COM S 687 Introduction to Cryptography November 21, 2006

Lecture 23: More on Zero-Knowledge

Instructor: Rafael Pass *Scribe: Krishnaprasad Vikram*

Two lectures ago we discussed interactive proofs, with an efficient prover. They had two properties

- Completeness
- Soundness - no prover, no matter how powerful can prove a false fact to the verifier except with a negligible probability

Interactive proofs have the Zero Knowledge (ZK) property. We saw the Graph isomorphism problem, which has a ZK proof system. Today, we'd like to prove more general statements. We'll show that any language in NP has a ZK proof system. There is a result that says "Everything provable is provable in ZK"

Definition: An interactive proof system (P,V) is perfect ZK for language $\mathcal{L}$ with witness relation R_L if $\forall p.p.t. V^*$ $\exists S$ s.t. $\forall (x,w) \in R_L$ and all $Z \in \{0,1\}^*$ it holds that

$$View_{V^*}[P(x,y) \leftrightarrow V^*(x,z)] \text{ identically distributed as } S(x,z)$$

where View$_{V^*}$ is the set of all messages received at V^* during a run of the protocol plus the random coins of V^*. This is a simulation based definition and the $*$ on V means that even a malicious (arbitrary) verifier cannot learn anything (earlier we assumed an honest verifier).

We can weaken this definition e.g. statistically or computationally close instead of identially distributed. So, for computational ZK, we require that

$$\{View_{V^*}[P(x,y) \leftrightarrow V^*(x,z)]\}_{(x,y)\in R_L, z\in\{0,1\}^*} \approx_x \{S(x,z)\}_{(x,y)\in R_L, z\in\{0,1\}^*}$$

where $\approx_x$ is a negligibility condition defined in terms of x. (Bonus Factoid: Computational Indistinguishability is always over ensembles). Or for statistical ZK, we have

$\forall n.u.D$ $\exists$ negligible ϵ $s.t. \forall x,y \in R_L, \forall z \in \{0,1\}^*$, it holds that

$$|Pr[real \leftarrow View_{V^*}[P(x,y) \leftrightarrow V^*(x,y)] : \mathcal{D}(real) = 1] - \\ Pr[sim \leftarrow S(x,z) : \mathcal{D}(sim) = 1]| \leq \epsilon(|x|)$$

Witness indistinguishability is a weaker form of ZK where prover doesn't reveal which witness he uses.

We also defined a notion of blackbox ZK. An interactive proof system (P, V) is blackbox ZK if

$\exists p.p.t. S\ \forall p.p.t.\ V^*\ s.t.\ \forall (x, y) \in R_L$ and $\forall z \in \{0,1\}^*$ it holds that

$$View_{V^*}[O(x, y) \leftrightarrow V^*(x, z)] \text{ identially distributed as } S^{V^*}(x, z)$$

Now to our theorem[1] of the day: Assume $\exists$ OWF. Then every language in NP has a ZK proof.(We show the proof for a slightly weaker statement where we assume $\exists$ OWP)

Proof:

Step 1 Show a ZK proof (with efficient prover) for NP-complete language graph 3 coloring: (P, V)

Step 2 To give a proof for $x \in \mathcal{L}$ using witness y, reduce $x \rightsquigarrow x'$ (instance of graph 3 coloring) and reduce $y \rightsquigarrow y'$. Run (P, V) on input x'. The honest prover uses y' as witness.

Let $\mathcal{L}$ be the language of all 3 colorable graphs. We need to prove that a ZK proof for this language exists.

In the physical analog the prover permutes the three colors randomly, then 3 colors the graph and covers the graph entirely. Now the verifier person enters the room and queries for the colors at the two ends of an edge, which is then revealed to him. In the physical world, the prover implicitly commits to the graph coloring, since the coloring cannot change once the verifier enters the room. In the electronic world though, we need an explicit commitment.

Electronically: $X = (V, E)$. Witness $w = \bar{c} = c_0, c_1, c_2, \ldots, c_m . m = |V|$

$P \to V$: Let π be a random permutation over $\{1, 2, 3\}$. **for** $i = 1$ to n : Commit to $\pi(c_i) = c'_i$
$V \to P$: Picks a random edge (i, j)
$P \to V$: reveal commitments c'_i and c'_j
V checks if $c'_i \neq c'_j$

A *commitment* is equivalent to a "physical" envelope. There are typically two phases
Commit phase: Sender puts V in a locked box
Reveal phase: Sender reveals V and the key to the box

After the commit phase, the value is hidden: this property is called the *hiding property*. Also, in the reveal phase, there is only one value that could be revealed: this is called the *binding property*. The binding property is usually unconditional, whereas the hiding property could be relaxed to be computationally or statistically hiding.

Soundness: by binding property, a cheating prover is caught with probability $1/|E|$.

We will look at commitments in details in the next lecture. Now we'll get back to our ZK proof.

ZK intuition: prover only reveals 2 random colors and by hiding of commitment nothing else is revealed. Although we've said this so concisely, it turns out that it is hard to formalize this and the proof we show does not use this intuition.

We construct the simulator in a similar fashion to the graph isomorphism simulator.

1. Pick a random edge $(i', j') \in E$ and picks random colors $c'_i, c'_j \in \{1, 2, 3\}, c'_i \neq c'_j$. Let $c_k = 1$ for all other $k \in [m]$
2. Act like the honest prover: commit to c_i $\forall i$ feed to V^*
3. Get back answer (i, j) from V^*
4. if $(i, j) = (i', j')$ reveal, otherwise restart V^*

By the hiding property of commitment: expected number of restarts $= |E|$ and so the simulator output is indistinguishable from the view at the verifier.

References

[1] Oded Goldreich, Silvio Micali, and Avi Wigderson. How to construct zero-knowledge proof systems for NP. In *FOCS '86: Proceedings of the 27th Annual IEEE Symposium on Foundations of Computer Science*, 1986.