Advanced Cryptography — Final Exam
Solution

Serge Vaudenay

18.6.2012

- duration: 3h00
- any document is allowed
- a pocket calculator is allowed
- communication devices are not allowed
- the exam invigilators will not answer any technical question during the exam
- the answers to each exercise must be provided on separate sheets
- readability and style of writing will be part of the grade
- do not forget to put your name on every sheet!

1 Some Decisional Diffie-Hellman Problems

For each of the group families below, give their order, say if they are cyclic, and show that the Decisional Diffie-Hellman problem (DDH) is not hard.

Q.1 $G = \mathbf{Z}_p^*$ where p is an odd prime number.

G has order $p-1$. We know from the theory of Galois fields theory that some elements generate $\mathbf{Z}_p^*$. So, it is cyclic.
We define $L(x) \in \{0,1\}$ such that $\left(\frac{x}{p}\right) = (-1)^{L(x)}$. If g is a generator of Z_p^*, we have $L(g^x) = x \bmod 2$ for all x. If (X,Y,Z) is such that $X = g^x$, $Y = g^y$, $Z = g^{xy}$, we must have $L(Z) = L(X)L(Y)$. If (X,Y,Z) is random in $\mathbf{Z}_p^3$, we have $L(Z) = L(X)L(Y)$ with probability $\frac{1}{2}$. So, a distinguisher checking that $L(Z) = L(X)L(Y)$ given (g,X,Y,Z) has an advantage of $\frac{1}{2}$ to distinguish a Diffie-Hellman tuple from a random one.

Q.2 $G = \{-1,+1\} \times H$ where H is a cyclic group of odd prime order q.

G has order $2q$. If h is a generator of H, we can check that $g = (-1,h)$ is a generator of G: for $y = ((-1)^b, x)$, let α be such that $x = h^\alpha$. If $b = \alpha \bmod 2$, then $g^\alpha = y$. Otherwise, $g^{\alpha+q} = y$.
Let $L((-1)^b, x) = b$. Again, a distinguisher checking that $L(Z) = L(X)L(Y)$ will output 1 with probability 1 for a Diffie-Hellman tuple (X,Y,Z) and with probability $\frac{1}{2}$ for a random one. So, the advantage is $\frac{1}{2}$.

Q.3 $G = \mathbf{Z}_q$ where q is a prime number.

Z_q has order q and 1 is a generator. For and integer x, the "logarithm" of x in basis 1 is x, modulo q.
Since the discrete logarithm problem is easy to solve, we can design a trivial distinguisher which checks whether $\log Z = (\log X)(\log Y)$. For a Diffie-Hellman tuple, it produces 1 with probability 1. For a random tuple, it produces 1 with probability $\frac{1}{q}$. So, the advantage is $1 - \frac{1}{q}$.

2 MAC Revisited

This exercise is inspired from Message Authentication, Revisited *by Dodis, Kiltz, Pietrzak, and Wichs. Published in the proceedings of Eurocrypt'12 pp. 355–374, LNCS vol. 7237 Springer 2012.*

Given a security parameter s, a set $\mathcal{X}_s$ and two groups $\mathcal{Y}_s$ and $\mathcal{K}_s$, we define a *function family* by a deterministic algorithm mapping (s,k,x) for $k \in \mathcal{K}_s$ and $x \in \mathcal{X}_s$ to some $y \in \mathcal{Y}_s$, in time bounded by a polynomial in terms of s. (By abuse of notation, we denote $y = f_k(x)$ and omit s.)

We say that this is a *key-homomorphic function* if for any s, any $x \in \mathcal{X}_s$, any $k_1, k_2 \in \mathcal{K}_s$, and any integers a, b, we have

$$f_{ak_1+bk_2}(x) = (f_{k_1}(x))^a (f_{k_2}(x))^b$$

Given a function family f, a function ℓ, and a bit b, we define the following game.

Game $\mathsf{wPRF}_\ell(b)$:

pick random coins r
pick $x_1, \ldots, x_{\ell(s)} \in \mathcal{X}_s$ uniformly
if $b = 0$ **then**
  pick $k \in \mathcal{K}_s$ uniformly
  compute $y_i = f_k(x_i)$, $i = 1, \ldots, \ell(s)$
else
  pick a random function $g : \mathcal{X}_s \to \mathcal{Y}_s$
  compute $y_i = g(x_i)$, $i = 1, \ldots, \ell(s)$
end if
$b' \leftarrow \mathcal{A}((x_1, y_1), \ldots, (x_{\ell(s)}, y_{\ell(s)}); r)$

