Advanced Cryptography — Midterm Exam
Solution

Serge Vaudenay

11.4.2024

- 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 Signatures with Malicious Setup

We recall the DSA signature scheme using a hash function H.

- Public parameters setup: set group parameters (p, q, g) such that p and q are large prime numbers, q divides $p-1$, and g has order q in $\mathbf{Z}_p^*$. The group parameters are implicit inputs of other algorithms.
- Key generation: pick a random $x \in \mathbf{Z}_q$ and set $y = g^x \bmod p$. The secret key is x and the public key is y.
- Signature: pick $k \in \mathbf{Z}_q^*$ and set $r = g^k \bmod p \bmod q$ and $s = \frac{H(M)+xr}{k} \bmod q$ where M is the message to be signed. The signature is (r, s).
- Verification: compare r with $g^{\frac{H(M)}{s}} y^{\frac{r}{s}} \bmod p \bmod q$.

Q.1 The above description does not fit the definition of a signature scheme in three algorithms: key generation, signature, verification. Propose a formal definition of a signature scheme which includes the notion of public parameters setup and the notion of correctness.

A ***digital signature scheme*** *is a tuple* $(\mathsf{Setup}, \mathsf{Gen}, \mathcal{D}, \mathsf{Sig}, \mathsf{Ver})$ *with a message domain* $\mathcal{D} \subseteq \{0,1\}^*$ *and four PPT algorithms* Setup, Gen, Sig, *and* Ver. *The algorithm* Ver *is deterministic and outputs 0 (reject) or 1 (accept). It is such that*

$$\forall X \in \mathcal{D} \quad \Pr_{r_i, r_g, r_s}[\mathsf{Ver}(\mathsf{pp}, \mathsf{pk}, X, \mathsf{Sig}(\mathsf{pp}, \mathsf{sk}, X; r_s)) = 1] = 1$$

where $\mathsf{pp} = \mathsf{Setup}(1^s; r_i)$ *and* $(\mathsf{pk}, \mathsf{sk}) = \mathsf{Gen}(\mathsf{pp}; r_g)$.
[This question has been misunderstood by many students. The question was to propose a definition for what is a digital signature scheme with public parameters setup, i.e. to define the interface. It was understood as paraphrasing the above DSA specifications. However, it was graded as correct if some algorithm names, inputs and outputs were clearly defined and the correctness property was written, but copying the specifications was graded 1pt only.]

Q.2 Formally define the notion of unforgeability which captures malicious setup.

A digital signature scheme $(\mathsf{Setup}, \mathsf{Gen}, \mathcal{D}, \mathsf{Sig}, \mathsf{Ver})$ *is* ***secure against existential forgery under chosen message attacks*** *(EF-CMA) with malicious setup if for any 2-stage PPT* $(\mathcal{A}_1, \mathcal{A}_2)$, *the advantage* Adv *is negligible.*

$$\mathsf{Adv} = \Pr[\textit{game returns } 1]$$

Game

```
A_1 --$--> (pp, st)
Gen(pp) --$--> (pk, sk)
Queries <- ∅
A_2^OSig(st, pk) -> (X, σ)
if X ∈ Queries then return 0
return 1_{Ver(pp,pk,X,σ)}
```

Oracle $\mathsf{OSig}(X)$*:*

```
σ <- Sig(pp, sk, X)
Queries <- Queries ∪ {X}
return σ
```

[One point less was given if the CMA part or setup part was missing.]

Q.3 Imagine that setup is done by a malicious adversary. Show that it is possible to generate some public parameters (p, q, g) which are correct together with a pair of messages (M_0, M_1) such that $M_0 \neq M_1$ and for any public key y and any $\sigma = (r, s)$, if σ is a valid signature of M_0 for y, then σ is a valid signature of M_1 for y as well.

Given M_0 *and* M_1 *random, we can set* $q = |H(M_1) - H(M_0)|$ *and generate* $p+1$ *multiple of* q *until* p *and* q *are both prime. Generating* g *follows. We have the property that* $H(M_1) \equiv H(M_0) \pmod{q}$. *Hence, for any public key, any signature* (r, s) *which is valid for* M_0 *is also valid for* M_1.
[Some students proposed to take public parameters with a very small q. *However, the parameter verification (for instance, during key generation) would fail in that case.]*

