TMA4160 CRYPTOGRAPHY
NTNU, FALL 2022

EXAM (NOVEMBER 2022)

Jiaxin Pan

Exercise 1:	15 points
Exercise 2:	5 points
Exercise 3:	18 points
Exercise 4:	13 points
Exercise 5:	25 points
Exercise 6:	24 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. Secure or Not (5 points each)

*Let $F : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ be a pseudorandom function (PRF). For each of the following symmetric-key encryption schemes, decide whether it is CPA secure **(S)** or not **(N)**. Note that the secret key to each scheme is a PRF key k chosen uniformly at random from $\mathcal{K}$. You do not need to prove your choice.*

(1) To encrypt $m \in \{0,1\}^n$, output the ciphertext $m \oplus F_k(0^n)$. As pointed out in the lecture, 0^n means n-bit string with all zero.

SUGGESTION FOR ANSWERS: *N. This is a stream cipher.*

(2) To encrypt $m := (m_1, m_2) \in \{0,1\}^{2n}$ where $|m_1| = |m_2| = n$, choose a random bit-string r in $\{0,1\}^n$ and output $(r, m_1 \oplus F_k(r), m_2 \oplus F_k(r))$

SUGGESTION FOR ANSWERS: *N. Because by xor-ing $(m_1 \oplus F_k(r)) \oplus (m_2 \oplus F_k(r)) = m_1 \oplus m_2$ the adversary can get $m_1 \oplus m_2$.*

(3) To encrypt $m := (m_1, m_2) \in \{0,1\}^{2n}$ where $|m_1| = |m_2| = n$, choose a random bit-string r in $\{0,1\}^n$ and output $(r, m_1 \oplus F_k(r), m_2 \oplus F_k(r \oplus m_1))$

SUGGESTION FOR ANSWERS: *N. Because an adversary can query two messages $(m_1 = 0^n, m_2)$ and $(m_1 = 1^n, m_2)$. For the first message, the ciphertext is $(r, F_k(r), m_2 \oplus F_k(r))$. An adversary can distinguish which one is encrypted.*

Grading Note: *For each sub-exercise, a candidate gets either 0 or 5 points.*

Exercise 2. (5 points) *Let* $\Pi = (Gen, Enc, Dec)$ *be a symmetric-key encryption scheme. Which of the following symmetric-key encryption schemes has the following property: for all* $m \in \mathcal{M}$ *and* $k \in \mathcal{K}$

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

There can be more than one correct choice.

(a) One-time pad;
(b) An authenticated encryption;
(c) Stream cipher.

SUGGESTION FOR ANSWERS: a,c
Grading Note: A candidate gets either 0 or 5 (makes all the correct choices) points.

Exercise 3. ***Square Diffie-Hellman*** (3+10+5=18 points)

Consider the following Computational Square Diffie-Hellman (SqCDH) problem for a cyclic group $\mathbb{G} := \langle g \rangle$ with prime-order q: Given $(\mathbb{G}, q, g, g^x)$ for a randomly chosen x in $\mathbb{Z}$, an adversary is asked to compute g^{x^2}. The SqCDH assumption states that it is hard for any probabilistic polynomial time adversary to solve the SqCDH problem.

(1) Define the Computational Diffie-Hellman (CDH) assumption.

(2) Show that the SqCDH assumption implies the CDH assumption, namely, if there is an adversary can efficiently solve the CDH problem, we can construct a reduction to solve the SqCDH problem.