Given some fixed b, r, and k or g, the game is deterministic and we define $\Gamma^{\mathsf{wPRF}}_{0,r,k}(\mathcal{A})$ or $\Gamma^{\mathsf{wPRF}}_{1,r,g}(\mathcal{A})$ as the outcome b'. We say that f is a *weak pseudorandom function (wPRF)* if for any polynomially bounded function $\ell(s)$ and for any probabilistic polynomial-time adversary $\mathcal{A}$, in the above game we have that $\Pr_{r,k}[\Gamma^{\mathsf{wPRF}}_{0,r,k}(\mathcal{A}) = 1] - \Pr_{r,g}[\Gamma^{\mathsf{wPRF}}_{1,r,g}(\mathcal{A}) = 1]$ is negligible in terms of s. (I.e., the probability that $b' = 1$ hardly depends on b.)

In what follows, we assume a polynomially bounded algorithm Gen which given s generates a prime number q of polynomially bounded length and a (multiplicatively denoted) group G_s of order q with basic operations (multiplication, inversion, comparison) computable in polynomial time. We set $\mathcal{X}_s = \mathcal{Y}_s = G_s$ and $\mathcal{K}_s = \mathbf{Z}_q$. We define $f_k(x) = x^k$. We refer to this as the *DH-based function*.

Q.1 Show that the DH-based function is: 1- a function family which is 2- key-homomorphic.

Clearly, $f_k(x)$ can be computed in polynomial time using the square-and-multiply algorithm. For any $x \in \mathcal{X}_s$, $k_1, k_2 \in \mathcal{K}_s$, and any integers a, b, we have

$$\begin{aligned} f_{ak_1+bk_2}(x) &= x^{ak_1+bk_2} \\ &= \left(x^{k_1}\right)^a \left(x^{k_2}\right)^b \\ &= (f_{k_1}(x))^a (f_{k_2}(x))^b \end{aligned}$$

So, we have the key-homomorphic property.

Q.2 Given (g, X, Y, Z) where g generates G and with $X = g^x$, $Y = g^y$, and $Z = g^z$, show that by picking $\alpha, \beta \in \mathbf{Z}_q$ uniformly at random, then the pair $(g^\alpha X^\beta, Y^\alpha Z^\beta)$ has a distribution which is uniform in G^2 when $z \neq xy$. Show that it has the same distribution as (T, T^y) with T uniformly distributed in the $z = xy$ case.

The distribution of $(g^\alpha X^\beta, Y^\alpha Z^\beta)$ is uniform in G^2 if and only if the distribution of $(\alpha + x\beta, y\alpha + z\beta)$ is uniform in $\mathbf{Z}_q^2$. We have

$$\begin{pmatrix} \alpha + x\beta \\ y\alpha + z\beta \end{pmatrix} = \begin{pmatrix} 1 & x \\ y & z \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

and (α, β) is uniformly distributed in $\mathbf{Z}_q^2$. Since the matrix

$$\begin{pmatrix} 1 & x \\ y & z \end{pmatrix}$$

is invertible when $z \neq xy$, we obtain that the pair is uniformly distributed in that case.
When $z = xy$, we observe that $T = g^\alpha X^\beta$ is uniformly distributed and that $Y^\alpha Z^\beta = T^y$.

Q.3 Show that if the decisional Diffie-Hellman (DDH) problem is hard for Gen, then the DH-based function is a wPRF.
Hint: given an adversary $\mathcal{A}$ playing the $\mathsf{wPRF}_{\ell(s)}(b)$ game, construct a distinguisher $\mathcal{D}(g, X, Y, Z)$ for the DDH problem by taking $x_i = g^{\alpha_i} X^{\beta_i}$ and $y_i = Y^{\alpha_i} Z^{\beta_i}$, $i = 1, \ldots, \ell(s)$.

