Novel CV QKD Protocol: Guess How You Got It

Ilhwan Park*, Junsang Oh*, Yongseen Kim, and June-Koo Kevin Rhee

School of Electrical Engineering, KAIST, Daejeon, S. Korea

rhee.jk@kaist.edu

Abstract Continuous variable quantum key distribution (CV QKD) utilizes homodyne detection (HOM) which requires phase-synchronized local oscillator (LO). Phase synchronization of LO at the optical frequency is extremely difficult and often achieved by LO pulse transmission from Alice, which is vulnerable to a side attack known as LO phase attack. This paper propose a new CV QKD protocol that requires no synchronization of LO phase by use of multi-dimensional reconciliation (MDR) property.

Introduction

In CV QKD, Bob obtains continuous variable measurement achieved by HOM with a qualified LO. In a typical CV QKD system, the LO is transmitted from Alice along with CV quantum states which are modulated optical pulses. Bob attains HOM by the LO from Alice with the quantum state of optical signal. In this protocol, there exists LO pulse side channel attack that can significantly reduce the secrecy of CV QKD sessions [1-4]. In our proposal, *we challenge if Alice can find the phase of LO at Bob even though it is asynchronous to the phase reference of Alice*.

Method

Multi-dimensional reconciliation in the reverse direction is known as an extremely powerful scheme that can extend the secure distance beyond the 3 dB loss allowance with GG02 CV QKD protocol [5]. In reverse MDR with an example of 8 dimensions, Bob creates raw key data, $\mathbf{u} = [u_0, \ldots u_7]^{\mathrm{T}}$, $u_k = \pm 1$, that is embedded as superposition of multi-dimension rotation matrices M with the CV quantum state measurement $\mathbf{y}$ by HOM with LO phase of θ_{B}:

$$\mathrm{M}\tilde{\mathbf{y}} = \mathbf{u},$$

where $\tilde{\mathbf{y}}$ is a normalized vector of $\mathbf{y}$, and $\mathrm{M} = \sum_{k=0}^{7} \alpha_k \mathrm{R}_k$. The basis rotations $\mathrm{R}_k \in$ {I⊗I⊗I, X⊗iY⊗Z, iY⊗I⊗I, Z⊗iY⊗I, X⊗I⊗iY, Z⊗X⊗iY, X⊗iY⊗X, Z⊗Z⊗iY} are commonly shared between Alice and Bob. Here, X, Y, and Z are Pauli's spin matrices. Bob can find real valued α_i's and share them with Alice on a public channel. In turn, Alice can obtain $\mathbf{u}' = \mathrm{M}\tilde{\mathbf{x}}$ where $\tilde{\mathbf{x}}$ is the normalized vector of $\mathbf{x}$ that can be determined by HOM measurements of Alice's quantum states of 8 qubits with respect to Bob's HOM LO phase. $\mathbf{y} = \mathbf{x} + \mathbf{n}$. Here, $\mathbf{n}$ is a noise introduced by shot noise of the quantum state that Bob has received. Then $\mathbf{u}' \approx \mathbf{u}$ in the low noise limit.

---

* Equal contributions

Now the question becomes what if Bob cannot provide θ_B *to Alice*. This happens when Bob uses a local LO – asynchronous LO running with a random phase.

In the MDR, fortunately, Alice can estimate θ_B, by searching the best $\mathbf{x} = \langle\theta^*|\psi^{(8)}\rangle$ that can separate two pdfs $p(u' > 0)$ and $p(u' < 0)$ the most. Figure 1 proves such behavior of estimating θ^* by simulation with 2^9 qubits generated from Gaussian modulation with variance V_A and create Bob's measurement data set with Gaussian noise. The figure shows probability of error being $\mathbf{u}' \neq \mathbf{u}$ as a function of Alice's phase θ to determine $\mathbf{x}$. In actual protocol, the phase estimation θ^* can obtained to minimize mean square error referenced to ± 1.

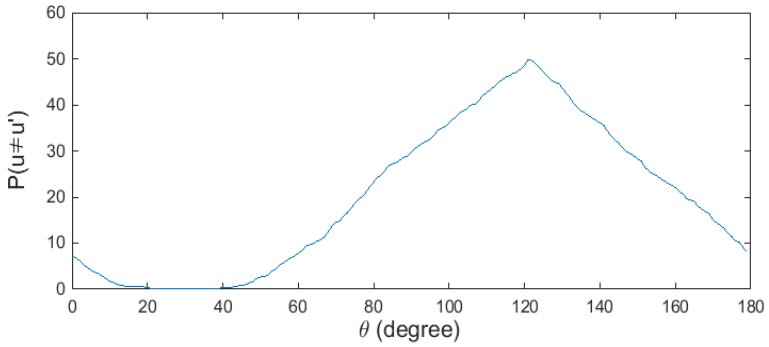

Figure 1: Reconciliation error versus Alice's phase guess for Bob's HOM LO phase.