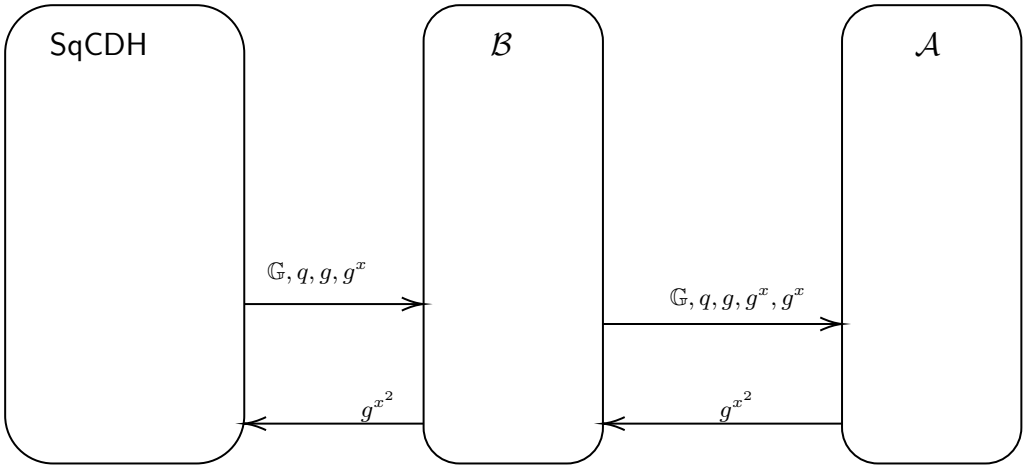
***(Hints)** It is sufficient to draw the reduction as we have done in the lecture.*

(3) What is the relation between the Discrete Logarithm (DLog) assumption and the SqCDH assumption?

SUGGESTION FOR ANSWERS:

(1) Computational Diffie-Hellman (CDH) problem for a cyclic group $\mathbb{G} := \langle g \rangle$ with prime-order q: Given $(\mathbb{G}, q, g, g^x, g^y)$ for randomly chosen x, y in $\mathbb{Z}$, an adversary is asked to compute g^{xy}. The CDH assumption states that it is hard for any probabilistic polynomial time adversary to solve the CDH problem.

(2) Let $\mathcal{A}$ be the attacker for CDH and $\mathcal{B}$ be the reduction against the SqCDH assumption.



(3) The SqCDH assumption implies the DLog assumption, since if an adversary can compute x from g^x then we can use x to compute g^{x^2} to break the SqCDH assumption. The other direction is unclear.

Grading Note: (3): 5 points are given as long as it is said that the SqCDH assumption implies the DLog assumption

Exercise 4. (MAC) (5+8=13 points)

Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ *be a pseudorandom function. Consider the following message authentication code (MAC) scheme* $\Pi = (Gen, Tag, Ver)$ *for messages* $m \in \{0,1\}^{\ell\cdot(n/2)}$ *where integer* ℓ *is smaller than* $2^{n/2}$*:*

- Gen*: Choose a random* k *from* $\{0,1\}^n$*, and return* k
- $\mathsf{Tag}(k,m)$*: Choose a random* r *from* $\{0,1\}^n$ *and return*

$$t := \Big(r, F_k(r) \oplus F_k(\langle 1\rangle, m_1) \oplus \cdots \oplus F_k(\langle \ell\rangle, m_\ell)\Big) \in \{0,1\}^n \times \{0,1\}^n$$

where $m := (m_1, \ldots, m_\ell)$ *for* $m_i \in \{0,1\}^{n/2}$ *and* $\langle i\rangle$ *is a* $n/2$*-bit representation of* i*. For example,* $\langle 1\rangle = 000\ldots1$.

(1) Describe the verification algorithm, Ver*, and show its correctness.*

(2) Give an attack to show that Π *is* <u>*not*</u> *a secure MAC in the sense of unforgeability against chosen-message attacks (UF-CMA).*

(Hints) *The chosen-message attack may not be necessary here, namely, an adversary can successfully forge without seeing any valid MAC tag on a message.*

SUGGESTION FOR ANSWERS:

(1) To verify a tag $t := (t_1, t_2)$ for message m, $Ver(k, m, t)$ check if

$$t_2 = F_k(t_1) \oplus F_k(\langle 1\rangle, m_1) \oplus \ldots F_k(\langle \ell\rangle, m_\ell).$$

For all keys k and all messages m,

$$t := \Big(t_1 = r, t_2 = F_k(r) \oplus F_k(\langle 1\rangle, m_1) \oplus \cdots \oplus F_k(\langle \ell\rangle, m_\ell)\Big) \xleftarrow{\$} \mathsf{Tag}(k, m)$$

For this tag, we have $t_2 = F_k(t_1) \oplus F_k(\langle 1\rangle, m_1) \oplus \ldots F_k(\langle \ell\rangle, m_\ell)$

(2) (There can be multiple attacks on it. Points will be given as long as it is correct.) Choose any message m' from $\{0,1\}^{n/2}$ and $t' := ((\langle 1\rangle, m'), 0^n)$ is a valid MAC tag on message m', since in this case $r = (\langle 1\rangle, m')$ and $m_1 = m'$ and

$$F_k(r) \oplus F_k(\langle 1\rangle, m_1) = F_k(\langle 1\rangle, m') \oplus F_k(\langle 1\rangle, m') = 0^n$$

Grading Note: There may be different ways to attack this MAC scheme. As long as your answer is sound, full scores will be given.