Let $\mathcal{A}$ be an adversary, let $\ell(s)$ be polynomially bounded.
Let (g, X, Y, Z) be a DDH input to $\mathcal{D}$. We pick $\alpha_i, \beta_i \in \mathbf{Z}_q$ uniformly at random, $i = 1, \ldots, \ell(s)$. We set $x_i = g^{\alpha_i} X^{\beta_i}$ and $y_i = Y^{\alpha_i} Z^{\beta_i}$, $i = 1, \ldots, \ell(s)$. We set $b' = \mathcal{A}((x_1, y_1), \ldots, (x_{\ell(s)}, y_{\ell(s)}); r)$ and return b' as the output from $\mathcal{D}$.
If X, Y, Z are uniformly distributed in G_s, then all (x_i, y_i) are independent and uniformly distributed in G_s^2 in the $z \neq xy$ case. If all x_i's are pairwise distinct, this has the same distribution as in the wPRF *game with $b = 1$. Since $z = xy$ and $x_i = x_j$ occur with negligible probabilities and since $\ell(s)$ is polynomially bounded, we obtain that* $\Pr[\mathcal{D} = 1 | X, Y, Z \text{ uniform}] = \Gamma_{1,r,g}^{\mathsf{wPRF}}(\mathcal{A}) + \mathsf{negl}(s)$.
If $X = g^x$, $Y = g^y$, $Z = g^{xy}$ for x, y random, then $y_i = x_i^y$ for all i, with all x_i independent and uniformly distributed and y is random. This corresponds to the distribution that $\mathcal{A}$ sees in the $b = 0$ case. So, $\Pr[\mathcal{D} = 1 | X, Y \text{ uniform}, Z = \mathsf{DH}(X, Y)] = \Gamma_{0,r,k}^{\mathsf{wPRF}}(\mathcal{A})$ *in that case.*
Finally, the DDH advantage of $\mathcal{D}$ is $\Gamma_{1,r,g}^{\mathsf{wPRF}}(\mathcal{A}) - \Gamma_{0,r,k}^{\mathsf{wPRF}}(\mathcal{A}) + \mathsf{negl}(s)$. Due to the DDH assumption, this must be negligible. So, $\Gamma_{1,r,g}^{\mathsf{wPRF}}(\mathcal{A}) - \Gamma_{0,r,k}^{\mathsf{wPRF}}(\mathcal{A})$ is negligible for all $\mathcal{A}$. So, we have a wPRF.

Given a bit b, we define a MAC scheme based on the three polynomial algorithms KG (to generate a symmetric key), TAG (to compute the authenticated tag of a message based on a key), VRFY (to verify the tag of a message based on a key).

We define the following game.

Game $\mathsf{IND\text{-}CMA}(b)$:

1: pick random coins r

if $b = 0$ **then**
  run $\mathsf{KG} \to k$
  set up the oracle $\mathsf{TAG}_k(\cdot)$
  $b' \leftarrow \mathcal{A}^{\mathsf{TAG}_k(\cdot)}(;r)$
else
  pick a random function $g : \mathcal{X}_s \to \mathcal{Y}_s$
  set up the oracle $g(\cdot)$
  $b' \leftarrow \mathcal{A}^{g(\cdot)}(;r)$
end if

Given some fixed b, r, and k or g, the game is deterministic and we define $\Gamma^{\mathsf{IND\text{-}CMA}}_{0,r,k}(\mathcal{A})$ or $\Gamma^{\mathsf{IND\text{-}CMA}}_{1,r,g}(\mathcal{A})$ as the outcome b'. We say that the MAC is IND-CMA-*secure* if for any probabilistic polynomial adversary $\mathcal{A}$, $\Pr_{r,k}[\Gamma^{\mathsf{IND\text{-}CMA}}_{0,r,k}(\mathcal{A}) = 1] - \Pr_{r,g}[\Gamma^{\mathsf{IND\text{-}CMA}}_{1,r,g}(\mathcal{A}) = 1]$ is negligible in terms of the security parameter s.

We construct a MAC scheme from a key-homomorphic function family as follows:

$$\begin{aligned} \mathsf{KG} &: \text{pick uniformly at random and yield } k_1, k_2 \in \mathcal{K}_s \\ \mathsf{TAG}_{k_1,k_2}(m) &: \text{pick } x \in \mathcal{X}_s, \quad \text{yield } (x, f_{mk_1+k_2}(x)) \\ \mathsf{VRFY}_{k_1,k_2}(m,(x,y)) &: \text{say whether } f_{mk_1+k_2}(x) = y \end{aligned}$$

Q.4 Assume that f is a key-homomorphic function family. Given an IND-CMA-adversary $\mathcal{A}$ on the above MAC scheme, we define a wPRF-adversary $\mathcal{B}$ on f as follows:

1: receives $x_1, y_1, \ldots, x_{\ell(s)}, y_{\ell(s)}$
2: pick $k_1 \in \mathcal{K}_s$ at random
3: simulate $b' \leftarrow \mathcal{A}$
  for the ith chosen message query m from $\mathcal{A}$, simulate answer by $t_i = f_{k_1}(x_i)^{m_i} y_i$
  (if there are more than $\ell(s)$ chosen message queries, abort)

Show that $\Gamma^{\mathsf{wPRF}}_{0,r,k_1}(\mathcal{B}) = \Gamma^{\mathsf{IND\text{-}CMA}}_{0,r,k_1}(\mathcal{A})$ and that $\Gamma^{\mathsf{wPRF}}_{1,r,g}(\mathcal{B}) = \Gamma^{\mathsf{IND\text{-}CMA}}_{1,r,g}(\mathcal{A})$.

