**Cryptographic Protocols**

**Spring 2017**

**Part 2**

### Zero-Knowledge

**Idea:** Protocol \((P, V)\) has transcript \(T\), Simulator \(S\) outputs similar \(T'\).

**Def:** (\((P, V)\) is **zero-knowledge (ZK)** \(\Longleftrightarrow \forall V \exists S:\))

- i) Transcript \(T\) of \((P \leftrightarrow V)\) and output \(T'\) of \(S\) are indistinguishable.
- ii) Running time of \(S\) is polynomially bounded in running time of \(V\).

**Def:** (\((P, V)\) is **black-box zero-knowledge (BB-ZK)** \(\Longleftrightarrow \exists S \forall V:\))

- i) Transcript \(T\) of \((P \leftrightarrow V)\) and output \(T'\) of \(S\) in \((S \leftrightarrow V)\) are indist.,
- 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.

### Interactive Proofs of Statements

**Def:** TM accepts language \(L\) iff \(x \in L \Longleftrightarrow TM(x)\) outputs 1

- i) \(\forall x:\) running time of \(V\) is polynomial in \(|x|\)
- ii) \(\exists V:\) \(Pr((P \leftrightarrow V) \rightarrow \text{accept}) \geq 3/4\)
- iii) \(\forall x \notin L, \forall P:\) \(Pr((P \leftrightarrow V) \rightarrow \text{accept}) \leq 1/2\)

**Remarks**

- Constants \(p, q\) are arbitrary, could be \(p = 1 - 2^{-|x|}\) and \(q = 2^{-|x|}\)
- However: only NP-languages have proofs with \(q = 0\)
- If ii) holds only for poly \(P\) \(\rightarrow\) interactive argument
- Probabilistic \(P\) is not more powerful than deterministic \(P\)

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

### Polynomial, Negligible, Noticeable

**Function** \(f : \mathbb{N} \rightarrow \mathbb{R}\)

- f is **polynomial** \(\iff \exists c \exists n_0 \forall n \geq n_0 : f(n) \leq nc\)
- f is **negligible** \(\iff \forall c : \exists n_0 \forall n \geq n_0 : f(n) \leq \frac{1}{n^c}\)
- f is **noticeable** \(\iff \exists c \exists n_0 \forall n \geq n_0 : f(n) \geq \frac{1}{n^c}\)

**Implications**

- \(\text{poly} \times \text{negligible} = \text{negligible} \) (cannot be amplified)
- \(\text{poly} \times \text{noticeable} = \) "large enough" (can be amplified)

### c-Simulatability

**Definition:** A three-move protocol (round) with challenge space \(C\) is \(c\)-**simulatable** if for any value \(c\) \(\exists C\) one can efficiently generate a triple \((t, c, r)\) with the same distribution as occurring in the protocol (conditioned on the challenge being \(c\)).

Formally: The cond. distribution \(P_{T|REC}\) is efficiently samplable.

**Lemma:** A 3-move \(c\)-simulatable protocol is HVZK.

(assumption: challenge is efficiently samplable)

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

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

**Lemma:** HVZK round with \(c\) uniform from \(C\), \(|C|\) small, is ZK.