Coherent State Quantum Key Distribution with Continuous-Wave Laser Beams

T. Symul[1,2], V. Sharma[2], T. C. Ralph[3] and P. K. Lam[1]

[1] *Department of Quantum Science, Research School of Physics and Engineering,*
The Australian National University, Canberra, ACT 0200, AUSTRALIA.
[2] *QuintessenceLabs, Suite 23 Building 38, Science Road,*
Canberra, ACT 0200, AUSTRALIA.
[3] *Centre for Quantum Computer Technology, Department of Physics,*
The University of Queensland, St. Lucia, QLD 4072, AUSTRALIA

Abstract: Continuous variable quantum key distribution relies on the transmission of weakly modulated coherent states and the detection of optical field for secure communication. In this talk, we give an overview of recent developments in continuous variable quantum key distribution. In particular, we discuss a scheme that uses continuous-wave laser beams without optical pulsing. Due to its continuous wave nature, our scheme is intrinsically broadband and does not require measurement basis switching. Finally, we present a status report on integration of this system into existing communication infrastructures at the Parliamentary Triangle of Australia in Canberra.

OCIS codes: (270.0270) Quantum optics; (060.4785) Optical security and encryption; (060.5565) Quantum communications

1. Continuous Variable Quantum Key Distribution

Introduced by Bennett and Brassard in 1984 [1], quantum key distribution (QKD) is a system that exploits the quantum nature of photons to enable distribution of one-time-pad keys for secure communication. The laws of physics guarantee that an ideal QKD system will offer absolute security against eavesdropping. Integration of QKD into existing layers of a communication network is therefore of significant interest to a wide range of end users. Originally thought to be a protocol requiring true single photon sources to operate, research in the past decade has relaxed this presumed necessity: Weakly attenuated light sources that may occasionally contain two or more photons per measurement window for discrete variable systems [2,3], as well as weakly modulated coherent states of light [4,5] for continuous variable (CV) systems, are now able to be deployed in QKD protocols. In CV systems, the quadrature amplitudes, X and Y, of a light field is typically used by Alice, the sender, to simultaneously encode a pair of random numbers for the transmission of one-time-pad keys. The quadrature amplitude information is subsequently measured by Bob, the receiver, with photodiode-based homodyne or heterodyne field detection systems. Finally, the CV discrepancies between sender's transmission and receiver's measurements are reconciled over a classical channel. Because of the apparent information advantage an eavesdropper could have with CV field measurements, the first CV QKD scheme proposed 10 years ago was originally thought to have a 50% loss limit beyond which secure communication could not work [4]. In 2002, two methods of overcoming this "3 dB limit" were simultaneously proposed by Grosshans and Grangier [6,7], and by Silberhorn et al. [8]. With this 3 dB limit overcome, CV system holds the promise to be a viable alternative that may better integrate QKD into existing communication infrastructures. In spite of its nascent status relative to discrete variable systems, there have been a number of recent significant theoretical [9-11] and experimental developments [12-15] towards realizing CV QKD.

2. CVQKD Key Protocols

To date, there have been a number of proof-of-principle experiments for CV QKD [7,12-15,16]. The key theoretical advances underpinning the success of these experiments are mainly reliant on adoptions of the following protocols:

Reverse reconciliation (RR): In RR, the reconciliation of the transmitted random numbers is done in reverse order. Instead of Bob guessing the data sent by Alice, Alice is asked to predict Bob's measured results and asked to reconcile her encoded data to Bob's. Through this method, Alice, who encoded the data into the light field in the first instance always has an information advantage over a potential eavesdropper, Eve, even when the transmission losses are significantly higher than 3 dB [6].

Post-selection (PS): In PS, Alice and Bob cryptically communicate the sent and measured results (Say, by only revealing the absolute value of the data, while make the sign of the data a "0" or "1" bit.) to establish the losses experienced by individual transmission events. Because transmission losses are stochastic, Alice and Bob can post-select events that are favorable for their final key generation and discard all other events that potentially favors an eavesdropper. Thus, this protocol allows Alice and Bob to overcoming Eve's information advantage even when the average transmission loss is higher than 3 dB [8].

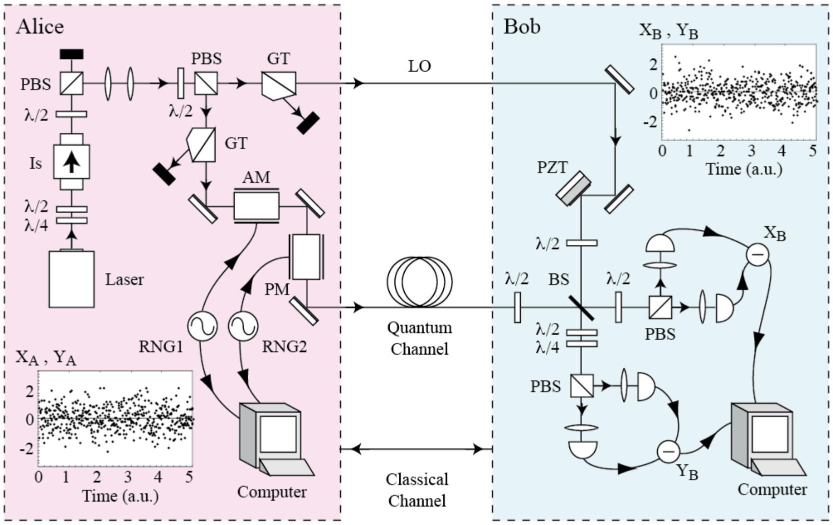

Figure 1. Experimental schematic of no-switch coherent state QKD.

