

Quantum Sword and Shields in Information Security

singhua University and Beijing Academy of Quantum Information Sciences

Gui-Lu Long

Email: gllong@tsinghua.edu.cn

Quantum computing holds the potential to undermine certain cryptographic algorithms. However, the requisite hardware is not expected to be accessible for at least another decade. In 2022, Chinese scholars proposed a hybrid quantum-classical algorithm for integer factorization (HAIFA), which aims to challenge the operational RSA algorithm with near-term quantum hardware. HAIFA has had a substantial impact and has expedited the process of post-quantum cryptography migration. Over the past three years, remarkable progress has been achieved, resolving some of the ambiguities surrounding HAIFA. A recent study by an Italy-German joint group indicates that both the qubit resource requirement and time complexity of HAIFA are polynomial, underscoring the urgency of post-quantum cryptography migration or the implementation of quantum key distribution. Moreover, there are indications that HAIFA also offers a notable speedup in lattice-based post-quantum cryptography algorithms. There are two strategies for countering quantum attacks. One is post-quantum cryptography methods, which are designed to withstand quantum computing attacks. The other is quantum communication, which employs quantum states as the transmission medium and encompasses quantum direct communication and quantum key distribution. This report will present the latest related advancements.

Short Bio:



Gui-Lu Long received his PhD degree in Physics from Tsinghua University. He is a professor of Tsinghua University, and vice-president of Beijing Academy of quantum Information Sciences, China.