Advanced Cryptography — Final Exam

Serge Vaudenay

3.7.2024

- duration: 2h
- any document allowed
- a pocket calculator is allowed
- communication devices are not allowed
- the exam invigilators will **not** answer any technical question during the exam
- readability and style of writing will be part of the grade

1 Soundness of DLEQ NIZK in ROM

This exercise studies the Discrete Logarithm EQuality (DLEQ) proof protocol and the batch version.

Q.1 What are the acronyms "NIZK" and "ROM". Explain what they mean.

Q.2 We assume that a setup phase defined a public group of prime order q. By using the generalized Schnorr Σ-protocol, design a Σ-protocol for the relation R between a tuple of group elements (S,T,U,V) and a witness $w \in \mathbf{Z}_q$ which is true if and only if $U = w \cdot S$ and $V = w \cdot T$.

$$R((S,T,U,V),w) \Longleftrightarrow U = w \cdot S \;\wedge\; V = w \cdot T$$

We later on call it the DLEQ protocol.

Q.3 The Fiat-Shamir transform sets the challenge to $e = H(S,T,U,V,\mathsf{message})$, where $\mathsf{message}$ is the first message by the prover, and produces a final "proof" π. If instead we use $e = H(S,T,\mathsf{message})$, show that we can make an algorithm $\mathcal{A}^H(S,T,\mathsf{message}) \to (U,V,\pi)$ making a valid proof for (S,T,U,V), i.e. passing the verification procedure of the Fiat-Shamir transform, even though no witness w may exist.

Q.4 We want to prove the hardness of forging a valid π. Why shall we better avoid using extractors in such a proof?

Q.5 We now take the correct Fiat-Shamir transform. We consider an adversary $\mathcal{A}^H$ who interacts with H and is only bounded by a number B of queries but not bounded in terms of computational complexity. The goal of the adversary is to output a tuple (S,T,U,V,π). If the verification passes but there exists no witness w for (S,T,U,V), we say that the adversary wins.

Q.5a Let $\pi = (\mathsf{message},\mathsf{response})$. Prove that if the final output (S,T,U,V,π) of $\mathcal{A}$ is such that $(S,T,U,V,\mathsf{message})$ was never queried to H, then the probability to win is bounded by $\frac{1}{q}$.

Q.5b For any fresh query $(S,T,U,V,\mathsf{message})$ to H, prove that the probability that there exists $\mathsf{response}$ such that the output $(S,T,U,V,\mathsf{message},\mathsf{response})$ would result in winning is bounded by $\frac{1}{q}$.

Q.5c Deduce that for any $\mathcal{A}^H$ limited to B queries, the probability to win is bounded by $\frac{1+B}{q}$.

2 A Simple PRF

We let $D = \{0,1\}^n$ be the domain of the n-bit strings. Given a hash function H from D to itself, we define the function $f_k(x) = H(x \oplus k)$, for $x, k \in D$. We call k a key and x an input to f. We want to show that f is a PRF in the random oracle model. We consider a PRF game in the random oracle model, where the adversary can query H, as well as the oracle which evaluates the function f_k. Let $\mathcal{A}$ be a PRF adversary and let Γ^b be the PRF game with input bit b. In what follows, we prove that $|\Pr[\Gamma^1_{\mathcal{A}} \to 1] - \Pr[\Gamma^0_{\mathcal{A}} \to 1]|$ is negligible.

Q.1 Why shall we indeed consider adversaries making queries to H?

Q.2 Prove that there exists an adversary $\mathcal{B}$ who never repeats any query to H nor any query to the f-evaluation oracle and such that $\Pr[\Gamma^b_{\mathcal{A}} \to 1] = \Pr[\Gamma^b_{\mathcal{B}} \to 1]$ for every b.

Q.3 Let i be an integer. We define the event E_i that the first i queries made by $\mathcal{B}$ lead to no repetitions on the side of H. Prove that $\Pr[\neg E_{i+1} | E_i] \leq i2^{-n}$.

Q.4 We modify the game Γ^b by making H always answer something random and freshly sampled. We denote by $\bar{\Gamma}^b$ the new game. Deduce from the previous question that $|\Pr[\bar{\Gamma}^1_{\mathcal{B}} \to 1] - \Pr[\Gamma^1_{\mathcal{B}} \to 1]| \leq \frac{m^2}{2}2^{-n}$ and $\Pr[\bar{\Gamma}^0_{\mathcal{B}} \to 1] = \Pr[\Gamma^0_{\mathcal{B}} \to 1]$, where m is the total number of oracle calls.

Q.5 Prove $\Pr[\bar{\Gamma}^1_{\mathcal{B}} \to 1] = \Pr[\bar{\Gamma}^0_{\mathcal{B}} \to 1]$ and conclude.

Q.6 Show that the security bound we obtained is pretty tight by constructing an adversary which (nearly) matches the bound.