CSC 591 Cryptography 9/24/2018

Lecture : CPA Security from Pseudorandom Function

Lecturer: Alessandra Scafuro *Scribe: Julia Minton*

Topic/Problem

In this class, we used the definition of a pseudorandom function (PRF) to construct an encryption scheme able to withstand chosen plaintext attacks (CPA). As a review, PRFs can be constructed using the Goldreich-Goldwater-Micali (GGM) construction. This construction takes the output of a pseudomrandom generator $G : \{0,1\}^n \rightarrow \{0,1\}^{2n}$ and divides it into left and right halves. Each half is used as a new seed for G; this process continues recursively, with each half of each new output becoming the next seed. The PRF with key k consists of the tree of these outputs with a starting seed of k. For a given seed x of F_k, the function traverses the tree. For every 0, the PRF travels left; for every 1, the PRF travels right. The current output when the seed contains no more bits is the final pseudorandom string.

The main difficulty of constructing a CPA-secure scheme is that pseudorandom functions are deterministic. As discussed previously, any deterministic algorithm can be broken by a chosen plaintext attack. This means that we cannot simply run the PRF with the message as a seed; with the right attack, an adversary could determine the original message with greater than $\frac{1}{2} + negl(n)$ probability. Therefore, the solution is to use the pseudorandom function using a randomly chosen seed r, which is sent with the ciphertext to the recipient. The output of the pseudorandom function is combined with the plaintext using the XOR operator to produce the ciphertext.

This method of encryption is non-deterministic and cannot be broken by a chosen plaintext attack (the proof is in the following lecture). As a result, one key and one pseudorandom function can be used to encrypt multiple messages, with only negligible danger of an adversary successfully finding the message.

Defintion

The definitions of CPA-security and pseudorandom functions were discussed on 9/19/2018.

Assumption

Assume that the adversary attacks in two phases. In the query phase, the adversary sends one or more messages to the oracle. After each message is sent, the adversary receives the ciphertext produced by the oracle. In the challenge phase, the adversary sends two messages. After seeing the final ciphertext, he must choose which message was originally encrypted.

Assume there exists a PRF $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$.

Scheme

Gen (n)
Key: $k \leftarrow \{0,1\}^n$

Enc (m, k)
Choose $r \leftarrow \{0,1\}^n$
$y := F_k(r)$
$e := y \oplus m$
Output $c = (e, r)$

Dec (c, k)
Parse $c = e, r$
$y := F_k(r)$
$m := e \oplus y$ Output m

Security Proof

The proof for this scheme was discussed on 9/26/2018.