Introduction to Cryptography – LMAT2450
Final Examination

January 6, 2017

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 Considering a pseudorandom function F and a one-way trapdoor permutation (OWTP) f we build a fixed-length MAC $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$.

$\mathsf{Gen}(1^n)$ picks a random key k to efficiently evaluate $F_k : \{0,1\}^n \mapsto \mathcal{T}$ and chooses an OWTP $f : \{0,1\}^n \mapsto \{0,1\}^n$ with trapdoor key tk (i.e. computing f_{tk}^{-1} is also efficient). It outputs $sk = (k, tk)$ and the number $\ell \in \mathsf{poly}(n)$ of block of messages to authenticate.

$\mathsf{Mac}_{sk}(m)$, to authenticate $m = (m_1, \ldots, m_\ell)$, where $m_1, \ldots, m_\ell \in \{0,1\}^n$, picks a random value $r_1 \leftarrow \{0,1\}^n$ and computes $t_i = F_k(m_i \oplus r_i)$ and $r_{i+1} = f_{tk}^{-1}(r_i)$, for $i = 1$ to ℓ. It outputs $\tau = (t_1, \ldots, t_\ell, r_{\ell+1})$.

$\mathsf{Vrfy}_{sk}(m, \tau)$, from $m = (m_1, \ldots, m_\ell)$ and $r_{\ell+1}$ of $\tau = (t_1, \ldots, t_\ell, r_{\ell+1})$, computes $r_i = f(r_{i+1})$ and $t'_i = F_k(m_i \oplus r_i)$ for $i = 1$ to ℓ. It outputs 1 only if $(t'_1, \ldots, t'_\ell) = (t_1, \ldots, t_\ell)$, and 0 otherwise.

Recall that an OWTP f is easy to compute but hard to invert without an additional secret, denoted tk here, called the trapdoor key. (For instance, the RSA permutation is an OWTP). We ask you to answer the following questions.

1. Describe the message space and the tag space.
2. Show that Π is correct and efficient.
3. Is Π existentially unforgeable against an adaptive chosen-message attack? Either build a reduction or exhibit an attack. Justify your answer.

Question 2 Considering two efficient, correct and existentially unforgeable signature schemes $\Pi_1 = (\mathsf{Gen}_1, \mathsf{Sign}_1, \mathsf{Vrfy}_1)$ and $\Pi_2 = (\mathsf{Gen}_2, \mathsf{Sign}_2, \mathsf{Vrfy}_2)$ against chosen-message attacks, we design a signature scheme $\Pi = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ on a vector of two messages as follows:

$\mathsf{Gen}(1^n)$ generates $(pk_1, sk_1) \leftarrow \mathsf{Gen}_1(1^n)$ and $(pk_2, sk_2) \leftarrow \mathsf{Gen}_2(1^n)$ and sets $pk = (pk_1, pk_2)$ and $sk = (sk_1, sk_2)$.

$\mathsf{Sign}_{sk}(m)$, given $m = (m_1, m_2)$, computes $\sigma_1 \leftarrow \mathsf{Sign}_1(sk_1, m_1)$ and $\sigma_2 \leftarrow \mathsf{Sign}_2(sk_2, m_2)$, and outputs $\sigma = (\sigma_1, \sigma_2)$.

$\mathsf{Vrfy}_{pk}(m, \sigma)$, on input $m = (m_1, m_2)$ and $\sigma = (\sigma_1, \sigma_2)$, outputs 1 only if $\mathsf{Vrfy}_1(pk_1, m_1, \sigma_1) = 1$ and $\mathsf{Vrfy}_2(pk_2, m_2, \sigma_2) = 1$, and 0 otherwise.

We ask you to answer the following questions.

1. Show that Π is existentially unforgeable against *one-time* chosen-message attacks. Recall that "one-time" here means that the adversary may only query a signature on a single message to the signing oracle $\mathsf{Sign}_{sk}(\cdot)$.
   Hint: show how to upper-bound the probability of success against Π by two other probabilities, then build two reductions to upper-bound each of these probabilities.

2. Is Π existentially unforgeable in the general sense, i.e. when the adversary can request a signature on as many chosen messages as wanted? Either build a reduction or exhibit an attack. Justify your answer.

Question 3 Let $\Pi_{com} = (\mathsf{Gen}, \mathsf{Com}, \mathsf{Vrfy})$ be the Gennaro commitment scheme. Recall that $\mathsf{Gen}(1^n)$ outputs $pk = (N, e, a)$ where $N = pq$ is an RSA modulus with $|p| = |q| = n$, $e < N$ is a random prime, a is random invertible element modulo N, and $\mathsf{Com}_{pk}(m)$ picks a random $r \leftarrow \mathbb{Z}_N^*$ and returns $(c, d) = (a^m r^e \bmod N, r)$.

Hereunder, we describe a sigma protocol for Π_{com} in which a prover $\mathcal{P}$ should convince a verifier $\mathcal{V}$ that he/she can efficiently open a given commitment c to some confidential value. At the beginning of the protocol $\mathcal{P}$ and $\mathcal{V}$ are given (pk, c) and a soundness parameter κ, but only $\mathcal{P}$ gets (m, r) such that $\mathsf{Vrfy}_{pk}(c, r, m) = 1$.

Commit: $\mathcal{P}$ picks at random $u \leftarrow \mathbb{Z}_e$ and $s \leftarrow \mathbb{Z}_N^*$, and sends $c' = a^u s^e \bmod N$ to $\mathcal{V}$.

Challenge: $\mathcal{V}$ selects and sends to $\mathcal{P}$ a random κ-bit string ρ.

Response: $\mathcal{P}$ computes the Euclidean division $(\rho m + u) = k \cdot e + z$, where $0 \leq z < e$, and $t = a^k r^\rho s \bmod N$. Eventually, $\mathcal{P}$ returns (z, t).

$\mathcal{V}$ accepts the proof $\pi = \langle c', \rho, (z, t) \rangle$ only if $\mathsf{Vrfy}_{pk}(c^\rho c', t, z) = 1$.

We ask you to answer the following questions.

1. Show the completeness of the above sigma protocol.

2. Assuming that $\kappa = 1$ (only for this item), build an adversary $\mathcal{P}^*$ who does not get (m, r) but who convinces $\mathcal{V}$ with a non negligible probability.

3. Prove that this protocol is honest-verifier zero-knowledge (HVZK).

4. Is this protocol still HVZK if $z = \rho m + u$ over the integers and $t = r^\rho s \bmod N$?