Photon-Level Simulation of Quantum Key Distribution with Picosecond Accuracy

Xiaoliang Wu[1,2], Joaquin Chung[1], Alexander Kolar[1,3], Eugene Wang[1],
Tian Zhong[4], Rajkumar Kettimuthu[1], Martin Suchara[1]

[1]Argonne National Laboratory, Lemont, IL, USA, [2]Illinois Institute of Technology, Chicago, IL, USA,
[3]Northwestern University, Evanston, IL, USA, [4]University of Chicago, Chicago, IL, USA

Recent experimental advances make quantum communication networks a reality. Experimentalists around the world are building quantum network testbeds with ever increasing complexity. These efforts include a 30-mile optical fiber link connecting Argonne and Fermilab to test long distance communication, and FQNET, an onsite teleportation and entanglement experiment at Fermilab. Our work complements these experimental efforts by building a Simulator of QUantum Network Communication (SeQUeNCe) that models quantum hardware, network protocols, and simulates transmission of individual photon pulses and control messages with picosecond accuracy. SeQUeNCe is capable of comparing alternative experiment design choices in highly complex systems with many possible designs of quantum repeaters, network topologies, quantum memories, and transduction systems.

Here we report on our use of SeQUeNCe to simulate quantum key distribution with the BB84 protocol [1], key reconciliation with Cascade [2], and detection of photon splitting attacks with a decoy-state protocol [3]. Fig. 1 depicts quantum and classical communication of the BB84 and Cascade protocols implemented in the simulator.

Our hardware model used an attenuated photon source with 80 MHz frequency and mean photon number 0.1. The detector had 80% efficiency, dark count rate 10 /sec, time resolution 10 ps, and maximum count rate 50,000,000 /sec. The quantum channel parameters were polarization fidelity of 97% and attenuation of 0.2 dB/km. The classical communication channel used by control messages had a round-trip-time of 2 ms in addition to propagation delay to accommodate message processing, TCP/IP packet formation, and buffering. The ratio among the signal pulses, decoy pulses, and vacuum pulses used by the decoy protocol were 8:1:1.

Fig. 2 shows the achieved key bit throughput (left axis) and the latency contributions of the BB84 and Cascade protocols (right axis) as a function of the optical fiber length. As expected, the key throughput (blue color) decreases exponentially with distance. Latency contribution of the BB84 protocol (red color) when transmitting a key was increasing with the fiber length due to decreasing throughput. The latency of Cascade (green color) was relatively constant at 1.8 sec to 2.4 sec. With 1.4% bit error rate, Cascade needed to correct approximately 140 error bits in each 10,240-bit frame, leading to 1,100 ~ 1,500 communication rounds.

In the past, quantum network simulations were used to study individual protocols in isolation or focused on applications [4]. Recently developed simulators, such as SeQUeNCe and NetSquid [5], allow comprehensive modeling of quantum hardware, quantum network protocols, and their interaction. We plan to use SeQUeNCe in the future to understand the effects of physical processes such as fiber dilation, perform hardware and software parameter tuning, as well as aid with experiment planning and design.

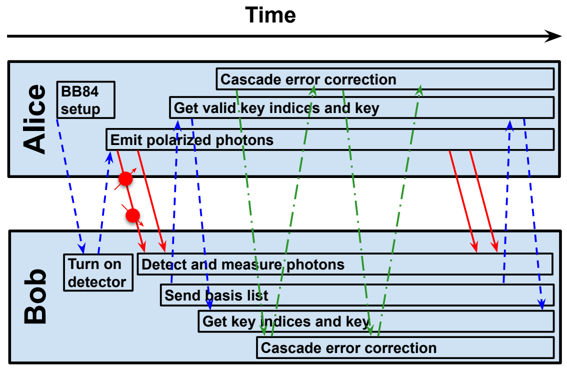

Fig. 1 Simulated photon pulses (red color), classical messages transmitted by BB84 (blue color), and Cascade (green color).

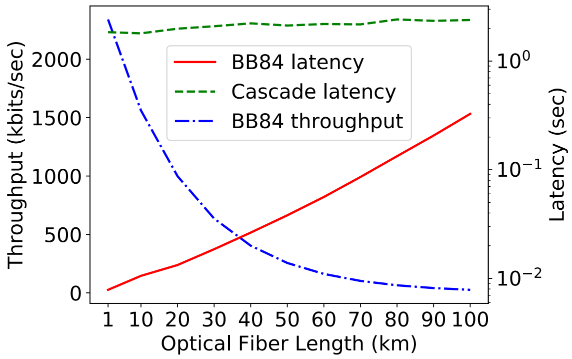

Fig. 2 Simulated key throughput and contributions of BB84 and Cascade protocols to latency.

References

[1] C. Bennett and G. Brassard, Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing, p.175, 1984

[2] G. Brassard and L. Salvail, Advances in Cryptology - EUROCRYPT '93, p.410, 1993

[3] W. Hwang, Physical Review Letters, 91, p. 057901, 2003

[4] A. Dahlberg and S. Wehner, Quantum Science and Technology, 4, p. 015001, 2014

[5] NetSquid: Network Simulator for Quantum Information Using Discrete Events, https://netsquid.org/

This material is based upon work supported by Laboratory Directed Research and Development (LDRD) funding from Argonne National Laboratory, provided by the Director, Office of Science, of the U.S. Department of Energy under contract DE-AC02-06CH11357.