Introduction to Cryptology

Lecture-05

Mathematical Background: Extension Finite Fields

28.03.2023, v52

Mathematical Background

In Discrete Mathematics, Number Theory

Outlines

Representing information in security systems as "Vectors"

(More flexible and efficient algebraic system for modern cryptography!)

Data representation in Integer algebra:

(1010) ⇔ 10 Element in GF(13)
(1010101) ⇔ 85 Element in GF(89)
Large data blocks require large field modulus and hence more complex arithmetic

Alternatively data may be represented as vectors having entries from GF(13):

(3 2 11 8 10) Vector having components from GF(13) with 5 entries, 4 bits each.
The result is a vector of 20 bits as follows:
. . .
(0011 0010 1011 1000 1010) (not all 4-bit combinations are usable!)

Or fully usable binary vectors when using GF(31):

(10101 00011 01110 … $10110)_{1 \times 1000}$, 5000 bits, with algebra over GF(31)!

Or simply: $(1\ 0\ 1\ 1\ 0\ 1\ 0\ 1..\ 1\ 0)_{1 \times 256}$ 256 bits block/tuple with algebra over GF(2)

Question: Can we construct a "*closed operational algebraic system*" when describing data as such large vectors from a GF ?

The answer is yes, by using what is called Extended Finite Fields (GF)

This section treats such data : $(1\ 0\ 1..\ 1\ 0)_{1 \times n}$ as n-bit tuples/vectors over GF(2)

Vectors Represented as Polynomials over GF(2)

A(x) is a Polynomial over GF(2), $a_i \in$ GF(2) $A(x) = a_0 + a_1x + a_2x^2 + .. a_mx^m$

Can represent a vector as polynomial A(x) with elements from GF(2)

Example : Polynomial $A(x) = x^6 + x^5 + x^3 + 1$ over GF(2)

Corresponding vector (1 1 0 1 0 0 1) MSB LSB

Position 6 5 4 3 2 1 0

And in reversed direction (vector to polynomial)

Example : Position 6 5 4 3 2 1 0

Vector (1 1 0 0 0 1 1)

Corresp. Polynomial $A(x) = x^6 + x^5 + x + 1$

Basic Vectors/Polynomial Arithmetic over GF(2)

Addition:

$A(x) = 1 + x$
$B(x) = 1 + x + x^3$
$A(x) + B(x) = 2 + 2x + x^3$
$A(x) + B(x) = x^3$
(as 1+1 =2 =0 in GF(2))

In binary form →

A(x) ⇔ 0011
B(x) ⇔ 1011
A(x) + B(x) ⇔ 1000

Multiplication:

$A(x)\,B(x) = (1 + x)(1 + x + x^3)$
$= 1(1 + x + x^3) + x(1 + x + x^3)$
$= 1 + x + x^3 + x + x^2 + x^4$
$= 1 + x^2 + x^3 + x^4$

In binary form →

B(x) ⇔ 1011
A(x) ⇔ 0011
1011
1011
0000
0000
A(x) * B(x) ⇔ 0011101

From now on, we will use the term polynomials to designate vectors and vice versa

How to create Algebra between vectors/polynomials?

For creating Finite Fields GF,
non-factoriseable numbers called Prime Numbers
were used as modulus (remainders modulo p)

Similarly:
For creating vector/polynomial-fields called "Extension Fields",
non-factoriseable polynomials called "Irreducible Polynomials"
are used as modulus (remainders modulo p(x))

What are "Irreducible Polynomials"

To attain closed field algebra “Irreducible Polynomials” are required!

