TMA4160 CRYPTOGRAPHY
NTNU, FALL 2021

EXAM (DECEMBER 2021)

Jiaxin Pan

Exercise 1:	25 points
Exercise 2:	5 points
Exercise 3:	7 points
Exercise 4:	23 points
Exercise 5:	12 points
Exercise 6:	28 points

Total: 100 points

Please make your choices for Exercises 1 and 2 in the Inspera system. Exercises 3 to 6 require hand-written answers.

Discretion is exercised when allocating points for Exercises 3 to 6.

Exercise 1. True or False (5 points each)

FOR EACH OF THE FOLLOWING STATEMENTS, DECIDE WHETHER IT IS **True (T)** OR **False (F)**. YOU DO NOT NEED TO PROVE YOUR CHOICE.

(1) Every pseudo-random function is a pseudo-random permutation.

ANSWER: *F*

(2) A semantically secure symmetric-key encryption scheme is not necessary CPA-secure (namely, secure against Chosen-Plaintext Attacks).

ANSWER: *T*

(3) Let H be a collision-resistant hash function. Then $H'(m) := \overline{H(m)}$ is collision-resistant as well.

($\overline{x}$ is bit-wise negation. For instance, $\overline{00101} = 11010$.)

ANSWER: *T*

(4) SHA-3 is a symmetric-key encryption scheme.

ANSWER: *F*

(5) Let $\mathbb{G} := \langle g \rangle$ be a cyclic of prime-order q. For all $x, y \in \mathbb{Z}_q$, $g^x \cdot g^y = g^{x+y}$.

ANSWER: *T*

Exercise 2. Multiple Choice (Negligible functions) (5 points)

Which of the following functions is negligible in λ?

(A) $f(\lambda) = 1/\lambda^{1024}$.

(B) $f(\lambda) = 2^{-\log_2(\lambda^8)}$.

(C) $f(\lambda) = 2^{-\log_2(\lambda)^2}$.

(D) $f(\lambda) = 2^{-\log_2(4^\lambda)}$.

ANSWER: *D*

Exercise 3. (7 points) *Let* $\Pi = (Gen, Enc, Dec)$ *be a symmetric-key encryption scheme. Assume* Π *has the following property: for all* $m \in \mathcal{M}$ *and* $k \in \mathcal{K}$

$$Enc(k, Enc(k, m)) = m$$

holds. Show that Π *is not CPA-secure.*

ANSWER: *The attacker* $\mathcal{A}$ *first asks an encryption query for* (m_0, m_1) *and* $m_0 \neq m_1$*, and let the answer be* c^**. After that,* $\mathcal{A}$ *asks another encryption query for* (c^*, c^*)*. By the equation in the exercise,* $\mathcal{A}$ *gets back* m_b *from which it learns* b*.*

Exercise 4. (23 points) *Let* $L \in \mathbb{N}$ *and* $F_k : \{0,1\}^L \to \{0,1\}^L$ *be a pseudo-random function.* $\lambda \in \mathbb{N}$ *is the security parameter. We construct the following symmetric-key encryption* $\Pi = (Gen, Enc, Dec)$ *with message space* $\mathcal{M} = \{0,1\}^{2L}$*:*

- $Gen(1^\lambda)$*: Return a random key* k*.*
- $Enc(k, m)$*: Return* $c := (F_k(0^\lambda), F_k(1^\lambda)) \oplus m$*.*

(1) (6 points) Describe the decryption algorithm $Dec(k, c)$ *and show its correctness.*

(2) (5 points) Give the definition of a pseudo-random function.

(3) (5 points) Is this encryption semantically secure? Why?
*(**Hints**: You don't need to give a detailed proof, but a few sentences to briefly justify your claim should be enough.)*

(4) (7 points) Π *is not CPA secure. Give a successful CPA attack on it.*

ANSWER:

(1) $Dec(k, c)$*: Return* $m = c \oplus (F_k(0^\lambda), F_k(1^\lambda))$*. The correctness is because for all keys* k *and all* $m \in \{0,1\}^{2L}$ *we have*

$$Enc(k, m) \oplus (F_k(0^\lambda), F_k(1^\lambda)) = ((F_k(0^\lambda), F_k(1^\lambda)) \oplus m) \oplus (F_k(0^\lambda), F_k(1^\lambda)) = m$$

(2) Cf. Attack Game 4.2 in the textbook BS.

