CS 601.442/642 – Modern Cryptography Instructor: Abhishek Jain

Homework 6

Deadline: November 11; 2020, 11:59 AM EST

1. **(15 points)** In class, we saw the definition of single-value hiding commitment schemes. Consider the following definition of a **multi-value hiding** commitment scheme:

A commitment scheme is said to achieve multi-value hiding if for every non-uniform PPT adversary $\mathcal{A}$, there exists a negligible function $\nu(\cdot)$ such that for any $v_1^0, v_1^1, \ldots, v_\ell^0, v_\ell^1 \in \{0,1\}^n$ chosen by the adversary $\mathcal{A}$, the probability that $\Pr[b' = b] \leq \frac{1}{2} + \nu(n)$, where b, b' are as defined in the following game.

Challenger		**Adversary $\mathcal{A}$**
	$\xleftarrow{\left((v_1^0, v_1^1), \cdots, (v_l^0, v_\ell^1)\right)}$	
$b \xleftarrow{\$} \{0,1\}$		
$\forall i \in [\ell],\ r_i \xleftarrow{\$} \{0,1\}^n$;		
$C_i = \mathsf{Com}(v_i^b; r_i)$		
	$\xrightarrow{(C_1, \cdots, C_n)}$	
	$\xleftarrow{b'}$	

Prove that any single-value hiding commitment scheme also satisfies multi-value hiding.

2. **(15 points)** Let $A \simeq B$ denote that graphs A and B are isomorphic to each other. Consider an NP language that consists of statements with 2 pairs of graphs, such that **at least one** of the pairs is isomorphic. Such a language can be formally defined as follows:

$$L = \left\{ ((G_0, G_1), (H_0, H_1)) \;\middle|\; (G_0 \simeq G_1) \vee (H_0 \simeq H_1) \right\}$$

Any **zero-knowledge** proof system for this language must prevent the verifier from learning which of the two pairs are isomorphic and the permutation between the isomorphic pair(s). One such interactive zero-knowledge proof system can be constructed as follows:

Common Input: $(G_0, G_1), (H_0, H_1)$

Prover's Private Input: If $G_0 \simeq G_1$, it has permutation π_G such that $G_1 = \pi_G(G_0)$. If $H_0 \simeq H_1$, it has permutation π_H such that $H_1 = \pi_H(H_0)$.

Protocol: Repeat the following procedure n times using fresh randomness:

- **Prover:** Randomly choose bits $b_1 \xleftarrow{\$} \{0,1\}$ and $b_2 \xleftarrow{\$} \{0,1\}$ and permutations $\pi_1 \xleftarrow{\$} \Pi_n$ and $\pi_2 \xleftarrow{\$} \Pi_n$. It generates Graphs G and H, such that, $G = \pi_1(G_{b_1})$ and

$H = \pi_2(H_{b_2})$. Sends G and H to the verifier.

- **Verifier:** Randomly chooses bit $b \leftarrow \{0,1\}$ and sends it to the prover.
- **Prover:** Chooses bits b'_1 and b'_2 such that if $(G_0 \not\simeq G_1)$, then set $b'_1 = b_1$ and set $b'_2 = b \oplus b'_1$, and if instead $(H_0 \not\simeq H_1)$, then set $b'_2 = b_2$ and set $b'_1 = b \oplus b'_2$ and if both pairs are isomorphic, then b'_1 and b'_2 can be chosen in any way ensuring $b = b'_1 \oplus b'_2$. Computes π'_1 and π'_2 such that $G = \pi'_1(G_{b'_1})$ and $H = \pi'_2(H_{b'_2})$. Sends b'_1, b'_2, π'_1 and π'_2 to the verifier.
- **Verifier:** Verifies if $G = \pi'_1(G_{b'_1})$ and $H = \pi'_2(H_{b'_2})$. If both are equal then it accepts.

(Notice that)

Prove **completeness, soundness and zero-knowledge property** of this protocol.

Hint: An interactive proof system for a related NP language $L = \left\{(G_0, G_1) \;\middle|\; (G_0 \simeq G_1)\right\}$ is given in Section 10.6.1 in the scribes posted on the course website. The proof of completeness and soundness for this proof system appears on page 115 and the proof of zero-knowledge appears on page 117-118 in the scribes. You may refer to that for help.

3. **(10 points)** Let L be an NP language with witness relation R such that every statement $x \in L$ has at least two different witnesses. **Witness indistinguishability** is a property of proof systems for such languages, that ensures that the verifier does not learn which of the witnesses was used by the prover in the proof system. This property can be formally defined as follows:

An interactive proof system (P, V) for a language L is called witness indistinguishable if for any triplet (x, w_0, w_1) such that $R(x, w_0) = 1$ and $R(x, w_1) = 1$, and for any auxiliary input $z \in \{0,1\}^*$, the distributions $\{\mathsf{View}_V(P(x, w_0) \leftrightarrow V(x, z))\}$ and $\{\mathsf{View}_V(P(x, w_1) \leftrightarrow V(x, z))\}$ are computationally indistinguishable.

Prove that any zero-knowledge proof system is also a witness indistinguishable proof system.