CSci 8271
Security and Privacy in Computing
Day 13: Bulletproofs

Stephen McCamant

University of Minnesota

Interactive proofs

- Used in complexity theory and cryptography
- A more capable prover P proves a fact to a weaker verifier V
  - Prover may have more computational power, and/or knowledge of a secret
- Power comes from interaction and randomized challenges

Interactive proof variants

- "Argument": proposed instead of "proof" when the soundness is computational
- Proof of knowledge: proves shows knowledge of a particular witness

Commitments

- Two phases: commit, later open
  - Similar to one use of envelopes
- Binding property: can only commit to a single value
- Hiding property: value not revealed until opened
- Either binding or hiding, but not both, can be perfect

Pedersen commitments

- Based on a discrete log group with generators g and h
- Commit to x with randomness r with $g^x h^r$
- Perfectly hiding because h^r is a random group element
- Computationally binding relates to discrete log

Zero knowledge

- A ZK interactive proof reveals no information besides the fact proven
- Classic example: prove that a graph is 3-colorable
  - Prover shuffles the coloring, and commits to this
  - Verifier picks an edge
  - Prover opens commitments to show the colors are different
  - Repeat λ (20, 80, 128) times
- Formalized by showing that anyone could make a fake transcript

Interactive $\longrightarrow$ non-interactive

- The Fiat-Shamir heuristic: turn interactive proof into non-interactive proof by replacing the verifier with a hash function
- Essentially a "random oracle" assumption, which is theoretically questionable
- But still seems relatively safe in practice

Practicality for crypto proofs

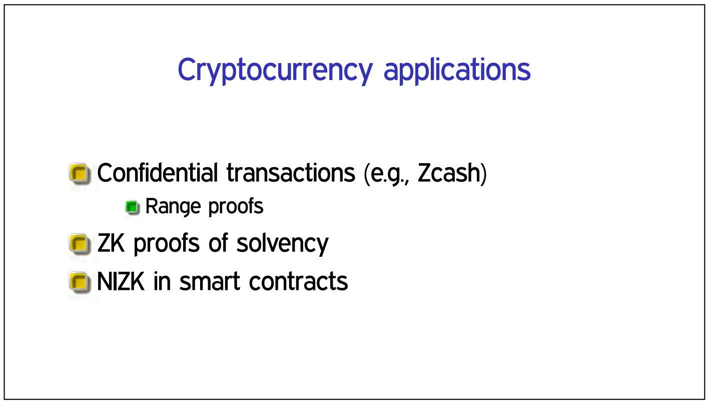
✓ Succinct proof

✓ No trusted setup

✓ Expressive

✓ Efficient proving

- Efficient verification
- Post-quantum security



Cryptocurrency applications

- Confidential transactions (e.g., Zcash)
  - Range proofs
- ZK proofs of solvency
- NIZK in smart contracts