(Again: such polynomials play a similar role of “prime numbers” as field modulus)

A polynomial g(x) of degree m over GF(2) (2 is a prime!)

$$g(x) = a_0 + a_1x + a_2x^2 + .. a_m x^m \quad (a_i \in GF(2))$$

Is said to be an irreducible polynomial over GF(2) if factorizing g(x) is not possible

Selected fundamental properties of irreducible polynomials

- The **period** e of g(x) is the **smallest e** such that $x^e = 1$ [mod g(x)]
- **The period e** is actually the multiplicative order of x modulo g(x). **e divides $2^m - 1$**
- If $e = 2^m - 1$, then the irreducible polynomial is then called a **primitive plynomial**
- The **reciprocal** of a polynomial g(x) is defined as $g^*(x) = x^m g(1/x)$ (mirror polynomial)
- The **reciprocal** g*(x) is also irreducible having the same period as that of g(x)
- If **g*(x) = g(x)**, then g(x) is said to be a **self-reciprocal irreducible polynomial** (symmetric)

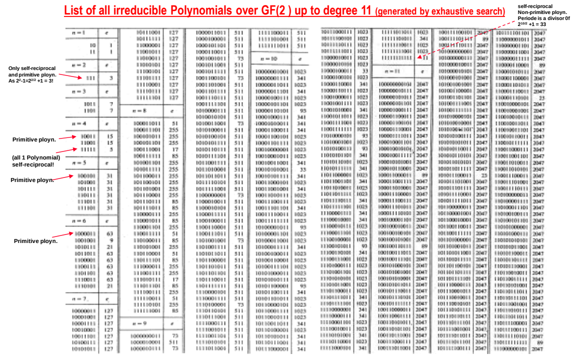
(highest possible period is a divisor of $2^{m/2} + 1$) **Non-trivial Self-reciprocal Polynomial can not be primitive!**

G(x) =1011
G*(x) =1101

G(x) =101
G*(x)=G(x)=101

- Generating “Irreducible Polynomials” is as difficult as generating prime numbers!
- Polynomial factorization is also an unsolved problem!?

List of all irreducible Polynomials over GF(2) up to degree 11 (generated by exhaustive search)



! The Use of Irreducible Polynomials !
The ring of polynomials modulo any irreducible g(x) is designated as $Z_{g(x)}$ and builds an Extension Field

The ring of polynomials $Z_{g(x)}$ modulo any irreducible polynomial g(x) of degree m over GF(2) is an Extension Field with 2^m elements of m-bit tuples. This is assigned as GF(2^m).

How to construct such m-bit closed vectors algebra?

- Select g(x) as any irreducible polynomial of degree m and use it as a field modulus. The result is an “extension field” algebraic system on all m-bit vectors
  (using prime number modulus in integer algebra. Corresponds to using irreducible polynomial modulus in polynomial algebra)

Finding irreducible polynomials :

There are theories and techniques (similar to those of prime integers but more complex) for testing and generating irreducible polynomial. (this is out of the scope of this lecture).

The table shown before includes a full list of all irreducible polynomials over GF(2) up to degree 11.

Smallest Extension Field GF(2^2) :
A full operational algebra on 2-bits vectors/polynomials

g(x) = $x^2 + x + 1$ = 111 is irreducible of degree m=2 over GF(2).
g(x) is the modulus, therefore $x^2 + x + 1 = 0$ => $x^2 = x + 1$
GF(2^2) elements are :

00	<=>	0
01	<=>	1
10	<=>	x
11	<=>	1+x

Addition and multiplication tables in GF(2^2) are:

⊕	0	1	x	1+x
0	0	1	x	1+x
1	1	0	1+x	x
x	x	1+x	0	1
1+x	1+x	x	1	0

⊙	0	1	x	1+x
0	0	0	0	0
1	0	1	x	1+x
x	0	x	1+x	1
1+x	0	1+x	1	x

⊕	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

⊙	00	01	10	11
00	00	00	00	00
01	00	01	10	11
10	00	10	11	01
11	00	11	01	10

(1+x) (1+x) mod ($x^2 + x + 1$)
= $x^2 + 2x + 1$
= $x^2 + 1 = (x+1)+1 =$ x   2=0 over GF(2).

or divide:
$(x^2 + 2x + 1) / (x^2 + x + 1) = 1 + x / (x^2 + x + 1)$

Remainder of division

Multiplicative order and primitive elements in GF (2^m)

Facts:

