Cryptographic Protocols

Spring 2019

Part 2

Polynomial, Negligible, Noticeable

Function $f : \mathbb{N} \to \mathbb{R}$

- f is polynomial $\Leftrightarrow$ $\exists c\ \exists n_0 \forall n \geq n_0 :\ f(n) \leq n^c$
- f is negligible $\Leftrightarrow$ $\forall c\ \exists n_0 \forall n \geq n_0 :\ f(n) \leq \frac{1}{n^c}$
- f is noticeable $\Leftrightarrow$ $\exists c\ \exists n_0 \forall n \geq n_0 :\ f(n) \geq \frac{1}{n^c}$
- f is overwhelming $\Leftrightarrow$ $1 - f$ is negligible

Implications

- poly $\times$ poly = poly; poly(poly) = poly
- poly $\times$ negligible $\subseteq$ negligible
- (poly $\times$ noticeable) $\cap$ overwhelming $\neq$ {}

P, NP, PSPACE, etc.

Running Time of a Turing machine (TM, aka algorithm)

- for input x: number of steps $s(x)$
- for n-bit input: $t(n) :=$ max$\{s(x) : x \in L, |x| \leq n\}$ (worst-case)
- TM is poly-time iff $t(n)$ is a polynomial function

Complexity Classes

- P $= \{L : \exists$ poly-time TM that decides $L\}$
- NP $= \{L : \exists$ poly-time comp. function $\varphi : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}$ s.t. $x \in L \Leftrightarrow \exists w\ (\varphi(x,w) = 1\ \wedge\ |w| \leq$ poly$(|x|))\ \}$
  (also: NP $= \{L : \exists$ non-det. poly-time TM that accepts $L\}$)
- NP-hard $= \{L : \forall L' \in$ NP: L' can be reduced to $L\}$
- NP-Complete $=$ NP $\cap$ NP-hard
- PSPACE $= \{L : \exists$ TM that accepts L with poly memory (in any time)$\}$

Interactive Proofs of Statements

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

i) $\forall x$: running time of V is polynomial in $|x|$

ii) $\forall x \in L$: Pr((P $\Leftrightarrow$ V) $\to$ "accept") $\geq 3/4$ [$p = 3/4$]

iii) $\forall x \notin L, \forall$P' : Pr((P' $\Leftrightarrow$ V) $\to$ "accept") $\leq 1/2$ [$q = 1/2$]

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

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 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.

Zero-Knowledge

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

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

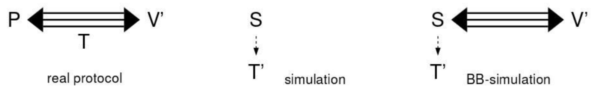
i) Transcript T of (P $\Leftrightarrow$ V') and output T' of S are indistinguishable.

ii) Running time of S is polynomially bounded.

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

i) Transcript T of (P $\Leftrightarrow$ V') and output T' of S in (S $\Leftrightarrow$ V') 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.