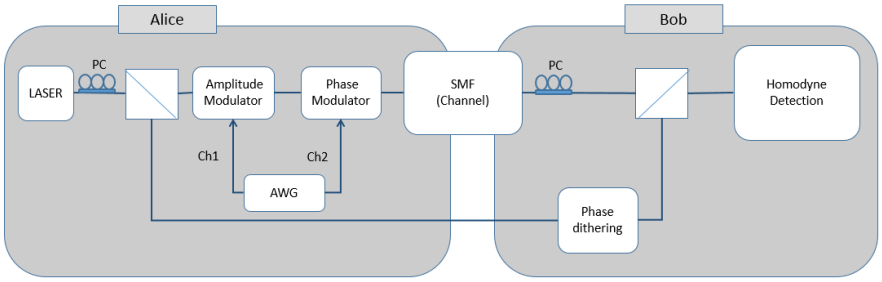

Figure 2: Experiment block diagram of the CV QKD system

Experimental Result

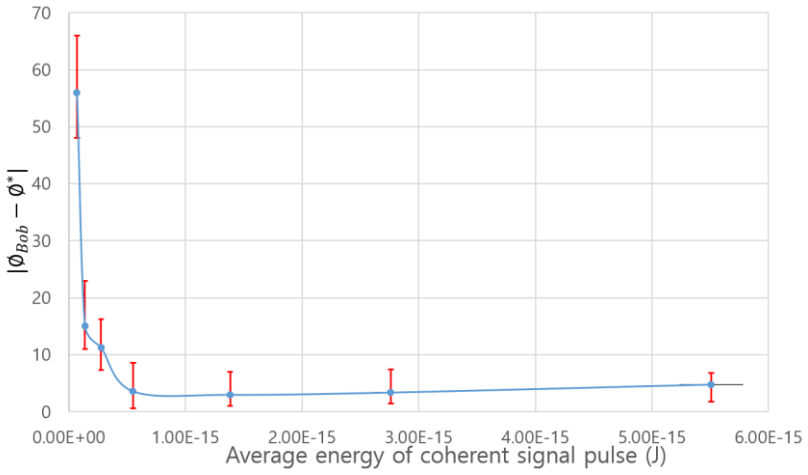

Figure 3: Phase difference vs. average energy of coherent signal pulse

The overall experiment set up is similar to conventional QKD system shown in Figure 2. Alice transmits Gaussian modulated signal with uniform random phase modulation at a repetition rate of 50 MHz. Also, The same laser with random phase dithering is shared with Bob to be used as LO for HOM. In this set up, when Bob received the highest signal power and LO power, the mean photon numbers are 4.3×10^4 photons/pulse (-35.6 dBm), 2.2×10^7 photons/pulse for signal and LO, respectively. We also varied the signal power from -35.6 to -51.6 dBm to see the effect of SNR changes. In Figure 3, the difference of θ^* and θ_B is $3^\circ \sim 5^\circ$ in the range of over -45.6 dBm signal power, which shows that our proposed system is valid to find the phase of LO at Bob.

Discussion

This paper reports an important achievement for realization of CV QKD where Bob can conduct homodyne detection using arbitrary measurement basis without any phase synchronization between Alice and Bob; If MDR is used, Alice can estimate the HOM LO phase of Bob later. This scheme can not only simplify the realization of the system but also reduce a possible side channel attack on the LO transmission. With this scheme Bob can use a low-cost CW laser with no phase locking to Alice. We anticipate a truly feasible application of CV QKD with the proposed scheme.

Acknowledgment

This work was supported by the ICT R&D program of MSIP/IITP. [1711028311, Reliable crypto-system standards and core technology development for secure quantum key distribution network].

This research was supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2017-2015-0-00385) supervised by the IITP(Institute for Information & communications Technology Promotion

References

[1]X. Ma, S. Sun, M. Jiang and L. Liang, "Wavelength attack on practical continuous-variable quantum-key-distribution system with a heterodyne protocol", 2017. .

[2]J. Huang, C. Weedbrook, Z. Yin, S. Wang, H. Li, W. Chen, G. Guo and Z. Han, "Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack", 2017. .

[3]P. Jouguet, S. Kunz-Jacques and E. Diamanti, "Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution", 2017. .

[4]J. Huang, S. Kunz-Jacques, P. Jouguet, C. Weedbrook, Z. Yin, S. Wang, W. Chen, G. Guo and Z. Han, "Quantum hacking on quantum key distribution using homodyne detection", 2017. .

[5]A. Leverrier, R. Alléaume, J. Boutros, G. Zémor and P. Grangier, "Multidimensional reconciliation for a continuous-variable quantum key distribution", 2017. .