2 Find-then-Guess Security for Deterministic Symmetric Encryption

We consider a symmetric encryption scheme $(\{0,1\}^k, \mathcal{D}, \mathsf{Enc}, \mathsf{Dec})$. (We recall that k depends on an implicit security parameter s; we recall that $\mathcal{D}$ is the set of all bitstrings of length in an admissible set $\mathcal{L}$; we assume the scheme to be variable-length by default; we assume no nonce; we may assume length-preservation or not.) In this exercise, we assume Enc to be deterministic. We define the Deterministic Find-then-Guess CPA security (DFG-CPA-security) as the indistinguishability between two games Γ_0 and Γ_1. The scheme is secure if for any PPT 2-stage adversary $(\mathcal{A}_1, \mathcal{A}_2)$, the advantage Adv is negligible. The advantage is $\mathsf{Adv} = \Pr[\Gamma_1 \to 1] - \Pr[\Gamma_0 \to 1]$ with the following games:

Game Γ_b:
1: pick $K \leftarrow \{0,1\}^k$ uniformly at random
2: $S \leftarrow \emptyset$
3: $\mathcal{A}_1^{\mathsf{OEnc}_1} \to (\mathsf{pt}_0, \mathsf{pt}_1, \mathsf{st})$
4: **if** $|\mathsf{pt}_0| \neq |\mathsf{pt}_1|$ **then return** $\perp$
5: **if** $\mathsf{pt}_0 \in S$ or $\mathsf{pt}_1 \in S$ **then return** $\perp$
6: $\mathsf{ct} \leftarrow \mathsf{Enc}(K, \mathsf{pt}_b)$
7: $\mathcal{A}_2^{\mathsf{OEnc}_2}(\mathsf{st}, \mathsf{ct}) \to z$
8: **return** z

Oracle $\mathsf{OEnc}_1(\mathsf{pt})$:
9: add pt in S
10: **return** $\mathsf{Enc}(K, \mathsf{pt})$

Oracle $\mathsf{OEnc}_2(\mathsf{pt})$:
11: **if** $\mathsf{pt} \in \{\mathsf{pt}_0, \mathsf{pt}_1\}$ **then return** $\perp$
12: **return** $\mathsf{Enc}(K, \mathsf{pt})$

Q.1 If we remove line 5 in the definition of the games, prove that no deterministic symmetric encryption is DFG-CPA-secure.

> *Essentially, we use that the encryption of pt_0 (or pt_1) is known from an OEnc query, then it is trivial to realize whether ct is that encryption because encryption is deterministic.*
>
> $\mathcal{A}_1^{\mathcal{O}}$:
> *pick $\mathsf{pt}_0, \mathsf{pt}_1$ different, of same length, and in the plaintext domain arbitrarily*
> $\mathsf{st} \leftarrow \mathcal{O}(\mathsf{pt}_0)$
> ***return*** $(\mathsf{pt}_0, \mathsf{pt}_1, \mathsf{st})$
>
> $\mathcal{A}_2^{\mathcal{O}}(\mathsf{st}, \mathsf{ct})$:
> ***return*** $1_{\mathsf{ct}=\mathsf{st}}$
>
> *Since encryption is deterministic, Γ_0 will encrypt pt_0 twice into $\mathsf{st} = \mathsf{ct}$ so we have $\Pr[\Gamma_0 \to 1] = 1$. In Γ_1, st and ct are encryptions of two different plaintexts pt_0 and pt_1. Due to the correctness of encryption, they cannot be equal so we have $\Pr[\Gamma_1 \to 1] = 0$. We deduce $\mathsf{Adv} = 1$ which is not negligible.*

Q.2 If we remove line 11 in the definition of the games, prove that no deterministic symmetric encryption is DFG-CPA-secure.

We apply a similar idea.

$\mathcal{A}_1^{\mathcal{O}}$:

1: *pick* $\mathsf{pt}_0, \mathsf{pt}_1$ *different, of same length, and in the plaintext domain arbitrarily*

2: $\mathsf{st} \leftarrow \mathsf{pt}_0$

3: ***return*** $(\mathsf{pt}_0, \mathsf{pt}_1, \mathsf{st})$

$\mathcal{A}_2^{\mathcal{O}}(\mathsf{st}, \mathsf{ct})$:

4: $\mathsf{ct}_0 \leftarrow \mathcal{O}(\mathsf{st})$

5: ***return*** $1_{\mathsf{ct}=\mathsf{ct}_0}$

We prove $\mathsf{Adv} = 1$ *in the same way.*

Q.3 Propose an extension to define DFG-CPCA-security in a way which is not trivially impossible to achieve like in the previous questions.

The point here is to take into account that some new encryptions will be known from decryption queries. Of course, we should exclude the decryption query set to the challenge ciphertext ct.

