Lesson 15 Lecture Notes

CS555

1 Review of building blocks

OWF + PRG $\Rightarrow$ PRF $\Rightarrow$ Symmetric Encryption $\Rightarrow$ Public-Key Encryption]

Beyond secure communication:

- **Example:** MAC (Message Authentication Code).
- **Zero-knowledge proofs:** shows a statement is correct without giving any additional information about the witness or the system beyond validity of the claim.
  - **Interaction:** back-and-forth between prover and verifier; not just passive sending.
  - Stronger adversaries, more nuanced security properties

1.1 Classical proofs vs. automatic verification

- **Classical:** Prover supplies a logical derivation; verifier checks each step.
- **Modern:** Have a mechanism take in a proof and output `Accept`/`Reject`.
- **Roles:** Both prover and verifier know the claim/theorem. Prover expends effort; verifier runs in polynomial time (PPT).

1.2 Example: Proving N is a product of two primes

- **Classic approach:** Reveal (p, q) to verifier; verifier checks $N = pq$. Hard part is finding (p, q); verifying is simple.
- **Issue:** After seeing (p, q), verifier learns more than just "N is composite with two prime factors."

2 Efficiently verifiable proofs (NP)

(defn): A language $L \subseteq \{0, 1\}^*$ is in NP if there exists a polynomial-time verifier V such that:

- **Completeness:** True theorems have proofs. That is, if $x \in L$, there exists a polynomial-length witness (proof) w with $V(x, w) = 1$.
- **Soundness:** False theorems have no short proofs. That is, if $x \notin L$, then no witness w makes $V(x, w) = 1$.

2.1 Witness leakage examples

- **Product of primes:** Revealing (p, q) proves the claim but leaks the factors.
- **Quadratic residue:** Proving y is a QR mod N by revealing x with $x^2 \equiv y \pmod{N}$ leaks x.

2.2 NP-completeness

Every problem in NP can be reduced (in polynomial time) to an NP-complete problem.

3 Constructing zero-knowledge protocols

We want to prove a claim to a verifier without giving any knowledge $\rightarrow$ idea is that a prover can show they have the capacity to send a full-knowledge proof if they wanted to

- **Interaction/conversation:** Verifier questions prover to determine prover's knowledge of a proof
- **Randomness:** Verifier uses randomness and can make errors with exponentially small probability. Fixed, predictable conversations leak structure (not zero-knowledge) and enable impersonation.

3.1 Rubik's cube example (existential K-move solution)

- **Claim:** There exists a $\leq K$-move solution from scrambled state A to solved state B.
- **Idea:** Precompute intermediate state(s) $C_1, C_2, \ldots, C_n$; choose one C_K at random.
- **Challenge:** Verifier randomly asks to see either $A \Rightarrow C_K$ in $K/2$ moves or $C_K \Rightarrow B$ in $K/2$ moves.
- **Intuition:** If prover consistently answers both types, they effectively demonstrate knowledge of a full K-move solution without revealing the entire sequence.
- **Remark:** Must have enough intermediate states so challenges remain unpredictable for random $A \in L$.

4 Interactive proof system definition

Let L be a language. There exists an unbounded prover P and a PPT verifier V such that:

- **Completeness:** If $x \in L$, then V accepts with high probability (typically 1 in perfect completeness).

$$\Pr[(P, V)(x) = \text{accept}] \geq C$$

- **Soundness:** If $x \notin L$, then V accepts only with negligible probability.

$$\Pr[(P^*, V)(x) = \text{accept}] \geq S$$

Let C denote completeness probability and S denote soundness error. We require $C - S \geq 1/\operatorname{poly}(n)$ to enable amplification via repetition.

- **Amplification:** Repeat protocol t times and accept by majority. Chernoff bounds imply exponentially small overall soundness error.

5 Quadratic residue (QR) identification protocol

Let N be a modulus and $y \in \mathbb{Z}_N^\times$ be the claimed QR ($\exists x$ with $x^2 \equiv y \pmod{N}$).

- **Commit:** Prover picks random $r \in \mathbb{Z}_N^\times$ and sends $S = r^2 \bmod N$.
- **Challenge:** Verifier sends random bit $b \in \{0, 1\}$.
- **Response:**
  - If $b = 0$, prover sends $z = r$; verifier checks $z^2 \equiv S \pmod{N}$.
  - If $b = 1$, prover sends $z = rx$; verifier checks $z^2 \equiv Sy \pmod{N}$.

5.1 Soundness sketch

If y is not a QR mod N, prover cannot produce valid z for both $b = 0$ and $b = 1$ consistently. Cheating succeeds with probability at most 1/2 per round; repetition reduces this to negligible.

6 Intuitive zero-knowledge

After interaction, verifier V learns:

- **Truth:** The statement is true (accepts).
- **View:** The transcript of the interaction.
- **No extra info:** Nothing they couldn't have generated themselves without the prover; the view is simulatable.

Formally, (P, V) is zero-knowledge if V can generate its view of the interaction by itself in PPT via a simulator.

7 Simulation paradigm

- **View structure:** $\text{view}_V(P, V) = (S, b, z)$ together with verifier coins b.
- **Simulator:** There exists S such that given (N, y), it outputs $\text{Sim}(N, y) = (S, b, z)$ indistinguishable from $\text{view}_V(P, V)$.

7.1 Perfect vs. statistical zero-knowledge

- **Perfect ZK:** $\text{view}_V(P, V) \equiv \text{Sim}(N, y)$ (identical distributions).
- **Statistical ZK:** No PPT distinguisher can tell $\text{view}_V(P, V)$ from $\text{Sim}(N, y)$ with non-negligible advantage.

7.2 Simulator for the QR protocol

1. Pick random bit $b \in \{0, 1\}$.
2. Pick random $z \in \mathbb{Z}_N^\times$.
3. Compute $S \equiv z^2 \cdot y^{-b} \pmod{N}$.
4. Output transcript (S, b, z).

If y is QR, the simulator's distribution over (S, b, z) matches the real protocol's view (perfect ZK); more generally, it is computationally/statistically indistinguishable under appropriate assumptions.