Outline

- Wrap-up commitments
- NIZKs from pairings
Pedersen Commitments
Pedersen Commitments

• Unconditionally hiding
  • Given a commitment c, every value x is equally likely to be the value committed in c.
  • For example, given x, r, and any x’, there exists r’ such that \( g^x h^r = g^{x'} h^{r'} \), in fact \( r = (x-x') a^{-1} + r \text{ mod } q. \)
Pedersen Commitments

• Computationally binding
  
  • Suppose committer sent $g^x h^r \mod p$ for some $(x, r)$
  
  • Now it finds $x' \neq x$ and $r'$ such that $c = g^{x'} h^{r'}$
  
  • This means that the sender ``knows'' $\log_g(h) = (x' - x) \cdot (r - r')^{-1}$.
  
  • This means: assuming DL is hard, the sender cannot open the commitment to a different value.
Application: Coin Tossing

• Alice and Bob want to decide on something by tossing a coin over a phone. How to do this securely?

• Solution: Alice commits to a random bit $b_A \leftarrow \{0, 1\}$, and sends $\text{Com}(b_A; r)$ to Bob

• Bob selects a random bit $b_B \leftarrow \{0, 1\}$ and sends it to Alice

• Alice decommits $b_A$

• Alice and Bob output $b_A \text{ xor } b_B$
Zero-Knowledge
Problems in NP
Graph Isomorphism
Graph Isomorphism
Real World

Prover

Verifier

NP Statement $x$
Witness that $x$ is true
Real World

Prover

Verifier

NP Statement $x$
Witness that $x$ is true

Didn't learn witness

Outputs
view
Real World

Prover

Verifier

Didn't learn witness

NP Statement $x$

Witness that $x$ is true

Outputs view

Ideal World (Proof)

Simulator

NP Statement $x$

Didn't learn witness

No witness
Real World

Prover

NP Statement $x$

Verifier

Witness that $x$ is true

Outputs view

Ideal World (Proof)

Simulator

NP Statement $x$

No witness

Verifier

Didn't learn witness

Witness that $x$ is true

Outputs view
Real World

Prover

NP Statement \( x \)

Witness that \( x \) is true

Verifier

Outputs view

Ideal World (Proof)

Simulator

NP Statement \( x \)

Didn't learn witness

Verifier

Didn't learn witness

Outputs similar view
Real World

Prover

NP Statement x

Verifier

Didn't learn witness

Outputs view

Ideal World (Proof)

Simulator

NP Statement x
No witness

Verifier

Didn't learn witness

Outputs similar view

Cannot distinguish the two
Graph Isomorphism
Graph Isomorphism
Graph Isomorphism

**Prover**

\[ X = (A, B) \]

**Verifier**

Knows \( \eta \) s.t.

\[ A = \eta (B) \]
Graph Isomorphism

**Prover**

\[ X = (A, B) \]

Knows \( \eta \) s.t.

\[ A = \eta(B) \]

**Verifier**
Permuting the Graph

\[ G = \varphi(A) \]
Graph Isomorphism

Prover

\[ X = (A, B) \]

Verifies that \( A = \eta(B) \) where \( \eta \) is a function known to be an isomorphism.

\[ G = \varphi(A) \]

Verifier

\[ c = A \text{ or } B \]
Graph Isomorphism

**Simulator**

\[ X = (A, B) \]

**Verifier**

Knows c in advance
Graph Isomorphism

**Simulator**

\[ X = (A, B) \]

**Verifier**

\[ G = \varphi(c) \]

Knows \( c \) in advance

\[ G \]

\[ \varphi \]
Graph Isomorphism

**Simulator**

$X = (A, B)$

**Verifier**

Knows $c$ in advance

$G = \varphi(c)$