University of California — Berkeley
CS276: Cryptography
Professors Luca Trevisan and David Wagner

Handout
March 15, 2002

# Midterm

This midterm is due at the start of class on **Tuesday, March 19th.**

When you are asked to prove or disprove a statement $S$, you actually have three options: you may show that $S$ is unconditionally true; you may show that $S$ is unconditionally false; or, you may show that $S$ is conditionally true under some standard assumption (e.g., that one-way functions exist) and false otherwise.

For each problem, be sure to state clearly and precisely what result you are going to prove before proving it.

You do not need to re-prove anything covered in class. This exam is “open-notes” (you may use anything in your notes or the online scribe notes) but “closed-book” (you may not use any textbook or other source).

---

**Problem 1.** [Injective Pseudorandom Generators]

We want to show that pseudorandom generators may or may not be 1-1 functions.

**(a)** Assuming the existence of one-way permutations of superpolynomial security, prove the existence of a pseudorandom generator $G : \{0,1\}^n \to \{0,1\}^{n+1}$ of superpolynomial security with the additional property that $G$ is a 1-1 function.

**(b)** Assuming the existence of pseudorandom generators of superpolynomial security, prove the existence of a pseudorandom generator $G : \{0,1\}^n \to \{0,1\}^{n+1}$ of superpolynomial security with the additional property that $G$ is not a 1-1 function.

**Problem 2.** [A Condition Equivalent to the Existence of One-Way Functions]

We want to show that one-way functions of superpolynomial security exist if and only if there are two efficiently samplable distributions that are computationally indistinguishable and whose supports are “almost disjoint.”

Formally, prove that one-way functions of superpolynomial security exist if and only if there are two probabilistic polynomial time algorithms $A$ and $B$, that on input $1^n$ (a sequence of $n$ ones) produce an output of length $n$ according to different distributions and such that:

- $A(1^n)$ and $B(1^n)$ are computationally indistinguishable distributions with superpolynomial security.

- $\Pr[A(1^n)$ is a possible output of $B(1^n)] \le 1/2^{n/2}$, where the probability is taken over the coin tosses of $A(1^n)$.

**Problem 3.** [2-Universal Hashing]

We say that $H : K \times X \to X$ is an $\epsilon$-almost 2-universal hash if

$$\left| \Pr_{k \leftarrow K}[H_k(x_1) = y_1 \text{ and } H_k(x_2) = y_2] - \frac{1}{|X|^2} \right| \le \epsilon$$

holds for all $x_1, x_2, y_1, y_2 \in X$ with $x_1 \neq x_2$.

In this problem, let $q$ be prime, $\mathbb{Z}_q = \{0, 1, 2, \ldots, q-1\}$, $K_F = \mathbb{Z}_q \times \mathbb{Z}_q$, and define $F : K_F \times \mathbb{Z}_q \to \mathbb{Z}_q$ by

$$F_{\alpha,\beta}(x) = \alpha \times x + \beta \bmod q.$$

It turns out that this $F$ is an $\epsilon$-almost 2-universal hash for $\epsilon = 0$, and moreover there is a general theorem which says that any 0-almost 2-universal hash function is also automatically an $(\infty, 2, 0)$-secure PRF. (You do not need to prove either of these statements; they are simply stated as motivation, and you may assume them to be true.)

**(a)** Prove or disprove: $F$ is an $(\infty, 3, 15/q)$-secure pseudorandom function (PRF) for all $q$.

**(b)** Prove or disprove: for all $H, K, X, \epsilon$, if $H : K \times X \to X$ is an $\epsilon$-almost 2-universal hash, then it is guaranteed to be a $(\infty, 2, 10\epsilon + 10/|X|)$-secure pseudorandom function (PRF).

(You may answer part (b) under the assumption that there is no requirement that $H$ be efficiently computable, if you like.)

**Problem 4.** [Trapdoor Permutations that are also Pseudorandom Permutations]

Assuming the existence of families of trapdoor permutations with superpolynomial security, give a construction of a family of trapdoor permutations $(G, F, I)$ of superpolynomial security and such that the $F(k, \cdot)$ for random $(k, tk) \leftarrow G$ form a family of pseudorandom permutations. That is, for some superpolynomial bounds $S$ and $1/\epsilon$, for every adversary $A$ of running time $\le S$,

$$\left| \Pr_{(k,tk) \leftarrow G}[A^{F(k,\cdot), I(tk,\cdot)} = 1] - \Pr[A^{P, P^{-1}} = 1] \right| \le \epsilon,$$

where $P$ is a random permutation and $P^{-1}$ is the inverse of $P$.

**Problem 5.** [Implications]

Prove or disprove: Assuming there exists a public-key cryptosystem with super-polynomial security in the IND-CPA sense, there exists a symmetric-key cryptosystem with super-polynomial security in the sense of left-or-right security against CPA.

**Problem 6.** [Counter Mode for Public-Key Encryption]

Let $(E, D, G)$ be a public-key cryptosystem with super-polynomial security in the IND-CPA sense. Consider using $(E, D, G)$ in counter mode. In other words, define a public-key cryptosystem $(E', D', G)$, using the same keyspace, as follows:

$$E'_{pk}(M) = (r, E_{pk}(r) \oplus M),$$

where $r$ denotes a fresh value chosen randomly for each message from the message space of $E$, and where "$\oplus$" represents the bitwise xor operation.

Prove or disprove: For all $(E, D, G)$, if $(E, D, G)$ has super-polynomial security in the IND-CPA sense, then $(E', D', G)$ as defined above is guaranteed to also have super-polynomial security in the IND-CPA sense.