Advanced Cryptography — Midterm Exam
Solution

Serge Vaudenay

7.5.2020

- 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

The exam grade follows a linear scale in which each question has the same weight.

1 Equivalence between OW-CPA and IND-CPA over the Binary Domain

We recall the definition of a public-key cryptosystem (PKC) from the course:

> A PKC is a tuple $(\mathsf{Gen}, \mathcal{M}, \mathsf{Enc}, \mathsf{Dec})$ with a plaintext domain $\mathcal{M}$ and three polynomially bounded algorithms Gen, Enc, and Dec. The algorithm Dec is deterministic and outputs either something in $\mathcal{M}$ or an error $\perp$. It is such that
>
> $$\forall X \in \mathcal{M} \quad \Pr_{r_g, r_e}[\mathsf{Dec}(\mathsf{sk}, \mathsf{Enc}(\mathsf{pk}, X; r_e)) = X] = 1$$
>
> where $(\mathsf{pk}, \mathsf{sk}) = \mathsf{Gen}(1^s; r_g)$.

We assume that $\mathcal{M} = \{0,1\}^\ell$. We recall the definition of IND-CPA security from the course:

> A PKC $(\mathsf{Gen}, \mathcal{M}, \mathsf{Enc}, \mathsf{Dec})$ is IND-CPA-secure if for any interactive PPT process $(\mathcal{A}_1, \mathcal{A}_2)$, the advantage Adv is negligible.
>
> $$\mathsf{Adv} = \Pr[\Gamma_1 \text{ returns } 1] - \Pr[\Gamma_0 \text{ returns } 1]$$
>
> Game Γ_b
> 1: $\mathsf{Gen} \xrightarrow{\$} (\mathsf{pk}, \mathsf{sk})$
> 2: $\mathcal{A}_1(\mathsf{pk}) \xrightarrow{\$} (\mathsf{pt}_0, \mathsf{pt}_1, \mathsf{st})$
> 3: **if** $|\mathsf{pt}_0| \neq |\mathsf{pt}_1|$ **then return** 0
> 4: $\mathsf{ct} \xleftarrow{\$} \mathsf{Enc}(\mathsf{pk}, \mathsf{pt}_b)$
> 5: $\mathcal{A}_2(\mathsf{st}, \mathsf{ct}) \xrightarrow{\$} z$

6: **return** z

Q.1 Precisely define OW-CPA security, the security notion of a PKC against decryption attacks. For that, define the OW-CPA game, consider the probability of success of the trivial random guessing attack, and define the advantage of an adversary of being the difference of its probability of success with the one of the trivial attack.

A PKC $(\mathsf{Gen}, \mathcal{M}, \mathsf{Enc}, \mathsf{Dec})$ *is OW-CPA-secure if for any PPT algorithm* $\mathcal{A}$*, the advantage* Adv *is negligible.*

Game

1: $\mathsf{Gen} \xrightarrow{\$} (\mathsf{pk}, \mathsf{sk})$
2: $\mathsf{pt}_0 \xleftarrow{\$} \{0,1\}^\ell$
3: $\mathsf{ct}_0 \leftarrow \mathsf{Enc}(\mathsf{pk}, \mathsf{pt}_0)$
4: $\mathcal{A}(\mathsf{pk}, \mathsf{ct}_0) \rightarrow \mathsf{pt}$
5: ***return*** $1_{\mathsf{pt}=\mathsf{pt}_0}$

Since the random guessing adversary succeeds with probability $2^{-\ell}$*, we define*

$$\mathsf{Adv} = \Pr[\textit{game returns } 1] - 2^{-\ell}$$

One student suggested to give to $\mathcal{A}$ *the random coins which were used in* Enc*. That could define a stronger security notion (which many current cryptosystems would not satisfy).*

Q.2 Formally (and clearly) prove that if a PKC is IND-CPA secure, then it is OW-CPA secure.

