Continuous-variable quantum key distribution with a “locally” generated local oscillator

Bing Qi, Pavel Lougovski, Raphael Pooser, Warren Grice, Miljko Bobrek, Charles Ci Wen Lim, and Philip G. Evans

Quantum information science group
Oak Ridge National Laboratory

Qcrypt 2016, Sept 12 – 16, 2016
Outline

- Continuous-variable (CV) QKD based on coherent detection
- Why *local* local oscillator (LO)?
- Our solution: theory & experiment
- Conclusion & outlook
Detection techniques in QKD

- **Single photon detector (SPD)**
  - Widely applied in various QKD protocols;
  - Performance improved over the years;
  - Presently, high cost.

- **Optical homodyne detection**
  - Build upon highly efficient photo-diodes working at room temperature—**cost effective**;
  - Immune to broadband background light—QKD through lit fiber\(^1,2\) or free space\(^3\);
  - Require a reliable phase reference.

References:

Gaussian-modulated coherent state (GMCS) QKD Protocol

1. Quantum state transmission

2. Classical Information Exchange

Single-homodyne—measure $X$ or $P$
Double-homodyne—measure $X$ and $P$

Uncertainty Principle

Gain information on $X$ ($P$) $\rightarrow$ introduce noise on $P$ ($X$)

A gap between theory and practice

**Theory**

- A crucial assumption—trusted LO
- Security could be compromised if Eve can manipulate the LO


**Practice**

- The LO propagates through the insecure channel—security issue
- LO $> 10^8$ photons/pulse vs. signal $\sim 1$ photon/pulse—complicated system design
CV-QKD with *locally* generated LO

- **Challenge**
  - How to establish phase reference between independent lasers?

- **Solution**
  - Quadrature-remapping scheme
  - Pilot-aided phase recovery
Quadrature-remapping scheme

Scheme

- Measure in *random* basis
- Determine phase difference $\phi$ & rotate data in post-processing
- **Slow** phase drift: $\phi$ can be determined from quantum signals


Fast phase change?

$$X_B = X_A \cos \phi + P_A \sin \phi$$
$$P_B = -X_A \sin \phi + P_A \cos \phi$$
Pilot-aided phase recovery scheme

Scheme

\[ \Phi_{S,i} = \frac{\Phi_{R,i} + \Phi_{R,i+1}}{2} \]

Noise analysis

- Phase noise

\[ \sigma = \frac{\langle (\Delta \theta_S(T_d))^2 \rangle + \langle (\Delta \theta_L(T_d))^2 \rangle}{2} + \frac{2N_0}{\eta n_{ref}} \]

\[ \langle (\Delta \theta(T_d))^2 \rangle = \frac{2T_d}{\tau_c} \]

\( \tau_c \) — laser coherence time

- Excess noise

\[ \varepsilon_\theta = V_A \sigma \]

Determine laser phase noise

**Setup**

- BS
- PC
- Delay $T_d$
- 90° Optical hybrid
- BD
- OSC
- 90° shift

- Sig
- LO

L—Clarity-NLL-1542-HP (Wavelength Reference)
BD—350MHz balanced photodetector (Thorlabs)

Phase noise @ $T_d=20$ns is $0.040\pm0.001$

- High rate QKD @ $T_d=100$ps phase noise could be 0.0002
  - Khan, et al., “Continuous-Variable Quantum Communication at 10 GHz and Compatible with Telecom Networks” Poster sessions (Thursday)

- Improved scheme
Proof-of-principle experiment

- AM
- PM
- AWG
- Ch1
- Ch2
- 25km SMF
- 90° Optical hybrid
- BD
- OSC
- Sync to OSC
- R_i
- S_i
- R_i+1
- 20ns
- L
- Vacuum state
- Coherent state with a random phase
Experimental results

- **Classical BPSK**
  - Measured phase noise: $0.040 \pm 0.001$

- **Reference photon number**

- **Quantum input**
  - Detector noise: $0.83$ in shot-noise unit
Simulation results

- Asymptotic key rate against collective attack

  "Realistic" model: Eve cannot control noise/loss in Bob. $\alpha=0.2\text{dB/km}$; $\nu_{el}=0.1$; $\eta=0.5$; $\sigma=0.04$; $f=0.95$; $V_A=1$

- Data size for composable security

  Fiber length=10km, $\nu_{el}=0$; other parameters are the same

Conclusion & outlook

- **Conclusion:** we proposed CV-QKD with local LO
  - Remove potential security loopholes
  - Simplify CV-QKD implementation

- **Outlook:** cost-effective QKD
  - The gap between classical and quantum coherent communication systems is becoming smaller
  - It is conceivable to conduct both classical communication and QKD using the **same** infrastructure

Related works

Papers


Poster sessions

- T. Iskhakov, et al., "Single Quadrature Continuous Variable Quantum Key Distribution with a Local Local Oscillator", Tuesday
- B. Schrenk, et al., "Pilot-Assisted Local Oscillator Synchronisation for CV-QKD", Thursday