No-switch (NS): Most QKD protocols rely on Bob having to randomly switch his measurement basis (e.g. H-V to D-A for polarization encoding) to foil any eavesdropping. In CV system, this requires random and rapid variation of Bob's quadrature amplitude measurements. An alternative to random basis switching is the no-switch protocol [9]. For Gaussian quantum states, it can be shown that a beam-splitter is a nearly ideal quantum-cloning device [10,17]. Bob can therefore split the received laser beam into two and perform simultaneous measurements on both of the quadrature amplitudes (as shown in Fig. 1). Paradoxically, this "no-switch" protocol not only offers equivalent security to random basis switching, but also offers higher bit rates [10, 18].

Two-way communication (TW): In a typical QKD protocol, Alice and Bob have very asymmetric roles, with Alice encoding the states, and Bob measuring them. Bob could choose not to measure the quantum states but instead encode additional information onto the received states. These states are then re-send back to Alice who would then perform the measurements. It has been shown recently that this two-way QKD protocol can be made more robust against excess noise on the transmission line [12].

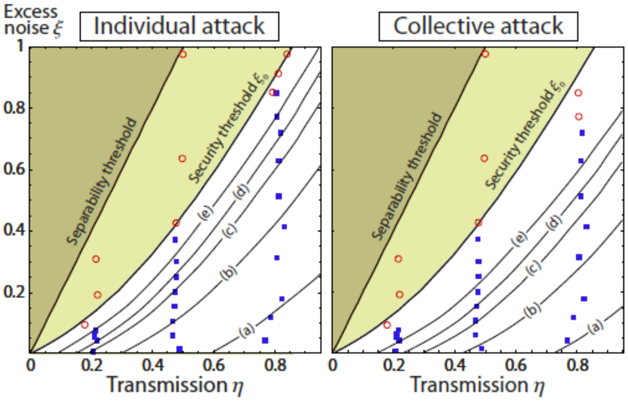

Figure 2. Proof-of-principle demonstration of CV QKD in the presence of environmental Gaussian noise.

3. ANU-UQ Experimental Scheme

In 2005, we implemented a broadband dual-homodyne no-switch post-selection CV QKD using tabletop optics. To maximize the secret key rate bandwidth, Alice employed electro-optic modulators to encode weak broadband modulations onto the radio-frequency sidebands of a continuous-wave laser to encode her random key (see Figure 1). The continuous-wave technique allows a linear increase in the final key rate of the coherent states if more of the radio-frequency spectrum is encoded and measured. To maximize his detection bandwidth, Bob simultaneously measured both the amplitude and phase quadratures using the no-switch protocol with broadband photodetectors. Under certain conditions, the no-switch protocol is simpler to implement than the basis switching protocol, for which the phase of the local oscillator needs to be randomly changed at the full bandwidth of the key generation. Moreover, the locked joint quadrature measurements may offer an improvement in key rate and a slight strengthening of the communication security. For example, the no-switch protocol is not susceptible to the Trojan-horse attack [19]. We demonstrated the successful generation of final keys in the presence of 10 dB of loss on the quantum channel at a minimum rate of 1 kbits/s for every 17MHz of sideband encoding.

In 2007 we extend this no-switch post-selection QKD protocol by considering the presence of excess Gaussian noise on the quantum channel. In contrast to our first experiment where we considered only vacuum field coupling on the quantum channel through passive losses [20], our second experiment simulated excess environmental noise that could potentially be coupled onto the quantum states during transmission. Both individual attacks, where Eve tries to measure each states as they are sent, and collective attacks, where Eve possesses a quantum computer and tries to gather information through attacking the entire set of quantum states by making the best use of the classical information exchanged between Alice and Bob, were considered in our proof of security. We showed that our scheme could remain secure as long as the excess noise on the quantum channel did not exceed a given threshold that is depending on the line transmission coefficient (see Figure 2).

Towards telecom integration: Figure 3 shows our plan to integrate the no-switch post-selection CV QKD system into existing communication infrastructure in the Parliamentary Triangle of Australia in Canberra. With the aim of realizing a turnkey system, Figure 3 shows a **QLE1** system that is currently under development. The system incorporates CV QKD into the layers of standard communication platform. **QLE1** aims to deliver ease of operation to end users that wish to communicate via one-time pad encryption over the Internet.

