Cryptographic Protocols

Spring 2021

Part 3

Zero-Knowledge

Idea: Protocol (P,V) has transcript U, simulator S outputs similar U'.

Def: (P,V) is **zero-knowledge (ZK)** $\Leftrightarrow$ $\forall$ poly-time V' $\exists$ S $\forall z \in L$:

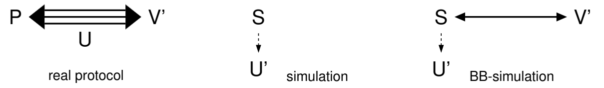
i) Transcript U of (P(z) $\Leftrightarrow$ V'(z)) and output U' of S(z) are indisting.

ii) Running time of S is polynomially bounded.

Def: (P,V) is **black-box zero-knowledge (BB-ZK)** $\Leftrightarrow$ $\exists$ S $\forall$ V' $\forall z \in L$:

i) U of (P(z) $\Leftrightarrow$ V'(z)) and U' of S(z) rewind. access to V'(z) are indisting.

ii) Running time of S is polynomially bounded.



Def: (P,V) is **honest-verifier zero-knowledge (HVZK)** if S exists for V' = V.

Types of ZK: perfect, statistical, computational (type of indisting.)

c-Simulatability and Zero-Knowledge

Definition: A three-move protocol (round) with challenge space $\mathcal{C}$ is **c-simulatable** if for any value $c \in \mathcal{C}$ 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 $\mathcal{C}$ for poly-bounded $|\mathcal{C}|$ 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 $\mathcal{C}$, is perfect ZK.

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: $\Delta^A(X,Y) := \left|\Pr_X[A(x) = \text{„X“}] - \Pr_Y[A(y) = \text{„X“}]\right|$

Asymptotics

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

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