Luca Trevisan
March 5, 2009

Notes for Lecture 14 (Draft)

Summary

Today we show how to construct a pseudorandom function from a pseudorandom generator.

1 Construction of Pseudorandom Functions

Lemma 1 (Generator Evaluated on Independent Seeds) *Suppose that $G : \{0,1\}^n \to \{0,1\}^m$ is a (t, ϵ) pseudorandom generator. Fix a parameter k, and define $G^k : \{0,1\}^{kn} \to \{0,1\}^{km}$ as*

$$G^k(x_1, \ldots, x_k) := G(x_1), G(x_2), \ldots, G(x_k)$$

Then G^k is a $(t - O(kn), k\epsilon)$ pseudorandom generator.

Let $G : \{0,1\}^n \to \{0,1\}^{2n}$ be a length-doubling pseudorandom generator. Define $G_0 : \{0,1\}^n \to \{0,1\}^n$ such that $G_0(x)$ equals the first n bits of $G(x)$, and define $G_1 : \{0,1\}^n \to \{0,1\}^n$ such that $G_1(x)$ equals the last n bits of $G(x)$.

The the GGM pseudorandom function based on G is defined as follows: for key $K \in \{0,1\}^n$ and input $x \in \{0,1\}^n$:

$$F_K(x) := G_{x_n}(G_{x_{n_1}}(\cdots G_{x_2}(G_{x_1}(K)) \cdots)) \tag{1}$$

Theorem 2 *If $G : \{0,1\}^n \to \{0,1\}^{2n}$ is a (t, ϵ) pseudorandom generator and G is computable in time r, then F is a $(t/O(nr), \epsilon \cdot n \cdot t)$ secure pseudorandom function.*