- Any non-zero element/vector in GF(2^m) builds a cyclic group.
- The multiplicative order of any element in GF(2^m) is a divisor of 2^m-1 .
  [The *possible multiplicative orders are only the divisors of (2^m-1)*]

A Primitive Element:

- Is the element having the highest possible multiplicative order, that is = 2^m-1.
- The exponents of such element generate the whole non-zero group elements

Number of all existing primitive elements: is φ (2^m-1)

Number of elements having order k: is φ (k)

Summary and some extension field properties

The algebra on m-bit vectors/polynomials over GF(2) using an irreducible polynomial g(x) of degree m as modulus, where $g(x) = 1 + g_1x^1 + g_2 x^2 ...+ g_m x^m$ · [all computations are modulo g(x)] result with what is called GF(2^m) having 2^m elements (vectors/polynomials).

In GF(2^m) the following relationships hold:

- Any non-zero element (multiplicative group element) β in GF(2^m) has a multiplicative inverse.
- The 2^m–1 non-zero elements build a cyclic group under multiplication.
  Group’s order is 2^m-1. (inverse computation: by using the extended gcd algorithm for polynomials)
- The multiplicative order of any element is a divisor of 2^m–1 , the number of elements with order t is φ(t)
- For any non-zero element β ∈ GF(2^m) the following holds $\beta^{2^m-1} = 1$
  (*reason:* the order of any element divides the group‘s order 2^m-1)
- If α, β ∈ GF(2^m) then : $(\alpha+\beta)^2 = \alpha^2 + \beta^2$ or $[f(x)]^2 = f(x^2)$
  (*Notice*: squaring is a linear operation in GF(2^m))

Example: Element's order over the extension field GF(2^4)

Compute the exponents of the element x over **GF(2^4)** which is generated by the irreducible polynomial $P(x)= (x^4+ x +1)$

Solution

If $P(x)= x^4+ x +1$ is the modulus then it is equal to zero, that is $x^4 + x +1 = 0$, thus $\mathbf{x^4 = x +1}$.
the exponents of **x** in GF(2^4) are:

	msb lsb	
→ $x = \mathbf{x}$	0010	mod $(x^4+ x +1)$
→ $x^2= \mathbf{x^2}$	0100	mod $(x^4+ x +1)$
$x^3= \mathbf{x^3}$	1000	mod $(x^4+ x +1)$
→ $x^4= x^4 = \mathbf{x + 1}$	0011	mod $(x^4+ x +1)$
$x^5= x\,x^4 = \mathbf{x^2 +x}$	0110	mod $(x^4+ x +1)$
$x^6= x\,(x^2 +x)= \mathbf{x^3 +x^2}$	1100	mod $(x^4+ x +1)$
→ $x^7= x\,(x^3 +x^2) = (x^4 +x^3) = \mathbf{x +1+x^3}$	1011	mod $(x^4+ x +1)$
→ $x^8= x^4 + x^2 +x = 1+x + x^2 +x = \mathbf{1+x^2}$	0101	mod $(x^4+ x +1)$
$x^9 = \mathbf{x^3 + x}$	1010	mod $(x^4+ x +1)$
$x^{10} = x^4 + x^2 = x\mathbf{+1 + x^2}$	0111	mod $(x^4+ x +1)$
→ $x^{11} = \mathbf{x^3 + x^2 +x}$	1110	mod $(x^4+ x +1)$
$x^{12}= x^4 + x^3 + x^2 = \mathbf{x +1+ x^3 + x^2}$	1111	mod $(x^4+ x +1)$
→ $x^{13}= x^4 + x^3 + x^2 +x = \mathbf{x^3 + x^2 + 1}$	1101	mod $(x^4+ x +1)$
→ $x^{14}= x^4 + x^3 + x= x+1+x^3 + x = \mathbf{x^3 +1}$	1001	mod $(x^4+ x +1)$
$x^{15}= x^4 + x = x + 1 + x = 1$	0001	mod $(x^4+ x +1)$

Important notice:
In GF (2^4): the order of any element Is a divisor of 2^4-1=15
Divisors of 15 are 1, 3,5,15 !
⇒The order can only be 1 or 3 or 5 or 15 !

