Lecture 08 ()

1 Proof of Bit Expanding Function's Pseudo Randomness

Hybrid world + reduction

2 PRGs are One Way Functions):)

In polynomial time

If we have a secure encryption scheme which is secure against key recovery attacks, then we can generate PRGs as:

$$f_m = enc(m, k)$$

One way functions imply PRGs. PRGs imply pretty much everything else. So one way functions are the most fundamental building blocks in cryptography.

3 AES

1. Practical implementation of one way function
2. $AES : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$, $\forall k$, $AES(x,k)$ is a permutation
3. $AES^{-1} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$, $\forall k$, $AES^{-1}(AES(x,k)) = x$