Advanced Cryptography — Final Exam

Serge Vaudenay

26.6.2019

- duration: 3h
- 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 Minimal Number of Samples to Distinguish Distributions

We consider two probability distributions P_0 and P_1 over a set $\mathcal{Z}$. We denote by $d(P_0, P_1)$ the *statistical distance* between them, which is

$$d(P_0, P_1) = \frac{1}{2} \sum_{z \in \mathcal{Z}} |P_0(z) - P_1(z)|$$

We also define the *Hellinger distance*

$$H(P_0, P_1) = \sqrt{1 - \sum_{z \in \mathcal{Z}} \sqrt{P_0(z) P_1(z)}}$$

This is a distance in the sense that we always have $H(P_0, P_1) \geq 0$, $H(P_0, P_1) = 0 \iff P_0 = P_1$, and the triangular inequality. We further define the *fidelity*

$$F(P_0, P_1) = 1 - H(P_0, P_1)^2$$

The Fuchs - van de Graaf inequalities relate d and F as follows

$$1 - F(P_0, P_1) \leq d(P_0, P_1) \leq \sqrt{1 - F(P_0, P_1)^2}$$

Given two distributions P and Q, we denote by $P \otimes Q$ the distribution of a pair (X, Y) of independent variables X and Y such that X follows P and Y follows Q. We also denote $P^{\otimes n} = \overbrace{P \otimes \cdots \otimes P}^{n \text{ times}}$.

We are interested in distinguishing the two distributions based on a vector of n i.i.d. samples following one or the other distribution. Given a real number $t \in [0, 1]$, we let n_t be the minimal integer such that there exists a distinguisher using n_t samples with advantage at least t.

Q.1 By using an easy bound on the statistical distance, show that for all t, we have

$$n_t \geq \frac{t}{d(P_0, P_1)}$$

Q.2 Prove that $F(P_0^{\otimes n}, P_1^{\otimes n}) = F(P_0, P_1)^n$.
HINT: first prove $F(P_0 \otimes Q_0, P_1 \otimes Q_1) = F(P_0, P_1)F(Q_0, Q_1)$.

Q.3 By writing $D_{1/2}(P_0\|P_1) = -2 \cdot \log_2 F(P_0, P_1)$, prove that

$$n_t \geq \frac{-\log_2(1 - t^2)}{D_{1/2}(P_0\|P_1)}$$

HINT: use the same technique as in Q.1 but get rid of d.

Q.4 Complete the previous bound by proving

$$\frac{-\log_2(1 - t^2)}{D_{1/2}(P_0\|P_1)} \leq n_t < 1 + \frac{-2 \cdot \log_2(1 - t)}{D_{1/2}(P_0\|P_1)}$$

HINT: use the second Fuchs - van de Graaf inequality.

Q.5 Prove that the minimum number n of samples to distinguish P_0 from P_1 with advantage at least $\frac{1}{2}$ is such that

$$\frac{0.41}{D_{1/2}(P_0\|P_1)} < n < 1 + \frac{2}{D_{1/2}(P_0\|P_1)}$$

2 An IND-CCA Variant of the ElGamal Cryptosytem

Given a key derivation function H and a correct symmetric encryption scheme E/D which can be computed in polynomial time, we define the following cryptosystem:

$\mathsf{Setup}(1^s) \to \mathsf{pp}$: generate a group G and its prime order q and define some public parameters pp from which we can extract s, q, the neutral element 1, a generator g, and parameters to be able to make multiplications in polyomially bounded time in terms of s. We assume that group elements have a unique representation.

$\mathsf{Gen}(\mathsf{pp}) \to \mathsf{pk}, \mathsf{sk}$: pick $x_1, x_2 \in \mathbf{Z}_q$, compute $X_1 = g^{x_1}$, $X_2 = g^{x_2}$, and define $\mathsf{pk} = (\mathsf{pp}, X_1, X_2)$, $\mathsf{sk} = (\mathsf{pp}, x_1, x_2)$.

$\mathsf{Enc}(\mathsf{pk}, m) \to \mathsf{ct}$: pick $y \in \mathbf{Z}_q$, compute $Y = g^y$, $Z_1 = X_1^y$, $Z_2 = X_2^y$, $k = H(Y, Z_1, Z_2)$, $c = E_k(m)$, and define $\mathsf{ct} = (Y, c)$.