The order of the element x is 15=2^4-1
=> x is a primitive element

Ord (α^i) = k / gcd (i,k)
Ord ($x^{1,2,4,7,8,11,13,14}$) = 15

Why Algebra over GF (2^m)
for modern Cryptographic Systems

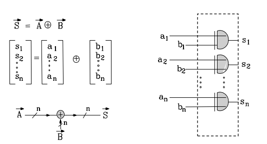
1- Less-complex processing for equivalent security levels
2- Faster running time
3- Lower hardware complexity and costs. Usable in modern smart card technology at commercially acceptable costs.

Contemporary "Modern Crypto-Systems" are deploying this algebra in practical applications more and more intensively

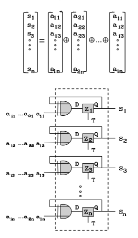
The basic hardware processing units for the primitive arithmetic operations; addition, multiplication and division over GF(2^n) are given in a compact template-form in the following sections

Hardware Architectures for Arithmetic in GF (2^n)
Addition

Parallel



Sequential

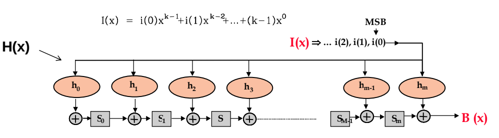


Hardware Architectures for Arithmetic in GF (2^m)
Multiplication

$$\boxed{B(x) = H(x) \cdot I(x)}$$

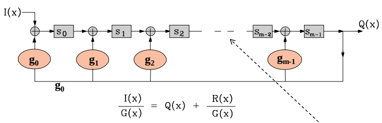
Multiplikator: $H(x) = h_0 + h_1 x + h_2 x^2 ... + h_m x^m$

$I(x) = i(0)x^{k-1} + i(1)x^{k-2} + ... + (k-1)x^0$



Hardware Architectures for Arithmetic in GF (2^m)
Division

$$\boxed{\frac{I(x)}{G(x)} = Q(x) + \frac{R(x)}{G(x)}}$$



$$\frac{I(x)}{G(x)} = Q(x) + \frac{R(x)}{G(x)}$$

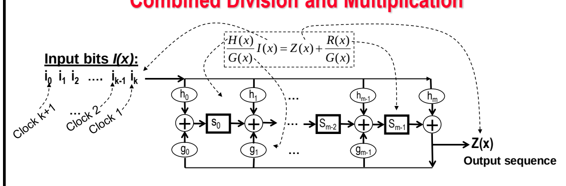
$G(x) = g_0 + g_1 x + g_2 x^2 ... g_m x^m$

$I(x) = i(0)x^{k-1} + i(1)x^{k-2} + ... + (k-1)x^0$

$R(x) = S_0 x^0 + S_1 x^1 + ... + S_{m-1} x^{m-1}\Big|_{t=k}$

NOTE: R(x) is the content of the register after entering all I(x) bits

Hardware Architectures for Arithmetic in GF (2^m)
Combined Division and Multiplication



Multiplier: $H(x) = h_0 + h_1x^1 + h_2x^2 \cdots + h_mx^m$

Divisor: $G(x) = g_0 + g_1x^1 + g_2x^2 \cdots + g_mx^m$

Input: $I(x) = i_0 + i_1x^1 + i_2x^2 \cdots + i_kx^k$

Remainder: $R(x) = r_0 + r_1x^1 + r_2x^2 \cdots + r_{m-1}x^{m-1}$
$R(x)=H(x) \cdot I(x) \bmod G(x)$
$= s_0 + s_1x^1 + s_2x^2 \cdots + s_{m-1}x^{m-1}$ *after clock k+1*

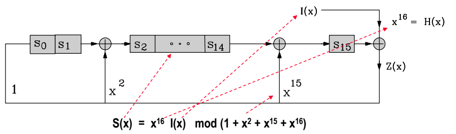
Arithmetic in $Z_{p(x)}$, size (2^{16})

Example: (CRC: Cyclic Redundancy Code/Check)

