Secure Outsourcing of Computation

Ron Rothblum
MIT
Motivation: allow a computationally weak client to outsource its computation to an untrusted server.

Main security concerns:
1. **Correctness:** $y = f(x)$?
2. **Privacy:** cloud learns our secret data $x$. 
Doubly Efficient Interactive Proofs

[GKR08]

Double efficiency requirement:
1. The verifier should be super efficient.
2. The prover should be relatively efficient.

Also want to minimize the interaction.
Some Results

• Linear-time constant-round verification for $TISP(poly(n), n^\epsilon)$ with statistical soundness (together with Omer Reingold and Guy Rothblum).

• Linear-time 1-round verification for $P$ with computational soundness, under cryptographic assumptions (together with Ran Raz and Yael Kalai).

• Study of sub-linear time verification (joint works with Oded Goldreich, Tom Gur and Yael Kalai).