Advanced Cryptography — Midterm Exam

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

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

```
$\mathsf{Gen} \xrightarrow{\$} (\mathsf{pk}, \mathsf{sk})$
$\mathcal{A}_1(\mathsf{pk}) \xrightarrow{\$} (\mathsf{pt}_0, \mathsf{pt}_1, \mathsf{st})$
if $|\mathsf{pt}_0| \neq |\mathsf{pt}_1|$ then return $0$
$\mathsf{ct} \xleftarrow{\$} \mathsf{Enc}(\mathsf{pk}, \mathsf{pt}_b)$
$\mathcal{A}_2(\mathsf{st}, \mathsf{ct}) \xrightarrow{\$} z$
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.

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

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.

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.

Q.3 What do you think of this scheme?

NOTE: There is no unique good answer. Feel free to make any properly supported statement.