Modulation leakage vulnerability in continuous-variable quantum key distribution

Vladyslav C. Usenko[1]
Nitin Jain[2], Ivan Derkach[1], Hou-Man Chin[2,3], Radim Filip[1], Ulrik L. Andersen[2], Tobias Gehring[2]

[1]*Department of Optics, Faculty of Science, Palacky University, 17. listopadu 50, 772 07 Olomouc, Czech Republic*
[2]*Center for Macroscopic Quantum States (bigQ), Department of Physics, Technical University of Denmark, 2800 Lyngby, Denmark*
[3]*Department of Photonics, Technical University of Denmark, 2800 Lyngby, Denmark*

usenko@optics.upol.cz

We address the issue of modulation leakage from the in-phase and quadrature (IQ) modulators, which are used in implementation of continuous-variable (CV) quantum key distribution (QKD). Following the previously obtained theoretical results, demonstrating the general negative effect of side-channel modulation leakage in CV QKD [1], we establish an equivalence between the unsuppressed sideband modulation and the modulation side-channel leakage. Using the set-up, incorporating a laser source, an IQ modulator, optical filters, and a homodyne detector, fed by a locally generated local oscillator (Fig. 1) and phase-referenced using pilot tones, we characterize the modulation leakage in terms of the main signal modulation. Assuming two different measurement strategies, used by an eavesdropper, namely availability of only a suppressed pilot tone or an unsuppressed desired pilot tone, we study the effect of modulation leakage on security of CV QKD. We analyse security of the scheme using a passive Trojan-horse attack model [2] in the purification-based security analysis method and incorporate additional sources of trusted noise in the sending and receiving stations. Our results show the reduction of secure key rate (Fig. 2) and, equivalently, secure regions of CV QKD in terms of tolerable channel losses and noise, when the sideband suppression is weak [3]. The effect is present in both direct and reverse reconciliation scenarios and is more pronounced for the former. On the other hand, the negative effect of modulation leakage can be removed when the sidebands are properly suppressed. We also show the positive effect of additional trusted noise in the leaking mode, particularly for the direct reconciliation. Our results reveal the importance of proper modulation sidebands suppression in practical realizations of CV QKD.

References

[1] I. Derkach, V. C. Usenko, and R. Filip, Phys. Rev. A 96 (2017) 062309
[2] J. Pereira, and S. Pirandola, Phys. Rev. A 98 (2018) 062319
[3] N. Jain, I. Derkach, H.-M. Chin, R. Filip, U. L. Andersen, V. C. Usenko, and T. Gehring, Quantum Science and Technology 6 (2021) 045001

Figures

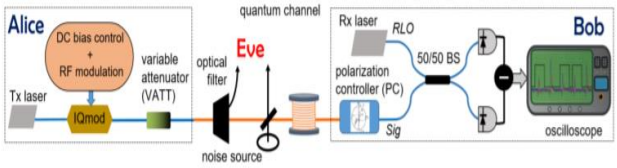

Figure 1: Experimental set-up used for studying the modulation leakage vulnerability in CV QKD.

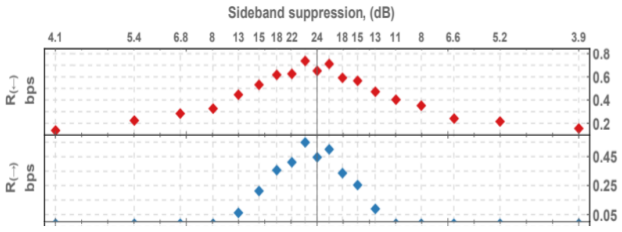

Figure 2: Effect of finite sideband suppression on secure key rate of CV QKD in reverse (top) and direct (bottom) reconciliation scenarios.