Advanced Cryptography — Final Exam

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.
Q.2 $G = \{-1, +1\} \times H$ where H is a cyclic group of odd prime order q.
Q.3 $G = \mathbf{Z}_q$ where q is a prime number.

2 MAC Revisited

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.

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.

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 $y_i = Y^{\alpha_i} Z^{\beta_i}$, $i = 1, \ldots, \ell(s)$.

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 IND-CMA(b):

```
pick random coins r
if b = 0 then
    run KG → k
    set up the oracle TAG_k(·)
    b' ← A^{TAG_k(·)}(; r)
else
    pick a random function g : X_s → Y_s
    set up the oracle g(·)
    b' ← A^{g(·)}(; 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:

receives $x_1, y_1, \ldots, x_{\ell(s)}, y_{\ell(s)}$
pick $k_1 \in \mathcal{K}_s$ at random
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 $\Gamma^{\mathsf{wPRF}}_{1,r,g}(\mathcal{B}) = \Gamma^{\mathsf{IND\text{-}CMA}}_{1,r,g}(\mathcal{A})$.

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

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

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 $\mathsf{IND}(b)$:

pick random coins r
pick $k \in \mathcal{K}$ uniformly
run $(m_0, m_1) \leftarrow \mathcal{A}(;r)$
compute $y = C_k(m_b)$
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.

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

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.

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