Efficient Protocols for Privacy and Integrity in the Cloud

Anca Nitulescu

ENS Paris
Cloud computing:
● provides computer processing resources
● access from anywhere
● shared pool of applications and services

Risks:
System or human vulnerability can be exploited against privacy and integrity.
Delegate Computation to Cloud

User

Cloud Provider

data
Delegate Computation to Cloud

User → Task → Cloud Provider

Data
Integrity of Delegated Computation

Solution

trust the server / ask for a proof
Proof of Computation

Input $x$

Computation $f(x)$

Solution $y = f(x)$
Proof of Computation

Input $x$

Computation $f(\cdot)$

Solution $y$

Proof

$$(y, w) \in R^\pi$$
Fast Sound

Down the Rabbit Hole
Nir Bitansky
Ran Canetti

Lewis Carroll

Alessandro Chiesa
Shafi Goldwasser
Huijia Lin
**SNARK: Succinct Non-Interactive Argument of Knowledge**

- **Proof of Knowledge**: all the steps have been performed
- **Non-Interactivity**: no exchange between prover and verifier
- **Efficiency**: verification easier than computing $f$
- **Succinctness**: proof size independent of NP witness size
Proving Security of Protocols

**Assumption**: Known hard problem

**Method**: Polynomial time reduction

**Security reduction**

Hard Problem $\mathcal{P} \rightarrow$ Protocol security claim
Assume: Efficient PPT Adversary $\mathcal{A}$ against Protocol security

Successful Adversary $\rightarrow$ Solution for $\mathcal{P}$
No Black-Box-Reduction proof of security for any SNARK construction under any Standard Assumption.

- Assuming the falsifiable assumption isn't false.
- Assuming sub-exponentially hard OWFs exist.
Directions of my research

- Standard
- Weaken SNARKs
- Protocols
- Proofs
- SNAR?
Thank You