Problem 1: Leaky PRF

Let $F : \{0, 1\}^k \times \{0, 1\}^k \rightarrow \{0, 1\}^k$ be a pseudorandom function. Give a construction for a PRF $F' : \{0, 1\}^{k+1} \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ with the property that $F'(s, \cdot)$ can be distinguished from a random function given just one bit of information, namely, the first bit of the seed $s$.

(a) Prove that your construction of $F'$ is a PRF.

(b) Show how the adversary can distinguish $F'$ from random if it knows the first bit of the secret key.

Problem 2: Zero-Knowledge Proofs and Secure Two-Party Computation

Many methods for doing zero-Knowledge proofs are based on very specific languages (e.g. Three-Colorability) or properties of algebraic structures like $\mathbb{Z}_p^*$. Of course an language in NP has a zero-knowledge proof system by reduction to Three-Colorability, the blow-up of the reduction often makes the resulting protocol impractical. In this problem, you will develop a method for doing ZKP for Circuit-SAT without reducing to Three-Colorability.

Recall that we are able to perform a secure two-party computation for any function by using Yao’s garbled circuit protocol. Consider the following protocol for performing a ZKP for a language $L \in \text{NP}$:

(1) The Prover and Verifier are given as input a circuit $C$. Recall that $C \in\text{Circuit-SAT}$ if there exists an input $w$ such that $C(w) = 1$. The Prover’s job is to convince the verifier that such a $w$ exists.

(2) The Verifier generates a garbled version of $C$, and sends it to the prover.

(3) The Prover and Verifier perform an Oblivious Transfer protocol, giving the Prover the inputs keys corresponding to his input. In particular, the Prover has the bits $w_1, \ldots, w_k$, and the Verifier has generated $k$ pairs of keys

$$(K_{w_1}^{\text{in}_1}, K_{w_1}^{\text{in}_2}), (K_{w_2}^{\text{in}_1}, K_{w_2}^{\text{in}_2}), \ldots, (K_{w_k}^{\text{in}_1}, K_{w_k}^{\text{in}_2}).$$

They then run $k$ rounds of one-out-of-two oblivious transfer, giving the Prover the inputs keys corresponding to his input:

$$K_{w_1}^{\text{in}_1}, K_{w_1}^{\text{in}_2}, \ldots, K_{w_k}^{\text{in}_k}.$$

(4) The Prover evaluates the circuit and gives the Verifier $K_b^{\text{out}}$, the key corresponding to the output wire (where $b$ is the output of the circuit).

(5) The Verifier accepts if and only if the Prover returned $K_b^{\text{out}} = K_1^{\text{out}}$ (i.e. the output was 1).
Let $G$ be a cyclic group of order $p$ and $q$ such that $p$ and $q$ are both prime, $p$ is $k$ bits long, and $p = 2q + 1$. We assume that the following distributions are computationally indistinguishable:

\[ D_0 = \{(p, q) \leftarrow \text{SafePrime}(k); g \leftarrow QR_p; x \leftarrow Z_q; y \leftarrow Z_q : (p, g, g^x, g^{xy})\} \]

\[ D_1 = \{(p, q) \leftarrow \text{SafePrime}(k); g \leftarrow QR_q; x \leftarrow Z_q; y \leftarrow Z_q; z \leftarrow Z_q : (p, g, g^x, g^y, g^z)\} \]

Prove that if you have access to a bimorphism $e : G \times G \mapsto G_t$ as described above, then DDH is easy in $G$ that is, distributions $D_0$ and $D_1$ are now distinguishable.

b. Recall the Diffie-Hellman key exchange protocol for two parties. Suppose Alice and Bob have access to a cyclic group $G$ of order $q$. Alice picks $a \leftarrow Z_q$, Bob picks $b \leftarrow Z_q$ and they send each other $A = g^a$ and $B = g^b$ respectively. Now both of them can compute a common key that is known only to the two of them: Alice computes $B^a$ and Bob computes $A^b$ making the shared key

Exam-2
key $g^{ab}$. Give a way of extending this key-exchange protocol for three parties assuming access to a bimorphism $e : G \times G \rightarrow G_t$. Come up with an assumption under which your three-way key-exchange would be secure.

c. These bimorphisms help us construct an encryption scheme called identity-based encryption. In this scheme, every person has their own private key, based on their identity. People can encrypt messages to a specific person and only that person would be able to decrypt the message with his/her private key. The encryption scheme is as follows:

**Setup** Choose a group $G$ of prime order $q$ and choose a bimorphism $e : G \times G \rightarrow G_t$. Let $g$ be a generator of $G$ and $\hat{g} = e(g,g)$ be a generator of $G_t$. Pick hash functions $h_1 : \{0,1\}^* \rightarrow G$ and $h_2 : G_t \rightarrow \{0,1\}^*$. Setup() picks $s \leftarrow Z_q$ and outputs $pk = g^s$ and the master secret key $msk = s$. The master secret key is needed to create the private key for each individual.

**KeyGen** This produces private keys for each person. For any individual Bob, the key will be generated as $K_B = \text{KeyGen}(s, "Bob") = h_1("Bob")^s$

**Encryption** If Alice wants to send message $m$ to Bob, she first picks $r \leftarrow Z_q$ and $\text{Enc}(g, pk, "Bob", m) = (c_1, c_2) = (g^r, m + h_2(e(h_1("Bob")^s, g^r)))$

**Decryption** Bob will decrypt a ciphertext meant for him as follows: Parse ciphertext as $(c_1, c_2)$. Then $\text{Dec}(c_1, c_2, K_B) = c_2 \oplus h_2(e(K_B, c_1))$

Prove that this encryption scheme is correct.

**Problem 4: Lattice-Based Cryptography**

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

For certain settings of $q$, $n$, $m$, $\beta$ 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** $(q,n,m,\beta)$-SIS problem. Given an $n \times m$ matrix $A$ with entries drawn from $Z_q$ uniformly at random, find a non-zero $\beta$-short integer solution for $A$.

Consider the following function $H_A : \{0,1\}^m \rightarrow Z_q^m$. On input an $m$-bit string $x$, $H_A$ treats it as an $m$-dimensional vector $x \in Z_q^m$ (since the values 0 and 1 are elements of $Z_q$) and outputs the vector $Ax$.

a. For what values of $m$ (as a function of $q$ and $n$) is the function $H_A$ length-reducing?

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

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