Advanced Cryptography — Midterm Exam

Serge Vaudenay

18.4.2019

- 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 On Various Equivalent Indistinguishability Notions

In this exercise, we consider two games $\Gamma_0(1^s)$ and $\Gamma_1(1^s)$ which can be played by an adversary $\mathcal{A}$. We assume that Γ_0 and Γ_1 are such that they output c if and only if $\mathcal{A}$ outputs a final message c. We define

$$\begin{aligned}
\mathsf{Adv}_1^{\mathcal{A}}(s) &= \Pr[\Gamma_1(1^s,\mathcal{A}) \to 1] - \Pr[\Gamma_0(1^s,\mathcal{A}) \to 1] \\
\mathsf{Adv}_2^{\mathcal{A}}(s) &= |\Pr[\Gamma_1(1^s,\mathcal{A}) \to 1] - \Pr[\Gamma_0(1^s,\mathcal{A}) \to 1]| \\
\mathsf{Adv}_3^{\mathcal{A}}(s) &= \frac{1}{2} - \Pr[\Gamma'(1^s,\mathcal{A}) \to 1]
\end{aligned}$$

where Γ' is a bit-guessing game defined by

Game $\Gamma'(1^s,\mathcal{A})$:

picks $b \in \{0,1\}$ uniformly at random
if $b = 0$ **then**
    simulate $\Gamma_0(1^s,\mathcal{A})$ which returns c
else
    simulate $\Gamma_1(1^s,\mathcal{A})$ which returns c
end if
$c' = 1_{c=1}$ ▷ this forces c' to be 0 or 1
return $1_{b=c'}$

Given a positive function $g(s)$, we define three notions of g-indistinguishability by

g-IND_i: "for any p.p.t. algorithm $\mathcal{A}$, $\exists s_0 \quad \forall s \geq s_0 \quad \mathsf{Adv}_i^{\mathcal{A}}(s) \leq g(s)$"

Q.1 Prove that g-IND_1 is equivalent to g-IND_2.
Warning: there are two directions in an equivalence!

Q.2 Prove that g-IND_1 is equivalent to $\frac{g}{2}$-IND_3.

2 Goldwasser-Micali Cryptosystem

We define the GM cryptosystem over the message space $\{0, 1\}$ as follows:

$\mathsf{Gen}(1^s)$:

generate two different prime numbers p and q of s bits
$N = pq$
pick $x \in \mathbf{Z}_N^*$ such that $(x/p) = (x/q) = -1$
$\mathsf{pk} = (x, N)$, $\mathsf{sk} = p$
return pk and sk

$\mathsf{Enc}(\mathsf{pk}, b)$:

parse $\mathsf{pk} = (x, N)$
pick $r \in \mathbf{Z}_N^*$ uniformly at random
$\mathsf{ct} = r^2 x^b \bmod N$
return ct

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

set $p = \mathsf{sk}$
$\sigma = (\mathsf{ct}/p)$
return $1_{\sigma=-1}$

Q.1 Prove that GM is public-key cryptosystem and that it is correct.
Hint: triple-check all what you must prove in this question!

Q.2 Prove that the key-recovery problem (KR-CPA) is equivalent to some well-known problem.

Q.3 We define the following game which depends on a bit b:

Game $\Gamma_b(1^s, \mathcal{A})$:

$\mathsf{Gen}(1^s) \to (\mathsf{pk}, \mathsf{sk})$
$\mathsf{Enc}(\mathsf{pk}, b) \to \mathsf{ct}$
$\mathcal{A}(\mathsf{pk}, \mathsf{ct}) \to c$
return c

We say that GM is Γ-secure if for every p.p.t. $\mathcal{A}$, $\Pr[\Gamma_1(1^s, \mathcal{A}) \to 1] - \Pr[\Gamma_0(1^s, \mathcal{A}) \to 1]$ is a negligible function of s.
Prove that IND-CPA security and Γ-security are equivalent for GM.

Q.4 We define the following game which depends on a bit b:

Game $\mathsf{QR}_b(1^s, \mathcal{A})$:

generate two different prime numbers p and q of s bits
$N = pq$
pick $x \in \mathbf{Z}_N^*$ such that $(x/p) = (x/q) = (-1)^b$
$\mathcal{A}(x, N) \to c$
return c

We define $\mathsf{Adv}^{\mathcal{A}}(s) = \Pr[\mathsf{QR}_1(1^s, \mathcal{A}) \to 1] - \Pr[\mathsf{QR}_0(1^s, \mathcal{A}) \to 1]$. We say that the QR problem is hard if for every p.p.t. $\mathcal{A}$, $\mathsf{Adv}^{\mathcal{A}}$ is a negligible function.
Prove that the IND-CPA security of GM implies the QR hardness.

Q.5 Prove that the IND-CPA security of GM is equivalent to the hardness of QR.

3 A Weird Signcryption

We consider the plain RSA cryptosystem $(\mathsf{RSA.Gen}, \mathsf{RSA.Enc}, \mathsf{RSA.Dec})$ and a digital signature scheme $(\mathsf{DS.Gen}, \mathsf{DS.Sign}, \mathsf{DS.Ver})$. We construct a *signcryption* scheme as follows:

$\mathsf{SC.Gen}$: ▷ generate a key pair for a user

- $\mathsf{RSA.Gen} \to (\mathsf{ek}, \mathsf{dk})$ ▷ encryption key and decryption key
- $\mathsf{DS.Gen} \to (\mathsf{sk}, \mathsf{vk})$ ▷ signing key and verification key
- $\mathsf{pubk} \leftarrow (\mathsf{ek}, \mathsf{vk})$ ▷ public key of user
- $\mathsf{privk} \leftarrow (\mathsf{dk}, \mathsf{sk})$ ▷ private key of user
- **return** $(\mathsf{pubk}, \mathsf{privk})$

$\mathsf{SC.Send}(\mathsf{pubk}_B, \mathsf{privk}_A, \mathsf{pt})$: ▷ user A sends a message to user B

- parse $\mathsf{pubk}_B = (\mathsf{ek}_B, \mathsf{vk}_B)$
- parse $\mathsf{privk}_A = (\mathsf{dk}_A, \mathsf{sk}_A)$
- $\mathsf{ct} \leftarrow \mathsf{RSA.Enc}(\mathsf{ek}_B, \mathsf{pt})$
- $\sigma \leftarrow \mathsf{DS.Sign}(\mathsf{sk}_A, \mathsf{ct})$
- **return** (ct, σ)

so that A can send (ct, σ) to B. Once B obtains pt, he can show $\mathsf{proof} = (\mathsf{vk}_A, \mathsf{ek}_B, \mathsf{ct}, \sigma, \mathsf{pt})$ as a proof that A sent pt. We call this property *non-repudiation*.

Q.1 Describe the algorithm using $(\mathsf{pubk}_A, \mathsf{privk}_B)$ to receive (ct, σ) and compute pt, as well as the algorithm to verify the proof.

Q.2 Given $(\mathsf{vk}_A, \mathsf{ct}, \sigma)$ such that $\mathsf{DS.Ver}(\mathsf{vk}_A, \mathsf{ct}, \sigma)$ is true and given an arbitrary pt, prove that we can easily find ek such that $(\mathsf{vk}_A, \mathsf{ek}, \mathsf{ct}, \sigma, \mathsf{pt})$ is a valid proof.

Q.3 Propose a fix to this problem so that we have non-repudiation.