Jointly organized by the Department of Physics and HK Quantum Institute of Science & Technology

CTCP SEMINAR

Authentication of Classical Channels in Quantum Key Distribution

Prof. Liujun WANG

Yunnan University

Monday, June 16, 2025, 3:00pm

Room 522, 5/F, Chong Yuet Ming Physics Building,

The University of Hong Kong

Abstract:

Quantum Key Distribution (QKD) offers information-theoretic security but relies critically on authenticated classical channels for post-processing steps (e.g., basis sifting and key reconciliation). Without authentication, these channels are vulnerable to man-in-the-middle attacks. Traditional methods require Alice and Bob to pre-share symmetric keys via physical meetings—a solution incompatible with multi-user QKD networks. We experimentally demonstrate a practical solution using post-quantum signature algorithms to authenticate QKD classical channels. This approach was validated under multiple QKD network topologies in laboratory environments and a real-world metropolitan QKD network operating continuously for 36 days. Our implementation provides quantum-resistant security while uniquely requiring only short-term security (e.g., ~1 second during authentication), contrasting with long-term security assumptions for post-quantum encryption. Additionally, we propose a quantum-teleportation-based protocol for message authentication that simultaneously ensures confidentiality—enabling secure key reconciliation in QKD.

Biography:

Dr. Liujun Wang is an Associate Professor in the Department of Physics at Yunnan University. He obtained his Ph.D. in Physics (Quantum Information Physics) from the University of Science and Technology of China (USTC) in 2016, where he also briefly worked as an Assistant Researcher. After gaining experience as an Engineer at the China Academy of Space Technology (CAST), he joined Yunnan University. His current research primarily revolves around quantum key distribution (QKD), encompassing experimental implementations, including the integration and co-propagation of quantum and classical signals in optical fibers, and the integration of QKD with post-quantum cryptography for securing communication networks.

ANYONE INTERESTED IS WELCOME TO ATTEND!

HK Institute of Quantum Science & Technology,
Room525, Chong Yuet Ming Physics Building, The University of Hong Kong
Phone: 3917 1108

HK Institute of Quantum Science & Technology 香港量子研究院

Department of Physics
THE UNIVERSITY OF HONG KONG