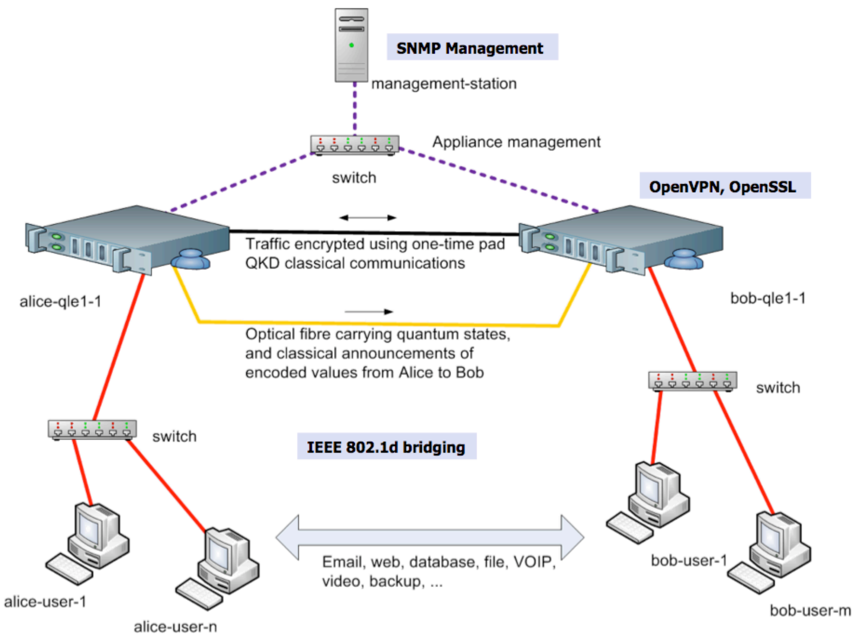
SNMP Management
management-station
Appliance management
switch
OpenVPN, OpenSSL
alice-qle1-1
Traffic encrypted using one-time pad
QKD classical communications
bob-qle1-1
Optical fibre carrying quantum states,
and classical announcements of
encoded values from Alice to Bob
switch
switch
IEEE 802.1d bridging
Email, web, database, file, VOIP,
video, backup, ...
alice-user-1
alice-user-n
bob-user-1
bob-user-m

Figure 3. Integration of CV QKD into existing telecommunication infra-structure.

4. References

[1] C. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing” Proc. of IEEE Intl. Conf. on Comp. Sys. and Sig. Proc. 175 (1984).

[2] H. Lo, X. Ma and K. Chen, “Decoy state quantum key distribution” Phys. Rev. Lett. **94**, 230504 (2005).

[3] V. Scarani et al., “The security of practical quantum key distribution” Rev. Mod. Phys. **81**, 1301 (2009).

[4] T. C. Ralph, “Continuous variable quantum cryptography” Phys. Rev. A **61**, 010303 (1999).

[5] T. C. Ralph and P. K. Lam, “A bright future for quantum communications” Nature Photonics **3**, 671 (2009).

[6] F. Grosshans and P. Grangier, “Continuous variable quantum cryptography using coherent states” Phys. Rev. Lett. 88, 057902 (2002).

[7] F. Grosshans et al., “Quantum key distribution using Gaussian-modulated coherent states” Nature **421**, 238 (2003).

[8] Ch. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, “Continuous variable quantum cryptography: Beating the 3 dB loss limit” Phys. Rev. Lett. **89**, 167901 (2002).

[9] C. Weedbrook et al., “Quantum cryptography without switching” Phys. Rev. Lett. **93**, 170504 (2004).

[10] C. Weedbrook et al., “Coherent-state quantum key distribution without random basis switching” Phys. Rev. A **73**, 022316 (2006).

[11] S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, “Continuous-variable quantum cryptography using two-way quantum communication” Nature Phys. **4**, 726 (2008).

[12] S. Lorenz, N. Korolkova, and G. Leuchs, “Continuous-variable quantum key distribution using polarization encoding and post-selection” Appl. Phys. B 79, 273 (2004).

[13] A. M. Lance et al.,”No-switching quantum key distribution using broadband modulated coherent light” Phys. Rev. Lett. **95**, 180503 (2005).

[14] J. Lodewyck et al.,”Quantum key distribution over 25 km with an all-fiber continuous variable system” Phys. Rev. A **76**, 042305 (2007).

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

[17] C. Weedbrook, N. B. Grosse, T. Symul, P. K. Lam and T. C. Ralph, “Quantum cloning of continuous-variable entangled states” Phys. Rev. A **77**, 052313 (2008).

[18] J. Lodewyck and P. Grangier, “Tight bound on the coherent-state quantum key distribution with heterodyne detection” Phys. Rev. A **76**, 022322 (2007).

[19] N. Gisin et al., “Trojan-hof”

[20] T. Symul, D.J. Alton, S.M. Assad, A.M. Lance, C. Weedbrook, T.C. Ralph and 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 (2007).