Long-distance two-way continuous variable quantum key distribution over optical fiber with Gaussian modulation

L. Gyongyosi*[a,b], S. Imre[a]
[a] Quantum Technologies Laboratory, Department of Telecommunications, Budapest University of Technology and Economics, 2 Magyar tudosok krt, H-1111, Budapest, Hungary;
[b] MTA-BME Information Systems Research Group, Hungarian Academy of Sciences, H-1518, Budapest, Hungary
gyongyosi@hit.bme.hu

ABSTRACT

To exploit the real potential of two-way CVQKD (continuous-variable quantum key distribution) systems a robust reconciliation technique is needed. It is currently unavailable, which makes it impossible to reach the real performance of a two-way CVQKD system. The reconciliation process of correlated Gaussian variables is a complex problem that requires either tomography in the physical layer that is intractable in a practical scenario, or high-cost calculations in the multidimensional spherical space with strict dimensional limitations. To avoid these issues, we propose an efficient logical layer-based reconciliation method for two-way CVQKD to extract binary information from correlated Gaussian variables. We demonstrate that by operating on the raw-data level, the noise of the quantum channel can be corrected in the scalar space and the reconciliation can be extended to arbitrary high dimensions. We prove that the error probability of scalar reconciliation is zero in any practical CVQKD scenario, and provides unconditional security. The results allow to significantly improve the currently available key rates and transmission distances of two-way CVQKD. The proposed scalar reconciliation can also be applied in one-way systems as well, to replace the existing reconciliation schemes.