CS 294 – Special Topic in Cryptography: Secure Computation Feb 4, 2016

Lecture 6: Zero Knowledge I

Instructor: Sanjam Garg *Scribe: Lynn Tsai*

Given $A(x), B(x)$ and corresponding shares a_i, b_i, we want to guarantee that the shares correspond to the correct degree-t polynomial for multiplication.

$$C(x) = D(x) - \sum_{k=1}^{t} x^k D_k(x)$$
$$D(x) = A(x) \cdot B(x)$$
$$C(\alpha_i) = a_i b_i - \sum_{k=1}^{t} \alpha_i^k D_k(\alpha_i) \quad \text{(each party can compute this)}$$

Now, back to the malicious computational setting.

1 Zero knowledge proofs

We define:

- P, the prover
- V, the verifier
- W, the witness

We want to prove x is in language l to the verifier.

$$x \in L, L \in NP$$

The prover gives the verifier and witness works to convince them, but doesn't want to reveal the witness or anything about the witness.
The verifier outputs 0 for "don't believe" or 1 for "believe".
Correctness requirement:

$$\forall x \in L, Pr[output_v < P(x,w) \iff v(x)] = 1 \quad \text{(or equal to 1-}neg(k))$$

Soundness requirement:

$$\forall x \notin L \cap \{0,1\}^k Pr[output_v < P(x,w) \iff v(x)] = neg(k)$$

where this applies only over the choice of verifier, and where k is the security parameter.

1.1 What can the prover do?

Soundness: prover is unbounded

$$\forall x \notin L \forall p^* Pr[output_v < p^*(x) \iff V(x) \geq 1] = neg(k) \quad \text{(evil prover, possibly unbounded)}$$

Still cannot convince verifier of false statement.
argument · system = polynomial time
proof system = unbounded case

1.2 Graph Non-isomorphism

$$\begin{aligned} GNI = \{G_0, G_1\} : \{G_o \not\simeq G_1\} \nexists F : V_{G_0} \to V_{G_1} \\ \text{s.t. } (u, v) \in E_{G_0} \iff (f(u), f(v)) \in E_{G_1} \\ E = \text{edge set} \\ GI = \{(G_0, G_1) : G_0 \sim G_1\} \end{aligned}$$

The verifier always takes polynomial time.

$$G_0 \simeq G_1$$

$$P \xleftarrow{H} V$$
$$\xrightarrow{b'}$$

Figure out which one it's isomorphic to, and send it.

1. Sample a random permutation π
2. $b \leftarrow \{0, 1\}$
3. $H = \pi(G_b)$
4. if $b = b'$ then output 1, else 0

$$G_0 \simeq G_1$$

$$P \xrightarrow{H} V$$
$$\xleftarrow{b}$$
$$\xrightarrow{\phi}$$

$$f = V_{G_0} \to V_{G_1}$$

1. Sample π random permutation

2. $H = \pi(G_0)$

3. Send ϕ s.t. $\phi : G_0 \to H$

Must be isomorphic, else can only cheat with probability $\frac{1}{2}$. Keep running over and over, eventually probability of being caught is $1 - \frac{1}{2^k}$, which is huge.
Correctness and soundness were proved, which also hold in unbounded.
No guarantee that verifier might learn something about witness. For example:

$$P \xleftarrow{H} V$$
$$\xrightarrow{b'}$$

If V sends wrong graph to get info. Want to know which graph is isomorphic, used the prover.

1.3 Honest verifiers

Semi-honest: follows the protocol, but wants to learn everything possible.

$$HVZK \exists \text{ a simulator } s, \text{s.t. } \forall x \in L, w \in R_L(x), z \in \{0,1\}^*$$
$$\{view_v \langle P(x,w) \iff v(x,z) \rangle\} = \{s(x)\}$$

Black box, stronger definition:

$$ZK : \exists \text{ a simulator} s, \text{s.t } \forall v^*, x \in L, w \in R_L(x), z \in \{0,1\}^*$$
$$\{view_{v^*} \langle P(x,w) \iff v^*(x,z) \rangle\} \simeq \{s^*(x,z)\}$$

Non-black box:

$$ZK : \forall V^* \exists s$$

Start with $HVZK$: $G \in$ 3 color

1. Sample random function g, C_v is commitment to coloring $g : f(u) \to$ separate box for every node in the box.

2. V sends $e, edge(u,v)$.

3. P sends key for u, v and open boxes

$$G \in 3 \text{ color} : \exists f : V_g \to \{K, B, G\} \text{ s.t. } \forall (u,v) \exists E_g, f(u) \neq f(v)$$

- P figured out how to color graph
- V failed, said impossible

- P convince V that graph is 3-colorable
- Both have access to the graph
- Cover all nodes, uncover 2 nodes connected by edge, then colors should not be the same. If it's possible, then they will be caught.
- $\frac{1}{e} \to torepeatmanytimes$
- Change colors each time.

1.4 Using commitment schemes to do this digitally

The idea is to write the answers, put them in locked boxes, and send with FedEx to the other guy.
P cannot change b since it has already been sent. If P wants to reveal it, it sends the key.
To implement it digitally, we use one-way functions.

- Cheat with probability $\frac{1}{e}$.
- Boxes are a commitment function $com(b, r)$ where the key is randomness.

Argue zero knowledge for honest receiver. Description of the simulator:

1. $e \leftarrow E_G$, colored differently
2. $l_u = com(F(u), v_u)$ where $I(U^*)$ and $I(V^*)$ are randomness in $\{RGB\}$.
   The distributions e and e^* are identical. $P(e^*) = e = \frac{1}{e}$.
   Discard with $P = 1 - \frac{1}{e}$.
   $f(u^*) \neq f(v^*)$
   $f(u) = k \forall u \in v_g \setminus \{u^*, v^*\}$
3. Output:

$$\xrightarrow{C_u}$$
$$\xleftarrow{e}$$
$$\xrightarrow{r_u^* r_v^*}$$

reality	*simulator*
$\rightarrow$	$\rightarrow$
$\xleftarrow{e}$	$\xleftarrow{e}$
$\rightarrow$	$\rightarrow$

Only works because V chose e honestly. Can be generated without access to the witness itself.

Want to prove true with a malicious verifier:

- Verifier can choose e incorrectly
- Cannot talk, can learn something sometimes