Abstract ID : **1046**

Insecurity of detector-device-independent quantum key distribution

Content

Quantum key distribution (QKD) [1] is a technique that allows distribution of a secret random bit string between two separated parties (Alice and Bob). In theory, QKD provides information-theoretic security based on the laws of quantum physics. In practice, however, it does not, as standard QKD realizations cannot typically fulfill the demands imposed by the theory. As a result, any unaccounted device imperfection might constitute a side-channel which could be used by an eavesdropper (Eve) to extract the secret key without being detected. To bridge this gap, various approaches have been proposed, with measurement-device-independent QKD (mdiQKD) [2] probably being the most promising one in terms of feasibility and performance. Compared to standard prepare-and-measure QKD schemes [1], its security is based on post-selected entanglement. This allows to remove all detector side-channels from QKD implementations. Also, its practicality has been already confirmed both in laboratories and via field trials [3, 4]. However, one drawback of mdiQKD is that it requires high-visibility two-photon interference between independent sources, which makes its implementation more demanding than that of standard prepare-and-measure QKD schemes. Another limitation is its security proofs require larger post-processing data block sizes than those of standard QKD.

To overcome these limitations, a novel approach, so-called detector-device-independent QKD (ddiQKD), has been introduced recently [5–8]. It avoids the problem of interfering photons from independent light sources by using the concept of a single-photon Bell state measurement (BSM) [9]. As a result, it achieves the robust security of MDI-QKD, and at the same time provides the ease of implementation like standard prepare-and-measure QKD schemes. Also, its post-processing data block sizes are expected to be similar to those of standard prepare-and-measure QKD schemes [10]. To summarize, DDI-QKD was assumed to become the 'holy grail' of quantum key distribution protocols.

In this talk, I will show that, although it is widely assumed that DDI-QKD is robust to detector side-channels, it is in practice not true. Our main contributions are twofold. First, we show that, in contrast to mdiQKD, the security of ddiQKD cannot be based on post-selected entanglement alone, as initially thought in [5–8]. Hence, its security is not as robust as MDI-QKD. Second, we show that DDI-QKD is actually insecure against detector side-channel attacks by presenting various eavesdropping strategies that can fully compromise the security of the system.

The manuscript can be found at: https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.117.250505

[1] C. H. Bennett and G. Brassard, in Proc. IEEE International Conference on Computers, Systems, and Signal Processing (Bangalore, India) (IEEE Press, New York, 1984) pp. 175– 179.

[2] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. 108, 130503 (2012).

[3] Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, M.- Q. Huang, W.-J. Zhang, S.-J. Chen, L. Zhang, L.-X. You, Z. Wang, Y. Liu, C.-Y. Lu, X. Jiang, X. Ma, Q. Zhang, T.- Y. Chen, and J.-W. Pan, Phys. Rev. X 6, 011024 (2016).

[4] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.- H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, Phys. Rev. Lett. (in press), arXiv:1606.06821 [quant-ph].

[5] P. Gonz´alez, L. Rebo´n, T. Ferreira da Silva, M. Figueroa, C. Saavedra, M. Curty, G. Lima, G. B. Xavier, and W. A. T. Nogueira, Phys. Rev. A 92, 022337 (2015).

[6] C. C. W. Lim, B. Korzh, A. Martin, F. Bussi‘eres, R. Thew, and H. Zbinden, Appl. Phys. Lett. 105, 221112 (2014).

[7] W.-F. Cao, Y.-Z. Zhen, Y.-L. Zheng, Z.-B. Chen, N.-L. Liu, K. Chen, and J.-W. Pan, manuscript withdrawn by au- thors on 23 Aug 2016 owing to the insecurity of the proposed scheme, arXiv:1410.2928v1 [quant-ph].

[8] W.-Y. Liang, M. Li, Z.-Q. Yin, W. Chen, S. Wang, X.-B. An, G.-C. Guo, and Z.-F. Han, Phys. Rev. A 92, 012319 (2015).

[9] Y.-H. Kim, Phys. Rev. A 67, 040301 (2003).

[10] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, Phys. Rev. A 89, 022307 (2014).

Summary

Topic:

Topic: Quantum Physics, Quantum Optics and Quantum Information

Primary author(s) : SAJEED, shihan (University of waterloo); HUANG, anqi (university of waterloo); Dr. SUN, Shihai (national university of defense technology, china); XU, feihu (MIT); Dr. MAKAROV, Vadim (university of waterloo); Dr. CURTY, marcos (University of Vigo)

Presenter(s) : SAJEED, shihan (University of waterloo)

Track Classi ication : C Quantum Physics, Quantum Optics and Quantum Information

Contribution Type : Poster