Homework 7

Due: Nov 8, 2024

CS 1510: Intro. to Cryptography and Computer Security

1 CPA-Secure PKE

Consider the following public-key encryption scheme. The public key is $(\mathbb{G}, q, g, h)$ and the secret key is x, generated exactly as in the ElGamal encryption scheme. To encrypt a bit $m \in \mathcal{M}$, where $\mathcal{M} = \{0, 1\}$:

- If $m = 0$, then choose a uniform $y \xleftarrow{\$} \mathbb{Z}_q$, compute $c_1 := g^y$ and $c_2 := h^y$. The ciphertext is $c = \langle c_1, c_2 \rangle$.
- If $m = 1$, then choose independent uniform $y, z \xleftarrow{\$} \mathbb{Z}_q$, compute $c_1 := g^y$ and $c_2 := g^z$. The ciphertext is $c = \langle c_1, c_2 \rangle$.

a. Show how to decrypt a ciphertext c given the secret key x.

b. Prove that this encryption scheme is CPA-secure if DDH is hard relative to $\mathcal{G}$.

2 Attacking the RSA Trapdoor Permutation

We saw in class how RSA is a candidate trapdoor permutation (TDP) with the following algorithms:

- **Key generation**: $\mathsf{KeyGen}(1^k)$ samples two distinct k-bit primes p and q. Let $N = pq$. Pick e that is co-prime to $\varphi(N) = (p-1)(q-1)$, where φ is Euler's totient function. Let d be such that $ed \equiv 1 \mod \varphi(N)$. Output $i = (N, e)$ and $t = d$.
- **Evalution**: $\mathsf{Eval}(i, x)$ checks if $x \in \mathbb{Z}_N^*$, and if so, outputs $x^e \mod N$. Otherwise, it fails.
- **Inversion**: $\mathsf{Invert}(i, t, y)$ checks if $y \in \mathbb{Z}_N^*$, and if so, outputs $y^d \mod N$. Otherwise, it fails.

We will denote the TDP instantiated by $(i, t) \leftarrow \mathsf{KeyGen}(1^k)$ as f_i. Evaluating the TDP is $f_i(x) = \mathsf{Eval}(i, x) = x^e \mod N$. We will now see how this TDP is vulnerable to certain types of attacks.

a. We say that a function f is *malleable* if given the value of $f(x)$, you can compute the value of $f(g(x))$ for some function g of your choice, without knowing x. Prove that f_i is malleable. In particular, show that given the value of $f_i(x)$, it is possible to compute the value of $f_i(g(x))$, where $g(x) = c \cdot x$ for a constant c and unknown x. Assume that $g(x) \in \mathbb{Z}_N^*$ so that $f_i(g(x))$ does not fail.

b. Propose another function $g(x)$ such that f_i is malleable with respect to g. Explain why.

3 Paillier Cryptosystem

Consider a public-key cryptosystem $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ that works as follows:

Gen: First $\mathsf{Gen}(1^k)$ samples two distinct k-bit primes p and q. Let $n = pq$ and α such that $\alpha n \equiv 1 \bmod \varphi(n)$. Set $pk = n$ and $sk = \alpha$ and output (pk, sk). (Note: This is similar to an RSA key pair, only here $e = n$.)

Enc: To encrypt a message m where $0 \le m < n$, pick a random $r \in \mathbb{Z}_n^*$ and treat it as an element of $\mathbb{Z}_{n^2}^*$. Then $\mathsf{Enc}_{pk}(m)$ outputs

$$c = (1+n)^m r^n \bmod n^2$$

where $(1+n)$ is treated as an element of $\mathbb{Z}_{n^2}^*$.

Dec: To decrypt a ciphertext c, $\mathsf{Dec}_{sk}(c)$ computes

$$\begin{aligned} R &= c^\alpha \bmod n \\ z &= \frac{c}{R^n} \bmod n^2 \\ M &= \frac{z-1}{n}. \end{aligned}$$

It then outputs M. Note: The first operation is modulo n, the second is modulo n^2, and the third is simply over the integers.

Also, consider these useful facts about modular arithmetic:

Lemma 1 $(1+n)^\alpha \equiv 1 + \alpha n \mod n^2$.

Lemma 2 $(1+\alpha n)^\beta \equiv 1 \mod n$.

