EE 720: An Introduction to Number Theory and Cryptography (Spring 2019)

Lecture 8 — January 28, 2019

Instructor: Saravanan Vijayakumaran *Scribe: Saravanan Vijayakumaran*

1 Lecture Plan

- Recall the definition of CPA-security
- Recall the definition of a pseudorandom function
- Give a construction of a CPA-secure encryption scheme and prove its security

2 Recap

Definition. *Let F be an efficient, length-preserving, keyed function. F is a* ***pseudorandom function*** *if for all PPT distinguishers D, there is a negligible function* $\texttt{negl}$ *such that:*

$$\left|\Pr\left[D^{F_k(\cdot)}(1^n)=1\right]-\Pr\left[D^{f(\cdot)}(1^n)=1\right]\right|\leq \texttt{negl}(n),$$

where the first probability is taken over uniform choice of $k\in\{0,1\}^n$ and the randomness of D, and the second probability is taken over uniform choice of $f\in\texttt{Func}_n$ and the randomness of D.

- Example of a non-pseudorandom, length-preserving, keyed function: $F(k,x)=k\oplus x$.
- D is *not* given access to the key k. If k is known, it is easy to construct a distinguisher which succeeds with non-negligible probability (how?).

3 CPA-Secure Encryption from Pseudorandom Functions

- Let F be a pseudorandom function. Define a private-key encryption scheme for messages of length n as follows:
  - `Gen`: On input 1^n, choose k uniformly from $\{0,1\}^n$.
  - `Enc`: Given $k\in\{0,1\}^n$ and message $m\in\{0,1\}^n$, choose uniform $r\in\{0,1\}^n$ and output the ciphertext
  $$c:=\langle r,F_k(r)\oplus m\rangle.$$
  - `Dec`: Given $k\in\{0,1\}^n$ and ciphertext $c=\langle r,s\rangle$, output the plaintext message
  $$m:=F_k(r)\oplus s.$$

Theorem (Thereom 3.31 of KL)**.** *If F is a pseudorandom function, then the above construction is a CPA-secure private-key encryption scheme for messages of length n.*

Proof. Done in class. □

- What is a drawback of this construction?

4 References and Additional Reading

- Section 3.4, 3.5 from Katz/Lindell