$\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) \to m$: [to be defined]

We want to prove the IND-CCA security in the random oracle model, which is defined by the following game Γ_b with an adversary $\mathcal{A}$ and the bit b:

Game Γ_b
- pick a function H at random
- $\mathsf{Setup} \xrightarrow{\$} \mathsf{pp}$
- $\mathsf{Gen}(\mathsf{pp}) \xrightarrow{\$} (\mathsf{pk}, \mathsf{sk})$
- $\mathcal{A}_1^{\mathsf{OH},\mathsf{ODec}_1}(\mathsf{pk}) \xrightarrow{\$} (\mathsf{pt}_0, \mathsf{pt}_1, \mathsf{st})$
- **if** $|\mathsf{pt}_0| \neq |\mathsf{pt}_1|$ **then return** 0
- $\mathsf{ct}^* \xleftarrow{\$} \mathsf{Enc}^{\mathsf{OH}}(\mathsf{pk}, \mathsf{pt}_b)$
- $\mathcal{A}_2^{\mathsf{OH},\mathsf{ODec}_2}(\mathsf{st}, \mathsf{ct}^*) \xrightarrow{\$} z$
- **return** z

Oracle $\mathsf{OH}(\mathsf{input})$
- **return** $H(\mathsf{input})$

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

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

Q.1 Describe the decryption algorithm and prove that we have a correct public-key cryptosystem.

Q.2 Let Γ'_b be the following variant of Γ_b:

Game Γ'_b

1: $\mathsf{Setup} \xrightarrow{\$} \mathsf{pp}$
2: $\mathsf{Gen}(\mathsf{pp}) \xrightarrow{\$} (\mathsf{pk}, \mathsf{sk})$
3: $(\mathsf{pp}, X_1, X_2) \leftarrow \mathsf{pk}$
4: initialize associative array T to empty
5: $\mathcal{A}_1^{\mathsf{OH},\mathsf{ODec}_1}(\mathsf{pk}) \xrightarrow{\$} (\mathsf{pt}_0, \mathsf{pt}_1, \mathsf{st})$
6: **if** $|\mathsf{pt}_0| \neq |\mathsf{pt}_1|$ **then return** 0
7: pick $y^* \in \mathbf{Z}_q$
8: $Y^* \leftarrow g^y$, $Z_1^* \leftarrow X_1^{y^*}$, $Z_2^* \leftarrow X_2^{y^*}$
9: $k^* \leftarrow \mathsf{OH}(Y^*, Z_1^*, Z_2^*)$
10: $c^* \leftarrow E_{k^*}(\mathsf{pt}_b)$
11: $\mathsf{ct}^* \leftarrow (Y^*, c^*)$
12: $\mathcal{A}_2^{\mathsf{OH},\mathsf{ODec}_2}(\mathsf{st}, \mathsf{ct}^*) \xrightarrow{\$} z$
13: **return** z

Oracle $\mathsf{OH}(\mathsf{input})$

1: **if** $T(\mathsf{input})$ is not defined **then**
2: pick $T(\mathsf{input})$ at random
3: **end if**
4: **return** $T(\mathsf{input})$

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

5: **return** $\mathsf{Dec}^{\mathsf{OH}}(\mathsf{sk}, \mathsf{ct})$

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

6: $(Y, c) \leftarrow \mathsf{ct}$
7: **if** $(Y, c) = \mathsf{ct}^*$ **then return** $\perp$
8: **if** $Y = Y^*$ **then return** $D_{k^*}(c)$
9: **return** $\mathsf{Dec}^{\mathsf{OH}}(\mathsf{sk}, \mathsf{ct})$

Prove that $\Pr[\Gamma_b \to 1] = \Pr[\Gamma'_b \to 1]$ for all b.

Q.3 Let Γ''_b be a variant of Γ'_b in which Step 9 of the game is replaced by

9: pick k^* at random

We define the failure event F that OH is queried with input (Y^*, Z_1^*, Z_2^*) in Γ_b' at some time during the game except on Step 9. Prove that $|\Pr[\Gamma_b' \to 1] - \Pr[\Gamma_b'' \to 1]| \leq \Pr[F]$.

Q.4 We say that E/D is secure if for any PPT algorithm $\mathcal{B}$, the advantage

$$\mathsf{Adv}_{\mathcal{B}} = \Pr[\Gamma_1^* \to 1] - \Pr[\Gamma_0^* \to 1]$$

is negligible, with Γ_b^* defined as follows:

Game Γ_b^*
1: $\mathcal{B}_1() \xrightarrow{\$} (m_0, m_1, \mathsf{st})$
2: **if** $|m_0| \neq |m_1|$ **then return** 0
3: pick a random key k^*
4: $c^* \leftarrow E_{k^*}(m_b)$
5: $\mathcal{B}_2^{\mathsf{OD}}(\mathsf{st}, c^*) \xrightarrow{\$} z$
6: **return** z

Oracle $\mathsf{OD}(c)$:
1: **if** $c = c^*$ **then return** $\perp$
2: **return** $D_{k^*}(c)$

Prove that if E/D is secure, then $\Pr[\Gamma_1'' \to 1] - \Pr[\Gamma_0'' \to 1]$ is negligible.

