Semi-Quantum Money

Roy Radian, Or Sattath

Ben Gurion University, Israel

Results

Quantum money with classical communication and a classical bank

Assumptions

Hardness of Learning with Errors for BQP

Security

An adversary holding n banknotes cannot pass $k > n$ verifications

1-of-2 Puzzle

A protocol between a challenger and an adversary. The challenger sends a puzzle to the adversary, who creates some appropriate quantum state along with an obligation string for it. For any obligation two challenges are available; once the adversary answers one correctly, they cannot find the right answer to the other.

Claw-free Trapdoor Functions

A family of functions with 2 pre-images per image (claw)

Pre-images are hard to compute without trapdoor

CONSTRUCTS

TCF to 1-of-2 puzzle

- Create a uniform superposition over $|x, f(x)\rangle$ for some TCF f
- Second register is measured to get $\frac{1}{\sqrt{2}}(|x_0, y\rangle + |x_1, y\rangle)$ for a random y
- Preimage challenge: find x_0 or x_1
- Equation challenge: find d s.t.:

$$d \cdot (x_0 \oplus x_1) = 0$$

Private Money Scheme

$keygen$: generate n puzzles

$mint$: user receives puzzles and prepares quantum states

$verify$: bank sends challenges to user. User must answer all challenges correctly (forcing measurement of minted money)

Completely Classical Transaction

Additional Results

- Parallel repetition theorem for TCF
- Public semi-quantum money from non-standard assumptions

Open Questions

- A general way to remove quantum communication from quantum protocols?
- Can we do better than computational security?

Full paper at: https://arxiv.org/abs/1908.08889