[CS309] Foundations of Cryptography and Security Networks

Instructor: Dr. Dibyendu Roy
Notes by: Tanuj Saini (202251141)

Autumn Semester 2024
Week 6 Lecture

1 Stream Cipher

A stream cipher consists of two components, a pseudo-random bit generator (PRBG) and an encryption and decryption technique. The PRBG generates keystream bits Z_i.

1.1 Encryption

$$C_i = m_i \oplus Z_i$$

1.2 Decryption

$$m_i = C_i \oplus Z_i$$

Here, XOR is used as the encryption technique, but other efficient computations may be used.

1.3 Synchronous Stream Cipher

In a synchronous stream cipher, the keystream is generated independently of the plaintext and ciphertext bits. The functions involved are:

- State Update function: $S_{i+1} = f(S_i, K)$
- Keystream Generator function: $Z_i = g(S_i, K)$
- Ciphertext Generation function: $C_i = h(Z_i, m_i)$

Here, S_0 is the initial state determined from K and IV. The functions f and g do not take plaintext or ciphertext as inputs in synchronous stream ciphers.

1.4 Asynchronous or Self-Synchronizing Stream Ciphers

In asynchronous stream ciphers, the keystream bits are generated as a function of the key and a fixed number of previous ciphertext bits.

- State Update Function: $\sigma_{i+1} = f(\sigma, K, IV)$ where $\sigma = (C_{i-t}, C_{i-t+1}, \ldots, C_{i-1})$
- Keystream Generation Function: $Z_i = g(\sigma_i, K)$
- Ciphertext Generation Function: $C_i = h(Z_i, m_i)$

The initial state $\sigma_0 = (C_{-t}, C_{-t+1}, \ldots, C_{-1})$ is the non-secret initial state.

2 Linear Feedback Shift Register (LFSR)

LFSRs are widely used in stream ciphers, for example, in 4G communication. It consists of an n-bit register, where the states are denoted by S and the bits by s. At each clock cycle, the state updates, and a keystream bit is generated.

2.1 Example of a 3-bit LFSR

At clock cycle $t = 0$, the state is:

$$S_0 = s_2, s_1, s_0$$

After one clock cycle (right shift for this example), the state becomes:

$$S_1 = s_1, s_0, s_2$$

Where the rightmost bit s_0 moves out as output, and the feedback bit s_n is calculated as:

$$s_n = L(s_0, s_1, \ldots, s_{n-1})$$

The function L is a linear function on the previous state:

$$L(s_0, s_1, \ldots, s_{n-1}) = a_0 s_0 \oplus a_1 s_1 \oplus \cdots \oplus a_{n-1} s_{n-1}$$

Where $a_i \in \{0, 1\}$.

2.2 Linear vs. Affine Functions

If $a_n = 0$, the function is linear:

$$L = a_0 s_0 \oplus a_1 s_1 \oplus \cdots \oplus a_{n-1} s_{n-1}$$

If $a_n = 1$, it becomes an affine function.

Example of linear function:

$$L_1(x, y) = x \oplus y$$

Example of non-linear function:

$$L_2(x, y) = 1 \oplus x \oplus y$$

3 Period of an LFSR

The period of an LFSR is defined as the number of clock cycles before the state repeats. The maximum period for an n-bit LFSR is $2^n - 1$.

3.1 Example of a 3-bit LFSR with $L = s_0 \oplus s_2$

Consider the following example:

At $t = 0$:

$$S_0 = 1, 1, 0$$

At $t = 1$:

$$S_1 = 0, 1, 1$$

This LFSR will repeat its states every $2^n - 1 = 7$ clock cycles.

4 LFSR with Non-Linear Filter Function

A non-linear filter function takes l-bits from the state of the LFSR and applies a non-linear function f. This makes the keystream bit Z_i a non-linear function of the state.

The output function is:

$$Z_i = f(s_0, s_1, \ldots, s_{l-1})$$

This improves security, making it harder to recover the secret key through a linear system of equations.

5 Hash Functions

A hash function maps input data to a fixed-size output. The key properties of a good hash function are:

1. A small change in input drastically changes the output.
2. It is computationally infeasible to reverse the function (find the pre-image).
3. It is infeasible to find two different inputs with the same hash (collision resistance).

5.1 Example of Pre-Image Finding Problem

The probability of finding a pre-image can be approximated as:

$$P[\text{pre-image finding}] \approx \frac{Q}{M}$$

Where Q is the number of guesses, and M is the output size.