Advanced Cryptography — Final Exam

Serge Vaudenay

25.6.2025

- duration: 3h
- any document allowed
- a pocket calculator is allowed
- communication devices are not allowed
- it is not allowed to write with a pencil
- it is not allowed to use the red color
- the exam invigilators will **not** answer any technical question during the exam
- readability and style of writing will be part of the grade

1 Damgård's ElGamal Encryption

We define the following variant of the ElGamal cryptosystem. We assume a constant c. The key generation is an algorithm $\mathsf{Gen}(1^s) \to (\mathsf{pp}, G, G_1, G_2, H, x_1, x_2)$. It sets up some public parameters pp which include the security parameter s, some group parameters (allowing to make additive group operations), and the order q of the group (which is a prime number). It also generates uniformly three generators G, G_1, G_2 of the group, two scalars x_1 and x_2 in $\mathbf{Z}_q$, and $H = x_1G_1 + x_2G_2$. The public key is $\mathsf{pk} = (\mathsf{pp}, G, G_1, G_2, H)$ and the secret key is $\mathsf{sk} = (\mathsf{pp}, G, x_1, x_2)$. Algorithms are polynomially bounded in terms of s. The message space is $\{0, 1, \ldots, s^c - 1\}$. Encryption consists of picking a random $r \in \mathbf{Z}_q^*$ and setting

$$\mathsf{Enc}(\mathsf{pk}, m; r) = (mG + rH, rG_1, rG_2)$$

The decryption algorithm $\mathsf{Dec}(\mathsf{sk}, C_0, C_1, C_2)$ returns either m or an error $\perp$.

Q.1 Explain how decryption works and what is its complexity.

Q.2 We consider the $\mathsf{INDCCA1}$ security which is defined by the following game.

Game $\Gamma_{\mathsf{INDCCA1}}(1^s, b)$
1: $\mathsf{Gen}(1^s) \to (\mathsf{pk}, \mathsf{sk})$
2: $\mathcal{A}^{\mathsf{ODec}}(\mathsf{pk}) \to (m_0, m_1, \mathsf{st})$
3: $\mathsf{Enc}(\mathsf{pk}, m_b; r) \to (C_0, C_1, C_2)$
4: $\mathcal{A}(\mathsf{st}, C_0, C_1, C_2) \to z$
5: **return** z

Oracle $\mathsf{ODec}(D_0, D_1, D_2)$
6: **return** $\mathsf{Dec}(\mathsf{sk}, D_0, D_1, D_2)$

The oracle $\mathsf{ODec}(\mathsf{input})$ which returns the result of $\mathsf{Dec}(\mathsf{sk}, \mathsf{input})$.

Define the advantage of $\mathcal{A}$.
What is the difference with the normal INDCCA game?
Prove that the cryptosystem is not INDCCA secure.

Q.3 Prove that the advantage in the $\mathsf{INDCCA1}$ game is equal to the advantage of the following game.

Game $\Gamma_1(1^s, b)$

1: $\mathsf{Gen}(1^s) \to (\mathsf{pp}, G, G_1, G_2, H, x_1, x_2)$
2: $\mathcal{A}^{\mathsf{ODec}}(\mathsf{pp}, G, G_1, G_2, H) \to (m_0, m_1, \mathsf{st})$
3: pick $r \in \mathbf{Z}_q^*$, set $C_1 = rG_1$, $C_2 = rG_2$, $C_0 = m_b G + x_1 C_1 + x_2 C_2$
4: $\mathcal{A}(\mathsf{st}, C_0, C_1, C_2) \to z$
5: **return** z

Q.4 We consider the following game.

Game $\Gamma_2(1^s, b)$

1: $\mathsf{Gen}(1^s) \to (\mathsf{pp}, G, G_1, G_2, H, x_1, x_2)$
2: $\mathcal{A}^{\mathsf{ODec}}(\mathsf{pp}, G, G_1, G_2, H) \to (m_0, m_1, \mathsf{st})$
3: pick $r, r' \in \mathbf{Z}_q^*$, set $C_1 = rG_1$, $C_2 = r'G_2$
4: $C_0 = m_b G + x_1 C_1 + x_2 C_2$
5: $\mathcal{A}(\mathsf{st}, C_0, C_1, C_2) \to z$
6: **return** z

Formulate a standard security assumption under which the difference of the advantages of Γ_1 and Γ_2 is negligible.

Q.5 Prove that $\Gamma_2(1^s, b)$ and the following game $\Gamma_3(1^s, b)$ give the same advantages.

Game $\Gamma_3(1^s, b)$

1: generate (pp, G, G_1) like with Gen
2: pick $\omega \in \mathbf{Z}_q^*$
3: pick $z, x_2 \in \mathbf{Z}_q$
4: set $x_1 = z - x_2\omega$
5: set $G_2 = \omega G_1$ and $H = zG_1$
6: $\mathcal{A}^{\mathsf{ODec}}(\mathsf{pp}, G, G_1, G_2, H) \to (m_0, m_1, \mathsf{st})$
7: pick $r, r' \in \mathbf{Z}_q^*$, set $C_1 = rG_1$, $C_2 = r'G_2$
8: $C_0 = m_b G + rH + x_2(r' - r)G_2$
9: $\mathcal{A}(\mathsf{st}, C_0, C_1, C_2) \to z$
10: **return** z

Q.6 Given an index i, we define the game Γ_i' as follows.

