Fundamentals of Cryptography: Midterm

Wednesday Nov 8, 3-6PM

Problem 1 (1pt) Complete the definition of polynomial growth. For a functions $f : \mathbb{N} \to \mathbb{R}^+$. We say $f(n) = \text{poly}(n)$ if <u>fill the blank</u>.

Problem 2 (1pt) Complete the definition of negligible functions. A function $f : \mathbb{N} \to \mathbb{R}^+$ is *negligible*, if <u>fill the blank</u>.

Problem 3 (1pt) Complete the definition of strong unforgeability of MAC schemes. A MAC scheme $(\mathsf{Gen}, \mathsf{MAC}, \mathsf{Verify})$ is strongly secure if for any p.p.t. adversary $\mathcal{A}$, the adversary wins the following game with at most negligible probability:

- The challenger samples key $k \leftarrow \mathsf{Gen}(1^\lambda)$.
- $\mathcal{A}$ repeatedly queries the challenger. For $i = 1, 2$ upto $\text{poly}(\lambda)$, the adversary chooses a message m_i, and the challenger answers $t_i \leftarrow \mathsf{MAC}(k, m_i)$.
- <u>fill the blank (How does the game finish? When will the adversary win?)</u>.

Problem 4 (2pt) The assumption that PRGs exist is known to be equivalent to the assumption that <u>choose all correct answers</u>

(a) OWFs exist; (b) CRHFs exist; (c) PRFs and PRPs exist; (d) $P \neq NP$.

Problem 5 (2pt) <u>choose all correct answers</u>

(a) if $f : \{0,1\}^\lambda \to \{0,1\}^\lambda$ is a OWF, then $f'(x) = f(f(x))$ is also a OWF;
(b) if $h : \{0,1\}^\lambda \to \{0,1\}^{\lambda-1}$ is a CRHF, then $h'(x) = h(h(x))$ is also a CRHF;
(c) if $F : \{0,1\}^\lambda \times \{0,1\}^\lambda \to \{0,1\}^\lambda$ is a PRF, then $F'(k, x) = F(k, F(k, x))$ is also a PRF;
(d) if $F : \{0,1\}^\lambda \times \{0,1\}^\lambda \to \{0,1\}^\lambda$ is a PRP, then $F'(k, x) = F(k, F(k, x))$ is also a PRP.

Problem 6 (2pt) Sort the following security definitions, from weakest to strongest.

(a) CPA-security; (b) CCA1-security; (c) CCA2-security;
(d) indistinguishable encryptions in the presence of an eavesdropper.

Problem 7 (3pt) Let $h : \{0,1\}^{2\lambda} \to \{0,1\}^\lambda$ be a hash function. If h is a CRHF, then h must be a OWF. The statement can be proved by reduction. Assume there is a p.p.t. adversary $\mathcal{A}$ that inverts h with non-negligible probability, construct another p.p.t. adversary $\mathcal{B}$ that finds collision of h with non-negligible probability. State how $\mathcal{B}$ is constructed based on $\mathcal{A}$.

Problem 8 (3pt) Let $g : \{0,1\}^\lambda \to \{0,1\}^{\lambda+1}$ be a PRG. We can construct a length-doubling PRG $g' : \{0,1\}^\lambda \to \{0,1\}^{2\lambda}$ as

$g'(x^0)$ takes $x^0 \in \{0,1\}^\lambda$ as input;
For $i = 1, \ldots, \lambda$, computes $y_i \| x^i = g(x^{i-1})$, where $y_i \in \{0,1\}$ and $x^i \in \{0,1\}^\lambda$;
Outputs $y_1 \| y_2 \| \ldots \| y_\lambda \| x^\lambda$.

No p.p.t. distinguisher can distinguish between $g'(s)$ (when $s \leftarrow \{0,1\}^\lambda$) and a random 2λ-bit string with non-negligible probability.

We prove g' is a PRG using hybrid argument. State the hybrid worlds or hybrid distributions that are used in the proof.

Problem 9 (5pt) In the class, we have considered the CPA security of a private-key encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$. In this problem, we consider a generalized security definition.

For a given constant integer q, define q-challenge CPA attack. q-challenge CPA attack is a game defined between an adversary $\mathcal{A}$ and a challenger.

q-challenge CPA game $\mathrm{PrivK}_{\Pi,\mathcal{A}}^{q\text{-CPA}}(1^\lambda)$

- The challenger samples a key $k \leftarrow \mathsf{Gen}(1^\lambda)$. During the game, the adversary can always queries the encryption oracle using key k. That is, at any point during the game, the adversary can choose a message m and ask the challenger to return the encryption $\mathsf{Enc}(k, m)$.
- For $i = 1, \ldots, q$,

  The adversary chooses a pair of messages $m_{i,0}, m_{i,1}$ such that $|m_{i,0}| = |m_{i,1}|$.

