COM S 6830 – Cryptography November 3, 2011

Lecture 17: Zero-knowledge proofs − Part 2

Instructor: Rafael Pass *Scribe: Remus Radu*

Definition 1 (Perfect ZK) *(P, V) is a perfect zero-knowledge proof for L with witness relation R_L if for every PPT V^*, there exists an expected PPT S, such that for every $x \in L$, $w \in R_L(x)$, $z \in \{0,1\}$ the following distributions are identically distributed.*

- $\left\{View_{V^*}\left[P(x,w) \leftrightarrow V^*(x,z)\right]\right\}$
- $\{S(x,z)\}$

Definition 2 (Computational ZK) *(P, V) is a perfect zero-knowledge proof for L with witness relation R_L if for every PPT V^*, there exists an expected PPT S, such that for every nuPPT distinguisher D, there exists a negligible function $\epsilon(\cdot)$ such that for every $x \in L$, $w \in R_L(x)$, $z \in \{0,1\}$, D distinguishes the following distributions with probability at most $\epsilon(|x|)$.*

- $\left\{View_{V^*}\left[P(x,w) \leftrightarrow V^*(x,z)\right]\right\}$
- $\{S(x,z)\}$

Definition 3 (Black-box ZK) *(P, V) is a perfect black-box (BB) zero-knowledge proof for L with witness relation R_L there exists an expected PPT S such that for every PPT V^*, for every $x \in L$, $w \in R_L(x)$, $z, r \in \{0,1\}^*$, the following distributions are identically distributed.*

- $\left\{View_{V_r^*}\left[P(x,w) \leftrightarrow V_r^*(x,z)\right]\right\}$
- $\left\{S^{V_r^*(x,z)}(x)\right\}$

Theorem 1 *There exists a perfect BB zero-knowledge proof for graph isomorphism.*

Proof. We construct a simulator S as follows:

$S^{V^*}(x = (G_1, G_2)$:	Pick $b \leftarrow \{0,1\}$ at random, $\pi \leftarrow$ random permutation $H = \pi(G_b)$ Feed H to V^* and let b' be the message output by V^*. If $b = b'$, then output (H, b, π^{-1}). Otherwise restart.

We need to show that

1. the expected running time of S is polynomial;
2. the output is correctly distributed.

Claim. $\Pr[b' = b] = 1/2$.

Proof. Since $G_1 \approx G_2$ there exists a permutation σ such that $G_2 = \sigma(G_1)$ and so

$$\begin{aligned}\{\pi \leftarrow \text{perm} : \pi(G1)\} &= \{\pi \leftarrow \text{perm} : \pi(G2)\} \\ &= \{\pi \leftarrow \text{perm} : \pi(\sigma(G1))\} \\ &= \{\pi' \leftarrow \text{perm} : \pi'(G1)\}\,.\end{aligned}$$

The lemma follows by closure under efficient operations and the fact that b is chosen at random from $\{0, 1\}$ with probability $1/2$. ■

The expected number of trials before terminating is 2, since S has probability $1/2$ of succeeding in each trial. Each time, the running time is polynomial, so S runs in expected polynomial time.

Note that H has the same distribution as $\pi(G_1)$ for random π, so H is independent of b. Moreover, V^* takes only H as input. The output of V^* is b', which is independent of b. In the claim above, if we can always output the corresponding π, then the output distribution of S would be the same as in the actual protocol. However, we only output H if $b = b'$, but H is independent from b so the output distribution does not change. ■

Theorem 2 *Assume there exist OWF, then every language in $\mathcal{NP}$ has a black-box computational ZK proof.*

Sketch of proof. The proof proceeds in two steps:

> **Step 1:** Show a ZK proof for $G3C$ (Graph 3 Coloring − the language of all graphs whose vertices can be colored using only three colors $1, 2, 3$ such that no two connected vertices have the same color.)
>
> **Step 2:** Reduce the language L to $G3C$: given $x \in L$, witness $w \in R_L(x)$, we can efficiently find $x' \in G3C$ and $w' \in R_{G3C}(x')$. Then run a proof for $G3C$ using x', w'.

We need to show that a ZK proof for $G3C$ exists. Let $X = (V, E)$, where V is the set of vertices, and E is the set of edges. Consider witness $w = \overrightarrow{c} = c_1 c_2 \dots c_n$, where $|V| = n$. Consider the following protocol.

P		V
$\pi \leftarrow$ perm over $\{1, 2, 3\}$		
for i=1 to n: Commit to $\pi(c_i)$	$\longrightarrow$	
	$\longleftarrow$	random edge $(i, j) \in E$
Reveals $\pi(c_i), \pi(c_j)$	$\longrightarrow$	

The completeness follows by inspection. Soundness follows by noticing that in each iteration, a cheating prover P^* can succeed with probability $\left(1 - \frac{1}{|E|}\right)$. The protocol is repeated $n|E|$ times, so P^* can succeed with probability at most

$$\left(1 - \frac{1}{|E|}\right)^{n|E|} \sim \left(\frac{1}{e}\right)^n.$$

Intuitively, it is ZK because the prover only "reveals" 2 random colors in each iteration. The hiding property of the commitment scheme intuitively guarantees that "everything else" is hidden. However, a formal proof is more involved. ■

Definition 4 (Commitment) *A polynomial-time machine Com is called a commitment scheme it there exists some polynomial $p(\cdot)$ such that the following two properties hold:*

1. *(Binding) for evert $r_0, r_1 \in \{0,1\}^{p(n)}$ it holds that $Com(1^n, 0, r_0) \neq Com(1^n, 1, r_1)$.*
2. *(Hiding) the following ensembles are identically distributed*

$$\left\{r \leftarrow \{0,1\}^{p(n)} : Com(1^n, 0, r)\right\}_{n\in\mathbb{N}}$$
$$\left\{r \leftarrow \{0,1\}^{p(n)} : Com(1^n, 1, r)\right\}_{n\in\mathbb{N}}$$

Example. The following is a good commitment scheme based on OWP: let f be a one-way permutation with a hard-core predicate h and consider $Com(1^n, b, r) = f(r), h(r) \oplus b$. It is binding if f is a OWP, by construction. There is only one inverse of $f(r)$ so $h(r)$ is well defined. It is hiding because the following distributions

$$\{r \leftarrow \{0,1\}^n : f(r), h(r) \oplus 0\}_{n\in\mathbb{N}}$$
$$\{r \leftarrow \{0,1\}^n : f(r), h(r) \oplus 1\}_{n\in\mathbb{N}}$$

are indistinguishable.