Exercises Week 2

Jordi Nadeu Ferran

Exercise 1

Prove that the Zero-Knowledge Proof (ZKP) for quadratic residuosity explained in class is Honest-Verifier Zero Knowledge and Special Sound.

The protocol is defined as follows:

- The common inputs are an integer n and an element $a \in \mathbb{Z}_n^*$.
- The secret witness is x.
- The prover picks a random $r \in \mathbb{Z}_n^*$ and sets
$$\text{cmt} = r^2 \pmod{n}.$$
- The prover sends cmt to the verifier.
- The verifier picks a random bit $b \in \{0, 1\}$ and sends it to the prover.
- The prover anwers:
$$y = a^b \cdot r \pmod{n}.$$

Honest-Verifier Zero Knowledge (HVZK)

To prove that the protocol is Honest-Verifier Zero Knowledge, we must show that a verifier who follows the protocol honestly does not learn any additional information about the secret witness x beyond the fact that $x^2 \equiv a \pmod{n}$.

This is done by constructing a simulator that can generate a valid conversation transcript without knowledge of x.

Simulator Construction:

1. Choose a random challenge $b \in \{0, 1\}$.
2. Pick a random element $y \in \mathbb{Z}_n^*$.
3. Compute the commitment as:
$$\text{cmt} = y^2 \cdot a^{-b} \pmod{n}.$$

Verification: The verifier checks whether:

$$y^2 \equiv \text{cmt} \cdot a^b \pmod{n}.$$

For the simulated transcript, we substitute:

$$\text{cmt} \cdot a^b = (y^2 \cdot a^{-b}) \cdot a^b = y^2 \pmod{n}.$$

Since y and b are chosen uniformly at random, the simulated transcript (cmt, b, y) is indistinguishable from an actual protocol execution.

Therefore, the protocol is Honest Verifier Zero Knowledge.

Special Soundness

To prove special soundness, we must show that given two accepting protocol transcripts with the same commitment cmt but different challenges, we can efficiently extract the secret witness x.

Assumption: Suppose we have two accepting transcripts:

$$(\text{cmt}, b = 0, y_0) \quad \text{and} \quad (\text{cmt}, b = 1, y_1).$$

From the verification conditions, we have:

$$y_0^2 \equiv \text{cmt} \pmod{n}, \quad y_1^2 \equiv \text{cmt} \cdot a \pmod{n}.$$

Dividing the second equation by the first:

$$\frac{y_1^2}{y_0^2} \equiv a \pmod{n}.$$

Taking square roots:

$$\left(\frac{y_1}{y_0}\right)^2 \equiv a \pmod{n}.$$

Thus, we can extract the witness:

$$x \equiv \frac{y_1}{y_0} \pmod{n}.$$

This demonstrates that the protocol satisfies the special soundness property, as the secret witness x can be recovered using two different challenge responses.

Conclusion

Since the protocol satisfies both Honest-Verifier Zero Knowledge and Special Soundness, it is a valid Zero-Knowledge Proof (ZKP) for quadratic residuosity.

Exercise 2

Shows that if the hash function H in Fiat-Shamir is not collision resistant then the obtained signature is not secure (i.e. shows that, given some signatures, is possible to produce a new signature without knowing the secret key).

Background: Fiat-Shamir Transform

The Fiat-Shamir transform converts an interactive Sigma protocol into a non-interactive signature scheme by replacing the verifier's random challenge with a hash of the commitment and the message. Concretely, given a Sigma protocol with:

- Commitment c,
- Challenge ch, and
- Response rsp,

the signature on a message m is formed by computing:

$$ch = H(c \,\|\, m),$$

and outputting the pair (c, rsp) as the signature. Verification involves recomputing the challenge using $H(c \,\|\, m)$ and checking that the response is consistent.

Attack Scenario if H is Not Collision Resistant

Assume that the hash function H is not collision resistant. Then there exists an efficient algorithm to find, for a given commitment c, two distinct messages m and m' such that:

$$H(c \,\|\, m) = H(c \,\|\, m').$$

Suppose an adversary obtains a valid signature (c, rsp) on a message m. The signature is valid because, during verification, the verifier computes:

$$ch = H(c \,\|\, m),$$

and the transcript (c, ch, rsp) satisfies the verification relation of the underlying Sigma protocol.

Since the adversary can find a message $m' \neq m$ with:

$$H(c \,\|\, m') = H(c \,\|\, m),$$

the same pair (c, rsp) will serve as a valid signature for the message m' as well. The verifier, when checking the signature for m', will compute the challenge:

$$H(c \,\|\, m') = H(c \,\|\, m),$$

and thus the verification condition will hold.

Conclusion

If H is not collision resistant, then an adversary can forge a signature on a new message m' by reusing a signature on m, thereby breaking the unforgeability of the signature scheme.

This demonstrates that the collision resistance of the hash function is crucial for the security of the Fiat-Shamir based signature.