Game $\Gamma_i'(1^s, b)$

1: generate (pp, G, G_1) like with Gen
2: pick $\omega \in \mathbf{Z}_q^*$
3: pick $z, x_2 \in \mathbf{Z}_q$
4: set $x_1 = z - x_2\omega$
5: set $G_2 = \omega G_1$ and $H = zG_1$
6: set $\mathsf{ct} = 0$
7: $\mathcal{A}^{\mathcal{O}}(\mathsf{pp}, G, G_1, G_2, H) \to (m_0, m_1, \mathsf{st})$
8: pick $r, r' \in \mathbf{Z}_q^*$, set $C_1 = rG_1$, $C_2 = r'G_2$
9: $C_0 = m_b G + rH + x_2(r' - r)G_2$
10: $\mathcal{A}(\mathsf{st}, C_0, C_1, C_2) \to z$

11: **return** z

Oracle $\mathcal{O}(D_0, D_1, D_2)$
12: increment ct
13: **if** $\mathsf{ct} > i$ **then**
14: **return** $\mathsf{Dec}(\mathsf{pp}, G, x_1, x_2, D_0, D_1, D_2)$
15: **else**
16: **if** $D_2 \neq \omega D_1$ **then return** $\perp$
17: **if** $D_1 = 0$ **then return** $\perp$
18: set $M = D_0 - zD_1$
19: find the discrete logarithm m of M in the message space (set $m = \perp$ if none)
20: **return** m
21: **end if**

Prove that $\Gamma'_0(1^s, b)$ gives the same advantage as $\Gamma_3(1^s, b)$. Further define an event Bad_i which can occur during the execution of the games and such that $\Pr[\Gamma'_{i-1} \to 1 | \neg\mathsf{Bad}_i] = \Pr[\Gamma'_i \to 1 | \neg\mathsf{Bad}_i]$.

Q.7 Prove that $\Pr[\mathsf{Bad}_i] \leq \frac{s^c}{q}$. Deduce that the difference between the advantages given by Γ'_{i-1} and Γ'_i is negligible.
Hint: when is the first time x_2 is used?

Q.8 Prove that there exists some polynomial $Q(s)$ such that the game $\Gamma'_{Q(s)}$ gives the advantage bounded by $\frac{1}{q}$.

2 PMAC Security via Tweakable Block Ciphers

A tweakable block cipher is a function pair defined by a block space $\{0,1\}^\ell$, a key space $\mathcal{K}$, and a tweak space $\mathcal{T}$. The functions are $\pi : \mathcal{K} \times \mathcal{T} \times \{0,1\}^\ell \to \{0,1\}^\ell$ and $\pi^{-1} : \mathcal{K} \times \mathcal{T} \times \{0,1\}^\ell \to \{0,1\}^\ell$. (The second function is denoted π^{-1} by abuse of notation. By abuse of notation, we also say that π is the tweakable block cipher.) They must be such that for every $k \in \mathcal{K}$ and $t \in \mathcal{T}$, the functions $x \mapsto \pi(k, t, x)$ and $y \mapsto \pi^{-1}(k, t, y)$ are permutations over $\{0,1\}^\ell$ which are inverse of each other. For more readability, we denote $\pi^t_k(x) = \pi(k, t, x)$.

Given an adversary $\mathcal{A}$ interacting with an oracle $\mathcal{O} : \mathcal{T} \times \{0,1\}^\ell \to \{0,1\}^\ell$, we define

$$\mathsf{Adv}^{\mathsf{PRP}}_\pi(\mathcal{A}) = \Pr[\mathsf{PRP}_\pi(\mathcal{A}, 1) \to 1] - \Pr[\mathsf{PRP}_\pi(\mathcal{A}, 0) \to 1]$$

where $\mathsf{PRP}_\pi(\mathcal{A}, b)$ is the following game.

Game $\mathsf{PRP}_\pi(\mathcal{A}, b)$
1: pick $k \in \mathcal{K}$ at random
2: pick a random function Π from $\mathcal{T}$ to the set of permutations of $\{0,1\}^\ell$
3: $\mathcal{A}^{\mathcal{O}} \to z$
4: **return** z

Oracle $\mathcal{O}(t, x)$:
5: **if** $b = 1$ **then**
6: **return** $\pi^t_k(x)$
7: **else**
8: **return** $(\Pi(t))(x)$
9: **end if**

In what follows, we assume that $\{0,1\}^\ell$ is given a field structure with addition $\oplus$ and multiplication. We also consider an injective function mapping $t \in \mathcal{T}$ to a nonzero field element α_t.