$\mathsf{ODec}_1(x)$:

1: $\mathsf{pt} \leftarrow \mathsf{Dec}(K, x)$

2: *add* pt *in* S

3: ***return*** pt

$\mathsf{ODec}_2(x)$:

4: ***if*** $x = \mathsf{ct}$ ***then return*** $\perp$

5: $\mathsf{pt} \leftarrow \mathsf{Dec}(K, x)$

6: ***return*** pt

Q.4 Construct a nonce-less deterministic symmetric encryption scheme which is not length-preserving, which is (presumably) DFG-CPA-secure, and which is (certainly) not secure against CPA real-or-ideal distinguishers.

Assume that a DFG-CPA-*secure scheme exists. We construct a new scheme by* $\mathsf{Enc}'(K, \mathsf{pt}) = \mathsf{Enc}(K, \mathsf{pt}) \| \mathsf{Enc}(K, \mathsf{pt})$ *and* $\mathsf{Dec}'(K, \mathsf{ct}) = \mathsf{Dec}(K, \mathsf{lefthalf}(\mathsf{ct}))$. *Clearly, this is still* DFG-CPA-*secure. However, we can trivially distinguish from an ideal cipher by checking that a ciphertext is not of form* $x \| x$.

Q.5 We assume that $\mathcal{D}$ is finite. Prove that CPA security against decryption implies that $2^{-\ell}$ is negligible, where ℓ is the largest length of an element in $\mathcal{D}$.

We have seen in class that security against decryption implies that $\frac{1}{\#\mathcal{D}}$ *is negligible. (The used decryption adversary essentially picks a random answer from* $\mathcal{D}$ *and has* $\frac{1}{\#\mathcal{D}}$ *as an advantage.)*

We recall that $\mathcal{D}$ *must be of form* $\{x \in \{0,1\}^*; |x| \in \mathcal{L}\}$ *for a set* $\mathcal{L}$ *of admissible lengths. Hence,* $\#\mathcal{D} = \sum_{\ell \in \mathcal{L}} 2^\ell$. *Let* $\ell = \max \mathcal{L}$ *be the largest length. We have* $\#\mathcal{D} \leq 2 \cdot 2^\ell$ *so* $\frac{1}{2} 2^{-\ell} \leq \frac{1}{\#\mathcal{D}} = \mathsf{negl}$. *We deduce that* $2^{-\ell}$ *is negligible.*

Q.6 Prove that CPA security against real-or-ideal distinguishers implies $\mathsf{DFG\text{-}CPA}$-security.

Assume CPA security against distinguishers. In order to prove $\mathsf{DFG\text{-}CPA}$*-security, consider an adversary $(\mathcal{A}_1, \mathcal{A}_2)$ playing the* $\mathsf{DFG\text{-}CPA}$ *game. We define a distinguisher $\mathcal{B}$ as follows:*

$\mathcal{B}^{\mathcal{O}}$:

- *pick* $\beta \in \{0,1\}$ *at random*
- $S \leftarrow \emptyset$
- $\mathcal{A}_1^{\mathsf{SEnc}_1} \rightarrow (\mathsf{pt}_0, \mathsf{pt}_1, \mathsf{st})$
- ***if*** $|\mathsf{pt}_0| \neq |\mathsf{pt}_1|$ ***then return*** β
- ***if*** $\mathsf{pt}_0 \in S$ *or* $\mathsf{pt}_1 \in S$ ***then return*** β
- $\mathsf{ct} \leftarrow \mathcal{O}(\mathsf{pt}_\beta)$
- $\mathcal{A}_2^{\mathsf{SEnc}_2}(\mathsf{st}, \mathsf{ct}) \rightarrow z$
- ***return*** $\beta \oplus 1_{z=1}$

Subroutine $\mathsf{SEnc}_1(\mathsf{pt})$:

- *add* pt *in* S
- ***return*** $\mathcal{O}(\mathsf{pt})$

Subroutine $\mathsf{SEnc}_2(\mathsf{pt})$:

- ***if*** $\mathsf{pt} \in \{\mathsf{pt}_0, \mathsf{pt}_1\}$ ***then*** *make $\mathcal{B}$ return β*
- ***return*** $\mathcal{O}(\mathsf{pt})$

The real game of indistinguishability returns 1 if Γ_β returns $1-\beta$:

$$\Pr[\mathsf{IND}_{\mathsf{real}} \rightarrow 1] = \frac{1}{2}(1 - \Pr[\Gamma_1 \rightarrow 1]) + \frac{1}{2}\Pr[\Gamma_0 \rightarrow 1] = \frac{1}{2} - \frac{1}{2}\mathsf{Adv}_{\mathcal{A}}$$