Q.5 We consider the game Γ_b' from Q.2 and the event F from Q.3. We consider a variant $\overline{\Gamma}_b$ of Γ_b' as follows:

Game $\overline{\Gamma}_b$
1: $\mathsf{Setup} \xrightarrow{\$} \mathsf{pp}$
2: $\mathsf{Gen}(\mathsf{pp}) \xrightarrow{\$} (\mathsf{pk}, \mathsf{sk})$
3: $(\mathsf{pp}, X_1, X_2) \leftarrow \mathsf{pk}$, $(\mathsf{pp}, x_1, x_2) \leftarrow \mathsf{sk}$
4: initialize associative arrays Good and T to empty
5: $\mathcal{A}_1^{\mathsf{OH},\mathsf{ODec}_1}(\mathsf{pk}) \xrightarrow{\$} (\mathsf{pt}_0, \mathsf{pt}_1, \mathsf{st})$
6: **if** $|\mathsf{pt}_0| \neq |\mathsf{pt}_1|$ **then return** 0
7: pick $y^* \in \mathbf{Z}_q$
8: $Y^* \leftarrow g^{y^*}$, $Z_1^* \leftarrow X_1^{y^*}$, $Z_2^* \leftarrow X_2^{y^*}$
9: $k^* \leftarrow \mathsf{OH}(Y^*, Z_1^*, Z_2^*)$
10: $c^* \leftarrow E_{k^*}(\mathsf{pt}_b)$
11: $\mathsf{ct}^* \leftarrow (Y^*, c^*)$
12: $\mathcal{A}_2^{\mathsf{OH},\mathsf{ODec}_2}(\mathsf{st}, \mathsf{ct}^*) \xrightarrow{\$} z$
13: **return** z

Oracle $\mathsf{OH}(\mathsf{input})$
1: $(Y, Z_1, Z_2) \leftarrow \mathsf{input}$
2: **if** $Z_1 = Y^{x_1}$ and $Z_2 = Y^{x_2}$ **then**
3: **if** $\mathsf{Good}(Y)$ undefined **then**
4: pick $\mathsf{Good}(Y)$ at random
5: **end if**
6: **return** $\mathsf{Good}(Y)$
7: **else**
8: **if** $T(\mathsf{input})$ is not defined **then**
9: pick $T(\mathsf{input})$ at random
10: **end if**
11: **return** $T(\mathsf{input})$
12: **end if**

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

Oracle $\mathsf{ODec}_2(\mathsf{ct})$:
14: $(Y, c) \leftarrow \mathsf{ct}$
15: **if** $(Y, c) = \mathsf{ct}^*$ **then return** $\perp$
16: **if** $Y = Y^*$ **then return** $D_{k^*}(c)$
17: **return** $\mathsf{Dec}^{\mathsf{OH}}(\mathsf{sk}, \mathsf{ct})$

We define the event $\overline{F}$ in $\overline{\Gamma}_b$ as the event F in Γ_b'. Prove that $\Pr[\overline{\Gamma}_b \to 1] = \Pr[\Gamma_b' \to 1]$ and that $\Pr[F] = \Pr[\overline{F}]$.

Q.6 We define the Strong Twin Diffie-Hellman game as follows:

Game STDH:
1: $\mathsf{Setup} \xrightarrow{\$} \mathsf{pp}$
2: pick $x_1, x_2 \in \mathbf{Z}_q$
3: $X_1 \leftarrow g^{x_1}$, $X_2 \leftarrow g^{x_2}$
4: pick $y^* \in \mathbf{Z}_q$
5: $Y^* \leftarrow g^{y^*}$, $Z_1^* \leftarrow X_1^{y^*}$, $Z_2^* \leftarrow X_2^{y^*}$
6: $\mathcal{C}^{\mathsf{ODTDH}}(\mathsf{pp}, X_1, X_2, Y^*) \xrightarrow{\$} (Z_1, Z_2)$
7: **return** $1_{Z_1 = Z_1^*, Z_2 = Z_2^*}$

Oracle $\mathsf{ODTDH}(Y, Z_1, Z_2)$:
1: **return** $1_{Z_1 = Y^{x_1} \wedge Z_2 = Y^{x_2}}$

We consider the game $\overline{\Gamma}_b$ and the event $\overline{F}$. Given an adversary $\mathcal{A}$ playing the $\overline{\Gamma}_b$ game, construct an adversary $\mathcal{C}$ playing the STDH game such that

$$\Pr[\overline{F}] = \Pr[\mathsf{STDH}_{\mathcal{C}} \to 1]$$

HINT: find a way to simulate $\overline{\Gamma}_b$ without sk.

