CS65500: Advanced Cryptography Instructor: Aarushi Goel

Homework 5

Due: April 11; 2025 (11:59 PM)

1 Witness Indistinguishability

Witness indistinguishability is a weaker privacy property than zero-knowledge and is defined as follows:

Definition 1 (Witness Indistinguishabile Poofs) *An interactive proof Π between a prover P and a verifier V is a witness indistinguishable interactive proof for an NP language L (with corresponding NP relation $\mathcal{R}_L$) if for all x, w_1, w_2, such that $\mathcal{R}_L(x, w_1) = 1$ and $\mathcal{R}_L(x, w_2) = 1$, for all n.u. PPT (malicious) verifiers V^* and for all $\lambda \in \mathbb{N}$, the following holds:*

$$\left\{\mathsf{View}^{V^*}_{\Pi\langle P(x,w_1),V^*(x)\rangle}(1^\lambda)\right\} \approx_c \left\{\mathsf{View}^{V^*}_{\Pi\langle P(x,w_2),V^*(x)\rangle}(1^\lambda)\right\}$$

1. **(10 Points)** Show that zero-knowledge implies witness indistinguishability. In other words, prove that a *zero-knowledge* interactive proof is also a *witness-indistinguishable* interactive proof.

2. **(5 Points)** The above definition of witness indistinguishability only considers a single statement. Prove that the witness indistinguishability property *composes*, i.e., if an interactive proof Π satisfies the above definition of witness indistinguishability, then it also satisfies the following definition: *for all $\lambda \in \mathcal{N}$, all polynomials $q(\cdot)$, all sets of triplets $\{x_i, w_{i,1}, w_{i,2}\}_{q(\lambda)}$, such that for all $i \in q(\lambda)$ $\mathcal{R}_L(x_i, w_{i,1}) = 1$ and $\mathcal{R}_L(x_i, w_{i,2}) = 1$, and for all n.u. PPT (malicious) verifiers V^*, the following holds:*

$$\left\{\mathsf{View}^{V^*}_{\Pi\langle P(x_i,w_{i,1}),V^*(x)\rangle}(1^\lambda)\right\}_{i\in q(\lambda)} \approx_c \left\{\mathsf{View}^{V^*}_{\Pi\langle P(x_i,w_{i,2}),V^*(x)\rangle}(1^\lambda)\right\}_{i\in q(\lambda)}$$

3. **(20 Points)** Let L be an NP language L (with corresponding relation $\mathcal{R}_L$). Let Π be a *witness indistinguishable proof of knowledge* and let f be a one-way function. Consider the following protocol between a prover (who has input x, w, such that $\mathcal{R}_L(x, w)$) and a verifier (who has input x):

   - **Verifier $\rightarrow$ Prover:** Samples $r_1, r_2 \xleftarrow{\$} \{0,1\}^\lambda$ and $\forall i \in [2]$, it computes $y_i = f(r_i)$. It sends y_1, y_2 to the prover.
   - **Verifier $\leftrightarrow$ Prover:** Verifier and prover engage in an interactive proof Π, where the verifier proves to the prover that it either knows $f^{-1}(y_1)$ or $f^{-1}(y_2)$.
   - **Prover $\leftrightarrow$ Verifier:** Prover and verifier engage in an interactive proof Π, where the prover proves to the verifier that it either knows w, such that $\mathcal{R}_L(x, w)$ or it knows $f^{-1}(y_1)$ or $f^{-1}(y_2)$.

   Prove that this is a zero-knowledge argument of knowledge for L, i.e., prove that this protocol satisfies completeness, knowledge soundness and zero-knowledge.

2 Maliciously Secure Garbled Circuits

(15 Points) Cut-and-choose is a technique used to enhance the security of a garbled-circuit-based, semi-honest two-party computation protocol, making it secure against malicious adversaries. To learn more about this technique, refer to Chapter 6.1 of "A Pragmatic Introduction to Secure Multiparty Computation" by *David Evans, Vladimir Kolesnikov, and Mike Rosulek*. After reading, summarize the technique in your own words.

3 Zero-Knowledge Proofs

(20 Points) Consider the following protocol to prove that $x \in L$. Let $\mathcal{R}_L$ be a associated relation (viewed as a circuit) such that $\mathcal{R}_L(x, w) = 1$ if and only if w is a witness for the fact that $x \in L$.

The prover constructs a garbled version of the circuit $\mathcal{R}_L(x, \cdot)$ with the statement x fixed. It sends the garbled circuit, along with commitments to the input wire keys to the verifier. The verifier samples a challenge bit and sends it to the prover. Depending on the challenge bit, the prover: (i)"un-garbles" the circuit by revealing the randomness used; or (ii) decommits to the keys corresponding to the witness. The verifier now correspondingly checks if (i) the garbled circuit was in fact a garbling of $\mathcal{R}_L(x, \cdot)$; or (ii) evaluation of the garbled circuit with the decommitted input wire keys results in output 1.

The full description is given below. For simplicitly, assume that all valid witnesses are of same length ℓ. Let $w[i]$ denote the i-th bit of a witness w. Let Com denote a non-interactive commitment scheme for strings.

Protocol

$\underline{\mathsf{P}(x,w)}$		$\underline{\mathsf{V}(x)}$
$r \leftarrow\!\!\$\ \{0,1\}^n$		
$\left(\widetilde{\mathcal{R}_L}, \{k_0^i, k_1^i\}_{i\in[\ell]}\right) \leftarrow \mathsf{Garble}\left(\mathcal{R}_L(x,\cdot); r\right)$		
For all $i \in [\ell], b \in \{0,1\}$		
$\quad c_b^i \leftarrow \mathsf{Com}(k_b^i)$		
For all $i \in [\ell]$		
$\quad (\widehat{c}_0^i, \widehat{c}_1^i) \leftarrow \mathsf{RandomShuffle}(c_0^i, c_1^i)$		
	$\xrightarrow{\widetilde{\mathcal{R}_L},\ \ \{\widehat{c}_0^i, \widehat{c}_1^i\}_{i\in[\ell]}}$	
		$ch \leftarrow\!\!\$\ \{0,1\}$
	$\xleftarrow{ch}$	
If $ch = 0$		
Set $d =$ garbling randomness r		
Else		
Set $d =$ open commitments of $k^i_{w[i]}$		
	$\xrightarrow{d}$	
		If $ch = 0$
		$\quad$ Accept if $\widetilde{\mathcal{R}_L} = \mathsf{Garble}\left(\mathcal{R}_L(x,\cdot); r\right)$
		else Reject
		If $ch = 1$
		$\quad$ Accept if (i) openings are correct
		$\quad$ AND (ii) $\mathsf{Eval}\left(\widetilde{\mathcal{R}_L}, \{k^i\}_{i\in[\ell]}\right) = 1$
		else Reject

Prove that the above protocol satisfies completeness, soundness (with error 1/2) and zero-knowledge properties. Also, explain the purpose of RandomShuffle in the above protocol. For zero-knowledge, it is sufficient to explain in words why the above protocol is zero-knowledge.