Lemma 3 $x^n \equiv (x \mod n)^n \mod n^2$.

a. Prove that this cryptosystem is correct. In other words, show that $\mathsf{Dec}_{sk}(\mathsf{Enc}_{pk}(m)) = m$. (Hint: how is R related to r? How is z related to $(1+n)^m \bmod n^2$?)

b. What makes this cryptosystem cool is that it is *additively homomorphic*. In other words, if $c_1 \leftarrow \mathsf{Enc}_{pk}(m_1)$ and $c_2 \leftarrow \mathsf{Enc}_{pk}(m_2)$, then

$$\mathsf{Dec}_{sk}(c_1 c_2 \bmod n^2) \equiv m_1 + m_2 \bmod n.$$

Prove this fact.

c. Another property similar to additive homomorphism is that, if $c_1 \leftarrow \mathsf{Enc}_{pk}(m_1)$ and $c_2 \leftarrow \mathsf{Enc}_{pk}(m_2)$, then

$$\mathsf{Dec}_{sk}(c_1^{m_2} \bmod n^2) \equiv \mathsf{Dec}_{sk}(c_2^{m_1} \bmod n^2) \equiv m_1 m_2 \bmod n.$$

Prove that this cryptosystem has this property as well.

4 Lattice-Based Collision-Resistance

Let q, n, m be integers. Let $\mathbf{A}$ be an $n \times m$ matrix with entries in $\mathbb{Z}_q$; let $a_{i,j}$ be the entry found in row i, column j of $\mathbf{A}$. Let $\mathbf{v}$ be an m-dimensional vector with entries in $\mathbb{Z}$. Let $|\mathbf{v}|$ denote the Euclidean length of $\mathbf{v}$; in other words $|\mathbf{v}| = \sqrt{\sum_{i=1}^{m} v_i^2}$, where v_i is the i^{th} entry in $\mathbf{v}$. Let $\mathbf{0}_\ell$ denote the ℓ-dimensional zero vector. We say that $\mathbf{v}$ is an *integer solution* for $\mathbf{A}$ if $\mathbf{A}\mathbf{v} = \mathbf{0}_n \pmod q$; put another way, for $1 \le i \le n$, $\sum_{j=1}^{m} a_{i,j} v_j = 0 \pmod q$. For $\beta \in \mathbb{R}^+$, we say that it is a β-short integer solution for $\mathbf{A}$ if $|\mathbf{v}| \le \beta$. We say that it is a non-zero solution if $\mathbf{v} \neq \mathbf{0}_m$.

For certain settings of q, n, m, β as a function of a security parameter k, the following problem, known as the short integer solution (SIS) problem, is conjectured to be hard:

Definition 1 ((q,n,m,β)-SIS problem) *Given an $n \times m$ matrix $\mathbf{A}$ with entries drawn from $\mathbb{Z}_q$ uniformly at random, find a non-zero β-short integer solution for $\mathbf{A}$.*

Consider the following function $H_{\mathbf{A}} : \{0,1\}^m \mapsto \mathbb{Z}_q^n$. On input an m-bit string x, $H_{\mathbf{A}}$ treats it as an m-dimensional vector $\mathbf{x} \in \mathbb{Z}_q^m$ (since the values 0 and 1 are elements of $\mathbb{Z}_q$) and outputs the vector $\mathbf{A}\mathbf{x}$.

a. For what values of m (as a function of q and n) is the function $H_{\mathbf{A}}$ length-reducing?

b. Show that, given $x \neq y$ such that $H_{\mathbf{A}}(x) = H_{\mathbf{A}}(y)$, you can find a non-zero $\sqrt{m}$-short integer solution for $\mathbf{A}$ in polynomial time.

c. Give a construction of a collision-resistant hash function family whose security relies on the hardness of the (q,n,m,β)-SIS problem, and prove its security.

5 LWE Implies SIS

Prove that the hardness of the LWE problem implies the hardness of the SIS problem (if LWE is hard, then SIS is hard). You may notice that while the parameters (q, n, m) line up between the two problems, β only appears in the SIS problem. As part of your proof, comment on the general constraints on β and where they come up in making the reduction go through. (You need not provide specifics on the size of β in comparison to other parameters, since the other parameters are not concretely specified in the problem statement.)

6 Summary Question

Summarize the most important insights from this week's material, including from the lectures, notes, textbooks, homework problems, and other resources you find helpful, into a one-page resource. We expect that these summary pages will help you with the take-home midterm and final. Please note this question is graded based on completion—we will not be checking it for correctness. However, we will be checking it for relevance to the week's content and length.