Homework 8

Due: November 17, 2023

CS 1510: Intro. to Cryptography and Computer Security

1 The Cramer-Shoup Cryptosystem

In this problem we will discuss the Cramer-Shoup cryptosystem, which roots its security in the DDH assumption. Let us begin with the "lite" version of this cryptosystem:

- Setup: We are given a cyclic group G of prime order q. Both parties also know two distinct generators g and h of G.
- Gen: The public key and secret key are generated as follows: first pick $x, y, a, b \leftarrow \mathbb{Z}_q$ and retain these values as the secret key. The public key will be $A = g^x h^y$ and $B = g^a h^b$.
- Enc: Given some message $m \in G$, first pick a random value $r \leftarrow \mathbb{Z}_q$. Output the tuple $(g^r, h^r, A^r \cdot m, B^r)$.
- Dec: Given the tuple (R, S, P, T) first check that $T = R^a S^b$. If this check passes, output $P/(R^x S^y)$. Otherwise, output $\perp$.

a. Show that the "lite" Cramer-Shoup cryptosystem is not CCA secure.

b. Since you just showed that the reduced version was not CCA secure, we will need to make some modifications to the cryptosystem. Here is the new version:

   - Setup: The setup here is the same as with the "lite" version.
   - KeyGen: The public key will contain the same values g, h, A, and B as in the simplified version, but it will also contain new values $C = g^w h^z$ for $w, z \leftarrow \mathbb{Z}_q$ and H, where H is a collision-resistant hash function. This means the secret key will be (x, y, a, b, w, z).
   - Enc: Given some message $m \in G$, first pick a random value $r \leftarrow \mathbb{Z}_q$. Output the tuple $(g^r, h^r, A^r \cdot m, (BC^\delta)^r)$, where $\delta = H(g^r, h^r, A^r \cdot m)$.
   - Dec: Given the tuple (R, S, P, T) first check that $T = R^{a+\delta w} S^{b+\delta z}$. If this check passes, output $P/(R^x S^y)$. Otherwise, output $\perp$.

   Demonstrate that this cryptosystem is correct; i.e. that given a valid ciphertext, the decryption algorithm will correctly compute the appropriate plaintext.

c. Show why your attack on the "lite" Cramer-Shoup cryptosystem does not work for this strengthened version.

2 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 $1 \leq i \leq n$, $\sum_{j=1}^{m} a_{i,j} v_j = 0 \pmod q$. For $\beta \in \mathbb{R}^+$, we say that it is a β-short integer solution for $\mathbf{A}$ if $|\mathbf{v}| \leq \beta$. 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.

3 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.)

4 Paillier Cryptosystem

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

Gen: First $\mathsf{Gen}(1^k)$ picks two 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 $0 \leq m < n$, 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, $\mathsf{Dec}(PK, SK, c)$ 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 this useful fact about working mod n^2:

Lemma 1 (Useful Fact) $(1+n)^m \equiv 1 + mn \mod n^2$.

a. Prove that this cryptosystem is correct. In other words, show that $\mathsf{Dec}(PK, SK, \mathsf{Enc}(PK, m)) = m$. (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

$$\mathsf{Dec}(PK, SK, c_1 c_2 \bmod n^2) \equiv m_1 + m_2 \bmod n.$$

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

$$\mathsf{Dec}(PK, SK, c_1^{m_2} \bmod n^2) \equiv \mathsf{Dec}(PK, SK, c_2^{m_1} \bmod n^2) \equiv m_1 m_2 \bmod n.$$

Prove that this cryptosystem has this property as well.

5 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. You will be permitted to use this one-page resource (along with the other weeks' resources) on the midterm and final.

Changes to this document prior to the exams are permitted, but for each change, you will be asked to state what you changed and why. For example, if you dropped something and replaced it with something else, justify why the thing you dropped wasn't as important as the thing you inserted, why you think it might be more useful for the exam, etc.

Please note that the purpose of this question is to help you organize and synthesize the material for your own future use. It will be graded based on completion—we will not be checking it for correctness.