Q.7 Summarize all what we did and prove that the cryptosystem is IND-CCA secure in the random oracle model, under the assumption that the strong twin Diffie-Hellman problem STDH is hard and that the E/D scheme is secure.
NOTE: in a twin exercise, we show STDH is equivalent to CDH.

3 Equivalence of CDH and the Strong Twin DH Problems

Note: this is a twin exercise of "An IND-CCA Variant of the ElGamal Cryptosystem". However, both exercises are totally independent.

We define the Strong Twin Diffie-Hellman STDH game and the classical CDH game as follows:

Game STDH:
$\mathsf{Setup} \xrightarrow{\$} \mathsf{pp}$
pick $x_1, x_2 \in \mathbf{Z}_q$
$X_1 \leftarrow g^{x_1}$, $X_2 \leftarrow g^{x_2}$
pick $y^* \in \mathbf{Z}_q$
$Y^* \leftarrow g^{y^*}$, $Z_1^* \leftarrow X_1^{y^*}$, $Z_2^* \leftarrow X_2^{y^*}$
$\mathcal{A}^{\mathsf{ODTDH}}(\mathsf{pp}, X_1, X_2, Y^*) \xrightarrow{\$} (Z_1, Z_2)$
return $1_{Z_1=Z_1^*, Z_2=Z_2^*}$

Oracle $\mathsf{ODTDH}(Y, Z_1, Z_2)$:
return $1_{Z_1=Y^{x_1} \wedge Z_2=Y^{x_2}}$

Game CDH
$\mathsf{Setup} \xrightarrow{\$} \mathsf{pp}$
pick $x, y \in \mathbf{Z}_q$
$X \leftarrow g^x$, $Y \leftarrow g^y$
$\mathcal{B}(\mathsf{pp}, X, Y) \xrightarrow{\$} Z$
return $1_{Z=Y^x}$

Our goal is to prove the equivalence between the two problems.

Here, $\mathsf{Setup}(1^s) \to \mathsf{pp}$ is an algorithm which generates a group G and its prime order q in some public parameters pp. Given pp, we can extract q, the neutral element 1, a generator g, and parameters to be able to make multiplications in polyomially bounded time. We assume that group elements have a unique representation.

Q.1 Given an adversary $\mathcal{B}$ playing the CDH game, construct and adversary $\mathcal{A}$ playing the STDH game such that $\Pr[\mathsf{STDH} \to 1] \geq \Pr[\mathsf{CDH} \to 1]^2$.

Q.2 We define the following random variables: $x, u, v, y, z_1, z_2 \in \mathbf{Z}_q$, $x_1 = x$, and $x_2 = v - xu \bmod q$. We assume that (x, u, v) is uniformly distributed in $\mathbf{Z}_q^3$ and that $(y, z_1, z_2) = f(x_1, x_2)$ for some function f.

Q.2a Prove that (x_1, x_2, u) is uniformly distributed in $\mathbf{Z}_q^3$.

Q.2b Prove that

$$\Pr[z_1u+z_2 = yv | z_1 = yx_1, z_2 = yx_2] = 1 \quad , \quad \Pr[z_1u+z_2 = yv | z_1 \neq yx_1 \vee z_2 \neq yx_2] \leq \frac{1}{q}$$

(where equalities are modulo q).

Q.3 Given an adversary $\mathcal{A}$ playing the STDH game, prove that the following $\mathcal{B}$ playing the CDH game is such that $\Pr[\mathsf{CDH} \to 1] \geq \Pr[\mathsf{STDH} \to 1] - \frac{Q}{q}$ where Q is the total number of queries of $\mathcal{A}$.

$\mathcal{B}(\mathsf{pp}, X, Y)$:
pick $u, v \in \mathbf{Z}_q$
$X_1 \leftarrow X$, $X_2 \leftarrow g^v X^{-u}$
simulate $\mathcal{A}(\mathsf{pp}, X_1, X_2, Y) \xrightarrow{\$} (Z_1, Z_2)$ with oracle O instead of ODTDH
return Z_1

Oracle $\mathsf{O}(\hat{Y}, \hat{Z}_1, \hat{Z}_2)$
return $1_{\hat{Z}_1^u \hat{Z}_2 = \hat{Y}^v}$