(3) Yes, this is semantically secure, since $G(k) := (F_k(0^\lambda), F_k(1^\lambda))$ *can be viewed as a PRG.*

(4) The same as the CPA attack on the stream cipher in the lecture: The attacker first asks for an encryption query of $m_0, m_1 (m_0 \neq m_1)$ *and gets back* c_1^**; and the second query of the attack is* m_0, m_0 *and the attacker gets back* c_2^**. If* $c_1^* = c_2^*$ *then the challenge bit* $b = 0$*; otherwise* $b = 1$*.*

Exercise 5. (Textbook RSA) (12 points)

(1) *(5 points) Show that the Textbook RSA signature scheme is not UF-CMA secure.*

(2) *(7 points) Consider the following Double Textbook RSA signature scheme:*

- $Gen(1^\lambda)$: *Choose two large primes* p, q *and compute* $N := p \cdot q$. *Choose two random* $e_1, e_2 \overset{\$}{\leftarrow} \mathbb{Z}^*_{\phi(N)}$ *and compute* $d_1 := e_1^{-1} \bmod \phi(N)$ *and* $d_2 := e_2^{-1} \bmod \phi(N)$. *Return* $pk := (N, e_1, e_2)$ *and* $sk := (d_1, d_2)$. *Here* ϕ *is the Euler totient function.*
- $Sign(sk, m)$: *Return* $(\sigma_1, \sigma_2) := (m^{d_1} \mod N, m^{d_2} \mod N)$.
- $Ver(pk, m, (\sigma_1, \sigma_2)) := \begin{cases} 1 & \text{if } {\sigma_1}^{e_1} = {\sigma_2}^{e_2} = m \mod N \\ 0 & \text{otherwise.} \end{cases}$

Show that the Double Textbook RSA signature is also not UF-CMA secure.

ANSWER:

(1) *(This is just one of many attacks on textbook RSA) The attacker* $\mathcal{A}$ *asks for a signing query of* m *and gets back* $\sigma = m^d \bmod N$. $\mathcal{A}$ *chooses an* $1 \neq x \in \mathbb{Z}_N^*$ *and return* $(m^*, \sigma^*) := (m \cdot x^e \bmod N, \sigma \cdot x \bmod N)$ *as its forgery. Note that* $m \cdot x^e \bmod N \neq m$ *and* σ^* *is a valid signature of* m^* *(since* $(\sigma^*)^e = m \cdot x^e \bmod N$*).*

(2) *The same idea from (1) also works for the Double Textbook RSA.*

Exercise 6. (28 points) *Let $\mathbb{G} := \langle g_1 \rangle$ be a cyclic of prime-order q. Here the group description of $\mathbb{G}$ is publicly known. Consider the following public-key encryption scheme $\Psi := (Gen, Enc, Dec)$ for message space $\mathcal{M} := \mathbb{G}$.*

- *$Gen(1^\lambda)$: Choose random elements $t, a_1, a_2 \xleftarrow{\$} \mathbb{Z}_q$. We require that $t \neq 0$. Compute $g_2 := g_1^t$ and $h := g_1^{a_1} \cdot g_2^{a_2}$. Define $pk := (g_2, h)$ and $sk := (a_1, a_2)$. Return (pk, sk).*
- *$Enc(pk, m)$: Choose a random $r \xleftarrow{\$} \mathbb{Z}_q$. Compute $C_1 := g_1^r$, $C_2 := g_2^r$, and $C_3 := h^r \cdot m$. Return the ciphertext (C_1, C_2, C_3).*

(1) (5 points) Describe the decryption algorithm Dec and show its correctness.

