COM S 6830 – Cryptography Nov 1, 2011

Lecture 16: Zero Knowledge proofs - Part 1

Instructor: Rafael Pass *Scribe: Lior Seeman*

1 Traditional Proofs

- non interactive
- can never prove false statements.

Definition 1 *V is an NP-verifier for L if V is poly time (in the length of the first input) and*

- *completeness: if* $x \in L$, $\exists \pi$ *s.t* $V(x, \pi) = 1$
- *soundness: if* $x \notin L$, $\forall \pi$ $V(x, \pi) = 0$

2 Interactive Proofs

Definition 2 (P, V) *is an interactive proof for L if V is a PPT and*

- *completeness:* $\forall x \in L$, $\exists y \in \{0,1\}^*$ *s.t* $Pr[Out_v[P(x,y) \leftrightarrow V(x)] = 1] = 1$
- *soundness:* $\forall P^*, \exists neg\ \epsilon, \forall x \notin L, \forall y \in \{0,1\}^*, Pr[Out_v[P(x,y) \leftrightarrow V(x)] = 1] \leq \epsilon(x)$

$P(x, y) \leftrightarrow V(x)$ means that P and V interact. The soundness part of the proof requires that even if the prover doesn't use the honest strategy, he won't be able to prove a false x except with negligible probability.

This proof can prove more than just NP problems. Example:

Graph Non-Isomorphism:
$L = \{G_0, G_1 : G_0 \not\simeq G_1\}$ - This problem is not believed to be in NP. The proof works as follows: V randomly choose $b \leftarrow \{0,1\}$, and a random permutation σ, computes $H = \sigma(G_b)$, and sent it to P. P then finds b' s.t. $H \simeq G_{b'}$, and sends b' to V. V outputs 1 iff $b = b'$.

Claim 1 *This proof is an interactive proof for the language L*

Proof. If $G_0 \not\simeq G_1$ then P can't go back from H to both of them so b' must be equal to b. If $G_0 \simeq G_1$, P can't know where H came from and the best he can do is guess. He has probability of $\frac{1}{2}$ of success. If we repeat n times he will have probability of 2^{-n} of success. ■

Definition 3 *An IP (P, V) for L has an efficient prover w.r.t. witness relation R_L if P is a PPT and completeness holds $\forall y \in R_L(x)$.*

Graph Isomorphism:
$x = (G_1, G_2), w = \pi$ s.t $\pi(G_1) = G_2$(more formally: $\pi \in R_L$ iff $\pi(G_1) = G_2$)
The proof works as follows: First, P chooses a random permutation σ, computes $H = \sigma(G_1)$, and sends H to V. V randomly choses $b \leftarrow \{1, 2\}$, and sends it to P. If $b = 1$, P sends V $\rho = \sigma^{-1}$, else he sends V $\rho = \pi\sigma^{-1}$. V outputs 1 iff $\rho(H) = G_b$.

Claim 2 *This proof is an efficent interactive proof for the language Graph Isomorphism.*

Proof. The proof is complete because if $G_1 \simeq G_2$, P can prove this because π really exists. If $G_1 \not\simeq G_2$, then an honest prover can't win when $b = 2$ is chosen, because the desired ρ doesn't exist, so if we repeat the proof we know he has only a negligible probability of success. If he is not honest, and sends something other than a permutation of G_1, we know that it can't send an H s.t. $G_1 \simeq H$ and $G_2 \simeq H$, since that will mean that $G_1 \simeq G_2$, so again he won't be able to win. ■

Intuitively, this proof is also ZK. The verifier is only given a random permutation of one of the graphs and its inverse, but he could have done that himself. We formally prove this next, for specific definition of ZK.

Definition 4 *(P, V) is a perfect (Honest Verifier) ZK proof for L w.r.t. witness relation R_L if $\exists$ PPT S s.t. $\forall x \in L, y \in R_L(G), \forall z \in \{0, 1\}^*$ the following are identically distributed:*

$$\{View_V[P(x, y) \leftrightarrow V(x, z)]\}$$
$$\{S(x, z)\}$$

$View_V$ is equal to all the messages V received, all of his coin tosses and all of his inputs.

The proof we gave is perfect honest verifier ZK. given $x = (G_1, G_2)$ and z, $S(x, z) = (x, z, b, (H, \rho^{-1})$, where $b \leftarrow \{1, 2\}$, ρ is a random permutation and $H = \rho(G_b)$. This has the exact same distribution as $View_V$ in our proof.