CS 601.442/642 – Modern Cryptography Instructor: Abhishek Jain

Homework 5

Deadline: December 6; 2017, 11:59 PM

1. (10 points) Let $\mathsf{PKE} = (\mathsf{KeyGen}, \mathsf{Encrypt}, \mathsf{Decrypt})$ be an **IND-CCA-2** secure public key encryption scheme with *one bit* message space $\mathcal{M} = \{0,1\}$. Consider a new encryption scheme $\mathsf{PKE}' = (\mathsf{KeyGen}', \mathsf{Encrypt}', \mathsf{Decrypt}')$ that encrypts ℓ-bit long messages:

   - $\mathsf{KeyGen}'(1^\lambda)$: On input a security parameter λ, compute $(sk, pk) \leftarrow \mathsf{KeyGen}(1^\lambda)$ and output $sk' = sk$ as the secret key and $pk' = pk$ as the public key.
   - $\mathsf{Encrypt}'(pk', m)$: On input a message $m = m_1, \ldots, m_\ell \in \{0,1\}^\ell$ (m_i denotes the i-th bit of m) and a public key $pk' = pk$, compute $c_i \leftarrow \mathsf{Encrypt}_{pk}(m_i)$ for all $i \in [\ell]$. Output the ciphertext $c = c_1, \ldots, c_\ell$.
   - $\mathsf{Decrypt}'(sk', c)$: On input a ciphertext $c = (c_1, \ldots, c_\ell)$ and a secret key $sk' = sk$, compute $m_i \leftarrow \mathsf{Decrypt}_{sk}(c_i)$ for all $i \in [\ell]$. Output $m = m_1, \ldots, m_\ell$.

   Is PKE' **IND-CCA-2** secure? Prove or disprove.

2. (20 points) Let $\mathcal{E} = (\mathcal{E}.\mathsf{Gen}, \mathcal{E}.\mathsf{Enc}, \mathcal{E}.\mathsf{Dec})$ be an **IND-CPA** secure secret key encryption scheme and $\mathcal{M} = (\mathcal{M}.\mathsf{Gen}, \mathcal{M}.\mathsf{Tag}, \mathcal{M}.\mathsf{Ver})$ be a **strongly UF-CMA** secure MAC scheme. Consider the following encryption scheme $(\mathsf{KeyGen}, \mathsf{Encrypt}, \mathsf{Decrypt})$:

   - $\mathsf{KeyGen}(1^\lambda)$: Generate $k_\mathcal{E} \leftarrow \mathcal{E}.\mathsf{Gen}(1^\lambda)$ and $k_\mathcal{M} \leftarrow \mathcal{M}.\mathsf{Gen}(1^\lambda)$. Output $k = (k_\mathcal{E}, k_\mathcal{M})$
   - $\mathsf{Encrypt}(k, m)$: Parse $k = (k_\mathcal{E}, k_\mathcal{M})$. Compute $c' \leftarrow \mathcal{E}.\mathsf{Enc}(k_\mathcal{E}, m)$, $\sigma \leftarrow \mathcal{M}.\mathsf{Tag}(k_\mathcal{M}, c')$. Output $c = (c', \sigma)$.
   - $\mathsf{Decrypt}(k, c)$: Parse $k = (k_\mathcal{E}, k_\mathcal{M})$ and $c = (c', \sigma)$. If $\mathcal{M}.\mathsf{Ver}(k_\mathcal{M}, c', \sigma) \neq 1$, output $\perp$. Else, output $m \leftarrow \mathcal{E}.\mathsf{Dec}(k_\mathcal{E}, c')$.

   Prove that this scheme is **IND-CCA-2** secure.