Cryptographic Protocols

Spring 2020

Part 2

Zero-Knowledge

Idea: Protocol $(P, V)$ has transcript $T$, simulator $S$ outputs similar $T'$. Def: $(P, V)$ is zero-knowledge (ZK) if $S$ exists for any $V' = V$.

Types of ZK:

- **Perfect**:
  - $P \parallel X : f(n) = 1 - f$ is negligible
  - $poly \times poly = poly$; $poly(poly) = poly$
  - $poly \times negligible \subseteq negligible$
  - $(poly \times negligible) \cap$ overwhelming $\neq \emptyset$

- **Statistical**:
  - $\forall \exists (\Delta(n) 
eq 0)$
  - $\exists$ families of random variables $\iff \exists f$ is noticeable
  - $\forall x, \exists f$ is polynomial
  - $\exists f$ is noticeable
  - $\forall x, \exists f$ is negligible

- **Computational**:
  - $\exists f$ is negligible
  - $\forall x, \exists f$ is negligible
  - $\forall x, f$ is negligible

Complexity Classes

- **$P$** = set of $L$ which are decidable in poly time.
- **$NP$** = set of $L$ which are polynomial in $|\cdot|$.
- **$NP$-hard** = set of $L$ which are at least as hard as any $NP$ problem.
- **$NP$-Complete** = set of $L$ which are both $NP$-hard and in $NP$.
- **$PSPACE$** = set of $L$ which are polynomial in space.

Interactive Proofs of Statements

Def: An interactive proof for language $L$ is a pair $(P, V)$ of int. programs s.t.

- i) Running time of $V$ is polynomial in $|\cdot|$.
- ii) Running time of $S$ is polynomially bounded.
- iii) Transcript $T$ of $(P, V)$ accepts $X$ if and only if $X \in L$.

Examples: Sudoku, GI, GNI, Fiat-Shamir.

Notes:

- Constants $p, q$ are arbitrary, could be $p = 1 - 2^{-|\cdot|}$ and $q = 2^{-|\cdot|}$.
- However, only $NP$-languages have proofs with $q = 0$.
- If iii) holds only for poly-time $P'$, interactive argument (not a proof).
- Probabilistic $P$ are not more powerful than deterministic $P$.

Def: $IP$ = set of $L$ which have an interactive proof.

Theorem: $IP = PSPACE$.

Distinguishing Advantage

Setting: Random variables $X$ and $Y$, distributions $P_X$ and $P_Y$.

Distinguisher

- Algorithm $A$ to distinguish $X$ from $Y$.
- Goal: on input $x \leftarrow X$, output $X'$; on input $y \leftarrow Y$, output $Y'$.

Advantage: $\Delta^A(X, Y) := \left| Pr_{X} [A(x) = X] - Pr_{Y} [A(y) = X] \right|$

Asymptotics

- Families of random variables $(X_n)_{n \in \mathbb{N}}$ and $(Y_n)_{n \in \mathbb{N}}$.
- $\Delta^A(X_n, Y_n) := \left| Pr_{X_n} [A(x) = X] - Pr_{Y_n} [A(y) = X] \right|$

Indistinguishability Levels

- Perfect: $P_X = P_Y$, i.e., $\forall A : \Delta^A(X_n, Y_n) = 0$.
- Statistical: $\forall A : \Delta^A(X_n, Y_n) = negligible$ in $n$.
- Computational: $\forall polytime A : \Delta^A(X_n, Y_n) = negligible$ in $n$.
**c-Simulatability and Zero-Knowledge**

**Definition:** A three-move protocol (round) with challenge space $C$ is $c$-**simulatable** if for any value $c \in C$ one can efficiently generate a triple $(t, c, r)$ with the same distribution as occurring in the protocol (conditioned on the challenge being $c$), i.e., the conditional distribution $P_{TR|C}$ is efficiently samplable.

**Lemma:** A 3-move $c$-simulatable protocol is HVZK.
(assumption: challenge is efficiently samplable)

**Lemma:** A HVZK round with $c$ uniform from $C$ for poly-bounded $|C|$ is ZK.

**Lemma:** A sequence of ZK protocols is a ZK protocol.

**Theorem:** A protocol consisting of $c$-simulatable rounds, with uniform challenge from a (per-round) polynomially bounded space $C$, is perfect ZK.