Fast implementation of privacy amplification in quantum key distribution

Chun-Mei Zhang[1,2], Chao Wang[1,2], Mo Li[1,2], Hong-Wei Li[1,2], Zhen-Qiang Yin[1,2], Wei Chen[1,2], Zhen-Fu Han[1,2]

[1]*Key Laboratory of Quantum Information, CAS, University of Science and Technology of China, Hefei, Anhui 230026, China*

[2]*Synergetic Innovation Center of Quantum Information & Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China*

Privacy amplification is one of the most important post-processing steps in quantum key dsitribution (QKD), which is used for distilling unconditional secret keys. What's more, with the development of high-speed QKD systems, privacy amplification is becoming a bottleneck due to the fact that the input length should be larger than at least several hundred kilobits to reduce the finite size effect. To fulfill the high-speed requirement and to reduce the finite size effect, we propose a universal method to speed up the privacy amplification process at large input lengths on different QKD systems. By choosing a simple multiplicative universal class of hash functions and constructing an optimal multiplication algorithm based on four basic multiplication algorithms, we give a fast software implementation of privacy amplification. In principle, there is no upper bound on the input length of privacy amplification, and the time overhead of privacy amplification is not affected by the shrink factor (the ratio of the length of the final secret keys to the length of the reconciled keys). When the lengths of the input blocks are 1 Mbit and 10 Mbit, the speed of privacy amplification can be as fast as 14.86 Mbps and 10.88 Mbps, respectively. Thus, it is practical for GHz or even higher repetition frequency QKD systems.

Keywords: privacy amplification, quantum key distribution, multiplication algorithms.