Towards an Open-source Software Platform for Numerical Key Rate Calculation of General Quantum Key Distribution Protocols

Jie Lin, Ian George, Kai-Hong Li, Kun Fang, Twesh Upadhyaya, Natansh Mathur, Max Chemtov, Shlok A. Nahar, Shahabeddin M. Aghmare, Thomas Van Himbeeck, Yanbao Zhang, Christopher Boehm, Patrick Coles, Adam Winick, Wenyuan Wang, and Norbert Lütkenhaus

1 Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1
2 University of Waterloo, Waterloo, Ontario, Canada N2L 3G1
3 NTT Basic Research Laboratories and NTT Research Center for Theoretical Quantum Physics, NTT Corporation, 3-1 Morinosato-Wakamiya, Atsugi, Kanagawa, Japan 243-0198
4 University of Freiburg, Freiburg im Breisgau, Germany 79108
5 Theoretical Division, Los Alamos National Laboratory, Los Alamos, NM 87545, US
6 email: wenyuan.wang@uwaterloo.ca; email: lutkenhaus.office@uwaterloo.ca

A numerical approach for the calculation of QKD key rates allows a uniform framework to be applied to general QKD protocols. Based on our group’s previous work, we would like to build a universal software platform that is fully modularized and user-friendly, where one can easily swap in and out different QKD protocol descriptions, channel simulation models or experimental data, backend numerical solvers, and parameter optimization algorithms. Our goal is to build an open-source platform that can be both useful for theorists testing new protocols as well as experimentalists looking for optimal parameters or analyzing their experimental data.

Applications and Ongoing Works

1. Protocol description - applying to various protocols & side-channels
   - DM-CVQKD (Jie, Twesh, Max) [3]
   - Detector efficiency mismatch (Yanbao, Jie) [4]
   - Unbalanced BB84 encoding (Nicky) [5]
   - Modeling of optical channel (Shahab)

2. Backend Solver
   - Finite-size model (Ian) [6]
   - Speedup from structure of protocols e.g. using flag-states (Yanbao, Nicky) [4,5]
   - High efficiency custom solver (Kun, Cunlu)

3. Main iteration
   - Local/global search (Wenyuan, Natansh)
   - Architecture & Unifying of interfaces (Wenyuan)

References