CS 276: Homework 2

Due Date: Monday, Mar 9, 2026 at 8:59pm via Gradescope

Usage of LLMs/Generative AI tools is prohibited. Other online resources (textbooks/lecture notes) are permissible.

1. **(Insecurity of Same-Seed UOWHF Composition.)**

   Let $\mathcal{H}^{2*,*} = \{h_s : \{0,1\}^{2*} \to \{0,1\}^*\}_{s\in\{0,1\}^*}$ be a $(2*,*)$-UOWHF. Recall that in Step IV of the UOWHF construction (construction 5.4 in the lecture notes), we use independent seeds $s_1, s_2, \ldots$ at each application. Consider instead the following simpler variant where we reuse the *same* seed and apply h_s twice (this can be extended to t applications):

   $$H_s(x) \;=\; h_s\big(h_s(x)\big),$$

   where $x \in \{0,1\}^{4n}$ and $H_s : \{0,1\}^{4n} \to \{0,1\}^n$. (Here h_s first compresses $4n$ bits to $2n$ bits, then $2n$ bits to n bits.)

   Show that even if $\mathcal{H}^{2*,*}$ is a secure UOWHF, the family $\mathcal{H} = \{H_s\}_{s\in\{0,1\}^*}$ is **not** necessarily a secure UOWHF. That is, describe a family $\{h_s\}$ that is a UOWHF but for which the above construction is insecure.

2. **(MAC Security over Vector Spaces.)**

   Let q be a prime with $q \geq 2^n$ and let $\mathbb{F}_q$ denote the field of integers modulo q. $[n]$ denotes the set of integers $\{1, \ldots, n\}$. Consider a MAC scheme where messages are *nonzero* vectors $\mathbf{m} \in \mathbb{F}_q^n \setminus \{\mathbf{0}\}$ and tags are elements $t \in \mathbb{F}_q$. We define the following security notion.

   Definition 0.1 *A* vector MAC scheme $\Pi = (\mathsf{Gen}, \mathsf{MAC}, \mathsf{Verify})$ *consists of:*

   (a) $k \leftarrow \mathsf{Gen}(1^n)$*: outputs a key* k*.*

   (b) $t \leftarrow \mathsf{MAC}(k, \mathbf{m})$*: on input key* k *and message* $\mathbf{m} \in \mathbb{F}_q^n \setminus \{\mathbf{0}\}$*, outputs a tag* $t \in \mathbb{F}_q$*.*

   (c) $0/1 \leftarrow \mathsf{Verify}(k, \mathbf{m}, t)$*: outputs 1 iff* t *is a valid tag for* $\mathbf{m}$*.*

   Definition 0.2 (Span-Forge Game: $\mathsf{SpanForge}_{\mathcal{A},\Pi}(n)$)

   (a) ***Setup:*** *The challenger samples* $k \leftarrow \mathsf{Gen}(1^n)$*.* $\mathcal{A}$ *is given* 1^n*.*

   (b) ***Queries:*** $\mathcal{A}$ *adaptively submits messages* $\mathbf{m}^{(1)}, \ldots, \mathbf{m}^{(q')} \in \mathbb{F}_q^n \setminus \{\mathbf{0}\}$*. For each query* $\mathbf{m}^{(i)}$*, the challenger returns* $t^{(i)} \leftarrow \mathsf{MAC}(k, \mathbf{m}^{(i)})$*.*

   (c) ***Forgery:*** $\mathcal{A}$ *outputs* $(\mathbf{m}^*, t^*)$*. The output of the game is 1 if:*

   $$\mathbf{m}^* \notin \mathrm{span}\{\mathbf{m}^{(1)}, \ldots, \mathbf{m}^{(q')}\} \quad \textit{and} \quad \mathsf{Verify}(k, \mathbf{m}^*, t^*) = 1.$$

   Definition 0.3 (Span-CMA Security) Π *is* Span-CMA-secure *if for all nu-PPT* $\mathcal{A}$*:* $\big|\Pr[\mathsf{SpanForge}_{\mathcal{A},\Pi}(n) = 1]\big| = \mathsf{negl}(n)$*.*

Construction. Let $F : \mathcal{K} \times [n] \to \mathbb{F}_q$ be a PRF. Define the vector MAC scheme Π as follows:

- $\mathsf{Gen}(1^n)$: Sample $k \xleftarrow{\$} \mathcal{K}$. Output k.
- $\mathsf{MAC}(k, \mathbf{m})$: Output $t = \sum_{i=1}^{n} m_i \cdot F(k, i) \in \mathbb{F}_q$.
- $\mathsf{Verify}(k, \mathbf{m}, t)$: Output 1 iff $t = \mathsf{MAC}(k, \mathbf{m})$.

(a) Prove that Π is Span-CMA-secure.

(b) Show that Π is **not** EUF-CMA-secure. That is, describe an efficient adversary that makes a single MAC query and produces a valid existential forgery.

(c) A natural attempt to fix the scheme is to add a constant term to break linearity. Consider the modified MAC:

$$\mathsf{MAC}'(k, \mathbf{m}) = F(k, 0) + \sum_{i=1}^{n} m_i \cdot F(k, i),$$

where $F(k, 0)$ is an additional PRF evaluation at a fixed input $0 \notin [n]$. Is MAC' EUF-CMA-secure? Justify your answer.