Introduction to Cryptography – LMAT2450
Practical Lesson 8

December 14, 2022

Exercise 1 (Schnorr ZKP with faulty PRG) Let us study what happens when the prover of a Schnorr ZKP uses a faulty random generator. This generator is used to choose the secret $r \in \mathbb{Z}_q$ used to generate the commitment $c = g^r$, where g is a generator of the group $\mathbb{G}$ or prime order q. Assuming that the prover made two proofs, one with secret r_0, and the other one with secret $r_1 = ar_0 + b \mod q$, how can you recover the secret witness, knowing the public values, the transcripts of the proofs, a and b?

Exercise 2 (Perfectly hiding authentication) We work in a group $\mathbb{G}$ of prime order q with generator g. The Schnorr protocol, used to prove the knowledge of discrete logarithm, is (honest-verifier) zero-knowledge. However, the value $y = g^x$ leaks some information about the discrete logarithm x (since there is exactly one such x in $\mathbb{Z}_q$). On the other hand, the Pedersen commitment is perfectly hiding and thus does not reveal information about the committed value. The following protocol attempts to merge the both properties i.e., to prove the knowledge of a commited value under the Pedersen commitment scheme in a zero-knowledge manner.

The protocol. The public inputs of the proof are the group $\mathbb{G}$, the Pedersen public key (g, h) (h is a generator of $\mathbb{G}$ such that $\log_g(h)$ is hard to find for both parties), a security parameter k and a commitment $c \in \mathbb{G}$. The prover's private inputs are x and r in $\mathbb{Z}_q$ s.t. $c = g^x h^r$. The protocol executes as follows.

- The prover chooses $y, s \in_R \mathbb{Z}_q$ and sends the commitment $d = g^y h^s$ to the verifier.
- The verifier chooses the challenge $e \in_R \{0, \ldots, 2^k - 1\}$ and sends it to the prover ($2^k < q$).
- The prover computes the response $z = y - ex \mod q$ and $t = s - er \mod q$ and sends it to the verifier.
- The verifier accepts the proof iff $d = c^e g^z h^t$.

If the verifier accepts the proof, we say that the transcript $\langle d, e, (z, t)\rangle$ is valid.

1. Prove the completeness property of this construction.
2. Assume that an adversary is able to produce two valid responses for two distinct challenges, under the same commitment message. How can you use this faculty to extract an opening of c? Discuss the soundness property of the protocol.
3. Show how a honestly distributed valid transcript $\langle d, e, (z, t)\rangle$ can be simulated from any c without the use of any private input.

Exercise 3 (Designated verifier signature) Sometimes, we want to have *off-the-record* conversations. Suppose Alice wants to send a message m to Bob. She wants to be sure that Bob knows that the message comes from her, but she also wants to be sure that Bob will not be able to prove to anyone else that she sent that message.

If Alice signs the message, the first goal can be achieved: Bob can be sure that the message originates from Alice. But the signature can also be verified by anyone else, so Bob can prove that Alice sent the message.

This can be avoided using a *designated verifier signature*. The idea is that Alice will send something that says: "either this message was signed by Alice or it was signed by Bob". We assume that the Schnorr signature scheme is used, that it operates in a group $\mathbb{G}$ of prime order q generated by g, that Alice's public/private key pair is $(h_A = g^{x_A}, x_A)$ and that Bob's public/private key pair is $(h_B = g^{x_B}, x_B)$.

1. Remember that a Schnorr signature is essentially a Schnorr proof of knowledge of a private key made non-interactive, and in which the message is added to the inputs of the hash function. Using the generic technique proposed to make disjunctive proofs, explain how Alice can modify this signature operation in such a way that it can be either a signature computed by Alice, or a signature computed by Bob.

2. Explain why Bob can be convinced that a message authenticated as proposed in the previous step comes from Alice.

3. Suppose that Bob wants to convince a third party that Alice sent that authenticated message and forwards the message and its signature to the third party, as evidence. Explain why this third party should not be convinced.