CSA E0 235: Cryptography	January 25, 2018
Scribe for Lecture 5	
Instructor: Arpita Patra	*Submitted by: Pranshu Gaba*

1 Introduction

In the last lecture, we looked at computational security. We made the definitions of PPT/negligible function precise in terms of security parameter n. We looked at the semantic and the indistinguishability based definitions of security.

Now we will look at the pseudorandomness and PRGs. We will find a construcction for ind-secure scheme. We will make use of reduction-based proofs to prove that if PRGs exist, then a construction is secure according to ind definition. Finally, we will discuss the short comings of the current construction/definition, and try to come up with a better defintion.

2 Pseudorandom Generators (PRGs)

G is a PRG if for every PPT D, there is a negligible function negl such that

$$|\Pr[D(r) = 1] - \Pr[D(G(s)) = 1]| \leq \mathsf{negl}(n)$$

3 PRG can be cracked by an unbounded adversary

4 Existence of PRGs

We assume that PRGs exist. It has neither been proven, nor disproven, although it is strongly believed that they exist.

5 Stream Ciphers

6 One-way functions

Functions that are "easy to compute" but almost always "difficult to invert".

6.1 The Inverting Experiment

Experiment $\mathsf{Invert}_{\mathcal{A},f}(n)$

6.2 Mathematical Formulation

Function f is a $\mathsf{one\text{-}way\ function}$ if the following two conditions hold:

- Easy to compute: for every $x \in \{0,1\}^*$, $f(x)$ can be computed in $\mathsf{poly}(n)$ time.

- Hard to invert: For every PPT algorithm A, there is a negligible function $\mathsf{negl}(n)$ such that

$$\Pr(\mathsf{Invert}_{\mathcal{A},f}(n) = 1) \leq \mathsf{negl}(n) \approx \Pr_{x \leftarrow \{0,1\}^n}[Af(x), 1^n) \in f^{-1}(f(x))] \leq \mathsf{negl}(n)$$

7 Reduction-based Proofs

References

[1] Jonathan Katz, Yehuda Lindell, *Introduction to Modern Cryptography*, CRC Press, Taylor & Francis Group, 2nd edition, 2015.