CS 601.442/642 – Modern Cryptography Instructors: Aditya Hegde and Harry Eldridge

Homework 7

Deadline: April 2; 2026, 11:59pm ET

Instructions

- The solutions must be submitted via Canvas.
- You must typeset your solutions. We suggest using LaTeX or Typst.

Problems

1. (10 points) Let $(\mathsf{KeyGen}, \mathsf{Tag}, \mathsf{Ver})$ be a UF-CMA secure MAC scheme. Define the following scheme.

   - $\mathsf{KeyGen}'(1^\lambda)$: **return** $\mathsf{KeyGen}(1^\lambda)$
   - $\mathsf{Tag}'(sk, m)$:
     - $\sigma_0 \leftarrow \mathsf{Tag}(sk, m)$
     - $\sigma_1 \leftarrow \mathsf{Tag}(sk, m)$
     - **return** (σ_0, σ_1)
   - $\mathsf{Ver}'(pk, m, (\sigma_0, \sigma_1))$
     - **return** $\mathsf{Ver}(\mathsf{pk}, m, \sigma_0) \vee \mathsf{Ver}(\mathsf{pk}, m, \sigma_1)$

   Note that Ver' returns true if *either* tag verifies. Prove that $(\mathsf{KeyGen}', \mathsf{Tag}', \mathsf{Ver}')$ is a UF-CMA secure MAC scheme.

2. (30 points) Let $(\mathsf{KeyGen}, \mathsf{Tag}, \mathsf{Ver})$ be a UF-CMA secure MAC scheme, and let $(\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ be an IND-CPA secure private key encryption scheme. Define the following MAC scheme:

   - $\mathsf{KeyGen}'(1^\lambda)$
     - $r \leftarrow\!\!\$\ \{0,1\}^\lambda$
     - $k_{\mathsf{Sign}} \leftarrow \mathsf{KeyGen}(1^\lambda)$
     - $k_{\mathsf{Enc}} \leftarrow \mathsf{KGen}(1^\lambda)$
     - **return** $(r, k_{\mathsf{tag}}, k_{\mathsf{enc}})$
   - $\mathsf{Tag}'((r, k_{\mathsf{tag}}, k_{\mathsf{enc}}), m)$
     - $\mathsf{ct} \leftarrow \mathsf{Enc}(k_{\mathsf{enc}}, r)$
     - $\sigma \leftarrow \mathsf{Tag}(k_{\mathsf{tag}}, m)$
     - **return** (ct, σ)
   - $\mathsf{Ver}'((r, k_{\mathsf{tag}}, k_{\mathsf{enc}}), m, (\mathsf{ct}, \sigma))$
     - **return** $\mathsf{Ver}(k_{\mathsf{tag}}, m, \sigma) \vee \sigma == r$

   The scheme acts just like the underlying MAC scheme, but also accepts all tags that are exactly equal to some special value r. The encryption of r is included in every tag.

   Prove that $(\mathsf{KeyGen}', \mathsf{Tag}', \mathsf{Ver}')$ is a UF-CMA secure MAC scheme.

   Hint: This would be easy if Ver' didn't check if $\sigma == r$. Can you do a sequence of game hops that allows you to remove that check?

3. (15 points) Let $(\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Ver})$ be a UF-CMA secure digital signature scheme for messages of lenth n. Define the following scheme for messages of length $2n$:

- $\mathsf{KeyGen}'(1^\lambda)$:
  - $(sk_0, pk_0) \leftarrow \mathsf{KeyGen}(1^\lambda)$
  - $(sk_1, pk_1) \leftarrow \mathsf{KeyGen}(1^\lambda)$
  - **return** $((sk_0, sk_1), (pk_1, pk_1))$
- $\mathsf{Sign}'((sk_0, sk_1), m)$:
  - $\sigma_0 = \mathsf{Sign}(sk_0, m[1, \ldots, n])$
  - $\sigma_1 = \mathsf{Sign}(sk_1, m[n+1, \ldots, 2n])$
  - **return** (σ_0, σ_1)
- $\mathsf{Ver}'((pk_0, pk_1), m, (\sigma_0, \sigma_1))$:
  - **return** $\mathsf{Ver}(pk_0, m[1, \ldots, n], \sigma_0) \wedge \mathsf{Ver}(pk_1, m[n+1, \ldots, 2n], \sigma_1)$

Prove that $(\mathsf{KeyGen}', \mathsf{Tag}', \mathsf{Ver}')$ is *not* a UF-CMA secure digital signature scheme.

4. (15 points) Let $(\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Ver})$ be a UF-CMA secure digital signature scheme with secret-key space $\{0,1\}^\lambda$. Construct a digital signature scheme $(\mathsf{KeyGen}', \mathsf{Sign}', \mathsf{Ver}')$, prove that it is correct, prove that it is one-time UF-CMA secure, and prove that it is *not* UF-CMA secure.

5. (10 points) Let $H = \{h_i\}_{i \in I}$ be a collision-resistant hash function family. Define a hash function family H', where for all $h'_i \in H'$, $h'_i(x) = h(x||0)||h(x||1)$. Prove that H' satisfies collision resistance.

6. (20 points) We can define another property for hash functions known as *second preimage resistance*. This property means that given some randomly chosen input x, it should be hard to find a *second* input x' such that $h(x) = h(x')$. We formally state the property below.

> We say that a hash function family $H = \{h_i : D_i \to R_i\}_{i \in I}$ satisfies *second preimage resistance* if for all NUPPT $\mathcal{A}$, there exists a negligible function $\nu(\cdot)$ such that $\forall \lambda \in \mathbb{N}$:
>
> $$\Pr\left[x' \neq x \wedge h_i(x) = h_i(x') \ : \begin{array}{c} i \leftarrow \mathsf{Gen}(1^\lambda) \\ x \leftarrow\!\!\$\ D_i \\ x' \leftarrow \mathcal{A}(1^\lambda, i, x) \end{array}\right] \leq \mathsf{negl}(\lambda)$$

We will prove here that collision resistance is strictly stronger than second preimage resistance.

(a) Let H be a hash function family that satisfies collision resistance. Prove that H satisfies second preimage resistance.

(b) Let $H = \{h_i : \{0,1\}^{2\lambda} \to \{0,1\}^\lambda\}_{i \in I}$ be a hash function family that satisfies second preimage resistance. Construct a hash function family H', prove that it satisfies second preimage resistance, and prove that it does *not* satisfy collision resistance.