1 Not a Zero-Knowledge Proof

Consider the following protocol with input an RSA modulus $N$ and a value $x \in \text{QNR}_N$. The prover $P$ knows the factorization of $N$ and wants to prove to the verifier $V$ that $x$ is in $\text{QNR}_N$. Note that here, $\text{QNR}_N$ denotes the set of elements of $\mathbb{Z}_N^*$ that are quadratic nonresidues both mod $p$ and mod $q$.

1. $V$ forms a challenge value as follows: Choose $c \leftarrow \{0, 1\}$ and $r \leftarrow \mathbb{Z}_N^*$, and send $y = r^2 x^c$ to $P$.

2. $P$ uses the factorization of $N$ to determine whether $y \in \text{QR}_N$. If so, let $c' = 0$; otherwise, let $c' = 1$. $P$ sends $c'$ to $V$.

3. $V$ checks that $c' = c$. If so, $V$ accepts, and otherwise rejects.

It turns out that this protocol is sound but not zero-knowledge.

a. Prove that this protocol satisfies the soundness property.

b. Explain where a proof of the zero-knowledge property would break down. Why wouldn’t we be able to build a valid simulator?

c. Explain how a cheating verifier could use an honest prover to learn something.
2 Oblivious Transfer

Suppose that Alice has two binary messages, \( m_0 \) and \( m_1 \), and she wishes to transfer one of them to Bob \( \text{obliviously} \), meaning that Alice does not learn which message Bob received and Bob does not learn more than one of \( m_0 \) and \( m_1 \). Bob has an input bit \( b \) indicating that he wishes to learn \( m_b \). Here is a candidate construction to achieve this goal, assuming that \( m_0 \) and \( m_1 \) are bits.

1. Bob generates a Blum integer \( N \) and retains its factorization \( N = pq \). If \( b = 0 \), Bob sends a value \( y \in \text{QNR}_N \) to Alice. If \( b = 1 \), Bob sends a value \( y \in \text{QR}_N \) to Alice. He also sends \( N \). Alice verifies that \( y \) has Jacobi symbol 1.\(^1\)

2. Bob proves to Alice, using a zero-knowledge proof, that \( N \) is a product of at most two distinct primes. (We will discuss below how this can be done.)

3. Alice and Bob engage in a zero-knowledge proof (outlined below) that the value \( x = (-y) \cdot y \) is in \( \text{QNR}_N \).

4. If Alice is satisfied with the proofs, she picks random values \( r_1, r_2 \leftarrow \mathbb{Z}_N^* \) and sends \( y^{m_0} \cdot r_1^3 \) and \( (-y)^{m_1} \cdot r_2^2 \) back to Bob.

Our goal is to show that this interaction is an oblivious transfer. To prove this, we need to satisfy the following three properties:

- **Correctness**: At the end of the transfer, Bob knows the message \( m_b \) for his chosen bit \( b \).

- **Alice’s security**: Bob does not learn anything about the message \( m_{\bar{b}} \), where \( \bar{b} = b \oplus 1 \). To that end, Bob should have identical views in the cases of \( m_{\bar{b}} = 0 \) and \( m_{\bar{b}} = 1 \).

- **Bob’s security**: Alice does not learn Bob’s bit \( b \); that is, Alice does not learn which of her messages was actually received by Bob. To that end, Alice’s view when \( b = 0 \) should be indistinguishable from her view when \( b = 1 \).

Before we can prove that these three properties hold, we need to define our zero-knowledge protocol.

\(^1\)You can read about the Jacobi symbol [here](#), but this check just verifies that \( y \) is either in \( \text{QR}_N \) or \( \text{QNR}_N \) as we have defined it.
a. First, let’s try to use the protocol in Problem 1, which we showed was not zero-
knowledge. If this protocol is used in step (3), how is Bob’s security broken? In
particular, describe an attack that Alice can use to learn Bob’s bit $b$.

b. Just because the protocol from Problem 1 isn’t zero-knowledge doesn’t mean that
we can’t make it so. Recall that the protocol works over the group $\mathbb{Z}_N^*$, where the
prover knows the factorization $N = pq$ of the modulus, the verifier does not, and the
prover is trying to convince the verifier that a certain value $x$ is in $\text{QNR}_N$. Using a
perfectly binding, computationally hiding commitment scheme over values in $\mathbb{Z}_N^*$, we
can fix the protocol by adding two extra steps as follows:

