Cryptography and Security

Cunsheng DING

HKUST, Hong Kong

Version 3

Lecture 03: Design Ideas of One-Key Block Ciphers

The Outline of this Lecture

1. Linear and nonlinear functions.
2. Shannon's confusion and diffusion.
3. Basic design ideas of one-key ciphers.
4. The finite field GF(2^8).

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 know 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?

Part 1: Linear and Nonlinear Functions

Abelian groups

Abelian group: An Abelian group is a set A associated with a binary operation $+$ with the following properties:

- $x + y \in A$ for any pair of x and y in A (A is closed under $+$).
- $(x + y) + c = x + (y + c)$ for any x, y and z in A ("+" is associative).
- $x + y = y + x$ for any pair of x and y in A ("+" is commutative).
- 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 consider only finite Abelian groups.

Examples of Abelian Groups

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

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

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

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

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

$$\mathbf{Z}_m^n = \mathbf{Z}_m \times \mathbf{Z}_m \times \cdots \times \mathbf{Z}_m \ (n \text{ copies of } \mathbf{Z}_m).$$

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 and Affine Functions

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

A function $g : A \to B$ is **affine** if and only if $g = f + b$ for a linear function $f : A \to B$ and a constant $b \in B$.

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 from $(\mathbf{Z}_2^n, +)$ to $(\mathbf{Z}_2, +)$. Note that $+$ denotes the bitwise exclusive-or and exclusive-or operations respectively.

The function $f(x) + 1$ is an affine 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 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: Any function that is not affine is called a nonlinear function.

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

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

and

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

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

Exercise: Prove that these two functions are nonlinear.

Linear and Nonlinear Functions

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

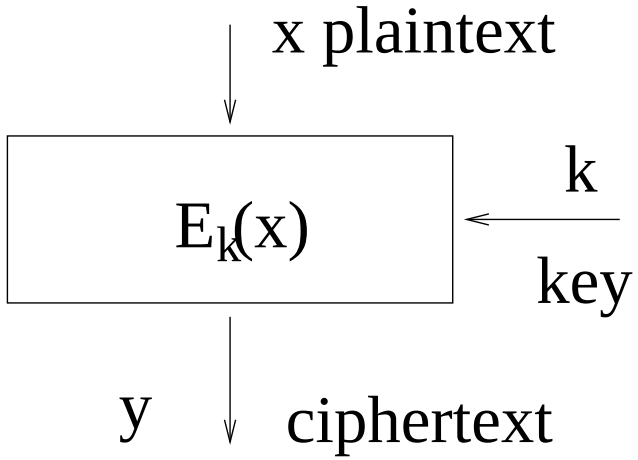
Answer: Both linear and highly nonlinear functions are needed in many cryptographic systems as basic building blocks.

Comment: Our human body needs both flesh (linear function) and bone (nonlinear function)!

Part 2: Shannon's Diffusion and Confusion

Diffusion Requirement

Diffusion: The minimum number of bits in the ciphertext block affected by changing one bit in the plaintext block or secret key `over the total number of bits in the ciphertext block`.



1. The higher this measure quantity, the better the diffusion.
2. Usually linear 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.

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

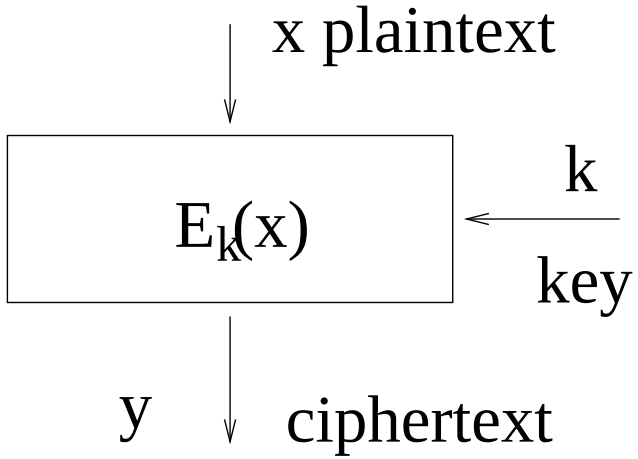
Example: Let x, y and k all have 8 bits, and $y = E_k(x)$ be defined by

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

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

Confusion Requirement

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



Remark: Nonlinear functions are used to provide confusion.

Example of Functions with Bad Confusion

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

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

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

Part 3: An Important Design Paradigm

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,

we could design a simple function f_k and define

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

where $k_1, k_2, \cdots$ and k_ℓ are binary string computed from the secret key k according to an algorithm, and ℓ is the number of rounds of iterations.

Remark: Most ciphers are designed with this approach.

Questions: How to design f_k? How many rounds of iterations?

Part 4: The Finite Field GF(2^8)

Polynomials over GF(2)

Notation: $\mathrm{GF}(2) = \mathbf{Z}_2 = \{0, 1\}$, the finite field with only two elements, with the associated two operations $\oplus$ and $\otimes$.

