CS 601.442/642 – Modern Cryptography Instructor: Abhishek Jain

Homework 4

Deadline: November 2; 2022, 1:30 PM EST

1. Let $\mathbb{G}$ be a cyclic group with order q and generator g. Consider the following Gen and Enc functions for a public-key encryption scheme with single bit messages:

   - $\mathsf{Gen}(1^n)$: Sample $x \xleftarrow{\$} \mathbb{Z}_q$ and compute $h := g^x$. The public key is h and the private key is x.
   - $\mathsf{Enc}(h, m)$:
     - If $m == 0$ then sample $y \xleftarrow{\$} \mathbb{Z}_q$ and compute $c_1 := g^y$ and $c_2 := h^y$. The ciphertext is (c_1, c_2).
     - Else, if $m == 1$ then sample $y, z \xleftarrow{\$} \mathbb{Z}_q$ and compute $c_1 := g^y$ and $c_2 := g^z$. The ciphertext is (c_1, c_2).

   (a) **(10 points)** Write the decryption algorithm $\mathsf{Dec}(x, (c_1, c_2))$ and show that it is correct with overwhelming probability.

   (b) **(10 points)** Prove *via reduction* that this encryption scheme is **IND-CPA secure** assuming that DDH is hard in $\mathbb{G}$.

2. An *order-preserving* encryption scheme is a scheme where the ciphertexts follow the same lexicographic order as the messages. Such a property would be extremely useful for computing on encrypted databases. In this question, we will see why this property is hard to achieve.

   (10 points) Let $\mathcal{E} := (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a public key encryption scheme such that for each $m_1, m_2 \in \mathcal{M}$, if $m_1 \leq m_2$, then $\mathsf{Enc}(\mathsf{pk}, m_1) \leq \mathsf{Enc}(\mathsf{pk}, m_2)$, where $\mathcal{M}$ is the message space and pk is the public key generated by the Gen algorithm. Show that $\mathcal{E}$ is **not** IND-CPA secure.

3. **(10 points)** Let $(\mathsf{Gen}, \mathsf{Sign}, \mathsf{Verify})$ be a multi-message UF-CMA secure digital signature scheme that can be used to sign messages of length n. Consider the following new scheme for signing messages of length $2n$:

   - $\mathsf{Gen}'(1^n)$: Compute $(\mathsf{sk}_1, \mathsf{pk}_1) \leftarrow \mathsf{Gen}(1^n)$ and $(\mathsf{sk}_2, \mathsf{pk}_2) \leftarrow \mathsf{Gen}(1^n)$. Set $\mathsf{sk} := (\mathsf{sk}_1, \mathsf{sk}_2)$ and $\mathsf{pk} := (\mathsf{pk}_1, \mathsf{pk}_2)$. Output $(\mathsf{sk}, \mathsf{pk})$.
   - $\mathsf{Sign}'(m, \mathsf{sk})$: Parse $\mathsf{sk} := (\mathsf{sk}_1, \mathsf{sk}_2)$. Compute $\sigma_1 \leftarrow \mathsf{Sign}(m[0 : n], \mathsf{sk}_1)$ and $\sigma_2 \leftarrow \mathsf{Sign}(m[n : 2n], \mathsf{sk}_2)$. Output $\sigma := \sigma_1 || \sigma_2$.
   - $\mathsf{Verify}'(\sigma, \mathsf{pk})$: Parse $\mathsf{pk} := (\mathsf{pk}_1, \mathsf{pk}_2)$ and $\sigma := \sigma_1 || \sigma_2$. Compute $b_1 \leftarrow \mathsf{Verify}(\sigma_1, \mathsf{pk}_1)$ and $b_2 \leftarrow \mathsf{Verify}(\sigma_2, \mathsf{pk}_2)$. Output $b := b_1 \wedge b_2$.

   Show that $(\mathsf{Gen}', \mathsf{Sign}', \mathsf{Verify}')$ is **not** a UF-CMA secure digital signature scheme.

4. (a) **(10 points)** Let $(\mathsf{Gen}, \mathsf{Sign}, \mathsf{Verify})$ be a multi-message UF-CMA secure digital signature scheme. Consider the following new scheme:

   - $\mathsf{Gen}'(1^n)$: Compute and output $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}(1^n)$.

- $\mathsf{Sign}'(m, \mathsf{sk})$: Compute $\sigma \leftarrow \mathsf{Sign}(m, \mathsf{sk})$ and output $\sigma' := \sigma || \sigma$.
- $\mathsf{Verify}'(\sigma, \mathsf{pk})$: Parse $\sigma := \sigma_1 || \sigma_2$. Compute $b \leftarrow \mathsf{Verify}(\sigma_1, \mathsf{pk})$. If $\sigma_1 = \sigma_2$ and $b = 1$, output 1, else output 0.

Show that $(\mathsf{Gen}', \mathsf{Sign}', \mathsf{Verify}')$ is also a multi-message UF-CMA secure digital signature scheme.

(b) **(10 points)** In the class we saw that PRFs imply MACs. You have to show that the converse is not true, i.e., a MAC scheme may not be a PRF. More specifically, given a UF-CMA secure MAC scheme $(\mathsf{Gen}, \mathsf{Tag}, \mathsf{Verify})$, show that $(\mathsf{Gen}, \mathsf{Tag})$ is not necessarily a PRF.