Week 3 **CS6160: Cryptology**

Blum-Micali Construction, PRPs and Block Ciphers

1 Blum-Micali Construction for Extending PRGs

Suppose that $G : \{0,1\}^n \to \{0,1\}^{n+1}$ is a PRG, i.e. given a random seed of length n, the PRG G produces a pseudorandom sequence of length $n+1$. Then we can extend G to a function $\hat{G} : \{0,1\}^n \to \{0,1\}^{n+2}$ such that $\hat{G}$ is also a PRG.

The construction (due to Blum and Micali) is as follows. Suppose that $G(x_1 \dots x_n) = y_1 \dots y_{n+1}$. Then:

$$\hat{G}(x_1 x_2 \dots x_n) = y_1 G||(y_2 \dots y_{n+1}).$$

The idea is that y_1 is a pseudorandom bit and the output of G on a pseudorandom sequence of length n (namely $y_2 \dots y_{n+1}$) is also pseudorandom.

Further we can iterate $\hat{G}$ many times and obtain a PRG output with $l(n)$ bits as long as $l(n)$ is at most a polynomial in n. [Note: If $l(n)$ is not polynomially-bounded, then the output cannot be guaranteed to remain a PRG because the adversary's advantage in distinguishing the output from a random string increases with longer ouputs.]

2 Pseudo-Random Permutations

The main primitive used a block cipher is a Pseudo-Random Permutation, which we define below.

Given $M = C = \{0,1\}^n$ and $K = \{0,1\}^l$, we say that a function $F : M \times K \to C$ is a **Pseudo-Random Permutation** if the random function F_k, obtained by picking a random key $k \in K$, and defined as $F_k(x) = F(x,k)$ is (a) a bijection, (b) indistinguishable from a random permutation on M.

We now make the second condition precise using the following indistinguishability experiment.

PRPExp(A):

1. Alice picks a random key $k \in K$, a random permutation $\pi : \{0,1\}^n \to \{0,1\}^n$, and a value $b \in \{0,1\}$ uniformly at random. Let $f_0 = F_k$ and $f_1 = \pi$.
2. For $i = 1$ to Q, we have the following communication between Alice and the Adversary A.
   - The Adversary A picks a message $x_i \in M$ and sends it to Alice.
   - Alice sends $y_i = f_b(x_i)$ to the Adversary.
3. The Adversary outputs a value $b' \in \{0,1\}$.

The value/result of the experiment is 1 if $b' = b$ and 0 if $b' \neq b$.

We say that F is a PRP if for every PPT adversary A, we have:

$$Pr[PRPExp(A) = 1] \leq 1/2 + negl(n).$$

An example of a function which is NOT a PRP is $F(x,k) = x \oplus k$. This is because if $F_k(x_1) = y_1$ and $F_k(x_2) = y_2$, then we must have: $F_k(x_1 \oplus x_2) = y_1 \oplus y_2$. A random permutation will with high probability not satisfy the above relation for most pairs (x_1, x_2); so the adversary can in fact choose any pair of messages and win the distinguishability game with a probability very close to 1.

3 Block Ciphers: Introduction

In a block cipher, each message is broken into blocks of n bits, and each block encrypted using the encryption function. Finally these blocks are combined; we remark that simply concatenating the individual encrypted blocks is not secure: we will see secure ways of combining the blocks later.

We want the encryption function to be used in an individual block to be a PRP. There are no unconditional constructions of PRPs; however PRPs, like other primitives, such as PRGs and PRFs (PseudoRandomFunctions) can be built assuming the existence of other primitives. In practice, block ciphers use encryption functions that are designed to prevent various known attacks and to behave pseudorandomly with respect to statistical properties.

Most block ciphers in practice have the following design.

- An auxiliary encryption function $\hat{E} : \{0,1\}^n \times \hat{K} \to \{0,1\}^n$ is used, which is by itself not secure.
- For encryption, the function $\hat{E}$ is iteratively applied to a n-bit block (starting with the initial message block) using different keys, called round keys.
- Suppose that the round keys are $k_1, k_2, \ldots, k_d$, where d is the number of rounds. Let the input message block be x. The encryption algorithm iteratively computes the following values.
  - $y_1 = \hat{E}(x, k_1)$.
  - For $i \geq 2$, $y_i = \hat{E}(y_{i-1}, k_i)$.
- The output y_d, obtained after d rounds, is the encryption of the message block x.

A comparison of 3-widely used block ciphers:

- DES: 56-bit key, 64-bit block, 16 rounds
- TripleDES: 168-bit key, 64-bit block, 48 rounds
- AES: 128-bit key, 128-bit block, 10 rounds

We now look at the design of DES and AES.

3.1 DES: Introduction

DES (Data Encryption Standard) was created by a team of cryptographers at IBM around 1976, to be used as a standard.

DES uses an idea by Fiestel to convert an arbitrary function $f : \{0,1\}^n \to \{0,1\}^n$ into a function $\pi : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n \times \{0,1\}^n$ such that π is a bijection with an easily computable inverse. This bijection, called the Fiestel permutation is given by:

$$\pi(x, y) = (y, x \oplus f(y)).$$

The unique inverse of (x_1, y_1) is then:

$$\pi^{-1}(x_1, y_1) = (y_1 \oplus f(x_1), x_1).$$

π is called a Fiestel permutation; notice that the inverse has the same structure as π.

We'll see the structure of DES in more detail in the next class.