


دانشکده‌ی علوم ریاضی

مقدمه‌ای بر رمزنگاری

آزمون میانترم

مدرّس: دکتر شهرام خزائی

تاریخ: ۱۳۹۹/۹/۲۳

Problem 1

Let F be a secure PRF. Define $\Pi = (\mathsf{Gen}, \mathsf{MAC}, \mathsf{Verify})$ that works on fixed-size messages of the form $m = m_1 m_2 ... m_l$ for $m_i \in \{0,1\}^n$, where

$$\mathsf{MAC}_k(m) := F_k(m_1) \oplus ... \oplus F_k(m_l)$$

and verification is canonical. Show that Π is insecure.

Problem 2

Say a public-key encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is a *homomorphic* encryption scheme if

- its message space forms a group $\mathbb{G}$ with operation $\odot$;
- there is a PPT algorithm Hom such that for $(pk, sk) \leftarrow \mathsf{Gen}(1^n)$, any $m_1, m_2 \in \mathbb{G}$, $c_1 \leftarrow \mathsf{Enc}_{pk}(m_1)$, $c_2 \leftarrow \mathsf{Enc}_{pk}(m_2)$, and $c \leftarrow \mathsf{Hom}(pk, c_1, c_2)$, we have $\mathsf{Dec}_{sk}(c) = m_1 \odot m_2$.

1. Show that the ElGamal encryption is homomorphic.
2. Show that homomorphic public-key encryption scheme cannot achieve CCA security.

Problem 3

Say a public-key encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ for n-bit messages is one-way if the probability $\Pr[\mathsf{PubK}^{\mathsf{ow}}_{\mathcal{A},\Pi}(n) = 1]$ is negligible for any PPT adversary $\mathcal{A}$. The experiment $\mathsf{PubK}^{\mathsf{ow}}_{\mathcal{A},\Pi}(n)$ is shown as follows.

- $\mathsf{Gen}(1^n)$ is run to obtain (pk, sk).

- A message m is chosen uniformly from $\{0,1\}^n$ and a ciphertext $c \leftarrow \mathsf{Enc}_{pk}(m)$ is generated.
- $\mathcal{A}$ is given (pk, c) and outputs m'.
- $\mathsf{PubK}^{\mathsf{ow}}_{\mathcal{A},\Pi}(n) = 1$ if $m' = m$.

1. Show that if a public-key encryption scheme Π for n-bit messages has CPA security, then Π is one-way.
2. Show that CPA security is strictly stronger than one-way security.
   Hint: Give a public-key encryption scheme example which has one-way security but does not have CPA security.
3. Construct a CPA secure KEM using one-way secure public-key encryption scheme in the random oracle model. Show your construction and proof ideas.