Advanced Cryptography — Midterm Exam

Serge Vaudenay

17.4.2025

- duration: 1h45
- any document allowed
- a pocket calculator is allowed
- communication devices are not allowed
- the exam invigilators will **not** answer any technical question during the exam
- readability and style of writing will be part of the grade

1 Alternate IND-CCA Security

Given a public-key cryptosystem $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$, we define the following games for $b = 0, 1$:

$\Gamma_b(\mathcal{A}_1, \mathcal{A}_2)$:
- $\mathsf{Gen} \xrightarrow{\$} (\mathsf{pk}, \mathsf{sk})$
- $\mathcal{A}_1^{\mathsf{ODec}_1}(\mathsf{pk}) \xrightarrow{\$} (\mathsf{pt}_0, \mathsf{pt}_1, \mathsf{st})$
- **if** $|\mathsf{pt}_0| \neq |\mathsf{pt}_1|$ **then return** 0
- $\mathsf{ct}_0 \xleftarrow{\$} \mathsf{Enc}(\mathsf{pk}, \mathsf{pt}_{1-b})$
- $\mathsf{ct}_1 \xleftarrow{\$} \mathsf{Enc}(\mathsf{pk}, \mathsf{pt}_b)$
- $\mathcal{A}_2^{\mathsf{ODec}_2}(\mathsf{st}, \mathsf{ct}_0, \mathsf{ct}_1) \xrightarrow{\$} z$
- **return** z

Oracle $\mathsf{ODec}_1(\mathsf{ct})$:
- **return** $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct})$

Oracle $\mathsf{ODec}_2(\mathsf{ct})$:
- **if** $\mathsf{ct} = \mathsf{ct}_0$ or $\mathsf{ct} = \mathsf{ct}_1$ **then return** $\perp$
- **return** $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct})$

The advantage is defined as $\mathsf{Adv}(\mathcal{A}_1, \mathcal{A}_2) = \Pr[\Gamma_1 \to 1] - \Pr[\Gamma_0 \to 1]$. We say that the cryptosystem is IND^2-CCA-secure if for any PPT $(\mathcal{A}_1, \mathcal{A}_2)$, the advantage is negligible.

Q.1 What is the difference between this notion and IND-CCA security?

Q.2 Prove that the plain ElGamal cryptosystem is not IND^2-CCA-secure by specifying an adversary and proving that it has a high advantage.

Q.3 We want to prove that IND^2-CCA security implies IND-CCA.

Q.3a We first consider the variant IND^2-CPA security of IND^2-CCA security where there is no decryption oracle. If the cryptosystem is IND^2-CPA-secure, prove that it is IND-CPA-secure.

Q.3b To extend the previous result to IND^2-CCA security implies IND-CCA security, show that we need to consider a failure case which reduces to the following game returning 1:

$\mathsf{Guess}(\mathcal{C})$:
- $\mathsf{Gen} \xrightarrow{\$} (\mathsf{pk}, \mathsf{sk})$

$\mathcal{C}^{\mathsf{ODec}}(\mathsf{pk}) \xrightarrow{\$} (\mathsf{pt}, \mathcal{L})$ $\triangleright$ $\mathcal{L}$ is a list of ciphertexts

$\mathsf{ct}_0 \xleftarrow{\$} \mathsf{Enc}(\mathsf{pk}, \mathsf{pt})$

return $1_{\mathsf{ct}_0 \in \mathcal{L}}$

Oracle $\mathsf{ODec}(\mathsf{ct})$:

return $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct})$

For this, construct a PPT adverdary $\mathcal{C}$ such that

$$\mathsf{Adv}(\mathcal{B}_1, \mathcal{B}_2) \leq \mathsf{Adv}(\mathcal{A}_1, \mathcal{A}_2) + \mathsf{Adv}(\mathcal{C})$$

Q.3c Construct an IND^2-CCA adversary $(\mathcal{D}_1, \mathcal{D}_2)$ making no ODec_2 oracle access and such that

$$\mathsf{Adv}(\mathcal{C}) = \mathsf{Adv}(\mathcal{D}_1, \mathcal{D}_2)$$

Then, conclude about the IND-CCA security of the cryptosystem.

