Quantum Hacking on Continuous-Variable Quantum Key Distribution System by using a Wavelength Attack

Jing-Zheng Huang*, Christian Weedbrook**, Zhen-Qiang Yin*, Mo Li*, and Zheng-Fu Han*

** Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei, 230026, China*

***Center for Quantum Information and Quantum Control, Department of Physics, University of Toronto, Toronto, M5S 3G4, Canada*

QCRYPT2013 August 5–9, 2013, Waterloo, Canada

Abstract :

The security proofs of continuous-variable quantum key distribution are based on the assumptions that the eavesdropper can neither act on the local oscillator nor control Bob's beam splitter. These assumptions may be invalid in practice due to potential imperfections in the implementations of such protocols. In the paper[1], we consider the problem of transmitting the local oscillator in a public channel and propose a wavelength attack which can allow the eavesdropper to control the intensity transmission of Bob's beam splitter by switching the wavelength of the input light[2]. Specifically we target continuous-variable quantum key distribution systems that use the heterodyne detection protocol using either direct or reverse reconciliation. Our attack is proved to be feasible and renders all of the final key shared between the legitimate parties insecure, even if they have monitored the intensity of the local oscillator. To prevent our attack on commercial systems, a simple wavelength filter should be randomly added before performing the monitoring detection.

Methods:

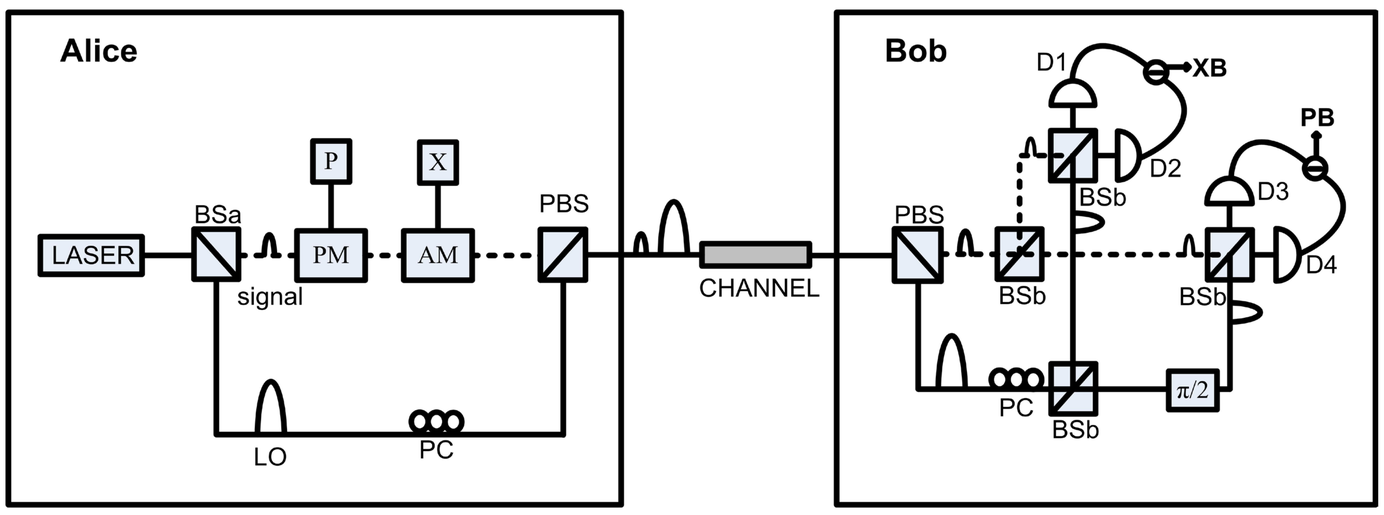

Fig.1 **Central idea of CV-QKD with heterodyne detection**: Using the interference between a **weak** coherent state and a **strong** LO light to measure the quadrature X and P , which have encoded the classical information about the secret key.