If the y_i's are computed from $f_k(x_i)$, then we clearly simulate the IND-CMA *attack with the correct MAC scheme.*
If the y_i's are computed from $g(x_i)$ with a random function g, we observe that $x \mapsto f_{k_1}(x)g(x)$ is also a uniformly distributed function. So, we simulate the IND-CMA *attack with an ideal MAC scheme.*

Q.5 Show that if f is a key-homomorphic wPRF, then the above construction is IND-CMA-secure.

We have already shown that for any IND-CMA *adversary $\mathcal{A}$ we have a wPRF adversary $\mathcal{B}$ with same advantage. Since the function is a wPRF function, the advantage of $\mathcal{B}$ must be negligible. Consequently, for any $\mathcal{A}$, its advantage is negligible. So, the MAC scheme is* IND-CMA-*secure.*

Q.6 Propose an IND-CMA-secure MAC scheme based on the decisional Diffie-Hellman problem.

We merge the two constructions and obtain the following scheme:

$$\begin{aligned} \mathsf{KG} &: \text{pick and yield } k_1, k_2 \in \mathbf{Z}_q \\ \mathsf{TAG}_{k_1,k_2}(m) &: \text{pick } x \in G_s, \quad \text{yield } (x, x^{mk_1+k_2}) \\ \mathsf{VRFY}_{k_1,k_2}(m,(x,y)) &: \text{say whether } x^{mk_1+k_2} = y \end{aligned}$$

Assuming that the DDH problem is hard on G, the MAC scheme is IND-CMA-*secure.*

3 Perfect Unbounded IND is Equivalent to Perfect Secrecy

Given a message block space $\mathcal{M}$ and a key space $\mathcal{K}$, we define a *block cipher* as a deterministic algorithm mapping (k,x) for $k \in \mathcal{K}$ and $x \in \mathcal{M}$ to some $y \in \mathcal{M}$. We denote $y = C_k(x)$. The algorithm must be such that there exists another algorithm C_k^{-1} such that for all k and x, we have $C_k^{-1}(C_k(x)) = x$.

We say that C provides *perfect secrecy* if for each x, the random variable $C_K(x)$ is uniformly distributed in $\mathcal{M}$ when the random variable K is uniformly distributed in $\mathcal{K}$.

Given a bit b, we define the following game.

Game $\mathsf{IND}(b)$:

1: pick random coins r
2: pick $k \in \mathcal{K}$ uniformly
3: run $(m_0, m_1) \leftarrow \mathcal{A}(;r)$
4: compute $y = C_k(m_b)$
5: run $b' \leftarrow \mathcal{A}(y;r)$

Given some fixed b, r, k, the game is deterministic and we define $\Gamma^{\mathsf{IND}}_{b,r,k}(\mathcal{A})$ as the outcome b'. We say that C provides *perfect unbounded IND-security* if for any (unbounded) adversary $\mathcal{A}$ playing the above game, we have $\Pr_{r,k}[\Gamma^{\mathsf{IND}}_{0,r,k}(\mathcal{A}) = 1] = \Pr_{r,k}[\Gamma^{\mathsf{IND}}_{1,r,k}(\mathcal{A}) = 1]$. (That is, the probability that $b' = 1$ does not depend on b.)

Q.1 This question is to see the link with a more standard notion of perfect secrecy.
Let X be a random variable of support $\mathcal{M}$, let K be independent, and uniformly distributed in $\mathcal{K}$, and let $Y = C_K(X)$. Show that X and Y are independent if and only if C provides perfect secrecy as defined in this exercise.
Hint: first show that for all x and y, $\Pr[Y = y, X = x] = \Pr[C_K(x) = y]\Pr[X = x]$. Then, deduce that if C provides perfect secrecy, then Y is uniformly distributed which implies that X and Y are independent. Conversely, if X and Y are independent, deduce that for all x and y we have $\Pr[C_K(X) = y] = \Pr[C_K(x) = y]$. Deduce that $C_K^{-1}(y)$ is uniformly distributed then that $C_K(x)$ is uniformly distributed.

