Cryptography and Security

Cunsheng DING

HKUST, Hong Kong

Version 3

Lecture 03: A Design Paradigm of One-Key Block Ciphers

The Outline of this Lecture

1. Linear and nonlinear functions.
2. Shannon's idea of confusion and diffusion.
3. A design paradigm of one-key block ciphers.
4. An example cipher following the design paradigm.

Designing a Secure & Practical One-key Block Cipher

In Lecture 2, we did the following:

1. We defined one-key block ciphers $(\mathcal{M}, \mathcal{C}, \mathcal{K}, E_k, D_k)$ and made three security requirements.
2. We discussed simple substitution ciphers, and realized that they are not secure.
3. We learnt the one-time pad cipher, which is secure in the information-theoretic sense, but impractical.

Question: How does one design a **secure** and **practical** cipher?

Remark: Today we will address this question.

Part 1: Linear and Nonlinear Functions

Abelian Groups

Abelian group: An Abelian group is a set A associated with a binary operation $+$ that satisfies the following five conditions:

- $x + y \in A$ for any pair of x and y in A (A is closed under $+$).
- $x + y = y + x$ for any pair of x and y in A ("$+$" is commutative).
- $(x + y) + z = x + (y + z)$ for any x, y and z in A ("$+$" is associative).
- There is a special element $0 \in A$ such that $0 + x = x$ for all $x \in A$ (identity element).
- For any $x \in A$ there is an element $y \in A$ such that $x + y = 0$ (y is the inverse of x with respect to $+$).

If A is a finite set, $(A, +)$ is called a finite Abelian group. In this course, we need only finite Abelian groups.

Examples of Abelian Groups

Example of Abelian groups: $(\mathbf{Z}, +)$ is an Abelian group, where $\mathbf{Z}$ is the set of all integers and $+$ is the integer addition we learnt in primary school.

Example of Abelian groups: $(\mathbf{Z}_p, \oplus_p)$ is a finite Abelian group with p elements, where p is any prime and $\mathbf{Z}_p = \{0, 1, 2, \ldots, p-1\}$.

Question: What is the identity element of $(\mathbf{Z}_p, \oplus_p)$?

Example of Abelian groups: $(\mathbf{Z}_p^{\times}, \otimes_p)$ is a finite Abelian group with $p-1$ elements, where p is any prime and $\mathbf{Z}_p^{\times} = \{1, 2, \cdots, p-1\}$.

Question: What is the identity element of $(\mathbf{Z}_p^{\times}, \otimes_p)$?

Remark: The finite field $\mathbf{Z}_p$ has two Abelian groups: the additive group $(\mathbf{Z}_p, \oplus_p)$, and multiplicative group $(\mathbf{Z}_p^{\times}, \otimes_p)$.

The Abelian Group $(\mathbf{Z}_m^n, +)$

Definition: Let $m \geq 2$ and $n \geq 1$ be integers. Let

$$\mathbf{Z}_m^n = \mathbf{Z}_m \times \mathbf{Z}_m \times \cdots \times \mathbf{Z}_m \ (n\text{-ary Cartesian product of } \mathbf{Z}_m).$$

For any two elements

$$x = (x_1, x_2, \cdots, x_n) \in \mathbf{Z}_m^n, \ y = (y_1, y_2, \cdots, y_n) \in \mathbf{Z}_m^n,$$

define

$$x + y = (x_1 \oplus_m y_1, x_2 \oplus_m y_2, \cdots, x_n \oplus_m y_n) \in \mathbf{Z}_m^n.$$

Proposition: $(\mathbf{Z}_m^n, +)$ is an Abelian group with m^n elements.

Remark: This Abelian group will be employed very often.

Linear Functions

Definition: A function f from an Abelian group $(A, +)$ to an Abelian group $(B, +)$ is called a **homomorphism** if $f(x + y) = f(x) + f(y)$ for all $x, y \in A$.

Remark: No confusion using symbol $+$ to denote two different operations.

Definition: A function $g : A \to B$ is **linear** if and only if $g = f + b$ for a homomorphism $f : A \to B$ and a constant $b \in B$. Equivalently, g is linear if and only if $g + b'$ is a homomorphism for some $b' \in B$. (b' the inverse of b.)