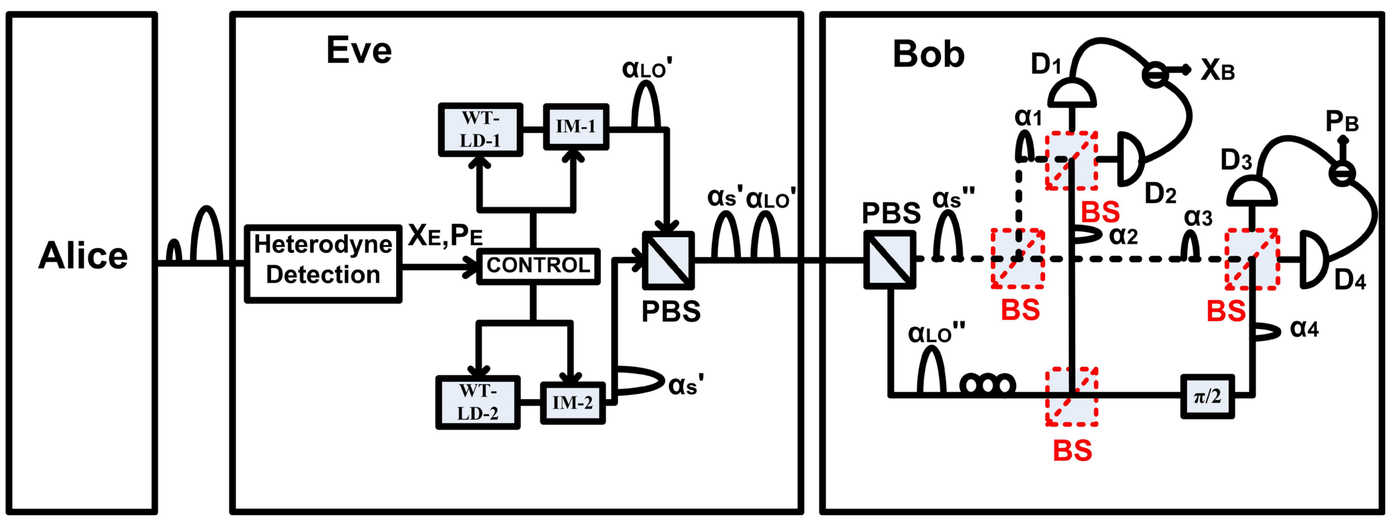

Fig.2 **Central idea of wavelength attack**: the transmittance of fiber beam splitter is **wavelength-dependent**[2], so that we can produce two fake states with **strong power** in **different wavelengths** to control Bob's beam splitter, therefore fake the records read by the four detectors, in order to force the measurement results as the same as the eavesdropper. The schematic diagram of the wavelength attack scheme. WT-LD: the wavelength tunable laser diode; IM: the intensity modulator; BS: 50/50 beam splitter.

Results:

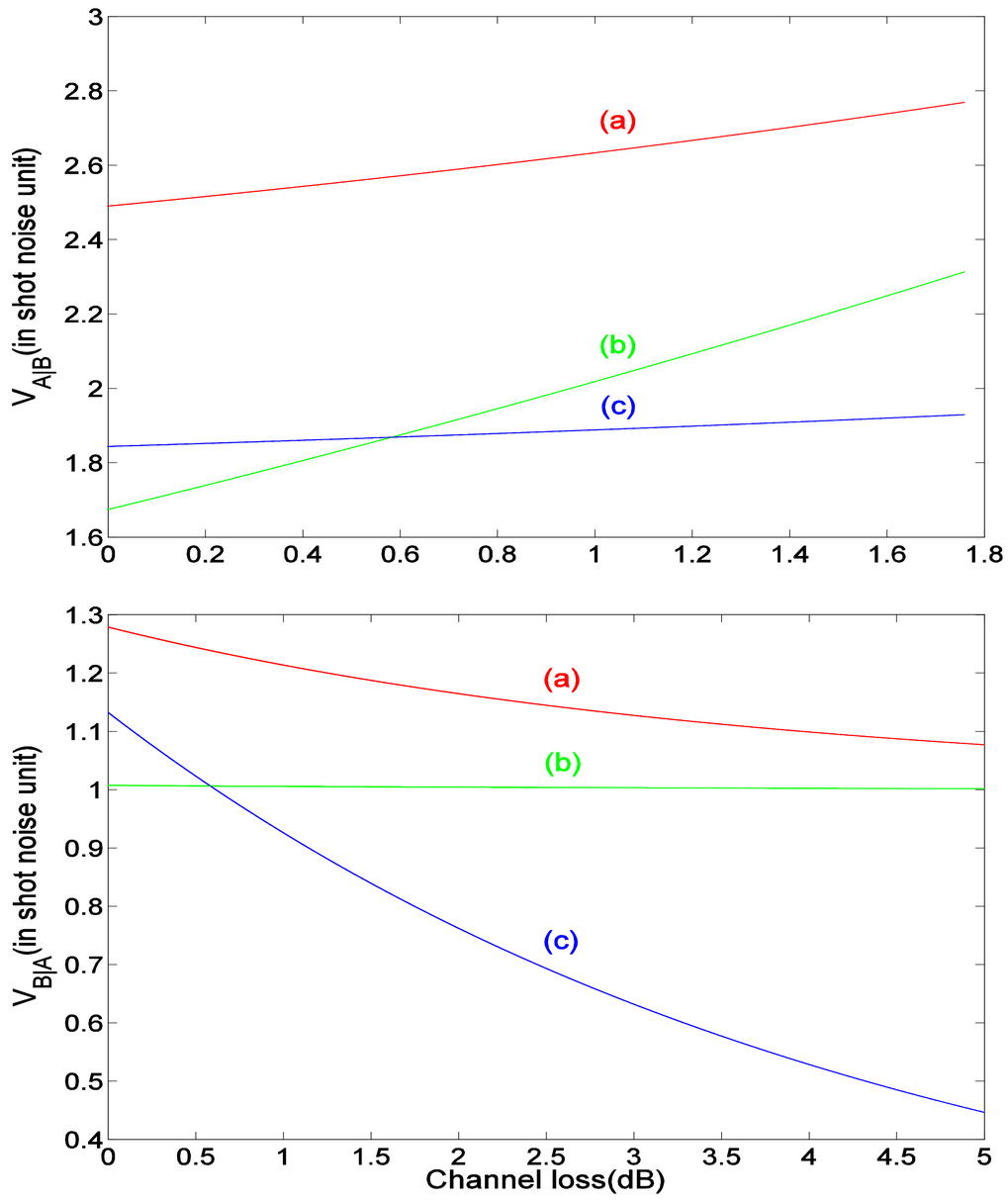

Fig.3 There are two post-processing methods to recover the classical information, namely the **direct reconciliation(DR)** and **reverse reconciliation(RR).** The two communication parties, Alice and Bob, compute the deviation between their preparations and measurement results, i.e. V(A|B) (in DR) and V(B|A) (in RR), to check whether there exits eavesdropper in the channel. Both in upper(DR) and lower(RR), **the deviations under attack (c) are always lower than the alarm threshold (a).** The normal values **(b)** are also presented.

Conclusion:

In conclusion, we have proposed a new type of realistic quantum hacking attack, namely the wavelength attack, on continuous-variable QKD systems using heterodyne detection. If Alice and Bob don't take the necessary precautions for such an attack, the final secret key is in principle, totally insecure as Eve can obtain all the information about the final key. This is different from the equal-amplitude attack proposed in Ref.[3] as in the wavelength attack, Eve has the ability to control Bob's beam splitter and therefore the suggestion of testing the total intensity in Ref.[3] would not prevent such an attack from occurring. To close such a loophole in practical CV-QKD systems, it is simply enough for Bob to randomly add a wavelength filter before his detection and monitor the differences.

Reference

[1] J. Huang, Y.Yin, S. Wang, et al., Phy. Rev. A. 87, 062329(2013).
[2] H. Li, S. Wang, J, Huang, et al., Phys.Rev.A, 84. 062308(2011).
[3] H. Haseler, T. Moroder and N.Lutkenhaus, Phy. Rev. A.77, 032303 (2008).