Given a block cipher $C : \mathcal{K} \times \{0,1\}^\ell \to \{0,1\}^\ell$, we define $\pi = \mathsf{XE}_C$ the tweakable block cipher by

$$\pi_k^t(x) = C_k\left(x \oplus \alpha_t \cdot C_k(0)\right)$$

Below, we define a (simplified) version of PMAC. We consider the message space $\mathcal{M}$ of finite sequences of blocks in $\{0,1\}^\ell$ with a number of blocks bounded by B, and $\mathcal{T} = \{1,\ldots,B\} \times \{2,3\}$. We let $\pi = \mathsf{XE}_C$ and

$$\mathsf{PMAC}(k,(x_1,\ldots,x_n)) = \pi_k^{n,3}\left(\pi_k^{1,2}(x_1) \oplus \cdots \oplus \pi_k^{n-1,2}(x_{n-1}) \oplus x_n\right)$$

with $n \leq B$. That is, the inner tweaks are pairs $t = (i,2)$ with i being the block index and the outer tweak is the pair $t = (n,3)$ with n being the number of blocks. If we denote $L = C_k(0)$ and $\Delta_t = \alpha_t \cdot L$, we have

$$\mathsf{PMAC}(k,(x_1,\ldots,x_n)) = C_k\left(C_k(x_1 \oplus \Delta_{1,2}) \oplus \cdots \oplus C_k(x_{n-1} \oplus \Delta_{n-1,2}) \oplus x_n \oplus \Delta_{n,3}\right)$$

With the tag length ℓ, a complete last block x_n, and an appropriate definition for α_t, this is the standard PMAC authentication code.

Q.1 When $\mathcal{T}$ has a single element, prove that a tweakable block cipher π over the tweak space $\mathcal{T}$ is totally defined by a block cipher C over the same key space and block space, and that the PRP security of π is equivalent to the CPA security of C against distinguishers (i.e. the real-or-ideal cipher security which has been seen in the class).

Q.2 When the function mapping $t \in \mathcal{T}$ to α_t is not injective, prove that XE_C is not a secure tweakable block cipher by describing an adversary achieving a high advantage.

Q.3 We consider the PRF security of PMAC over the key space $\mathcal{K}$, the input space $\mathcal{M}$, and the output space $\{0,1\}^\ell$. We denote by $\mathsf{PMAC}[\pi]$ the authentication code which is defined by the tweakable block cipher π. We also denote by π^* the ideal tweakable block cipher over the same tweak space and block space. (I.e., the key space of π^* is the set of all functions from the tweak space to the set of block permutations and $\pi^*(k,t,x) = (k(t))(x)$.)

Given an adversary $\mathcal{A}$ against the PRF security of PMAC which is limited to a time complexity T (which include the running time and the size of the code of adversary) and to a number of queries with a total length of q blocks, prove that we can construct an adversary $\mathcal{B}$ against the PRP security of π with number of queries limited to q and a complexity of T plus a small overhead and such that $\mathsf{Adv}^{\mathsf{PRF}}_{\mathsf{PMAC}[\pi]}(\mathcal{A}) \leq \mathsf{Adv}^{\mathsf{PRP}}_{\pi}(\mathcal{B}) + \mathsf{Adv}^{\mathsf{PRF}}_{\mathsf{PMAC}[\pi^*]}(\mathcal{A})$.

Q.4 Given an adversary $\mathcal{B}$ against the PRP security of $\pi = \mathsf{XE}_C$ which is limited to a time complexity T' (which include the running time and the size of the code of adversary) and to a number of queries of q, prove that we can construct an adversary $\mathcal{C}$ against the PRP security of C with number of queries limited to $q+1$ and a complexity of T plus a small overhead and such that $\mathsf{Adv}^{\mathsf{PRP}}_{\pi}(\mathcal{B}) \leq \mathsf{Adv}^{\mathsf{PRP}}_{C}(\mathcal{C}) + \mathsf{Adv}^{\mathsf{PRP}}_{\pi'}(\mathcal{B})$, where $\pi' = \mathsf{XE}_{C^*}$ and C^* is an ideal block cipher over the same block space.

Q.5 Given an adversary $\mathcal{B}$ against the PRP security of $\pi' = \mathsf{XE}_{C^*}$ which is limited to a number of queries of q', prove that $\mathsf{Adv}^{\mathsf{PRP}}_{\pi'}(\mathcal{B}) \leq \mathsf{Adv}^{\mathsf{PRF}}_{\pi''}(\mathcal{B}) + \frac{q'^2}{2^\ell}$, where $\pi'' = \mathsf{XE}_{F^*}$ and F^* is an ideal random function from $\{0,1\}^\ell$ to $\{0,1\}^\ell$.

Q.6 Given an adversary $\mathcal{B}$ against the PRF security of $\pi'' = \mathsf{XE}_{F^*}$ which is limited to a number of queries of q', prove that $\mathsf{Adv}^{\mathsf{PRF}}_{\pi''}(\mathcal{B}) \leq \frac{q'^2}{2^\ell}$.