COS 522: Complexity Theory : Boaz Barak
Handout 5: Cryptography.

Reading: Chapter 10

Defining security Main model E, D satisfying $D_k(E_k(x)) = x$. Definition of Shannon / unconditional security. The one-time pad.

Lower bound on key length Unconditional security implies key length $\geq$ message length.

Computational security Goldwasser-Micali definition.

Pseudorandom generator Definition, application to encryption, length extension.

Yao's Theorem unpredictability = pseudorandomness.

One-way permutations, one way functions

Goldreich-Levin Hardcore-bit theorem Application to pseudorandom generators.

Pseudorandom functions Construction, applications to message authentication codes, multiple-message private key encryption.

Zero Knowledge Statistical zero knowledge proof for graph isomorphism, computational zero knowledge.

Homework Assignments

§1 (30 points) Show that it is necessary to use computational security even if we only want to ensure that an attacker cannot distinguish between the encryptions of two messages with high probability.

That is, prove for large enough n and every pair of functions $E : \{0,1\}^{0.9n} \times \{0,1\}^n \to \{0,1\}^*$ and $D : \{0,1\}^* \times \{0,1\}^{0.9n} \to \{0,1\}^n$ satisfying

$$\forall x \in \{0,1\}^n, k \in \{0,1\}^{0.9n} D(k, E(k, x)) = x$$

there exists a pair of messages $x_0, x_1 \in \{0,1\}^n$ and a (not necessarily efficiently computable) function $E : \{0,1\}^* \to \{0,1\}$ such that for $i = 0, 1$

$$\Pr_{k \leftarrow_R \{0,1\}^{0.9n}}[A(E(k, x_i)) = i] \geq \tfrac{2}{3}$$

§2 (20 points) Prove the easy direction of Yao's Theorem. That is, prove that if a distribution X over $\{0,1\}^n$ is pseudorandom then there is no polynomial time algorithm P, polynomial $q()$ and $i \in [n]$ such that $\Pr[P(X_1..X_{i-1}) = X_i] \geq 1/2 + 1/q(n)$.

§3 (30 points) A *trapdoor* one-way permutation collection is a collection of functions $\{f_k\}_{k \in I}$ (where $I \subseteq \{0,1\}^*$) such that

(a) f_k is a permutation over, say, $\{0,1\}^{|k|^{1/3}}$

(b) There is an efficient algorithm that given k, x computes $f_k(x)$.

(c) There is a probabilistic key generator algorithm that on input 1^n outputs a pair $\langle k, t \rangle$ such that **(1)** one can compute efficiently from t, y the values $f_k^{-1}(y)$ but **(2)** for every polynomial time algorithm A the probability that $A(k, f_k(x)) = x$ is at most $n^{-\omega(1)}$, where this probability is over the choice of k by the generator and a random x in $\{0,1\}^{|k|^{1/3}}$.

Prove that if trapdoor permutations exist then there exists a secure *public key* encryption scheme, where the adversary breaking the system can be given the encryption key. (Make a suitable definition of security.)

§4 (30 points) The Goldreich-Levin algorithm shows that given black-box access to a function $f : \{0,1\}^n \to \{0,1\}$ that agrees with a linear function L with probability $1/2 + e$, we can compute L with probability $1/\text{poly}(1/\epsilon)$. In particular, this implies that there exist at most $\text{poly}(1/\epsilon)$ such functions. Prove directly that for every function $f : \{0,1\}^n \to \{0,1\}$ there exist at most $1/(10\epsilon^2)$ linear functions that agree with L on a $1/2 + \epsilon$ fraction of the inputs. See footnote for hint[1]

[1] **Hint:** After performing the map $0 \mapsto +1, 1 \mapsto -1$, the linear functions become orthogonal to one another (having inner product zero). Thus, after normalization, they form an orthonormal basis for the space $\mathbb{R}^{2^n}$ and every function f can be expressed in that basis. Use the fact that the L_2 norm is invariant under different orthonormal bases to finish the proof.