We want to prove that PKC is OW-CPA secure. So, we take an adversary $\mathcal{A}$ playing the OW-CPA game. We define $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ as follows:

$\mathcal{B}_1(\mathsf{pk})$*:*

1: $\mathsf{pt}_0, \mathsf{pt}_1 \xleftarrow{\$} \{0,1\}^\ell$ *of same length*
2: $\mathsf{st} \leftarrow (\mathsf{pk}, \mathsf{pt}_1)$
3: ***return*** $(\mathsf{pt}_0, \mathsf{pt}_1, \mathsf{st})$

$\mathcal{B}_2(\mathsf{st}, \mathsf{ct})$*:*

4: *parse* $(\mathsf{pk}, \mathsf{pt}_1) = \mathsf{st}$
5: $\mathsf{pt} \leftarrow \mathcal{A}(\mathsf{pk}, \mathsf{ct})$
6: ***return*** $1_{\mathsf{pt}=\mathsf{pt}_1}$

We assume that PKC is IND We let p be the probability that the OW-CPA game with $\mathcal{A}$ returns 1. The advantage of $\mathcal{A}$ is $p - 2^{-\ell}$.
The Γ_b game with $\mathcal{B}$ rewrites as follows.

Game Γ_b

1: $\mathsf{Gen} \xrightarrow{\$} (\mathsf{pk}, \mathsf{sk})$
2: $\mathsf{pt}_0, \mathsf{pt}_1 \xleftarrow{\$} \{0,1\}^\ell$ *of same length*
3: $\mathsf{ct} \xleftarrow{\$} \mathsf{Enc}(\mathsf{pk}, \mathsf{pt}_b)$
4: $\mathsf{pt} \leftarrow \mathcal{A}(\mathsf{pk}, \mathsf{ct})$
5: ***return*** $1_{\mathsf{pt}=\mathsf{pt}_1}$

The $b = 1$ case boils down to the OW-CPA game and we have $\Pr[\Gamma_1 \to 1] = p$. In the $b = 0$ case, the output of $\mathcal{A}$ is independent from pt_1 and pt_1 is uniformly distributed. Hence, $\Pr[\Gamma_0 \to 1] \leq 2^{-\ell}$ (to take into account the cases where the output of $\mathcal{A}$ is not in $\mathcal{M}$.) We deduce that the advantage of $\mathcal{B}$ in the IND-CPA game is $\mathsf{Adv} \geq p - 2^{-\ell}$. Assuming IND-CPA security, we deduce that $p - 2^{-\ell}$ is negligible. As this is the advantage of $\mathcal{A}$, we deduce that the advantage of every $\mathcal{A}$ playing the OW-CPA game is negligible. Hence, PKC is OW-CPA secure.

Q.3 For a PKC which is OW-CPA secure, formally prove that if $\ell = 1$, then the PKC is IND-CPA secure.

To prove IND-CPA security, we take an IND-CPA adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$. We define an OW-CPA adversary $\mathcal{B}$ as follows:

$\mathcal{B}(\mathsf{pk}, \mathsf{ct})$*:*

1: $\mathcal{A}_1(\mathsf{pk}) \to (\mathsf{pt}_0, \mathsf{pt}_1, \mathsf{st})$
2: ***if*** $\mathsf{pt}_0 = \mathsf{pt}_1$ ***then return*** *a random bit*
3: $\mathcal{A}_2(\mathsf{st}, \mathsf{ct}) \to z$
4: ***return*** $z \oplus \mathsf{pt}_0$

The OW-CPA game becomes

Game

1: $\mathsf{Gen} \xrightarrow{\$} (\mathsf{pk}, \mathsf{sk})$
2: $\mathsf{pt} \xleftarrow{\$} \{0,1\}^\ell$
3: $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, \mathsf{pt})$
4: $\mathcal{A}_1(\mathsf{pk}) \to (\mathsf{pt}_0, \mathsf{pt}_1, \mathsf{st})$
5: ***if*** $\mathsf{pt}_0 = \mathsf{pt}_1$ ***then return*** *a random bit*
6: $\mathcal{A}_2(\mathsf{st}, \mathsf{ct}) \to z$
7: ***return*** $1_{z=\mathsf{pt}\oplus\mathsf{pt}_0}$

We use a bridging step to claim that it is equivalent to the game where $\mathcal{A}_1$ is run and $\mathsf{pt}_0 = \mathsf{pt}_1$ is tested before selecting pt, and where we use the change of variable $b = \mathsf{pt} \oplus \mathsf{pt}_0$.