(1) $V$ picks $c \leftarrow \{0, 1\}$ and $r \leftarrow \mathbb{Z}_N^*$ and sends $R = r^2 x^c$ to $P$.
(2) $P$ uses $p$ and $q$ to determine whether or not $R \in \text{QR}_N$. If so, let $c' = 0$; otherwise,
    let $c' = 1$. Now, instead of sending $c'$ in the clear, $P$ sends a commitment
    $C = \text{commit}(c')$.
(3) Upon receiving $C$, $V$ sends back the values $r$ and $c$.
(4) $P$ checks that $R = r^2 x^c$. If this check passes, $P$ sends back the opening to the
    commitment. If not, the protocol terminates.
(5) $V$ checks that the opening is valid for the commitment $C$ and also that $c' = c$.
    If both of these checks pass, $V$ accepts, and otherwise rejects.

The completeness and soundness properties follow directly from the solution to Prob-
lem 1 and the fact that $\text{commit}$ is perfectly binding, so they are still satisfied. We now
just need to show that this improved protocol satisfies the zero-knowledge property.
To do so, construct a simulator $S$ that, on input $N$ and $x$, interacts with $V$ in a way
that is indistinguishable from the actual interaction with $P$.

c. Now, using the improved zero-knowledge proof from part (b) (repeated $k$ times to
reduce soundness error to $2^{-k}$), prove that the resulting oblivious transfer protocol is
secure; that is, that is satisfies the three properties outlined above.

d. Explain how to modify the construction to handle bit strings $m_0$ and $m_1$, rather than
bits.

e. **Bonus:** Here is an interesting fact: If $N$ has $\ell$ distinct prime divisors, then one in
every $2^\ell$ elements of $\mathbb{Z}_N^*$ is a square. A corollary is that quadratic residues constitute
exactly one-fourth of the group $\mathbb{Z}_N^*$ if and only if $N$ has exactly two distinct prime
divisors (so $N = p^\alpha q^\beta$ for primes $p \neq q$, where $\alpha, \beta \geq 1$ and $p \equiv q \equiv 3$ (mod 4)).

Use this fact to devise a zero-knowledge proof that allows a prover who knows the
factorization of $N$ to convince a verifier who only knows $N$ that $N$ has at most two
distinct prime divisors. Then show that if we use this proof system in step (2) of the
oblivious transfer, we still get a secure oblivious transfer.
3 Bit Commitment from PRGs

Recall that a bit commitment scheme is a protocol between two parties, the committer $C$ and the receiver $R$. In the protocol, $C$ commits to a single bit value $b \in \{0,1\}$. The protocol consists of two phases:

- During the commitment phase, $C$ and $R$ interact in such a way that $C$ has committed to its secret choice $b$.
- In the opening phase, $C$ reveals its secret choice $b$.

In order for the protocol to be secure, the following (informal) conditions need to hold. First, after the commitment phase, $R$ shouldn’t be able to learn anything about $C$’s secret bit $b$; this is called the hiding property. Second, $C$ shouldn’t be able to change its mind after it has sent its commitment to $R$; this is called the binding property.

Consider the following construction. Let $G : \{0,1\}^k \rightarrow \{0,1\}^{3k}$ be a PRG.

- **Commitment phase**: $R$ sends $z \leftarrow \{0,1\}^{3k}$ to $C$. Then, $C$ generates $s \leftarrow \{0,1\}^k$ and computes $c$ to be $c = G(s)$ if $b = 0$, or $c = G(s) \oplus z$ if $b = 1$. $C$ sends $c$ to $R$.

- **Opening phase**: $C$ sends $s$ and $b$ to $R$. If $b = 0$, $R$ checks that $c = G(s)$; otherwise $R$ checks that $c = G(s) \oplus z$. If the check succeeds, then $R$ outputs $b$. Otherwise, it outputs fail.

a. Prove that this scheme is hiding; that is, $R$ cannot output a correct guess for $b$ with nonnegligible advantage.

b. Prove that this scheme is binding; that is, for all p.p.t. $A$, there exists a negligible $\nu$ such that:

$$\Pr[z \leftarrow \{0,1\}^{3k}; (s_0, s_1) \leftarrow A(1^k, z) : c = G(s_0) = G(s_1) \oplus z] \leq \nu(k)$$

**Hint**: How many $z$'s are there that allow an unbounded committer to change its mind? What is the probability of choosing such a $z$?