Introduction to Cryptography – LMAT2450
Final Examination

January 8, 2014

Instructions

1. You can use the slides presented during the class, and all your personal notes. No book or other printed/photocopied material is allowed.
2. The duration of the exam is 3 hours. Answer the questions on ***separate*** sheets of paper.
3. You have the possibility to present your answers to the examiners.

Question 1 Let $\Pi_{\mathsf{MAC}} = \langle \mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy} \rangle$ be a Message Authentication Code defined as follows.

6

$\mathsf{Gen}(1^\lambda)$: from the security parameter λ, choose $x, y \xleftarrow{R} \{0,1\}^\lambda$ and set $\mathsf{sk} := (x, y)$.

$\mathsf{Mac}_{\mathsf{sk}}(m)$: choose $r \xleftarrow{R} \{0,1\}^\lambda$ and set $m_x := m \oplus r$ and $m_y := r$, then compute and output the tag $t := (t_x, t_y)$ for the message m where $t_x = x \oplus m_x$ and $t_y = y \oplus m_y$.

$\mathsf{Vrfy}_{\mathsf{sk}}(t)$: parse t as $t = (t_x, t_y)$ and compute $m_x = t_x \oplus x$ and $m_y = t_y \oplus y$ from the secret key $\mathsf{sk} = (x, y)$ and then return 1 if and only if $m_x \neq 0^\lambda$, $m_y \neq 0^\lambda$ and $m = m_x \oplus m_y$ hold.

$(1 - \varepsilon(n))$

1. Show that the MAC scheme is correct (i.e. that $\mathsf{Vrfy}_{\mathsf{sk}}(\mathsf{Mac}_{\mathsf{sk}}(m)) = 1$) with overwhelming probability. Check vérification
2. Give the best forgery attack that you can. Mais qui pas bon ① Faut montrer attaque ② le + simple, + chaud à détecter forgery sur ce qu'on veut

Question 2 Let $\Pi_{\mathsf{SIG}} = \langle \mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy} \rangle$ be an EUF-CMA secure signature scheme with signatures that are 2λ-bit long, λ being the security parameter.

6

From Π_{SIG}, we build a second signature scheme $\Pi'_{\mathsf{SIG}} = \langle \mathsf{Gen}, \mathsf{Sign}', \mathsf{Vrfy}' \rangle$, where $\mathsf{Sign}'_{\mathsf{sk}}(m) := \mathsf{Sign}_{\mathsf{sk}}(m)|_\lambda$, that is, the first λ bits of a signature produced by Sign on the same inputs.

1. Define Vrfy' such that Π'_{SIG} is not EUF-CMA anymore.
2. Show one way to define Π_{SIG} and Vrfy' that makes Π'_{SIG} EUF-CMA-secure as well.

Indication: you can start from the assumption of the existence of a secure signature scheme producing signatures of any length linear in λ.

8

Question 3 The IND-CPA security of ElGamal encryption in a group $\mathbb{G}$ relies on the decisional Diffie-Hellman (DDH) assumption in $\mathbb{G}$. In this question, we are interested in extending ElGamal to be able to encrypt l messages in an efficient way. A trivial method is to encrypt each message separetely using ElGamal, but this results in ciphertexts containing $2l$ elements in $\mathbb{G}$, and in the need to select l random values taken in $\mathbb{Z}_q$ (where q is the prime order of the group $\mathbb{G}$).
We propose the following scheme in order to save $l-1$ group elements and $l-1$ random values, while still relying on the same DDH assumption. Let $\Pi_{\mathsf{ENC}} = \langle \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec} \rangle$ be such that:

$\mathsf{Gen}(1^\lambda, l)$: for the security parameter λ, select a generator g of a group $\mathbb{G}$ of prime order $q \geq 2^\lambda$ where the DDH assumption is assumed to hold. Then pick l random secret keys $\alpha_1, \ldots, \alpha_l \xleftarrow{R} \mathbb{Z}_q$ and compute $h_1 = g^{\alpha_1}, \ldots, h_l = g^{\alpha_l}$ in $\mathbb{G}$. Return the public key $\mathrm{pk} = (\mathbb{G}, q, g, h_1, \ldots, h_l)$ and the secret key $\mathrm{sk} = (\alpha_1, \ldots, \alpha_l)$.

$\mathsf{Enc}_{\mathsf{pk}}(m)$: for a message $m = (m_1, \ldots, m_l) \in \mathbb{G}^l$ choose one $r \xleftarrow{R} \mathbb{Z}_q$ and return the ciphertext $c = (c_0, c_1, \ldots, c_l)$ such that $c_0 = g^r$, $c_1 = m_1 \cdot h_1^r, \ldots, c_l = m_l \cdot h_l^r$ in $\mathbb{G}$.

$\mathsf{Dec}_{\mathsf{sk}}(c)$: return the decryption of each ElGamal ciphertext (c_0, c_i) using the secret key α_i, for each $i \in \{1, \ldots, l\}$, in order to recover and return $(m_1, \ldots, m_l)$.

Before answering the following questions, notice that an instance $(g_0, g_1, g_2, g_3) \in \mathbb{G}^4$ of the DDH problem can be sampled as $(g_0, g_1, g_2, g_3) = (g, g^x, g^y, g^{xy+bz})$ for random $x, y, z \xleftarrow{R} \mathbb{Z}_q$. Solving the DDH experiment is then equivalent to guessing the random bit b.

1. Given a DDH instance (g_0, g_1, g_2, g_3), show that, by selecting random $s, t \xleftarrow{R} \mathbb{Z}_q$, we can define $(g_0', g_1', g_2', g_3') := (g_0,\ g_0^s \cdot g_1^t,\ g_2,\ g_2^s \cdot g_3^t)$, which is another DDH instance with the same bit b.

   Hint: simply specify the new x', y', z' and show that they are uniformly distributed in $\mathbb{Z}_q$.

2. Prove the CPA security of the *extended* ElGamal cryptosystem Π_{ENC} for $l = 2$. A fully rigorous reduction is required.

   Hint: apply the argument used to prove the security of the traditional ElGamal encryption scheme by using both DDH instances, (g_0, g_1, g_2, g_3) and (g_0', g_1', g_2', g_3'). Note that $g_0 = g_0'$ and $g_2 = g_2'$.