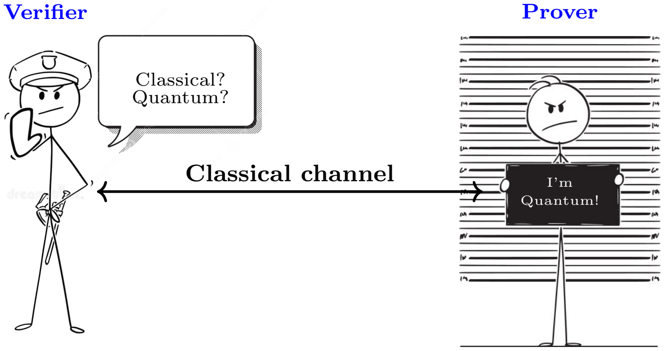
Quantum cryptography over classical channels



Supervisor : Weiqiang Wen
Minimum number of students per group : 4
Maximum number of students per group : 4
How many groups for this project ? 1
Tags : cryptography, quantum, lattices

1 Context

Quantum computing offers new perspectives for cryptographic design. For example, quantum key distribution (QKD) can achieve unconditional security, a feat unattainable in classical cryptography. Recently, Chung et al [3] proposed a novel framework for quantum cryptography based on classical channels. Quantum cryptography relying on classical channels significantly reduces implementation complexity by eliminating the need for quantum transmission.

In this setting, we can realize functionalities that are unachievable by either purely classical cryptography or information-theoretic secure quantum protocols. The proofs of quantumness and key leasing over classical channels are two examples. This project will focus on the implementation of such protocols. If time and progress permit, we will also explore potential improvements to these protocols.

2 Expectations

- Implementation of proof of quantumness by Brakerski et al [1] in Qiskit.
- Implementation of key leasing by Chardouvelis et al [2] in Qiskit.
- Implementation of the improved versions of the above schemes in [4] and if time permits, try to extend functionality (e.g., broadcast encryption with key leasing).

References

[1] Zvika Brakerski, Paul F. Christiano, Urmila Mahadev, Umesh V. Vazirani, and Thomas Vidick. A cryptographic test of quantumness and certifiable randomness from a single quantum device. In Mikkel Thorup, editor, *FOCS 2018*, 2018.

[2] Orestis Chardouvelis, Vipul Goyal, Aayush Jain, and Jiahui Liu. Quantum key leasing for PKE and FHE with a classical lessor. *IACR Cryptol. ePrint Arch.*, page 1640, 2023.

[3] Kai-Min Chung, Yao-Ting Lin, and Mohammad Mahmoody. Black-box separations for non-interactive classical commitments in a quantum world. In Carmit Hazay and Martijn Stam, editors, *EUROCRYPT 2023*, 2023.

[4] Duong Hieu Phan, Weiqiang Wen, Xingyu Yan, and Jinwei Zheng. Adaptive hardcore bit and quantum key leasing over classical channel from LWE with polynomial modulus. In Kai-Min Chung and Yu Sasaki, editors, *ASIACRYPT 2024*, 2024.