Q.4 We now want to prove that IND-CCA security implies IND^2-CCA. For that, we consider the following intermediary game:

$\Gamma_{b,b'}(\mathcal{A}_1, \mathcal{A}_2)$:

$\mathsf{Gen} \xrightarrow{\$} (\mathsf{pk}, \mathsf{sk})$

$\mathcal{A}_1^{\mathsf{ODec}_1}(\mathsf{pk}) \xrightarrow{\$} (\mathsf{pt}_0, \mathsf{pt}_1, \mathsf{st})$

if $|\mathsf{pt}_0| \neq |\mathsf{pt}_1|$ **then return** 0

$\mathsf{ct}_0 \xleftarrow{\$} \mathsf{Enc}(\mathsf{pk}, \mathsf{pt}_{1-b'})$

$\mathsf{ct}_1 \xleftarrow{\$} \mathsf{Enc}(\mathsf{pk}, \mathsf{pt}_b)$

$\mathcal{A}_2^{\mathsf{ODec}_2}(\mathsf{st}, \mathsf{ct}_0, \mathsf{ct}_1) \xrightarrow{\$} z$

return z

Oracle $\mathsf{ODec}_1(\mathsf{ct})$:

return $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct})$

Oracle $\mathsf{ODec}_2(\mathsf{ct})$:

if $\mathsf{ct} = \mathsf{ct}_0$ or $\mathsf{ct} = \mathsf{ct}_1$ **then return** $\perp$

return $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct})$

Q.4a Construct an IND-CCA adversary $(\mathcal{B}_1, \mathcal{B}_2)$ such that

$$\Pr[\Gamma_{1,1}(\mathcal{A}_1, \mathcal{A}_2) \to 1] - \Pr[\Gamma_{1,0}(\mathcal{A}_1, \mathcal{A}_2) \to 1] \leq \mathsf{Adv}(\mathcal{B}_1, \mathcal{B}_2)$$

Q.4b Construct an IND-CCA adversary $(\mathcal{C}_1, \mathcal{C}_2)$ such that

$$\Pr[\Gamma_{1,0}(\mathcal{A}_1, \mathcal{A}_2) \to 1] - \Pr[\Gamma_{0,0}(\mathcal{A}_1, \mathcal{A}_2) \to 1] \leq \mathsf{Adv}(\mathcal{C}_1, \mathcal{C}_2)$$

Then, conclude about the IND^2-CCA security of the cryptosystem.

2 Proofs for ElGamal

In this exercise, we consider the plain ElGamal cryptosystem from the course. We use a multiplicatively denoted group of prime order q with generator g.

Q.1 After a sender computes $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, \mathsf{pt}; r)$ with a random $r \in \mathbf{Z}_q$, we define an "instance" $x = (\mathsf{pk}, \mathsf{pt}, \mathsf{ct})$ and a "witness" $w = r$. They are connected by a relation $R(x, w)$ to express that ct is the correct encryption of pt. Specify R, propose a Σ-protocol for this relation R, and prove that it is a Σ-protocol.

Q.2 After a receiver computes $\mathsf{pt} \leftarrow \mathsf{Dec}(\mathsf{sk}, \mathsf{ct})$, we define an "instance" $x = (\mathsf{pk}, \mathsf{pt}, \mathsf{ct})$ and a "witness" $w' = \mathsf{sk}$. They are connected by a relation $R'(x, w)$ to express that pt is the correct decryption of ct. Specify R', propose a Σ-protocol for this relation R', and prove that it is a Σ-protocol.

Q.3 In the last proof of knowledge of w' such that $R'((\mathsf{pk}, \mathsf{pt}, \mathsf{ct}), w')$, we want to adapt it into a batch proof for $R'((\mathsf{pk}, \mathsf{pt}_i, \mathsf{ct}_i), w')$ for $i = 1, \ldots, n$. For that, we pick a random seed and use a pseudorandom generator set up with seed in order to generate some $\alpha_1, \ldots, \alpha_n \in \mathbf{Z}_q$. We define $\mathsf{pt} = \prod_{i=1}^{n} \mathsf{pt}_i^{\alpha_i}$ and $\mathsf{ct} = \prod_{i=1}^{n} \mathsf{ct}_i^{\alpha_i}$. (The product of ct_i pairs is done component-wise.) We modify the previous Σ-protocol by sending seed in the first message and proving $R'((\mathsf{pk}, \mathsf{pt}, \mathsf{ct}), w')$ only. Prove that it is a Σ-protocol for the relation $\forall i = 1, \ldots, n \quad R'((\mathsf{pk}, \mathsf{pt}_i, \mathsf{ct}_i), w')$.
Note: it is recommended not to loose too much time on soundness as it is quite tricky.

Q.4 Can we do the same with the protocol of the first question?