Problem 1. (1-out-of-k Oblivious Transfer)

1. Show how to construct an OT$_k^1$ protocol (secure against honest-but-curious adversaries) from a family of trapdoor permutations, for any $k \leq \text{poly}(n)$, where $n$ is the security parameter.

2. Show how to use a single application of an OT$_k^1$ protocol to construct a two-party protocol (secure against honest-but-curious adversaries) for any polynomial-time computable function $f : \{0, 1\}^n \times \{0, 1\}^{\log k} \rightarrow \{0, 1\}$. (Note that the domain of Bob’s input is of size $k$.) How does this construction compare in efficiency to the construction given in class, based on a boolean circuit for computing $f$?

3. Extra credit: Show how to construct an OT$_3^1$ protocol from any OT$_2^1$ protocol.

Problem 2. (Proving Inequality of Encrypted Messages) When we covered homomorphic encryption in class (Lecture Notes 15), we saw various techniques for proving various properties of encrypted messages (such as equality) without revealing any additional information about the messages. With a bit more work, these can be made into genuine zero-knowledge proofs (currently, the proofs reveal information about the randomization used in the encryption process). Here you will see a zero-knowledge protocol for proving inequality of encrypted messages.

Consider a public-key encryption scheme $(G, E, D)$ with the property that ciphertexts can be efficiently re-randomized. That is, there is a probabilistic polynomial-time algorithm $T$ such that given any valid public key $pk$ and a ciphertext $c = E_{pk}(m;r)$ for some message $m$ and randomness $r$, $T(pk,c)$ outputs a random encryption of $m$ with respect to $pk$. That is, $T(pk,c) \equiv E_{pk}(m;R)$ for uniformly random $R$. The homomorphic encryption schemes described in class (e.g. El Gamal, Paillier) both have this property. Assume for simplicity that it is also easy to recognize valid public keys and valid ciphertexts. (This holds for El Gamal.)

1. Prove that the following protocol is an interactive proof system for the language $L = \{(pk, E_{pk}(m_0), E_{pk}(m_1)) : m_0 \neq m_1\}$.

Interactive proof $(P,V)$

Common input: $(pk, c_0, c_1)$

Prover’s private input: $sk$ corresponding to $pk$

(a) $V$: Choose $b \overset{R}{\leftarrow} \{0,1\}$, let $c \overset{R}{\leftarrow} T(c_b)$, and send $c$ to $P$. 

1
(b) \( P \): Let \( m = D_k(c) \). If \( m = m_0 \), let \( g = 0 \), else let \( g = 1 \). Send \( g \) to \( V \).

(c) \( V \): Accept iff \( g = b \).

2. Show that the above protocol is perfect zero knowledge for honest-but-curious verifiers. That is, exhibit a simulator whose output distribution is identical to the view of the honest verifier \( V \) when \((pk, c_0, c_1) \in L\).

Problem 3. (Public-Key Identification Schemes) On Problem Set 6, you showed how to construct a protocol that allows a user to identify herself to a server, provided the user and the server share a secret key \( k \). Here you will see how zero-knowledge proofs can be used to construct public-key identification schemes, where the user has a secret key \( sk \) and publishes a public key \( pk \). The server only needs to know the public key of the user to verify the user’s identity. For security, we require that an adversary who is given the public key \( pk \) and engages in polynomially many executions of the identification protocol with the user still cannot successfully impersonate the user, except with negligible probability.

Here is a construction of such a public-key identification scheme based on the zero-knowledge proof for Quadratic Residuosity given in class. On security parameter \( n \), the user generates her keys by picking two random \( n \)-bit primes \( p_1, p_2 \), computing \( N = p_1 \cdot p_2 \), choosing \( q \leftarrow Z_N^* \), computing \( x = q^2 \mod N \), and setting \( pk = (N, x) \) and \( sk = (N, q) \).

A single execution of the identification protocol between the user \( U \) and a server \( S \) proceeds as follows.

1. \( U = U(sk) \) and \( S = S(pk) \) run \( n \) sequential executions of the zero-knowledge proof for Quadratic Residuosity on input \((N, x)\), with \( S \) playing the role of the verifier and \( U \) playing the role of the prover with \( NP \) witness \( q \).

2. \( S \) accepts if all executions of the zero-knowledge proof are accepting.

You will justify the security of this identification scheme in 3 steps.

1. Argue that the zero-knowledge proof for Quadratic Residuosity on input \((N, x)\) not only proves that \( x \in QR_N \), but actually that the prover ‘knows’ a square root of \( x \). To make this more precise, suppose \( P^* \) is a prover strategy that convinces the verifier to accept with probability at least \( 1/2 + \varepsilon \) in one execution of the Quadratic Residuosity interactive proof, for any constant \( \varepsilon > 0 \). Show how to use \( P^* \) to obtain a square root of \( x \) modulo \( N \) in polynomial time. (Hint: first argue that \( P^* \) can answer both challenges at least an \( \varepsilon \) fraction of the time.)

2. Suppose that an adversary \( A = A(pk) \) (playing the role of \( U \)) convinces the server \( S \) to accept in a single execution of the identification scheme above with nonnegligible probability (over the choice of \( pk \) and the randomness in the interactive proof). Using the previous item, explain how \( A \) can be used to invert Rabin’s function (and thus factor) with nonnegligible probability. (You do not need to give a full formal proof here, since the details are rather messy.)

3. Now use the zero-knowledge property of the Quadratic Residuosity interactive proof to argue that engaging in polynomially many executions of the identification scheme with the honest user \( U = U(sk) \) does not enable an adversary \( A = A(pk) \) to later impersonate \( U \), except with negligible probability (under the Factoring Assumption).
Remark: The ‘Fiat-Shamir heuristic’ is a method for converting identification schemes such as the above into digital signature schemes. The public key and secret key of the signature scheme are as in the identification scheme. To sign a message $m$, the $U = U(sk)$ runs an execution of the ID scheme on its own, but uses a hash of the message, $H(m) \in \{0, 1\}^n$, for the random challenge bits of the verifier in the $n$ executions of the Quadratic Residuosity interactive proof. The intuition is that if $H$ is a strong enough hash function, then an adversary will have no control over these challenge bits (even given hash values on other messages), so it is just like running the actual interactive proof. The resulting signature scheme is conjectured to be secure (and this intuition is supported by a proof of security in the idealized ‘random oracle model’). This heuristic yields some of the most efficient digital signature schemes used in practice.