Homework 5

Due date: Thursday , April 29$^{\text{nd}}$

Question 1 (20 points)

Consider a variant of the Fiat-Shamir transform (Construction 12.9 page 454) in which the signature is (I, s) rather than (r, s) and verification is changed in the natural way. Show that if the underlying identificaiton scheme is secure, then the resulting signature scheme is secure here as well.

Answer: ...

Resource and Collaborator Statement: ...

Question 2 (20 points)

Given a prime $p > 2$ we say that $x \in \mathbb{Z}_p^*$ is a quadratic residue if $x = y^2 \mod p$ for some $y \in \mathbb{Z}_p^*$. Assume that $g \in \mathbb{Z}_p^*$ is a generator such that $\langle g \rangle = \mathbb{Z}_p^*$. Let $QR_p = \{x \in \mathbb{Z}_p^* : \exists y \text{ s.t. } y^2 = x \mod p\}$.

a. Show that QR_p is a subgroup of $\mathbb{Z}_p^*$.

b. Show that $g \notin QR_p$, but that $g^{2i} \in QR_p$ for every $i \geq 0$.

c. Show that $|QR_p| = \frac{p-1}{2}$ (Hint: Look at Lemma 8.37).

d. Show that $y \in QR_p$ if and only if $y^{\frac{p-1}{2}} = 1$. In particular, this means that there is a polynomial time algorithm to test if $y \in QR_p$.

e. Show that the Decisional Diffie-Hellman Problem does not hold over the cyclic group $\mathbb{Z}_p^*$ (although the computational Diffie-Hellman Assumption is believed to hold). Hint: Use the properties you proved in previous items about quadratic residues. You may assume $g \in \mathbb{Z}_p^*$ is a generator such that $\langle g \rangle = \mathbb{Z}_p^*$.

Answer:

Resource and Collaborator Statement: ...

Question 3 (20 points)

Definition 12.14 of the reference book[1] presents a formal definition of weak one-time signature. According to this definition, the adversary makes the single signing query for message m' and will output (σ, m) and wins the **One-time signature** experiment $\mathsf{Sig-forge}^{\mathsf{1-time}}_{\mathcal{A},\Pi}$ if $m \neq m'$ and σ is a valid signature.

A strong one-time secure signature scheme satisfies the following: 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)

1. Give a formal definition of strong one-time secure signatures.
2. 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.
3. Construct a strong one-time secure signature scheme based on any assumption use in the book. **Hint:** Try to find a particular one-way function for which Lamport's signature are strongly secure.

Answer: ...

Resource and Collaborator Statement: ...

Question 4 (20 points)

Consider the following construction of hash function based on discrete logarithm.

We define a fixed length hash function (Gen, H) as follows:

- $s \leftarrow \mathsf{Gen}(1^n)$: On input 1^n, this algorithm runs discrete logarithm parameter generator $\mathcal{G}(1^n)$ to obtains the public parameters of $(\mathbb{G}, q, h_i)$. Then this algorithm randomly samples the group elements $h_2, \ldots, h_t \leftarrow \mathbb{G}$ and set $s := \langle \mathbb{G}, q, (h_1, \ldots, h_t) \rangle$ as the output hash key.
- $h = H^s(x_1, \ldots, x_t)$: This the hash algorithm which takes as input the hash key $s = \langle \mathbb{G}, q, (h_1, \ldots, h_t) \rangle$ and message $(x_1, \ldots, x_t)$ with $x_i \in \mathbb{Z}_q$ for all $1 \leq i \leq t$, and computes the hash h of the input message as follows: $h = \prod_i h_i^{x_i}$.

(a) Prove that if the discrete logarithm problem is hard relative to $\mathcal{G}$, and q is prime, then for any $t = \mathsf{poly}(n)$ the construction is a fixed- length collision resistance hash function.

(b) Discuss how this construction can be used to obtain compression regardless of the number of bits needed to represent elements of $\mathbb{G}$ (as long as it is polynomial in n). You can denote the bit length of elements in $\mathbb{G}$ is a polynomial like $p(n)$.

[1] Introduction to Modern Cryptography, 2nd Edition

Answer: ...

Resource and Collaborator Statement: ...

Question 5 (20 points)

Consider the following Zero-Knowledge Proof for the the DDH problem. In particular, Bob (prover) and Alice (Verifier) are both given a triple (X, Y, Z) where $X, Y, Z \in \langle g \rangle$ are all elements of a cycle group of prime order p. Bob is also given $x, y, z = xy$ such that $X = g^x, Y = g^y$ and $Z = g^z$ and wishes to prove to Alice in Zero-Knowledge that (X, Y, Z) is a DDH triple. Consider the following protocol. 1) Bob picks random integer r_1 and r_2 and sends the triple (X_1, Y_1, Z_1) to Alice where $X_1 = g^{r_1+x}$, $Y_1 = g^{r_2+y}$ and $Z_1 = g^{(r_1+x)(r_2+y)}$. 2) Alice sends a challenge bit b to Bob. 3) Bob reveals $e = r_1 + bx \mod p$ and $f = r_2 + by \mod p$ to Alice. 4) Alice accepts if and only if $X_b = g^e, Y_b = g^f$ and $Z_b = g^{ef}$ where $X_0 := X_1/X$, $Y_0 := Y_1/Y$ and $Z_0 := Z_1/(ZX^fY^e)$.

(a) (2 points) Prove that the protocol is complete.

(b) (3 points) Prove that the protocol is sound in the sense that the probability Alice accepts when (X, Y, Z) is not a DDH triple is at most $\frac{1}{2}$.

(c) (5 points) Prove that the protocol is zero-knowledge (Your proof should work even if the verifier behaves maliciously).

(d) (10 points) Using the Fiat-Shamir paradigm develop a non-interactive version of the above Zero-Knowledge proof (NIZK) in the random oracle model. Your protocol should be complete and should have soundness $2^{-\ell}$ for a security parameter ℓ against any attacker making at most 2^ℓ queries to the random oracle. You should also prove that your protocol is ZK by showing that a simulator can produce an identical looking proof without knowledge of x, y, z (Hint: the simulator should exploit program-ability of the random oracle).

Answer: ...

Resource and Collaborator Statement: ...