ETH Zurich, Department of Computer Science
SS 2017

Dr. Martin Hirt
Chen-Da Liu Zhang

Cryptographic Protocols
Exercise 2

2.1 Complexity Theory

In the lecture we defined the notion of polynomial, negligible and noticeable functions. We also defined complexity classes such as **P** and **NP**.

a) Let A be an algorithm that has negligible failure probability to solve a task. Show that repeating the algorithm polynomially many times yields a new algorithm that also has negligible failure probability for the same task.

b) In the lecture it was mentioned that the definition of a noticeable function is not equivalent to the negation of the definition of a negligible function. To prove that, give an example of a function that is neither noticeable nor negligible.

c) In the lecture, two definitions of **NP** were described. In the first definition, a language L is in **NP** if for all x a non-deterministic Turing machine can decide whether $x \in L$ or $x \notin L$ in polynomial time. In the second definition, a language L is in **NP** if there is a verification algorithm V such that for all x we have that $x \in L$ if and only if there is a witness w such that $V(x, w) = 1$, and the witness has polynomial size.

Show that both definitions are equivalent.

2.2 Identification Protocols

Alice and Bob meet in a cryptography conference and agree on working together in a project about zero-knowledge proofs. They exchange some information before each one goes home. At the same conference, Eve wants to collaborate with Bob, but Bob is not interested. When Alice and Bob arrive home, Alice starts chatting with Bob. However, since they chat over an insecure channel, Bob suspects that he might be talking to a malicious Eve instead of Alice, so he first wants to ensure that he is talking to Alice. How can Alice prove her identity to Bob?

a) Assume the information Alice and Bob exchanged is a (secret) key k. In order for Alice to identify herself, she sends k to Bob. How can Eve violate such a scheme?

b) Alternatively, Alice and Bob use the following identification protocol:

1. Alice chooses a random value v and sends (v, c) to Bob, where c is an encryption of v with key k.
2. Bob decrypts c and checks that the result equals v.

How can Eve violate the security of this identification protocol?

c) Modify the protocol in **b)** to solve the security problem.

d) Solve the above problem using the Fiat-Shamir protocol described in the lecture.

1. Argue that Alice always succeeds in authenticating herself, whereas someone else (almost) always fails to do so.

2. Explain why the eavesdropping Eve cannot use the transcript of an authentication by Alice to later impersonate her.
3. What are the advantages/disadvantages of using the Fiat-Shamir protocol for identification?

2.3 Graph (Non-)Isomorphism

In the lecture we saw different interactive proofs between a prover Peggy and a verifier Vic. We saw a protocol for graph isomorphism, and a protocol for graph non-isomorphism (GNI), i.e., for proving that two graphs $\mathcal{G}_0$ and $\mathcal{G}_1$ are isomorphic or not, respectively.

a) Argue why the GNI protocol is not zero-knowledge.

b) A protocol is said to be honest-verifier zero-knowledge if it is zero-knowledge in the case where the verifier follows the protocol. Is the GNI protocol honest-verifier zero-knowledge?

c) Assume that there are three graphs. Construct a honest-verifier zero-knowledge protocol that allows Peggy to prove that not all three graphs are isomorphic.