Simultaneous Division and Multiplication

S(x) = x^{16} I(x) mod ($1 + x^2 + x^{15} + x^{16}$)

Multiply the data stream I(x) by x^{16} and divide it simultaneously by ($1 + x^2 + x^{15} + x^{16}$)



The contents of the register after entering all I(x) bits is the rest of x^{16} I(x) mod ($1 + x^2 + x^{15} + x^{16}$)

Example: order of x over an extension field GF(2^3) and hardware implementation

Compute the exponents of the element x over **GF(2^3)** which is generated by the irreducible polynomial P(x)= (x^3+ x +1)

Solution

If P(x)= x^3+ x +1 is the modulus then it is equal to zero, that is $x^3 + x + 1 = 0$, thus $x^3 = x + 1$.

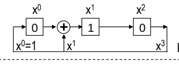
the exponents of **x** in GF(2^3) are:

	msb lsb	
$x = \mathbf{x}$	010	mod (x^3+ x +1)
$x^2 = \mathbf{x^2}$	100	mod (x^3+ x +1)
$x^3 = x^3 = \mathbf{x + 1}$	011	mod (x^3+ x +1)
$x^4 = x\,x^3 = \mathbf{x^2 + x}$	110	mod (x^3+ x +1)
$x^5 = x\,x^4 = x^3 + x^2 = \mathbf{x + 1 + x^2}$	111	mod (x^3+ x +1)
$x^6 = (x^3)^2 = (x+1)^2 = \mathbf{x^2 + 1}$	101	mod (x^3+ x +1)
$x^7 = x\,(x^2 + 1) = (x^3 + x) = x+1+x = \mathbf{1}$	001	mod (x^3+ x +1)
$x^8 = \mathbf{x}$		

Important notice:
In GF (2^3): the order of any element Is a divisor of 2^3-1=7
Divisors of 7 are 1, 7 !
⇒The order can only be 1 or 7 !

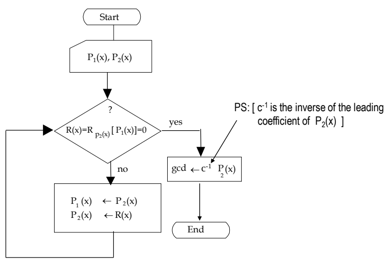
The order of the element x is 7=2^3-1
=> x is a primitive element

A possible hardware generator for the exponents of x is as follows:



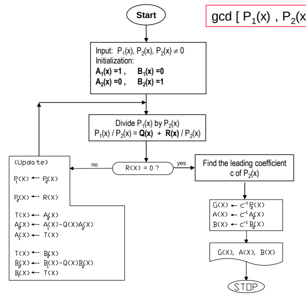
Initial state = x = 010 (LSB MSB)

Euclidian gcd Algorithm for Polynomials



Extended gcd Algorithm for Polynomials

gcd [$P_1(x)$, $P_2(x)$] = **A(x)** $P_1(x)$ + **B(x)** $P_2(x)$



Example: Compute the multiplicative inverse of $\mathbf{x^3 + x + 1}$ modulo $\mathbf{x^4 + x + 1}$

Solution: Compute gcd [$P_1(x)$, $P_2(x)$] = **A(x)** $P_1(x)$ + **B(x)** $P_2(x)$
if **gcd =1**, then the inverse is **B(x)**

Extended gcd Algorithm:

A2 = A1 – q A2   B2 = B1 – q B2

$P_1(x)$	$P_2(x)$	A1(x)	A2(x)	B1(x)	B2(x)	Qx)	R(x)
$x^4 + x + 1$	$x^3 + x + 1$	1	0	0	1	x	$x^2 + 1$
$x^3 + x + 1$	$x^2 + 1$	0	1	1	0 - x . 1= x	x	1
$x^2 + 1$	1	1	0 – x . 1 = x	x	1 – x . x = $x^2 + 1$	$x^2 + 1$	0

gcd [$P_1(x)$, $P_2(x)$] = **(x)** **(x^4 + x + 1)** + **(x^2 + 1)** **(x^3 + x + 1**) = 1

