Strong Reference Quantum Key Distribution: Security Consideration and Experimental Realization

V Rodimin[1,2], A Tayduganov[2], D Kronberg[1], Y Durkin[2], A Zharinov[2], and Y Kurochkin[1,3]

[1] *Quantum communication group, Russian Quantum Center, Moscow, Russia*
[2] *National University of Science and Technology (NUST) 'MISIS', Moscow, Russia*
[3] *National University of Science and Technology 'MISIS', Moscow, Russia*
Contact Email: y.kurochkin@gmail.com

Here we have presented the theoretical consideration of strong reference QKD security based on the properties of realistic photon detectors. For the given setup parameters, the optimal photons number values in SP were from 0.15 for 50 km to 0.35 for 10 km at 65 dB between reference and signal pulses. Secure key generation is possible only with a bright reference pulse starting from 4x10^4 photons at 10 km, and more than 5×10^5 photons are needed to maximize the secure key generation rate at 50 km. Our study shows that SR QKD has advantages for short distances. At 20 km, the B92 with SR protocol has more than four times higher generation speed compared to the decoy-state BB84 protocol, while at 60 km, their rates become equal, Fig. 1.

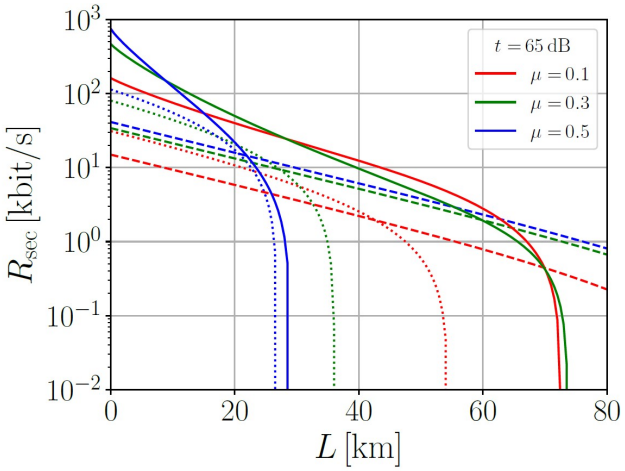

Figure 1: Distance dependence of secure key generation rate. Solid, dotted and dashed lines represent B92 with SRP, standard BB84 and decoy-state BB84 protocols, respectively

Our approach relies on particular Eve's attack using the soft filtering operation, which is very effective but might be not the ultimate attack on SR QKD. We use the characteristics of realistic equipment available in our laboratory to parametrize the formula for the secret key generation rate. In that sense, the obtained results may be regarded as a somewhat pessimistic estimate since, for theoretical calculations, one can use the best attainable characteristics of the equipment.

We have developed the go&return optical scheme, which allows forming laser pulse trains for SR QKD. This scheme was tested by running the sifted key generation, demonstrating the technical feasibility of a 65 dB difference between signal and reference. Mostly, the scheme setup is identical to the well-researched and commercially available plug&play scheme. The frequency of the polarization correction is related to the thermal stability of the segment responsible for the polarization distortion, mainly the storage line. In our experience, the characteristic drift time of polarization, even in field conditions, might be minutes per tens of kilometers.

Acknowledgements: This work is supported by the Russian Science Foundation under project 17-71-20146.