Title: Numerical Framework for Finite-size Security of Quantum Cryptography

Abstract: Quantum cryptography is one of the most widely applied research fields in quantum information science. It includes two main branches, quantum key distribution and quantum random number generation. The central task in the studies of quantum cryptography is to prove the security regardless of the eavesdropper's computational power. In literature, the security analysis has been done both analytically and numerically. Compared to analytical methods which tend to require techniques specific to quantum cryptography protocols, numerical ones are more general since they can be directly applied to general protocols with little adaptation. However, current numerical methods are carried out based on some assumptions such as working in the asymptotic limit and collective attacks from eavesdroppers. In this talk, I will introduce how to remove these assumptions and develop a numerical finite-size security analysis framework against general attacks. This talk is based on the following two papers: arXiv 2111.08315 and arXiv 2207.02611.

Bio: Prof. Hongyi Zhou received his Bachelor in theoretical physics from Peking University in 2014. He received his Ph.D. degree from Tsinghua University in 2019. From 2019 to 2021, he worked as a postdoctoral researcher at the University of Tokyo. He is now an assistant professor in Institute of Computing Technology, Chinese Academy of Sciences. His current research is focused on quantum cryptography, quantum optics and quantum algorithms.