In the ideal game of indistinguishability, no information leaks on whether ct *is the encryption of* pt_0 *or* pt_1 *with the random permutation. Hence,* $\Pr[\mathsf{IND}_{\mathsf{ideal}} \rightarrow 1] = \frac{1}{2}$*. Finally, we obtain that* $\mathsf{Adv}_{\mathcal{B}} = -\frac{1}{2}\mathsf{Adv}_{\mathcal{A}}$*.*
Due to CPA security against disginguishers, we know that $\mathsf{Adv}_{\mathcal{B}}$ *is negligible. Therefore,* $\mathsf{Adv}_{\mathcal{A}}$ *is negligible. This proves* $\mathsf{DFG\text{-}CPA}$ *security.*

Q.7 Prove that $\mathsf{DFG\text{-}CPA}$-security implies CPA security against decryption attacks, assuming that the $\mathcal{D}$ includes elements of length ℓ such that $2^{-\ell}$ is negligible and that $\mathcal{D}$ is finite.

Assume DFG-CPA*-security. In order to prove CPA security against decryption attacks, consider an adversary* $\mathcal{B}$ *playing the CPA decryption game. We define an* DFG-CPA *adversary* $(\mathcal{A}_1, \mathcal{A}_2)$ *as follows:*

$\mathcal{A}_1^{\mathcal{O}}$*:*

- *select an admissible length* ℓ *in* $\mathcal{D}$ *such that* $2^{-\ell}$ *is negligible*
- *pick* $\mathsf{pt}_0, \mathsf{pt}_1$ *different, of same length* ℓ*, and in the plaintext domain arbitrarily*
- $\mathsf{st} \leftarrow \mathsf{pt}_0$
- ***return*** $(\mathsf{pt}_0, \mathsf{pt}_1, \mathsf{st})$

$\mathcal{A}_2^{\mathcal{O}}(\mathsf{st}, \mathsf{ct})$*:*

- $\mathcal{B}^{\mathsf{SEnc}}(\mathsf{ct}) \rightarrow x$
- ***return*** $1_{x=\mathsf{st}}$

Subroutine $\mathsf{SEnc}(\mathsf{pt})$*:*

- $x \leftarrow \mathcal{O}(\mathsf{pt})$
- ***if*** $x \neq \perp$ ***then return*** x
- *make* $\mathcal{A}_2$ *return* $1_{\mathsf{pt}=\mathsf{st}}$

In order for Γ_b *to return 1,* $\mathcal{B}$ *must not query* OEnc *with* pt_1 *and must either query* OEnc *with* pt_0 *or return* $x = \mathsf{pt}_0$*.*

In Γ_0*, no information on* pt_1 *is given to* $\mathcal{A}_2$ *(except it has the same length as the decryption of* ct *and it is different). Let* p_i *be the probability that the* i*-th query from* $\mathcal{B}$ *is* pt_1*. For any* i*, we have* $p_i \leq \frac{1}{2^\ell - 1}$*. Let* q *be the number of oracle queries. So, the probability that* $\mathcal{B}$ *ever queries* OEnc *with* pt_1 *is bounded by* $\frac{q}{2^\ell - 1}$*.*

In Γ_0*, except with this failure case, when* $\mathcal{B}$ *wins the decryption game, no matter if* $\mathcal{B}$ *queries* OEnc *with* pt_0 *or not, the outcome of the game would be 1. Hence,* $\Pr[\Gamma_0 \rightarrow 1] \geq \mathsf{Adv}_{\mathcal{B}} - \frac{q}{2^\ell - 1}$*.*

In Γ_1*,* $\mathcal{B}$ *has no information about* pt_0 *(except that it is different from the decryption of* ct *but of same length* ℓ*). Let* p_i *be the probability that the* i*-th query from* $\mathcal{B}$ *is* pt_0*. Let* p_0 *be the probability that the output of* $\mathcal{B}$ *is* pt_0*. For any* i*, we have* $p_i \leq \frac{1}{2^\ell - 1}$*. Let* q *be the number of oracle queries. We have* $\Pr[\Gamma_1 \rightarrow 1] \leq \frac{q+1}{2^\ell - 1}$*.*

We deduce that $\mathsf{Adv}_{\mathcal{A}} \geq \mathsf{Adv}_{\mathcal{B}} - \frac{2q}{2^\ell - 1}$*. Due to* DFG-CPA*-security., we know that* $\mathsf{Adv}_{\mathcal{A}}$ *is negligible. Therefore,* $\mathsf{Adv}_{\mathcal{B}}$ *is negligible. This proves CPA security against decryption attacks.*