CS 601.442/642 – Modern Cryptography Instructor: Abhishek Jain

Bonus Homework

Deadline: December 9; 2020, 11:59 AM

1. (10 points) **Hard-core predicates:** Let f be a length-preserving one-way function. Let $\mathsf{bit}(i, x) \coloneqq x_i$, the i-th bit of x (defined for $1 \leq i \leq |x|$). Prove that the function f' defined by

$$f'(x) \coloneqq f(x) \,||\, \mathsf{bit}(1, x) \,||\, 1$$

is a one-way function, but that the predicate $\mathsf{bit}(1, \cdot) : \{0,1\} \to \{0,1\}$ is not hard-core for f'.

2. (15 Points) **Encryption:** Consider the following alternate definition of **IND-CPA** security for secret-key encryption, where the adversary also gets access to an encryption oracle. The oracle takes a message m as input and returns a ciphertext $c \leftarrow \mathsf{Enc}(m, k)$:

IND-CPA$^+$ Security: A secret-key encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is IND-CPA$^+$ secure if for all n.u. PPT adversaries $\mathcal{A}$, there exists a negligible function $\mu(\cdot)$ such that:

$$\Pr\left[\begin{array}{rl} k \xleftarrow{\$} \mathsf{Gen}(1^n), & \\ (m_0, m_1) \leftarrow \mathcal{A}^{\mathsf{Enc}(\mathsf{k},.)}(1^n), & : \mathcal{A}^{\mathsf{Enc}(\mathsf{k},.)}(\mathsf{Enc}(k, m_b)) = b \\ b \xleftarrow{\$} \{0,1\} & \end{array}\right] \leq \frac{1}{2} + \mu(n)$$

Note that since the adversary runs in polynomial time, it can only make polynomial number of queries to the oracle.

   (a) Show that for an encryption scheme to be IND-CPA$^+$ secure, its Enc function must be randomized.

   (b) Prove that under this setting (where the adversary has access to encryption oracle), one-message security implies multi-message security.

3. (15 points) **Signatures and PRFs:** Let $\mathcal{S} = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Ver})$ be a **UF-CMA** secure signature scheme where the Sign algorithm is randomized. In particular, the signing algorithm additionally takes a random string as input i.e., $\sigma \leftarrow \mathsf{sign}(sk, m; r)$, where $m \in \{0,1\}^n$ and $r \in \{0,1\}^n$. Let F be a secure PRF such that $F : \{0,1\}^n \times \{0,1\}^k \to \{0,1\}^n$. Consider the following new signature scheme $\mathcal{S}' = (\mathsf{Gen}', \mathsf{Sign}', \mathsf{Ver}')$:

   - $\mathsf{Gen}'(1^\lambda)$: $(sk, vk) \leftarrow \mathsf{Gen}(1^\lambda)$, $k \xleftarrow{\$} \{0,1\}^k$, $sk' = (sk, k)$ Output (sk', vk).
   - $\mathsf{Sign}'(sk', m)$: Parse $sk' = (sk, k)$. Compute $r \leftarrow F(k, m)$, $\sigma \leftarrow \mathsf{Sign}(sk, m; r)$. Output σ.
   - $\mathsf{Ver}'(vk, m, \sigma)$: Output 1 if $\mathsf{Ver}(vk, m, \sigma)$ outputs 1, else output 0.

Note that the modified signature scheme $\mathcal{S}'$ has a deterministic signing algorithm. Prove that $\mathcal{S}'$ is also **UF-CMA** secure.

4. (15 points) **(Zero-Knowledge)** Consider the following protocol to prove that $x \in L$. Let R be a associated relation (viewed as a circuit) such that $R(x, w) = 1$ if and only if w is a witness for the fact that $x \in L$.

   The prover constructs a garbled version of the circuit $R(x, \cdot)$ 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 $R(x, \cdot)$; 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

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