Remark: A homomorphism is a special linear function by definition, as $f(x) = f(x) + 0$ is linear by definition for every homomorphism $f(x)$.

Example: Let $f(x) = x_1 + x_2 + \cdots + x_n$, where $x = (x_1, \cdots, x_n) \in \mathbf{Z}_2^n$ and $x_i \in \mathbf{Z}_2$. Then f is a linear function (homomorphism) from $(\mathbf{Z}_2^n, +)$ to $(\mathbf{Z}_2, +)$. The function $f(x) + 1$ is a linear function from $(\mathbf{Z}_2^n, +)$ to $(\mathbf{Z}_2, +)$.

Linear Functions: Example

Let P be a permutation of the set $\{1, \cdots, n\}$. Define a function L_P from $\mathbf{Z}_2^n$ to itself by

$$L_P((x_1, x_2, \cdots, x_n)) = (x_{P(1)}, x_{P(2)}, \cdots, x_{P(n)})$$

for any $x = (x_1, x_2, \ldots, x_n) \in \mathbf{Z}_2^n$.

The function L_P is a linear function (homomorphism) from $(\mathbf{Z}_2^n, +)$ to $(\mathbf{Z}_2^n, +)$.

Exercise: Prove that L_P is a linear function from $(\mathbf{Z}_2^n, +)$ to $(\mathbf{Z}_2^n, +)$.

Nonlinear Functions

Definition: A function that is not linear is called a **nonlinear function**.

Remark: To prove that a function f from an Abelian group $(A, +)$ to an Abelian group $(B, +)$ is nonlinear, by definition you need to prove that $f(x) + b$ is not a homomorphism for each fixed $b \in B$.

Example: The following function from $(\mathbf{Z}_2^4, +)$ to $(\mathbf{Z}_2, +)$ is nonlinear:

$$f((x_1, x_2, x_3, x_4)) = x_1 + x_2 + x_3 + x_4 + x_1 \times x_2 \times x_3 \times x_4,$$

where the $+$ and $\times$ are the modulo-2 addition and modulo-2 multiplication.

Question: How do you prove that f is nonlinear.

Answer: Prove that both $f(x)$ and $1 + f(x)$ are not homomorphisms using the definition of homomorphisms.

Linear and Nonlinear Functions

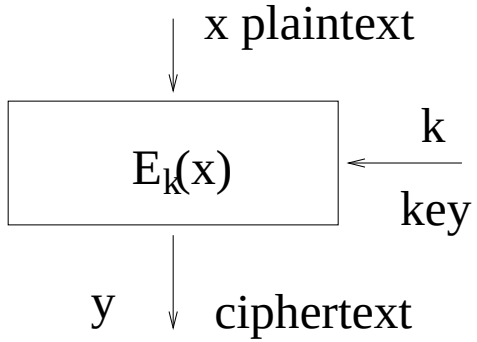
Question: Why are we interested in linear and nonlinear functions?

Answer: Both linear and nonlinear functions are needed in many cryptographic systems as basic building blocks (including one-key block ciphers).

Part 2: Shannon's Idea of Diffusion and Confusion for Constructing One-key Block Ciphers

Diffusion Measure

Message (respectively, key) bit diffusion measure: The minimum number of bits in the ciphertext block $y = (y_1, \ldots, y_n)$ affected by changing one bit in the plaintext block $x = (x_1, \ldots, x_n)$ (respectively, secret key $k = (k_1, \ldots, k_t)$) `divided by` n.



1. The higher this diffusion measure, the better the diffusion.
2. The encryption and decryption function should have good diffusion.
3. Both linear and nonlinear functions are employed to provide diffusion.

Example of Bad Diffusion

Example: Suppose that x, y and k all have 8 bits. Let $y = E_k(x)$ be defined by

$$y_1 = x_1 + k_1, \quad y_2 = x_2 + k_2, \quad y_3 = x_3 + k_3, \quad y_4 = x_4 + k_4,$$
$$y_5 = x_5 + k_5, \quad y_6 = x_6 + k_6, \quad y_7 = x_7 + k_7, \quad y_8 = x_8 + k_8,$$

where all the additions + are the integer addition modulo 2.

Message bit diffusion: 1/8.

Key bit diffusion: 1/8.

