CS 409M : Introduction to Cryptography Fall 2024

Assignment 6
End of an Era

Instructor: Sruthi Sekar *TAs:* Giriraj Singh, Gyara Pragathi, Nilabha Saha

Problem 1: One-Wayness

Let F be a length-preserving pseudorandom permutation.

(a) Show that the function $f(x, y) = F_x(y)$ is not one-way.

(b) Show that the function $f(y) = F_{0^n}(y)$ (where $n = |y|$) is not one-way.

(c) Prove that the function $f(x) = F_x(0^n)$ (where $n = |x|$) is one-way.

Problem 2: OWF with Specific Bit-Hiding

Let $x \in \{0, 1\}^n$ and denote $x = x_1 \cdots x_n$. Prove that if there exists a one-way function, then there exists a one-way function f such that for every i there is an algorithm A_i such that

$$\Pr_{x \leftarrow \{0,1\}^n}[A_i(f(x)) = x_i] \geq \frac{1}{2} + \frac{1}{2n}.$$

(This exercise demonstrates that it is not possible to claim that every one-way function hides at least one *specific* bit of the input.)

Problem 3: A New Key Exchange

Consider the following key exchange protocol:

(a) Alice chooses uniform $k, r \in \{0, 1\}^n$, and sends $s := k \oplus r$ to Bob.

(b) Bob chooses uniform $t \in \{0, 1\}^n$, and sends $u := s \oplus t$ to Alice.

(c) Alice computes $w := u \oplus r$ and sends w to Bob.

(d) Alice outputs k and Bob outputs $w \oplus t$.

Show that Alice and Bob output the same key. Analyze the security of the scheme (i.e., either prove its security or show a concrete attack).

Problem 4: KeyXCHG to CPA-PKE

Show that any two-round key-exchange protocol (that is, where each party sends a single message) satisfying Definition 10.1 (from the book[1]) can be converted into a CPA-secure public-key encryption scheme.

Definition 10.1

A key exchange protocol Π is secure in the presence of an eavesdropper if for all probabilistic polynomial-time adversaries $\mathcal{A}$ there is a negligible function negl such that

$$\Pr[KE^{\text{eav}}_{\mathcal{A},\Pi}(n) = 1] \le \frac{1}{2} + \text{negl}(n).$$

Problem 5: The ElGamal Variance Authority

Consider the following variant of ElGamal encryption. Let $p = 2q + 1$, let $\mathbb{G}$ be the group of squares modulo p (so $\mathbb{G}$ is a subgroup of $\mathbb{Z}_p^*$ of order q), and let g be a generator of $\mathbb{G}$. The private key is $(\mathbb{G}, g, q, x)$ and the public key is $(\mathbb{G}, g, q, h)$ where $h = g^x$ and $x \in \mathbb{Z}_q$, choose a uniform $r \in \mathbb{Z}_q$, compute $c_1 := g^r \pmod p$ and $c_2 := h^r + m \pmod p$, and let the ciphertext be $\langle c_1, c_2 \rangle$. Is this scheme CPA-secure? Prove your answer.

Problem 6: Public Key Secure(?)-ity

Consider the following construction:

Construction

Let `GenRSA` be as usual, and define a public-key encryption scheme as follows:

- `Gen`: on input 1^n, run $\texttt{GenRSA}(1^n)$ to obtain (N, e, d). Output the public key $pk = \langle N, e \rangle$, and the private key $sk = \langle N, d \rangle$.
- `Enc`: on input a public key $pk = \langle N, e \rangle$ and a message $m \in \{0, 1\}$, choose a uniform $r \in \mathbb{Z}_N^*$. Output the ciphertext $\langle [r^e \pmod N], \text{lsb}(r) \oplus m \rangle$.
- `Dec`: on input a private key $sk = \langle N, d \rangle$ and a ciphertext $\langle c, b \rangle$, compute $r := [c^d \pmod N]$ and output $\text{lsb}(r) \oplus b$.

Prove that this scheme is CPA-secure.

Problem 7: Hard-Core RSA

Fix an RSA public key $\langle N, e \rangle$ and define

$$\text{half}(x) = \begin{cases} 0 & \text{if } 0 < x < N/2 \\ 1 & \text{if } N/2 < x < N \end{cases}$$

Prove that half is a hard-core predicate for the RSA problem.
Hint: Reduce to hardness of computing lsb.

[1]Introduction to Modern Cryptography, Second Edition - Jonathan Katz, Yehuda Lindell

Problem 8: Strong One-Time Signatures

A strong one-time signature scheme satisfies the following (informally): given a signature σ' on a message m', it is infeasible to output $(m, \sigma) \neq (m', \sigma')$ for which σ is a valid signature on m (note that $m = m'$ is allowed).

Strong One-Time Signature Scheme

Let $\Pi = (\texttt{Gen}, \texttt{Sign}, \texttt{Vrfy})$ be a signature scheme, and consider the following experiment for an adversary $\mathcal{A}$ and parameter n:

The strong one-time signature experiment $\texttt{Sig-forge}^{\texttt{1-strong}}_{\mathcal{A},\Pi}(n)$**:**

i. $\texttt{Gen}(1^n)$ is run to obtain keys (pk, sk).

ii. Adversary $\mathcal{A}$ is given pk and asks a single query m' to oracle $\texttt{Sign}_{\text{sk}}(\cdot)$. Let σ' denote the signature that was returned. $\mathcal{A}$ then outputs (m, σ) where $(m, \sigma) \neq (m', \sigma')$.

iii. The output of the experiment is defined to be 1 if and only if $\texttt{Vrfy}_{\text{pk}}(m, \sigma) = 1$.

A signature scheme $\Pi = (\texttt{Gen}, \texttt{Sign}, \texttt{Vrfy})$ is a strong one-time signature scheme if for all probabilistic polynomial-time adversaries $\mathcal{A}$, there exists a negligible function negl such that:

$$\Pr[\texttt{Sig-forge}^{\texttt{1-strong}}_{\mathcal{A},\Pi}(n) = 1] \leq \text{negl}(n).$$

(a) Assuming the existence of one-way functions, show a one-way function for which Lamport's scheme is not a strong one-time-secure signature scheme.

(b) Construct a strong one-time-secure signature scheme based on any assumption you've seen so far in class.
Hint: Use a particular one-way function in Lamport's scheme.

Problem 9: Varying Lamport

The Lamport scheme uses 2ℓ values in the public key to sign messages of length ℓ. Consider the variant in which the private key contains 2ℓ values $x_1, \ldots, x_{2\ell}$ and the public key contains the values $y_1, \ldots, y_{2\ell}$ with $y_i := f(x_i)$. A message $m \in \{0,1\}^{\ell'}$ is mapped in a one-to-one fashion to a subset $S_m \subset \{1, \ldots, 2\ell\}$ of size ℓ. To sign m, the signer reveals $\{x_i\}_{i \in S_m}$. Prove that this gives a one-time-secure signature scheme. What is the maximum message length ℓ' that this scheme supports?

Problem 10: Soft-Core DLOG

Let $\mathcal{G}$ be a polynomial-time algorithm that, on input 1^n, outputs a prime p with $\|p\| = n$ 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 $\text{lsb}(x)$ denote the least-significant bit of x. Show that lsb is not a hard-core predicate for $f_{p,g}$.