Cryptography

Cunsheng DING

HKUST, Hong Kong

COMP3631

The S-Box and the Function $M(x)$ in AES

The Outline of This Reading Material

1. The finite field GF(2^8).
2. The highly nonlinear function x^{254} over GF(2^8).
3. The linear function $M(x_0, x_1, x_2, x_3)$ function.

Part 1: 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 $a_i \in \mathrm{GF}(2)$.

Coefficients of $a(x)$: these a_j.

Degree of $a(x)$: $\deg(a(x))$ is the largest integer j such that $a_j \neq 0$.

The total number of polynomials of degree at most t: 2^{t+1}.

Definition: Let $\mathrm{GF}(2)[x]$ denote the set of all polynomials over GF(2).

Irreducible 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: If $a(x)$ cannot be expressed as the product of two polynomials over GF(2) with smaller degrees., it is then called *irreducible*.

Example: $p(x) = x^8 + x^4 + x^3 + x + 1 \in \mathrm{GF}(2)[x]$.

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

Remark: The total number of irreducible polynomials of any fixed degree is known.

Reducible 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 $a_i \in \mathrm{GF}(2)$.

Reducible polynomial: If there are two polynomials $b(x)$ and $c(x)$ of degree at least one in $\mathrm{GF}(2)[x]$ such that $a(x) = b(x)c(x)$, then $a(x)$ is called *reducible*.

Remark: Reducible polynomials are similar to **composite numbers**.

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 $2^8 = 256$ elements.

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

Proof: Let $a(x) \in \mathrm{GF}(2^8)^\times = \mathrm{GF}(2^8) \setminus \{0\}$. 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: The two previous propositions conclude the following:

- $(\mathrm{GF}(2^8), +)$ is an abelian group with identity 0, the zero polynomial.
- $(\mathrm{GF}(2^8)^\times, \times)$ is an abelian group with identity 1.

In addition, it is easily seen that

$$(a(x) + b(x)) \times c(x) = a(x) \times c(x) + b(x) \times c(x)$$

for all $a(x)$, $b(x)$ and $c(x)$ in $\mathrm{GF}(2^8)$. The desired conclusion then follows.

Representations of the Elements in GF(2^8)

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

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

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:

$$(a_0a_1a_2a_3a_4a_5a_6a_7)$$

$$(a_0a_1a_2a_3)(a_4a_5a_6a_7)$$

$$(a_0 + a_12 + a_22^2 + a_32^3)(a_4 + a_52 + a_62^2 + a_72^3) = uv$$

where $u = a_0 + a_12 + a_22^2a_32^3$ and $v = a_4 + a_52 + a_62^2 + a_72^3$ are in $\{0, 1, ..., 9, A, B, C, D, E, F\}$.
$A = 10, B = 11, C = 12, D = 13, E = 14, F = 15$

Part 2: The Highly Nonlinear Function x^{254} over GF(2^8)

The Permutation y^{254} over GF(2^8)

Proposition: For each $a(x) \in \mathrm{GF}(2^8)^*$, we have $a(x)^{255} = 1$.

Claim: $S(y) = y^{2^8-2} = y^{254}$ is a permutation on GF(2^8) and is a `highly nonlinear` function from $(\mathrm{GF}(2^8), +)$ to $(\mathrm{GF}(2^8), +)$.

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

Part 3: The Linear Functions x^{2^j} over GF(2^8)

The Linear Permutations y^{2^j} on GF(2^8)

Proposition: For any two elements $a(x)$ and $b(x)$ in GF(2^8), we have

$$(a(x)+b(x))^2 = a(x)^2 + 2a(x) \times b(x) + b(x)^2 = a(x)^2 + b(x)^2$$

and

$$(a(x)+b(x))^{2^j} = a(x)^{2^j} + b(x)^{2^j}$$

for each $j \geq 0$.

Proposition: For each $j \geq 0$, y^{2^j} is a linear permutation from $(\mathrm{GF}(2^8), +)$ to $(\mathrm{GF}(2^8), +)$.

Remark: The degree of a polynomial may not indicate the nonlinearity level of a function.

Part 4: The Linear Function $M(x)$

The Hexadecimal Expression of Elements in GF(2^8)

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

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

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:

$$(a_0a_1a_2a_3a_4a_5a_6a_7)$$

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

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 Linear Function $M(x_0, x_1, x_2, x_3)$

For each $0 \leq i \leq 3$, let $x_i = u_i v_i \in \mathrm{GF}(2^8)$, where u_i and v_i are in $\{0, 1, ..., 9, A, B, C, D, E, F\}$. For each (x_0, x_1, x_2, x_3), we define a new polynomial

$$x_3 x^3 + x_2 x^2 + x_1 x + x_0 \in \mathrm{GF}(2^8)[x].$$

Define $M(x_0, x_1, x_2, x_3) = (y_0, y_1, y_2, y_3)$, where

$$y_3 x^3 + y_2 x^2 + y_1 x + y_0 \quad = \quad c(x)(x_3 x^3 + x_2 x^2 + x_1 x + x_0) \bmod (x^4 + 1)$$

and $c(x) = 03x^3 + 01x^2 + 01x + 02$, which is defined with "coding theory".

We have to skip the technical details of the design of the polynomial $c(x)$, as coding theory is out of the scope of this course.