Comments: The function $y = E_k(x)$ has very bad diffusion, because each plaintext bit or key bit affects only one bit in the output block y.

Example of Good Diffusion

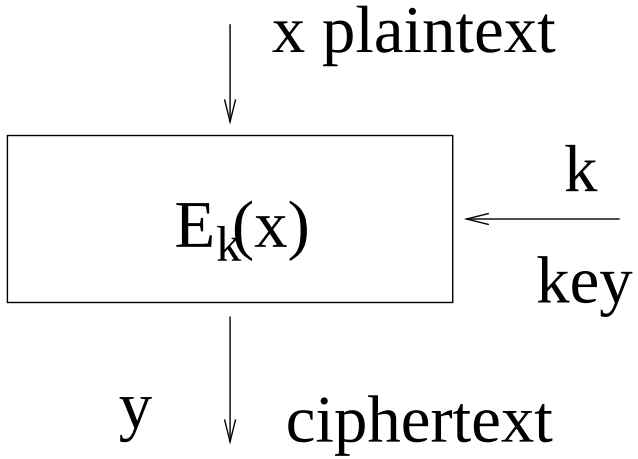
Example: Let x, y and k all have 8 bits, and $y = E_k(x)$ be defined by

$$\begin{aligned}
y_1 &= x_1 + x_2 + x_3 + x_4 + x_5 + k_1 + k_2 + k_3 + k_4 + k_5, \\
y_2 &= x_2 + x_3 + x_4 + x_5 + x_6 + k_2 + k_3 + k_4 + k_5 + k_6, \\
y_3 &= x_3 + x_4 + x_5 + x_6 + x_7 + k_3 + k_4 + k_5 + k_6 + k_7, \\
y_4 &= x_4 + x_5 + x_6 + x_7 + x_8 + k_4 + k_5 + k_6 + k_7 + k_8, \\
y_5 &= x_5 + x_6 + x_7 + x_8 + x_1 + k_5 + k_6 + k_7 + k_8 + k_1, \\
y_6 &= x_6 + x_7 + x_8 + x_1 + x_2 + k_6 + k_7 + k_8 + k_1 + k_2, \\
y_7 &= x_7 + x_8 + x_1 + x_2 + x_3 + k_7 + k_8 + k_1 + k_2, + k_3 \\
y_8 &= x_8 + x_1 + x_2 + x_3 + x_4 + k_8 + k_1 + k_2 + k_3 + k_4.
\end{aligned}$$

Comments: It has very good diffusion, as each plaintext bit or key bit affects 5 bits in the output block $y = (y_1, y_2, \cdots, y_8)$.

Confusion Measure

Confusion measure: The "complexity" of the relations between the ciphertext block bits and the plaintext block bits and the key bits.



Remark: Nonlinear functions are necessary for providing confusion.

Bad Confusion

Let $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ be the plaintext block and ciphertext block, respectively. Let $k = (k_1, \ldots, k_t)$ be the secret key such that $y = E_k(x)$.

Bad confusion: It means that the relations among the plaintext block bits, ciphertext block bits and the key bits are so **simple** that it is **feasible** to recover k by solving the following system of equations

$$y = E_k(x)$$

for a number of given pairs (x, y).

Warning: If the encryption and decryption function of a one-key cipher have bad confusion, then the cipher is not secure w.r.t. known-plaintext attacks.

Example of Functions with Bad Confusion

Example: Suppose that $x = (x_1, x_2, \ldots, x_8)$, $y = (y_1, y_2, \ldots, y_8)$ and $k = (k_1, k_2, \ldots, k_8)$ all have 8 bits. Let $y = E_k(x)$

$$
\begin{aligned}
y_1 &= x_1 + x_2 + x_3 + x_4 + x_5 + k_1 + k_2 + k_3 + k_4 + k_5, \\
y_2 &= x_2 + x_3 + x_4 + x_5 + x_6 + k_2 + k_3 + k_4 + k_5 + k_6, \\
y_3 &= x_3 + x_4 + x_5 + x_6 + x_7 + k_3 + k_4 + k_5 + k_6 + k_7, \\
y_4 &= x_4 + x_5 + x_6 + x_7 + x_8 + k_4 + k_5 + k_6 + k_7 + k_8, \\
y_5 &= x_5 + x_6 + x_7 + x_8 + x_1 + k_5 + k_6 + k_7 + k_8 + k_1, \\
y_6 &= x_6 + x_7 + x_8 + x_1 + x_2 + k_6 + k_7 + k_8 + k_1 + k_2, \\
y_7 &= x_7 + x_8 + x_1 + x_2 + x_3 + k_7 + k_8 + k_1 + k_2, + k_3 \\
y_8 &= x_8 + x_1 + x_2 + x_3 + x_4 + k_8 + k_1 + k_2 + k_3 + k_4.
\end{aligned}
$$

