Reference pulse attack on continuous-variable quantum key distribution with Local local oscillator

S. Ren[1], R. Kumar[2], A. Wonfor[1], X.Tang[1], R. V. Penty[1], and I. H. White[1]
[1]*Centre for Photonic Systems, University of Cambridge, 9 JJ Thomson Avenue, Cambridge, CB3 0FA, United Kingdom*
[2]*Quantum Communication Hub, University of York, UK*
Author e-mail address: sr734@cam.ac.uk

Continuous Variable Quantum Key Distribution (CV-QKD) has attracted increasing interest in recent years as a secure form of transmission which is able to use conventional telecommunications equipment. In the past, a number of security obstacles have been identified, such as those associated with transmitted local oscillator (LO) [1]. This has led to the requirement for a second independent laser located at Bob to generate a secure fully-trusted local LO (LLO). This approach however results in unavoidable phase noise between the two lasers. To achieve security there, efficient phase reference sharing and noise estimation under the GMCS protocol has already been achieved [2-4]. The excessive phase noise stems from two contributions: lasers phase drift noise and phase estimation error noise, which are determined by the laser linewidth and reference pulse magnitude respectively [5]. Due to the relatively small magnitude of the reference pulse, its quantum uncertainty should be taken into consideration, so that the phase difference estimation error inevitably exists for the quadrature case. This feature provides vulnerability for an eavesdropper to utilize.

Here, we, for the first time, reveal a security loophole in the current state-of-art phase reference sharing scheme for CV-QKD with LLO. The loophole is achieved by manipulating the magnitude of the reference pulses to mislead detection by monitoring the phase difference estimation error. Even though the reference pulses do not contain any useful key information and their quadrature values are publically available, Eve can manipulate the reference pulses to hide her attacks since its magnitude is related to the overall excess noise estimation result. As a result, we propose a new theoretical quantum attack, which we call the 'reference pulse attack', for the LLO CV-QKD system using the reference sharing scheme. We apply channel separation to replace the original quantum channel using two branches: (i) one standard fibre channel to transmit quantum signals, and (ii) a second channel with lower attenuation coefficient for delivering reference pulses. Our attack has two stages: 1. The attacker selectively switches the quantum and reference pulses and carries out an increasing number of attacks on the quantum signals; 2. The attacker compensates the additive excess noise due to attacks by decreasing the phase estimation error noise through reduced reference pulse propagation attenuation. Using this approach, the overall excess noise estimated by Alice and Bob does not change even though Eve actually can extract useful information. By analytic analysis, it is shown that the 62% of phase estimation error noise can be sufficiently tuned by eavesdropper to mislead Alice and Bob to underestimate Eve's maximum information rate and hence allow Eve to access a partial and even a full secure key without revealing her presence. To validate the attack, a linear model of transmitted states under attack is analytically developed and the simulated results for excess noise margin and mutual information levels have been determined. The insecure key ratio gradually increases with transmission distance and with decreasing reference path attenuation. A 100% insecure key region is achieved when one approaches the null key distance. Our attack breaks the immunity of LLO CV-QKD to a great extent, but can be patched with a countermeasure that we will propose at the conference.

Reference:

1. X.C. Ma *et al*., *Phys.Rev.A* 89, 032310. (2014)

2. Q. Bing et al., *Phys.Rev.X* 5, 041009 (2015)

3. S. Daniel et al., *Phys.Rev.X* 5, 041010(2015)

4. H. Duan et al., *Opt. Letters* 40, 3695-3968 (2015)

5. A, Maire and R, Alleaume, *Phys.Rev.A* 95, 0.12316 (2017)