Operating modulo $\mathbf{x^4 + x + 1}$: $R_{(x^4+x+1)}$ [**(x)** **(x^4 + x + 1)** + **(x^2 + 1)** **(x^3 + x + 1**)] = 1

$R_{(x^4+x+1)}$ [**(x^2 + 1)** **(x^3 + x + 1**)] = 1

$\boxed{\text{=> } (\mathbf{x^2 + 1}) \equiv (\mathbf{x^3 + x + 1})^{-1} \quad \text{modulo } (\mathbf{x^4 + x + 1})}$

$x^4 + x + 1 = 0$
$x^4 = x + 1$
$x^5 = x^2 + x$

Check: **(x^2 + 1) (x^3 + x + 1**) = **$x^5 + \cancel{x^3} + x^2 + \cancel{x^3} + x + 1$**
$\equiv (\cancel{x^2} + \cancel{x}) + \cancel{x^2} + \cancel{x} + 1 = 1$ modulo **(x^4 + x + 1)**

GF (2^m) as a vector space

Some additional extension field properties of interest

GF(2^m) algebra is in general very attractive for implementing modern low-cost crypto systems. The way of representing of data plays a major role in some cases to result with extremely low-cost implementations.

- If $\alpha \in$ GF(2^m) is a root for g(x)=0, then α , α^2, α^3, α^4,... $\alpha^{m-1}$are the roots of g(x)
- These roots build what is called the **Canonical Base** for the vector space representing that field.

– If ($\alpha, \alpha^2, \alpha^{2^2}, \alpha^{2^3}, \ldots \alpha^{2^{m-1}}$) are linearly-independent, then they build what is called the **Normal Base** for this GF(2^m)

The “Normal base “ for a vector space representation of GF(2^m) results with extremely simple squaring arithmetic for polynomials/vectors as elements of GF(2^m) .

The following example shows one interesting efficient implementing of a squaring operation in GF(2^m)

Particular Arithmetic cases in GF (2^m) are sometimes very attractive for practical hardware implementations

Example: Squaring in Normal Base representation (Massey-Omura US Patent 1982)

GF(2^m) is equivalent to a vector space with the dimension m:

$\alpha_0, \alpha_1, \alpha_2, \ldots \alpha_{m-1}$ represent a base for a vector space if: $b_0\alpha_0 + b_1\alpha_1 + b_2\alpha_2 + \ldots + b_{m-1}\alpha_{m-1} = 0$

If and only if for $b_0 = b_1 = b_2 = \ldots = b_{m-1} = 0$, (Base vectors are linearly independent).

If α is a root of the field generating irreducible polynomial g(x) over GF(2), then α^0 α^1 α^2 α^3 $\cdots$ α^{m-1} build the Canonical Base for GF(2^m). (example α=x)

If however, $\alpha \ \ \alpha^2 \ \ \alpha^{2^2} \ \ \alpha^{2^3} \ldots \alpha^{2^{m-1}}$ are linearly independent,

then $\alpha \ \ \alpha^2 \ \ \alpha^{2^2} \ \ \alpha^{2^3} \ldots \alpha^{2^{m-1}}$ represent the so called a Normal Base

Example of squaring in a normal base system:
If a = 1 0 1 1
$\Rightarrow$ a^2 = 1 1 0 1

Squaring is equivalent to a "ring rotation" in normal base representation:

i.e if $\boxed{\underline{b} = [\, b_0 \ b_1 \ b_2 \ \ldots \ b_{m-1} \,]}$

then: $b^2 = b_{m-1}\alpha + b_0\alpha^{2^1} + b_1\alpha^{2^2} \ldots b_{m-2}\alpha^{2^{m-1}}$

Or $b^2 = [b_{m-1} \ b_0 \ b_1 \ \ldots \ b_{m-2}]$ in normal base representation

Exponentiation for polynomials/vectors by square-and-multiply technique

Example: setup a hardware structure to compute $b(x)^{25}$ in GF(2^5)

$25 = (11001)_2 = 2^0 + 2^3 + 2^4 = 1 + 8 + 16$