Comments: $y = E_k(x)$ has very bad confusion, as the relation between the input bits and output bits is linear. It is easy to recover k given a pair (x, y).

Good Confusion

Let $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ be the plaintext block and ciphertext block, respectively. Let $k = (k_1, \ldots, k_t)$ be the secret key such that $y = E_k(x)$.

Good confusion: It means that the relations among the plaintext block bits, ciphertext block bits and the key bits are so **complex** that it is **infeasible** to recover k by solving the following system of equations

$$y = E_k(x)$$

for a number of given pairs (x, y).

Good confusion requirement: The encryption and decryption function of a secure and practical one-key block cipher should have good confusion.

Part 3: An Important Design Paradigm for One-Key Block Ciphers

The Iterative Design Paradigm

In order to design E_k and D_k such that

1. they have good diffusion and confusion with respect to the secret key bits and message bits, and
2. they are fast in software and hardware implementation,

we could design a simple one-to-one function f_h (called, **round function**) and define

$$E_k(m) = f_{k_\ell}(f_{k_{\ell-1}}(\cdots f_{k_2}(f_{k_1}(m))\cdots))$$

where the **round keys** $k_1, k_2, \cdots, k_\ell$ are computed from the secret key k according to an algorithm (called the **key schedule/expansion algorithm**), and ℓ is the number of rounds of iteration.

Questions: How to design f_h and the key schedule algorithm? How many rounds of iteration?

Part 4: An Example Cipher Following the Design Paradigm

An Example Cipher Following the Iterative Approach (1)

The System Parameters of a One-Key Block Cipher

Let p be a large prime with $\gcd(3, p-1) = 1$ and α be a *primitive root* of p, i.e., every integer a with $1 \leq a \leq p-1$ can be expressed as $a = \alpha^j \bmod p$ for a unique j with $0 \leq j \leq p-2$. **Assume that both p and α are in the public domain.**

Proposition: Every prime $p \geq 3$ has a primitive root α.

Remark: The proof of this proposition can be found in a textbook about elementary number theory.

Proposition: x^3 is a permutation on $\mathbf{Z}_p$. Its inverse function is x^u, where u is the multiplicative inverse of 3 modulo $p-1$.

Proof: Note that $\gcd(3, p-1) = 1$. The desired conclusions then follow.

An Example Cipher Following the Iterative Approach (2)

The Description of the One-Key Block Cipher

Let ℓ be a fixed positive integer. Let $\mathcal{M} = \mathcal{C} = \mathcal{K} = \mathbf{Z}_p$. Define the round function by $f_h(x) = ((x+h)^3 + h) \bmod p$.

For any secret key k, define round keys $k_i = \alpha^{k+i} \bmod p$ for each $i \geq 1$.

Define

$$E_k(m) = f_{k_\ell}(f_{k_{\ell-1}}(\cdots f_{k_2}(f_{k_1}(m))\cdots)),$$
$$D_k(c) = f_{k_1}^{-1}(f_{k_2}^{-1}(\cdots f_{k_{\ell-1}}^{-1}(f_{k_\ell}^{-1}(c))\cdots,))$$

where $f_h^{-1}(x) = ((x-h)^u - h) \bmod p$ and u is the multiplicative inverse of 3 modulo $p-1$.

Question: How many rounds of iteration should this cipher have?

Remark: It may take many years to answer this hard question.

Summary of This Lecture

- We defined linear functions and nonlinear functions, which are necessary building blocks in cryptographic systems.
- We introduced Shannon's idea of confusion and diffusion, and learnt that a **secure and practical** one-key block cipher should have good confusion and good diffusion.
- We introduced a design paradigm for one-key block ciphers, and studied an example cipher following the design paradigm.