  The challenger samples a random bit $b_i \leftarrow \{0,1\}$, and returns the encryption $c_i \leftarrow \mathsf{Enc}(k, m_{i,b_i})$.
- The adversary outputs its guesses $(b'_1, \ldots, b'_q)$.
- The game outputs 1 if and only if $(b'_1, \ldots, b'_q) = (b_1, \ldots, b_q)$.

We say that an encryption scheme Π is q-challenge CPA-secure, if for any p.p.t. adversary $\mathcal{A}$, there exists a negligible function ε such that

$$\Pr[\mathrm{PrivK}_{\Pi,\mathcal{A}}^{q\text{-CPA}}(1^\lambda) \to 1] \leq \frac{1}{2^q} + \varepsilon(\lambda).$$

Prove or disprove the following statement: for any constant q, any CPA-secure encryption scheme is also q-challenge CPA-secure.

Problem 10 (5pt) Let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a CPA-secure encryption scheme.

Part A Is $\mathsf{Enc}_A(k, m) = \mathsf{Enc}(k, \mathsf{Enc}(k, m))$ the encryption function of a CPA-secure encryption scheme? Formally, $\mathsf{Enc}_A(k, m)$ computes $c_1 \leftarrow \mathsf{Enc}(k, m)$, $c_2 \leftarrow \mathsf{Enc}(k, c_1)$ and outputs c_2.

Part B Is $\mathsf{Enc}_B((k_1, k_2), m) = \mathsf{Enc}(k_1, \mathsf{Enc}(k_2, \mathsf{Enc}(k_1, m)))$ the encryption function of a CPA-secure encryption scheme? Formally, $\mathsf{Enc}_B((k_1, k_2), m)$ computes $c_1 \leftarrow \mathsf{Enc}(k_1, m)$, $c_2 \leftarrow \mathsf{Enc}(k_2, c_1)$, $c_3 \leftarrow \mathsf{Enc}(k_1, c_2)$ and outputs c_3.

If the answer is negative, present a counter-example. If the answer is affirmative, state the reduction. In either case, you don't need to prove in detail why the counter-example or the reduction works.

Problem 11 (5pt) Let $F : \{0,1\}^\lambda \times \{0,1\}^\lambda \to \{0,1\}^\lambda$ be a secure PRF. Let F_{CBC} be the basic CBC-MAC (illustrated in Figure 1).

$$\begin{aligned} F_{\mathrm{CBC}}(k, (m_1, m_2, \ldots, m_\ell)) &:= \begin{cases} F(k, m_\ell \oplus F_{\mathrm{CBC}}(k, (m_1, m_2, \ldots, m_{\ell-1}))), & \text{if } \ell > 1 \\ F(k, m_1), & \text{if } \ell = 1 \end{cases} \\ &= F(k, m_\ell \oplus F(k, m_{\ell-1} \oplus \ldots F(k, m_2 \oplus F(k, m_1)) \ldots)). \end{aligned}$$

Is the following a strongly secure MAC scheme?

- $\mathsf{Gen}(1^\lambda)$ samples $k, k' \leftarrow \{0,1\}^\lambda$, outputs key (k, k').
- $\mathsf{MAC}((k, k'), m) = F_{\mathrm{CBC}}(k, (k' \| m \| k'))$. (For simplicity, we ignoring the padding, and assume the message length is always a multiple of λ.)
- Verify is automatically defined since MAC is deterministic.

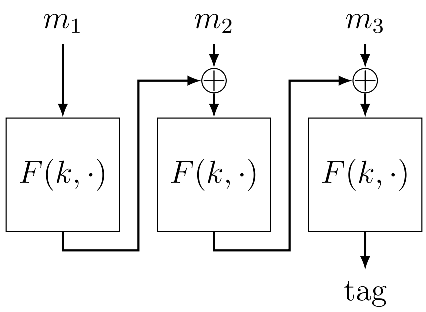

Figure 1: Basic CBC-MAC

Problem 12 (5pt) Given two hash functions $H_1, H_2 : \{0,1\}^{\ell(\lambda)} \to \{0,1\}^\lambda$ for fixed-length messages. Construct another hash function H for fixed-length messages based on H_1, H_2, such that H is a CRHF when either H_1 or H_2 is a CRHF.

Recall the definition of CRHF. A hash function $H : \{0,1\}^{\ell(\lambda)} \to \{0,1\}^\lambda$ is a CRHF (for fixed-length messages) if

- H is shrinking. $\ell(\lambda) > \lambda$.
- H is polynomial-time computable and $\ell(\lambda) = \mathrm{poly}(\lambda)$.
- H resists collision attack. For any p.p.t. adversary $\mathcal{A}$, the probability that $\mathcal{A}(1^\lambda)$ outputs two distinct messages $m_0, m_1 \in \{0,1\}^{\ell(\lambda)}$ such that $H(m_0) = H(m_1)$ is negligible.