*(2) (5 points) Show that this PKE Ψ is malleable. More precisely, show that, given a ciphertext (C_1, C_2, C_3) of message m and another message m', one can publicly generate an encryption of message $m \cdot m'$ **without** decrypting (C_1, C_2, C_3).*

(3) (5 points) Show that Ψ is homomorphic. More precisely, given two ciphertexts (C_1, C_2, C_3) and (C_1', C_2', C_3') of messages m and m', respectively, show how to compute another ciphertext that can be decrypted to $m \cdot m'$.

(4) Ψ is semantically secure (namely, CPA security with only one encryption query). This exercise corresponds to the proof about that:

(a) (4 points) Given only $sk \in \mathbb{Z}_q^2$, $C_1 \in \mathbb{G}$, $C_2 \in \mathbb{G}$ and a message $m \in \mathbb{G}$, how to compute C_3 such that (C_1, C_2, C_3) can be decrypted to m?

(b) (9 points) Show that, under the DDH (aka Decisional Diffie-Hellman) assumption, Ψ is semantically secure.

*(**Hints**: You should find a way to put a DDH instance (g_1^x, g_1^y, g_1^z) into pk and the challenge ciphertext. Then show that if $z = x \cdot y$ then the simulated distribution is the same as in the real scheme; and if $z \in \mathbb{Z}_q$ is random, then the challenge ciphertext is random.)*

ANSWER:

(1) $Dec(sk, (C_1, C_2, C_3))$: Return $m = C_3/(C_1^{a_1} \cdot C_2^{a_2})$. The correctness is because for all $((g_2, h), (a_1, a_2))$ generated by Gen and all message $m \in \mathbb{G}$:

$$(C_1^{a_1} \cdot C_2^{a_2}) = g_1^{ra_1} g_2^{ra_2} = (g_1^{a_1} g_2^{a_2})^r = h^r.$$

Thus, $C_3/(C_1^{a_1} \cdot C_2^{a_2}) = (m \cdot h^r)/(h^r) = m$.

(2) Ciphertext $C' := (C_1, C_2, C_3 \cdot m')$ is the required ciphertext. Since $(C_3 \cdot m')/(C_1^{a_1} \cdot C_2^{a_2}) = m \cdot m'$.

(3) Ciphertext $\hat{C} := (C_1 \cdot C_1', C_2 \cdot C_2', C_3 \cdot C_3')$ is the required ciphertext, since $\hat{C} = (g_1^{r+r'}, g_2^{r+r'}, h^{r+r'} \cdot m \cdot m')$ where $C = (g_1^r, g_2^r, h^r \cdot m)$ and $C' = (g_1^{r'}, g_2^{r'}, h^{r'} \cdot m')$.

(4) Use one of the previous two exercises to present the attack.

(5) (a) $C_3 = (C_1^{a_1} C_2^{a_2}) \cdot m$

(b) In Gen, the reduction $\mathcal{B}$ chooses a challenge bit $b \xleftarrow{\$} \{0,1\}$ and chooses $a_1, a_2 \xleftarrow{\$} \mathbb{Z}_q$ and embeds $g_2 := g_1^x$. For the challenge ciphertext, $\mathcal{B}$ defines $C_1 := g_1^y, C_2 := g_1^z$ and computes $C_3 = (C_1^{a_1} C_2^{a_2}) \cdot m_b$.

- *If $z = xy$, then the simulation is exactly the same as in the real scheme.*
- *But if z is random, C_2 is random and $(C_1^{a_1} C_2^{a_2})$ is also random. The reason is: Let*

$$F(a_1, a_2) := \underbrace{\begin{pmatrix} g_1 & g_2 = g_1^x \\ C_1 = g_1^y & C_2 = g_1^z \end{pmatrix}}_{=:\mathbf{M}} \cdot \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} h \\ C_1^{a_1} C_2^{a_2} \end{pmatrix}.$$

If $z \neq xy$, then $\mathbf{M}$ is a full-rank 2×2 matrix. So, F is bijective and the random a_1, a_2 imply $\begin{pmatrix} h \\ C_1^{a_1} C_2^{a_2} \end{pmatrix}$ is random.