noise spectra measured with 6 dB more LO power than used in actual QKD runs. In Fig. 2, at 2GHz phase-modulator frequency, the excess noise power is almost 1% of the shot noise limit. This is due to imperfect frequency translation. By optimizing the polarization going into the phase modulators and laser power of the local oscillator, 0.3% excess noise was achievable in experimental runs.

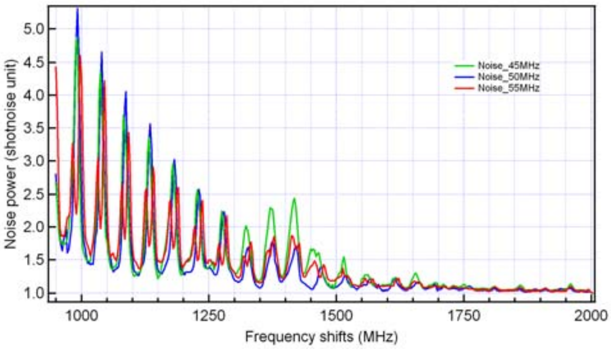


Fig.(2) GAWBS noise power vs. translation frequency, corresponding to 45MHz (green), 50MHz (blue), and 55MHZ(red) RF double sidebands

Under the described conditions, we achieve 27 dB suppression of GAWBS noise and a final secure key rate of 3.45 kb/sec over 24.2 km of optical fiber. This compares favorably to the best reported CVQKD final key generation rate of 2 kb/s for 25 km. The system is rate limited by the data acquisition card and not by reconciliation speed. With faster signaling a final key rate of 60 kb/s would be possible at the same post-selection threshold. Tomographic measurements of received quantum states and GAWBS noise have been made and will be presented at the conference. Work on a system that does not require a frequency translation scheme and that would be completely immune to GAWBS noise is ongoing.

We acknowledge funding from the Agence Nationale de la Recherche in the framework of the project HQNET.

References

1. F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, “Quantum key distribution using gaussian-modulated coherent states” Nature **421**, pp. 238-241 (2003).

2. A. Leverrier and P. Grangier, “Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation” Phys. Rev. Lett. **102**, 180504 (2009).

3. Y. Zhao, M. Heid, J. Rigas, and N. L¨utkenhaus, “Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks” Phys. Rev. A **79**, 012307 (2009).

4. Z. Zhang and P. L. Voss, “Security of a discretely signaled continuous variable quantum key distribution protocol for high rate systems” Opt. Exp. **17**, pp. 12090-12108 (2009).

5. J. Lodewyck, M. Bloch, R. Garcia-Patron, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N.J. Cerf, R. Tualle-Brouri, S.W. McLaughlin, P. Grangier, “Quantum key distribution over 25 km with an all-fiber continuous variable system” Phys. Rev. A **76**, 042305 (2007).

6. S. Fossier, E. Diamanti, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, “Field test of a continuous-variable quantum key distribution prototype” New. J. Phys. **11**, 045023 (2009).

7. B. Qi, L.L. Huang, L. Qian, and H.K. Lo, “Experimental study on the Gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers” Phys. Rev. A **76**, 052323 (2007).

8. A.M. Lance, T. Symul, V. Sharma, C.Weedbrook, T.C. Ralph,P.K. Lam, “No-switching quantum key distribution using broadband modulated coherent light” Phys. Rev. Lett. **95**, 180503 (2005).

9. T. Symul, D.J. Alton, S.M. Assad, A.M. Lance, C. Weedbrook, T.C. Ralph, P.K. Lam, “Experimental demonstration of post-selection-based continuous-variable quantum key distribution in the presence of Gaussian noise” Phys. Rev. A **76**, 030303(R) (2007).

10. A.J. Poustie, “Guided acoustic-wave Brillouin scattering with optical pulses” Opt. Lett. 17, No. 8 (1992).