Polynomials over GF(2)**:** $a(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$, where $a_i \in \mathrm{GF}(2)$.

Irreducible polynomial: $p(x) = x^8 + x^4 + x^3 + x + 1 \in \mathrm{GF}(2)[x]$, which means that $p(x)$ cannot be expressed as the product of two polynomials over GF(2) with smaller degrees.

Remark: Irreducible polynomials are similar to **primes**.

A reducible polynomial over GF(2)**:**

$$x^4 + x^3 + x + 1 = (x + 1)^2 (x^2 + x + 1)$$

The Elements in GF(2^8)

The set GF(2^8) consists of all the polynomials

$$a(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5 + a_6x^6 + a_7x^7 \in \mathrm{GF}(2)[x].$$

where each $a_i \in \{0, 1\}$. Hence the set GF(2^8) has 2^8 elements.

We identify $a(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5 + a_6x^6 + a_7x^7$ with:

$$(a_0a_1a_2a_3a_4a_5a_6a_7)$$

$$(a_0a_1a_2a_3)(a_4a_5a_6a_7)$$

$$(a_0 + a_1 2 + a_2 2^2 a_3 2^3)(a_4 + a_5 2 + a_6 2^2 + a_7 2^3) = uv$$

where $u = a_0 + a_1 2 + a_2 2^2 a_3 2^3$ and $v = a_4 + a_5 2 + a_6 2^2 + a_7 2^3$ are in $\{0, 1, ..., 9, A, B, C, D, E, F\}$.

$A = 10, B = 11, C = 12, D = 13, E = 14, F = 15$

The Addition Operation of GF(2^8)

For any two elements in GF(2^8),

$$a(x) = a_0 + a_1x + a_2x^2 + \cdots + a_7x^7, \quad b(x) = b_0 + b_1x + b_2x^2 + \cdots + b_7x^7,$$

their addition is defined by

$$a(x) + b(x) = \sum_{i=0}^{7} (a_i \oplus b_i)x^i \in \mathrm{GF}(2^8),$$

Proposition: (GF(2^8), +) is an abelian group with identity 0, the zero polynomial.

Proof: It is trivial and left as an exercise.

The Multiplication Operation of GF(2^8)

For any two elements in GF(2^8),

$$a(x) = a_0 + a_1x + a_2x^2 + \cdots + a_7x^7, \quad b(x) = b_0 + b_1x + b_2x^2 + \cdots + b_7x^7,$$

their multiplication is defined by

$$a(x) \times b(x) = a(x)b(x) \bmod p(x) \in \mathrm{GF}(2^8),$$

where $p(x) = x^8 + x^4 + x^3 + x + 1$ and is irreducible over GF(2), and $a(x)b(x)$ is the school multiplication.

The Multiplication Operation of GF(2^8)

Example: Let $a(x) = 1 + x^3 + x^6$ and $b(x) = x + x^2 + x^5$ in GF(2^8). Then

$$\begin{aligned} a(x)b(x) &= (x + x^2 + x^5) + (x^4 + x^5 + x^8) + (x^7 + x^8 + x^{11}) \\ &= x + x^2 + x^4 + x^7 + x^{11} \end{aligned}$$

and

$$\begin{aligned} a(x) \times b(x) &= a(x)b(x) \bmod p(x) \\ &= x + x^2 + x^4 + x^7 + x^{11} \bmod (x^8 + x^4 + x^3 + x + 1) \\ &= x + x^2 + x^3 + x^6 \in \mathrm{GF}(2^8). \end{aligned}$$

The Multiplication Operation of GF(2^8)

Proposition: $(\mathrm{GF}(2^8)^*, \times)$ is an abelian group with identity 1.

Proof: Let $a(x) \in \mathrm{GF}(2^8)^*$. Then $a(x) \neq 0$. Since $p(x)$ is irreducible over GF(2), we have $\gcd(a(x), p(x)) = 1$.

Applying the "Extended Euclidean Algorithm" for polynomials to $a(x)$ and $p(x)$, we obtain two polynomials $u(x)$ and $v(x)$ such that
$1 = u(x)a(x) + v(x)p(x)$. Then

$$1 = u(x)a(x) \bmod p(x).$$

Hence $b(x) := u(x) \bmod p(x) \in \mathrm{GF}(2^8)$ is the multiplicative inverse of $a(x)$.

The Finite Field GF(2^8)

Proposition: $(\mathrm{GF}(2^8), +, \times)$ is a finite field with 2^8 elements.

Proof: Combining the two previous propositions proves the conclusion.

Claim: $S(y) = y^{2^8-2} = y^{254}$ is a permutation on $\mathrm{GF}(2^8)$ and is `highly nonlinear` with respect to the binary operation $+$.

Remark: This permutation $S(x)$ on $\mathrm{GF}(2^8)$ is employed in the Advanced Encryption Standard. This is why we introduced the finite field $\mathrm{GF}(2^8)$ in this lecture. Notice that $S(y) = y^{-1}$ for all $y \neq 0$.