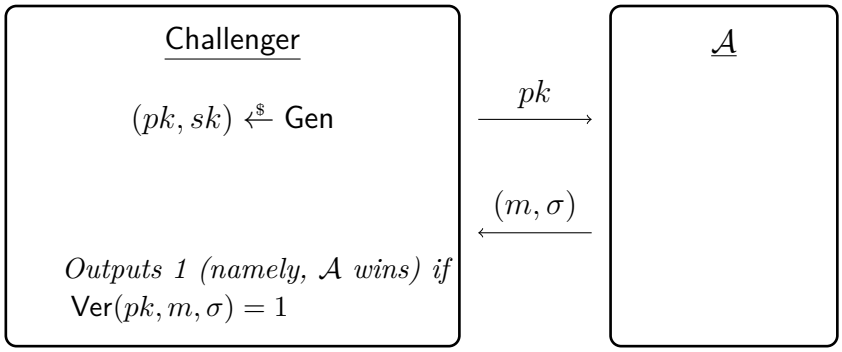
Exercise 5. (5+12+8=25 points)

Let $\mathbb{G} := \langle g \rangle$ be a cyclic group of prime order q. For simplicity, assume the group description such as g and q are publicly known. Consider the following signature scheme:

- Gen*: Choose a random x from $\mathbb{Z}_q^*$, and compute $X := g^x$. Return $pk := X, sk = x$. Here the signing message space $\mathcal{M} = \mathbb{Z}_q^*$.*
- $\mathsf{Sign}(sk, m)$*: $\sigma = xm \in \mathbb{Z}_q^*$.*
- $\mathsf{Ver}(pk, m, \sigma)$*: Return* $\begin{cases} 1 & \text{if } g^\sigma = X^m \\ 0 & \text{else.} \end{cases}$

(1) Show the correctness of this signature scheme.

(2) Let $\mathcal{A}$ be an adversary. Define the following security, unforgeability against key-only attack (UF-KOA) for a signature scheme $\Pi = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Ver})$.



Essentially, this is a weaker variant of UF-CMA security by not allowing $\mathcal{A}$ to ask any signing query.

Π is called UF-KOA security, if for all PPT adversary $\mathcal{A}$,

$$\Pr[\mathcal{A} \text{ wins}] \leq negl.$$

The probability space is the random coins of $\mathcal{A}$ and Challenger*.*

Show the given signature scheme is UF-KOA secure if the discrete logarithm assumption holds with respect to $\mathbb{G}$.

(3) Is this signature unforgeability against chosen-message attacks (namely, UF-CMA secure)? Why?

SUGGESTION FOR ANSWERS:

(1) For all $m \in \mathbb{Z}_q^*$, and all (pk, sk) generated by Gen, we have

$$\mathsf{Ver}(pk, m, \mathsf{Sign}(sk, m)) = \mathsf{Ver}(pk, m, xm) = 1$$

since $g^{xm} = X^m = pk^m$

(2) We only give some key points in the proof here. Given a DLog instance, g^x. We define the signature public key to be g^x. Upon (m, σ), Challenger checks if $g^\sigma = X^m$. This implies $\sigma = xm$. Since Challenger knows $m \neq 0$, it can recover $x := \sigma/m$

(3) (There can be multiple attacks on it. Points will be given as long as it is correct.) No, because adversary $\mathcal{A}$ can choose a message $m' \neq 0$ and ask a signature for it, denoted

by σ'. Here $\sigma' = xm'$, since $g^{\sigma'} = X^{m'}$. Now $\mathcal{A}$ can recover the secret key by computing $x := \sigma'/m'$.

Grading Note:

(2) Partial points will be given if it is correctly stated where g^x is embedded or how to compute the discrete log, x.

