CS 409M : Introduction to Cryptography Fall 2024

Quiz III

Full Marks: 20, **Time**: 1 hour (+ 15 minutes)

Roll Number: ______________________ **Name:** ______________________

1. **Answer each question on a new page of the answer booklet.**
2. Do not use pencils. Pens only!
3. **Write complete reductions/hybrids to get full marks.** Intuitions and wordy answers will only get you part points (if correct).

Problem 1: [4 marks]

Let $\Pi = (\mathsf{Gen}^{\mathsf{td}}, f, \mathsf{Inv})$ be a trapdoor permutation family with its hard-core predicate hc. Consider the following encryption scheme:

- $\mathsf{Gen}(1^n)$: Generate $I, td \leftarrow \mathsf{Gen}^{\mathsf{td}}(1^n)$ and output $pk = I$, $sk = td$.
- $\mathsf{Enc}(pk, m)$: For bit $m \in \{0,1\}$, choose $r \in_R \{0,1\}^n$ and output $(f_I(r), \mathsf{hc}_I(r) \oplus m)$.
- $\mathsf{Dec}(sk, (c_1, c_2))$: Compute the inverse $r = \mathsf{Inv}_{td}(c_1)$, and output $c_2 \oplus \mathsf{hc}_I(r)$.

Is this an IND-CPA secure public key encryption? If yes, give a formal proof of security, else show an attack.

Problem 2: [4 marks]

Let factoring be hard relative to $\mathsf{GenModulus}$, where $\mathsf{GenModulus}(1^n) \rightarrow (N, p, q)$, such that $N = pq$ and p and q are n-bit primes. Assuming that factoring is hard, prove that the following is a trapdoor permutation family:

$$f_N(x) := x^2 \pmod{N}, \ \forall x \in \mathsf{QR}(\mathbb{Z}_N^*),$$

i.e., $x \in \mathbb{Z}_N^*$ such that x is a quadratic residue modulo N.

Problem 3: [9 marks (3+3+3)]

Are the following functions one-way? If yes, prove it, else show an attack:

1. $f(x_1, x_2) = (g(x_1), x_2)$, where $|x_1| = |x_2|$ and g is a one-way function.
2. $f(x, y) = F_x(y)$, where $|x| = |y|$ and F is a length-preserving pseudorandom permutation.
3. Is this a one-way function family? (Prove or show an attack):
   $f_n(x) := pk$, for $(pk, sk) \leftarrow \mathsf{Gen}(1^n; x)$, where $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is an IND-CPA secure public key encryption.

Problem 4: [3 marks]

Let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be an IND-CCA secure public key encryption for 1-bit messages. Consider the following encryption scheme $\Pi' = (\mathsf{Gen}, \mathsf{Enc}', \mathsf{Dec}')$ for message space $\mathcal{M} = \{0,1\}^\ell$, with the same Gen algorithm:

- $\mathsf{Enc}'_{pk}(m) := \mathsf{Enc}_{pk}(m_1), \mathsf{Enc}_{pk}(m_2), \ldots, \mathsf{Enc}_{pk}(m_\ell)$, for $m = m_1, m_2, \ldots, m_\ell$, with $m_i \in \{0,1\}$, $\forall i \in \{1, 2, \ldots, \ell\}$.
- $\mathsf{Dec}'_{sk}(c) := \mathsf{Dec}_{sk}(c_1), \mathsf{Dec}_{sk}(c_2), \ldots, \mathsf{Dec}_{sk}(c_\ell)$, where $c = (c_1, c_2, \ldots, c_\ell)$

Is Π' IND-CCA secure? If yes, prove it. Else, show an explicit attack.

Problem 5 (bonus): [4 marks]

Let $\mathcal{G}$ be a polynomial-time algorithm that, on input 1^n, outputs a prime p and a generator g of $\mathbb{Z}_p^*$. The discrete logarithm problem is believed to be hard for $\mathcal{G}$. This means that the function (family) $f_{p,g}$ where $f_{p,g}(x) := [g^x \pmod{p}]$ is one-way. Let $\operatorname{lsb}(x)$ denote the least-significant bit of x. Show that lsb is not a hard-core predicate for $f_{p,g}$.