

Theoretical Foundations of Cryptography

close-book final exam

June 24, 2003

Instructions

- Cheating will be most seriously punished. Any dishonest attempt from any person in this exam immediately implies an “F” as his/her final grade.
- This is designed to be a 2.5-hour exam. So, you should be able to answer each problem in roughly 30 minutes. You may answer the problems in any order.

Problem 1 (20 points)

- (5 points) Explain what do we mean by “ensembles $\{X_n\}_{n \in \mathbb{N}}$ and $\{Y_n\}_{n \in \mathbb{N}}$ are indistinguishable.”
- (15 points) Let 1^n denote the string with n 1 bits. Let G_ℓ be an arbitrary pseudorandom generator with extension factor $\ell(\cdot)$. Rigorously prove that ensembles $\{G_\ell(U_n)\}_{n \in \mathbb{N}}$ and $\{G_\ell(U_n) \oplus 1^{\ell(n)}\}_{n \in \mathbb{N}}$ are indistinguishable, where \oplus denotes bit-wise exclusive-or.

Problem 2 (20 points)

Let G_ℓ be a pseudorandom generator with extension factor $\ell(n) = n + 1$. Let U be the uniform ensemble. Let X be the ensemble such that X_n is the first n bits of $G_\ell(U_n)$. Prove that X is pseudorandom.

Problem 3 (20 points)

- (5 points) What is a bit-commitment scheme?
- (15 points) Let G_ℓ be a pseudorandom generator with extension factor $\ell(n) = n + 1$. (That is, we have $|G_\ell(x)| = |x| + 1$.) You are asked to *explicitly* construct a bit-commitment scheme based upon G_ℓ . You are welcome to directly use any results that we proved in the class as subroutines of your answer. If you use anything else, please provide its proof.

Problem 4 (20 points)

- (10 points) Let L be a language. What do we mean by “ L admits a computational zero-knowledge proof”?
- (10 points) Let L^* be an NP-complete language that admits a computational zero knowledge proof. Explain how to construct a computational zero-knowledge proof for any language L in NP.

Problem 5 (20 points)

Let G_ℓ be a pseudorandom generator with extension factor $\ell(n) = n + 1$. Prove that H_r with $H_r(x) = G_\ell(G_\ell(x))$ is a pseudorandom generator with extension factor $r(n) = n + 2$.