(3) As long as the attack is sound, points will be given.

Exercise 6. (5+7+7+5=24 points)

Suppose t people publish their public-keys $(pk_1, ..., pk_t)$. Alice sends an encrypted message to one of them, say pk_5, but she wants to ensure that no one (other than user 5) can tell which of the t users is the intended recipient. You may assume that every user, other than user 5, who tries to decrypt Alice's message with their secret key, obtains fail.

(1) Define a security model that captures this requirement in a simple setting with 2 users. The adversary will be given 2 distinct public keys (pk_1, pk_2), and it then selects the message m and sends it to the challenger. Upon receiving a challenge ciphertext from the challenger, the adversary should learn nothing about which of the public keys that is used to encrypt. A system that has this property is said to be an anonymous public-key encryption scheme.

***(Hints)** The most important is to write down the security game in the style of our lecture.*

(2) Show that the semantically secure RSA PKE scheme is not anonymous. Assume that all the public keys are generated using the same RSA parameters ℓ and e.

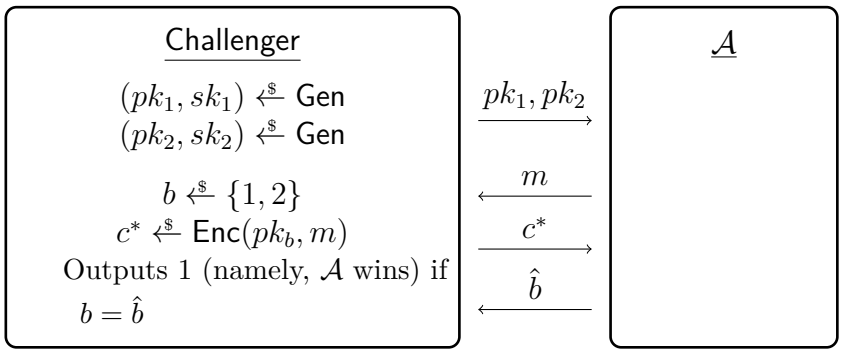
***(Hints)** Recall the ciphertext has the form $(c', c'') = (r^e \bmod N, H(r) \oplus m)$ where r is chosen randomly from $\mathbb{Z}_N$*

(3) Is the semantically secure Hashed ElGamal PKE scheme (as in Section 11.5 of BS) anonymous? Please briefly justify your answer.

(4) What is the relation between semantic security and anonymous security? Please briefly justify your answer.

SUGGESTION FOR ANSWERS:

(1) See the following:



(2) Imagine the public keys are $pk_1 = (N_1, e)$ and $pk_2 = (N_2, e)$ and $N_1 < N_2$. Recall the challenge ciphertext as $c^* = (c', c'')$. Here c' is either equal to $x^e \bmod N_1 \in \mathbb{Z}_{N_1}$ or $x^e \bmod N_2 \in \mathbb{Z}_{N_2}$ depending on which public key is used to encrypt. If $c' > N_1$ then the adversary bets c^* is generated with pk_2; otherwise with pk_1. With non-negligible probability the adversary will win.

Another attack can assume that c' is represented in different bit-lengths depending on the size of N_1 or N_2. In this case, an adversary can only look at the bit-length to break the scheme's anonymity.

(3) Yes, it is anonymous. If the CDH assumption holds, given a public key g^x, an adversary cannot decide if a hashed ElGamal ciphertext $(g^r, E_s(H(g^r, (g^x)^r), m))$ belongs to public key g^x.

(4) They are independent. Because Exercise (2) shows that semantic security does not imply anonymous security. For the other direction, imagine a PKE whose encryption algorithm just outputs the input message as the ciphertext. It is clearly not semantically secure, but it is anonymous.

Grading Note:

(2) This exercise is a bit open-ended. The key point here is to decide whether c' in $\mathbb{Z}_{N_1}$ or $\mathbb{Z}_{N_2}$. As long as this is mentioned, we will give all the points.

(3) If someone uses the (plain) ElGamal or the hashed ElGamal in the lecture (namely, g^r is not included in the hash) to do this exercise, full score will be given, as long as the answer is sound. Actually, the same argument holds for these scheme as well. Only that, for the plain ElGamal, we require the DDH assumption.