First note that in any case, for any x and y we have

$$\Pr[Y = y, X = x] = \Pr[C_K(X) = y, X = x] = \Pr[C_K(x) = y, X = x] = \Pr[C_K(x) = y]\Pr[X = x]$$

If C provides perfect secrecy, then, we deduce $\Pr[Y = y, X = x] = \frac{1}{\#\mathcal{M}}\Pr[X = x]$. *By summing this over x, we further obtain* $\Pr[Y = y] = \frac{1}{\#\mathcal{M}}$. *So,* $\Pr[Y = y, X = x] = \Pr[Y = y]\Pr[X = x]$ *for all x and y: X and Y are independent.*
Conversely, if X and Y are independent, the above property gives

$$\Pr[C_K(X) = y]\Pr[X = x] = \Pr[Y = y]\Pr[X = x] = \Pr[Y = y, X = x] = \Pr[C_K(x) = y]\Pr[X = x]$$

Since X has support $\mathcal{M}$, *we have* $\Pr[X = x] \neq 0$, *so we can simplify by* $\Pr[X = x]$ *and get* $\Pr[C_K(X) = y] = \Pr[C_K(x) = y]$ *for all x and y. This implies that* $\Pr[C_K^{-1}(y) = x]$ *does not depend on x, so* $C_K^{-1}(y)$ *is uniformly distributed, for all y. So,* $\Pr[C_K(x) = y] = \frac{1}{\#\mathcal{M}}$ *for all x and y. Therefore,* $C_K(x)$ *is uniformly distributed for all x: C provides perfect secrecy as defined in this exercise.*

Q.2 Show that if C provides perfect secrecy, then it is perfect unbounded IND-secure.

Since we have perfect secrecy, when b and r are fixed and k random, y is uniformly distributed whatever b. So, the distribution of $b' = \mathcal{A}(y;r)$ does not depend on b when b and r are fixed. So, $\Pr_k[\Gamma^{\mathsf{IND}}_{0,r,k}(\mathcal{A}) = 1] = \Pr_k[\Gamma^{\mathsf{IND}}_{1,r,k}(\mathcal{A}) = 1]$ for all r. Thus, on average over r, we have $\Pr_{r,k}[\Gamma^{\mathsf{IND}}_{0,r,k}(\mathcal{A}) = 1] = \Pr_{r,k}[\Gamma^{\mathsf{IND}}_{1,r,k}(\mathcal{A}) = 1]$. Therefore, we have perfect unbounded IND-security.

Q.3 Show that if C is perfect unbounded IND-secure, then for all $x_1, x_2, z \in \mathcal{M}$, we have that $\Pr[C_K(x_1) = z] = \Pr[C_K(x_2) = z]$ when K is uniformly distributed in $\mathcal{K}$.
Hint: define a deterministic adversary $\mathcal{A}_{x_1,x_2,z}$ based on x_1, x_2, and z.

We define the following adversary $\mathcal{A}$. First, $\mathcal{A}(;r)$ produces $m_0 = x_1$ and $m_1 = x_2$. Then, $\mathcal{A}(y;r) = 1$ if and only if $y = z$.
We have $\Pr_k[\Gamma^{\mathsf{IND}}_{b,r,k}(\mathcal{A}) = 1] = \Pr[C_K(x_b) = z]$. Furthermore, since $\mathcal{A}$ is deterministic, $\Gamma^{\mathsf{IND}}_{b,r,k}(\mathcal{A})$ does not depend on r. So, $\Pr_{r,k}[\Gamma^{\mathsf{IND}}_{b,r,k}(\mathcal{A}) = 1] = \Pr[C_K(x_b) = z]$.
Since the cipher is perfect unbounded IND-secure, we have $\Pr_{r,k}[\Gamma^{\mathsf{IND}}_{0,r,k}(\mathcal{A}) = 1] = \Pr_{r,k}[\Gamma^{\mathsf{IND}}_{1,r,k}(\mathcal{A}) = 1]$. Therefore, $\Pr[C_K(x_1) = z] = \Pr[C_K(x_2) = z]$.
We deduce that the distribution of $C_K(x)$ does not depend on x.

Q.4 Deduce that if C is perfect unbounded IND-secure, then it provides perfect secrecy.

Given x_0 and y, we have that

$$\Pr[C_K(x_0) = y] \times \#\mathcal{M} = \sum_x \Pr[C_K(x) = y] = \sum_x \Pr[C_K^{-1}(y) = x] = 1$$

The first equality coming from the previous question. So, $\Pr[C_K(x_0) = y] = 1/\#\mathcal{M}$: $C_K(x_0)$ is uniformly distributed, for any x_0. Therefore, we have perfect secrecy.