Cybersecurity Transition to Practice Workshop

April 17, 2018 | New York, NY

Quad Chart for: *Practical Zero-Knowledge Proofs*

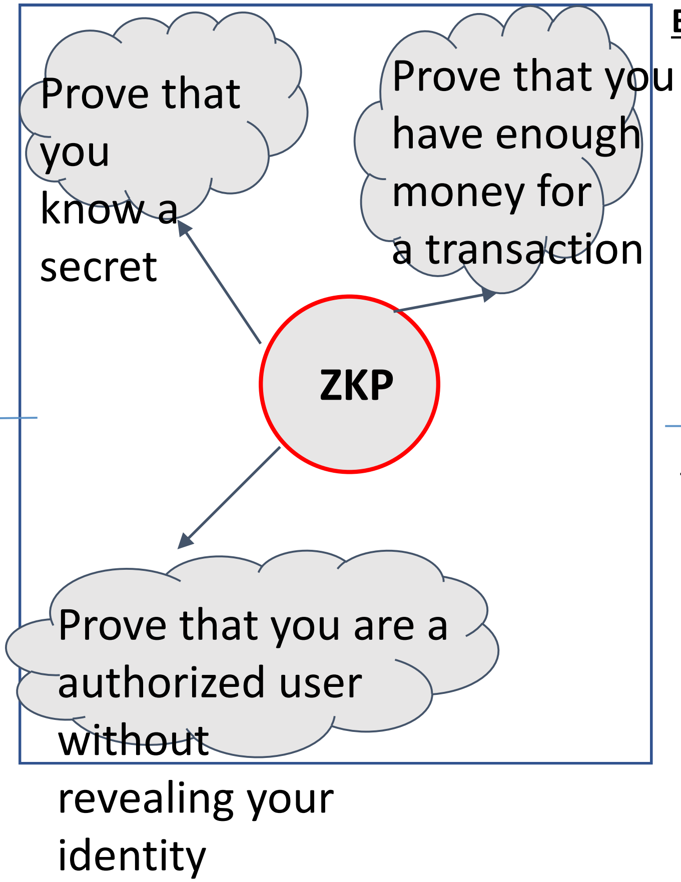
Rosario Gennaro -- The City College of New York

Challenge:

- ZKPs that can enforce correct behaviour by any party in a distributed network protocol.
- Theoretically possible for any computation
- Challenge is to scale them for real-life computation

Solutions:

- **ZK-SNARKS:** Zero-Knolwedge Succinct Non-Interactive Proofs
- Short, non-interactive proofs which are easy to verify
- Limit is the overhead in producing such proofs
- State of the art is a new approach based on a new abstract model of computation.


Prove that you know a secret
Prove that you have enough money for a transaction
ZKP
Prove that you are a authorized user without revealing your identity

Broader Impact: ***<pick one>***

- New teachniques have enabled the use of ZKPs for real-life applications
  - Anonymity in cryptocurrencies
  - Private Smart Contracts
  - Distributed Cryptocurrency wallets.

Metadata tag:

- *Already transitioning to practice*
- *Need collaborators (developers)*
- *Need funding*
- *Great Student Engagement*