Game

1: $\mathsf{Gen} \xrightarrow{\$} (\mathsf{pk}, \mathsf{sk})$
2: $\mathcal{A}_1(\mathsf{pk}) \to (\mathsf{pt}_0, \mathsf{pt}_1, \mathsf{st})$
3: ***if*** $\mathsf{pt}_0 = \mathsf{pt}_1$ ***then return*** *a random bit*
4: $b \xleftarrow{\$} \{0,1\}^\ell$
5: $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, b \oplus \mathsf{pt}_0)$
6: $\mathcal{A}_2(\mathsf{st}, \mathsf{ct}) \to z$
7: ***return*** $1_{z=b}$

In the IND-CPA game, we let E be the event that $\mathsf{pt}_0 = \mathsf{pt}_1$. When $\neg E$ holds, we note that $b \oplus \mathsf{pt}_0 = \mathsf{pt}_b$.

The probability that the OW-CPA game returns 1 is

$$\frac{1}{2}\Pr[E] + \Pr[z = b | \neg E] \times \Pr[\neg E]$$

Hence, the OW-CPA advantage is

$$\left(\Pr[z = b | \neg E] - \frac{1}{2}\right) \times \Pr[\neg E]$$

We notice that

$$\Pr[z = 1 | b = 1, \neg E] - \Pr[z = 1 | b = 0, \neg E] = 2\Pr[z = b | \neg E] - 1$$

Since $\Pr[z = 1 | b = 1, E] - \Pr[z = 1 | b = 0, E] = 0$, we deduce that the advantage of $\mathcal{A}$ in the IND-CPA game is twice the advantage of $\mathcal{B}$ in the OW-CPA game. Assuming OW-CPA security, this must be negligible. As this holds for any $\mathcal{A}$, we deduce IND-CPA security.

2 Strengthening Contact Tracing against Replay Attacks

We consider a contact tracing scheme. This schemes runs in the smartphones of all users. The purpose of this scheme is to make sure that a user who have met another user who ended up being diagnosed with COVID-19 can receive an alert, self-isolate, and get a test. The scheme works as follows.

Each phone A sets up a new key k every day. Quite regularly, the phone broadcasts $\mathsf{EphID} = \mathsf{PRF}(k, t)$, where t is a counter. The broadcast is done with Bluetooth, so that other phones B in proximity can obtain EphID and store it. If A even get diagnosed of COVID-19, a public health authority gives A some credential allowing A to publish the past used k on a server. Regularly, the phone B checks if new k values have been published. If it is the case, B tries to match any $\mathsf{PRF}_k(t)$ with any of the stored EphID. A match indicates that B has met a user who later got diagnosed.

Q.1 Propose a scenario of attack by which a healthy adversary A could broadcast to B an EphID which will cause a false alert on B with good probability.

A could buy EphID on a darknet. The darknet would be populated by EphID caught by hunters in places which are likely to have people C who will be declared sick soon, like a hospital, or the neighborhood of someone who has just been diagnosed. By broadcasting this EphID to B, once C is diagnosed and reported, B has an alert.
Many students suggested that A could reuse the published k to generate EphID and broadcast to B. This works as well, but is defeated by the server publishing the date when k was reported and B checking that the reported date is posterior to the reception date (assuming secure clocks).
One student suggested to break the reporting scheme. If A manages to report k without being infected, this attack works too. Assuming that the credential system is well done, the attack is defeated.

Q.2 We propose a change in the protocol in which $\mathsf{EphID} = [\mathsf{time}\|r\|\tau]$ where time is the clock value when EphID is broadcasted, r is a random value, and $\tau = \mathsf{PRF}_k(h)$ where $h = H(\mathsf{time}\|r)$ and H is a hash function. At reception, the receiver takes its clock value time' and checks that $|\mathsf{time} - \mathsf{time}'|$ is small enough. After that, the receiver stores $[h\|\tau]$ and discards the rest.
Explain what else the receiver should do before raising an alert to mitigate the previous attack.

When getting k from the server, the receiver B should check that his stored $[h\|\tau]$ verifies $\tau = \mathsf{PRF}_k(h)$. This way, a replay attack must make sure that the replay is done immediately after having obtained EphID.
Corresponding to the other attack mentioned by students, B should also check that the reception time of EphID is prior to the reporting time of k.

Q.3 What do you think of this scheme?
NOTE: There is no unique good answer. Feel free to make any properly supported statement.

We had many different good answers. Students gave many remarks about the security or the potential insecurity of this scheme. Many possible answers could be found in https://eprint.iacr.org/2020/399 or https://eprint.iacr.org/2020/531. The objective of this question was to see if students could say anything meaningful about this scheme. It was not to make a complete survey of things to say about it.