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 $G = \mathbb{Z}_p^*$ 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 $G = \mathbb{Z}_q$ where $q$ is a prime number.

2 MAC Revisited

Given a security parameter $s$, a set $X_s$ and two groups $Y_s$ and $K_s$, we define a function family by a deterministic algorithm mapping $(s, k, x)$ for $k \in K_s$ and $x \in X_s$ to some $y \in Y_s$, 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 $x \in X_s$, any $k_1, k_2 \in K_s$, 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 $\ell$, and a bit $b$, we define the following game.

**Game wPRF$_{\ell}(b)$:**
1. pick random coins $r$
2. pick $x_1, \ldots, x_{\ell(s)} \in X_s$ uniformly
3. if $b = 0$ then
4. pick $k \in K_s$ uniformly
5. compute $y_i = f_k(x_i), i = 1, \ldots, \ell(s)$
6. else
7. pick a random function $g : X_s \rightarrow Y_s$
8. compute $y_i = g(x_i), i = 1, \ldots, \ell(s)$
9. end if
10. $b' \leftarrow A((x_1, y_1), \ldots, (x_{\ell(s)}, y_{\ell(s)}); r)$
Given some fixed \( b, r, \) and \( k \) or \( g \), the game is deterministic and we define \( \Gamma_{0,r,k}^{\text{wPRF}}(\mathcal{A}) \) or \( \Gamma_{1,r,g}^{\text{wPRF}}(\mathcal{A}) \) 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 \( \Pr_{r,k}[\Gamma_{0,r,k}^{\text{wPRF}}(\mathcal{A}) = 1] - \Pr_{r,g}[\Gamma_{1,r,g}^{\text{wPRF}}(\mathcal{A}) = 1] \) 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 \( \text{Gen} \) which given \( s \) generates a prime number \( q \) of polynomially bounded length and a (multiplicatively denoted) group \( G \) of order \( q \) with basic operations (multiplication, inversion, comparison) computable in polynomial time. We set \( X = G \) and \( \mathcal{K}_0 = \mathbb{Z}_q \). 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 \( X = g^s, Y = g^r, \) and \( Z = g^z \), show that by picking \( \alpha, \beta \in \mathbb{Z}_q \) 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 \( \text{Gen} \), then the DH-based function is a wPRF.

**Hint:** given an adversary \( \mathcal{A} \) playing the 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 \( \text{KG} \) (to generate a symmetric key), \( \text{TAG} \) (to compute the authenticated tag of a message based on a key), \( \text{VRFY} \) (to verify the tag of a message based on a key).

We define the following game.

**Game **IND-CMA\((b)\):

1. pick random coins \( r \)
2. if \( b = 0 \) then
3. run \( \text{KG} \rightarrow k \)
4. set up the oracle \( \text{TAG}_k(\cdot) \)
5. \( b' \leftarrow \mathcal{A}_{\text{TAG}_k(\cdot)}(r) \)
6. else
7. pick a random function \( g : X \rightarrow Y \)
8. set up the oracle \( g(\cdot) \)
9. \( b' \leftarrow \mathcal{A}_{g(\cdot)}(r) \)
10. end if

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

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

\[
\text{KG} : \text{pick uniformly at random and yield } k_1, k_2 \in \mathcal{K}_0 \\
\text{TAG}_{k_1,k_2}(m) : \text{pick } x \in X, \text{ yield } (x, f_{mk_1+k_2}(x)) \\
\text{VRFY}_{k_1,k_2}(m,(x,y)) : \text{say whether } f_{mk_1+k_2}(x) = y
\]

**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:
Show that if $Q.1$

This question is to see the link with a more standard notion of perfect secrecy.

$Q.4$

Deduce that if $Q.5$

Prove that $Q.6$

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 $M$ and a key space $K$, we define a block cipher as a deterministic algorithm mapping $(k, x)$ for $k \in K$ and $x \in M$ to some $y \in M$. 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 $M$ when the random variable $K$ is uniformly distributed in $K$.

Given a bit $b$, we define the following game.

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

Show that $\Gamma^w_{0,k_1}(B) = \Gamma^{IND-CMA}_{0,k_1}(A)$ and that $\Gamma^w_{1,k_1}(B) = \Gamma^{IND-CMA}_{1,k_1}(A)$.

$Q.5$ 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.