The Evolution of Proofs in Computer Science:

Zero-Knowledge Proofs
Zero-Knowledge Proofs

[Goldwasser-Micali-Rackoff85]

Proofs that reveal no information beyond the validity of the statement
Zero-Knowledge Proofs

[Goldwasser-Micali-Rackoff85]

Impossible!

This is information!
Interactive Proofs
[Goldwasser-Micali-Rackoff85]

Completeness:  \( \forall x \in L \ \Pr[(P, V)(x) = 1] \geq 2/3 \)

Soundness:  \( \forall x \notin L, \forall P^* \ \Pr[(P^*, V)(x) = 1] \leq 1/3 \)

Note:  By repetition, we can get completeness \( 1 - 2^{-k} \), and soundness \( 2^{-k} \)
Interactive Proofs

[Goldwasser-Micali-Rackoff85]:

For ZK the prover needs to be randomized

\[ P \quad V \]

[Goldreich-Micali-Wigderson87]: Every statement that has a classical proof has zero-knowledge (ZK) interactive proof, assuming one-way functions exist.
Defining Zero-Knowledge

Formally: There exists a PPT algorithm $S$ (called a simulator), such that for every $x \in L$:

$$S(x) \approx (P, V)(x)$$

Denotes the transcript

This transcript reveals no information
ZK Proofs for NP

For the $NP$-complete language of all 3-colorable graphs

$G = (V, E)$

Vertices can be colored by $\{1, 2, 3\}$ s.t. no two adjacent vertices are colored by the same color

Randomly permute the coloring, to obtain valid coloring $(c_1, \ldots, c_n)$

Locked safe, reveals no information about its content

Choose a random edge $(i, j) \in E$

Open safes $i, j$

Soundness: Only $1 - \frac{1}{|E|}$ but can be amplified via repetition.
ZK Proofs for NP

For the *NP*-complete language of all 3-colorable graphs

\[ G = (V, E) \]

1. Choose a random \((i, j) \in E\)
2. Choose random distinct colors \(c_i, c_j\)
3. The simulated transcript is:
   - \((i, j) \in E\)
   - Safes \(i, j\) have values \(c_i, c_j\)

Open safes \(i, j\)
Implementing Digital Safes: Commitment Scheme

Commitment scheme is a randomized algorithm $Com$ s.t.

- **Computationally Hiding:**
  \[ \forall m, m' \quad Com(m; r) \approx Com(m'; r') \]

- **Statistically Binding:** \[ \exists (m, r), (m', r') \text{ s.t. } m \neq m' \text{ and } \]
  \[ Com(m; r) = Com(m'; r') \]
Constructing a Commitment Scheme

Construction 1:

Let \( f: \{0,1\}^* \rightarrow \{0,1\}^* \) be an injective OWF, and \( p: \{0,1\}^* \rightarrow \{0,1\} \) be a corresponding hardcore predicate.

\[
\text{Com}(b; r) = (f(r), p(r) \oplus b)
\]

Binding: Follows from the fact that \( f \) is injective

Hiding: Relies on the fact that if \( f \) is one-way then:

\[
(f(r), p(r)) \approx (f(r), U)
\]
Let $G$ be a group of prime order $p$, let $g \in G$ be any generator, and $h$ be a random group element.

$$\text{Com}_{g,h}(m,r) = g^m h^r$$

**Hiding:** Information theoretically!

**Binding:** Follows from the Discrete Log assumption.
Perfect ZK Computationally Sound Proofs

For the $NP$-complete language of all 3-colorable graphs

$G = (V, E)$

Randomly permute the coloring, to obtain valid coloring $(c_1, ..., c_n)$

Choose a random edge $(i, j) \in E$

Reveal $c_i, c_j$, with corresponding randomness

$Com_{g,h}(c_1), ..., Com_{g,h}(c_n)$
So Far...

• **Constructed ZK proofs for all of NP**
  – using commitment schemes

• **Constructed commitment schemes**
  – Based on injective OWF
  – Based on Discrete Log
Interactive Proofs are more efficient!
Classical Proofs
Conjecture: \( \exists \) succinct classical proof for correctness of any computation \( M(x) = 1 \) within \( T \) steps
Interactive Proofs are More Efficient!
[Lund-Fortnow-Karloff-Nissan90, Shamir90]

Example: Chess
Interactive Proofs are More Efficient!

[Lund-Fortnow-Karloff-Nissan90, Shamir90]

correctness of any computation can be proved:

\[
\text{Time to verify } \approx \text{ Space required to do the computation}
\]

\[\text{IP} = \text{PSPACE}\]
Interactive Proofs are More Efficient!
[Lund-Fortnow-Karloff-Nissan90, Shamir90]

correctness of any computation can be proved:

\[
\text{Time to verify} \approx \text{Space required to do the computation}
\]

Succinct space \rightarrow succinct interactive proof
Multi-Prover Interactive Proofs

[BenOr-Goldwasser-Kilian-Wigderson88]

\[ \exists f \text{ computable in time } T: \]

2-provers can convince verifier that \( f(x) = y \),
where the **runtime** of the **verifier** is only \(|x| \cdot \text{polylog}(T)\)
and the **communication** is \(\text{polylog}(T)\)

\[ \forall P_1, P_2, V, q_1, q_2, a_1, a_2 \]

motivated by constructing perfect ZK proofs
[Fortnow-Rompel-Sipser88]:

\[
V_q^a a^*_a a^*_a \]
Probabilistically Checkable Proofs

Read only 3 bits of the proof, and obtain soundness 1/8

Classical proofs

(Zero-knowledge) Interactive proofs

Multi-prover interactive proofs

Probabilistically checkable proofs (PCPs)

Interactive PCP/Interactive oracle proofs

Fiat-Shamir paradigm

SNARGs
THANK YOU