Cryptography

Lecture 3 : Mathematics Background – Part 2

Dr. Muhammad Hataba

Muhammad.Hataba@giu-uni.de

References and Legalities

These slides are in part based on:

- Understanding Cryptography, Christof Paar and Jan Pelzl
- Cryptography and Network Security Course, Swansea University,
- Information Security Course, German International University, Amr ElMougy
- Cryptography Course, German International University, *Alia El Bolock*

Arithmetic for Extension Fields

Arithmetic for Extension Fields

- Addition
- Subtraction
- Multiplication
- Inversion (Division)

Addition and Subtraction in *GF(2^m)*

Definition 4.3.3 Extension field addition and subtraction
Let $A(x), B(x) \in GF(2^m)$. The sum of the two elements is then computed according to:

$$C(x) = A(x) + B(x) = \sum_{i=0}^{m-1} c_i x^i, \quad c_i \equiv a_i + b_i \bmod 2$$

and the difference is computed according to:

$$C(x) = A(x) - B(x) = \sum_{i=0}^{m-1} c_i x^i, \quad c_i \equiv a_i - b_i \equiv a_i + b_i \bmod 2.$$

Addition and Subtraction in *GF(2^m)*

- As we are performing operations mod2, the addition and subtraction are the same operation.
- Addition *mod2* is equivalent to bitwise XOR.

C(x) = A(x)+B(x) of two elements from GF(2^8) is computed as:

$$\begin{array}{rcl} A(x) & = & x^7 + x^6 + x^4 + 1 \\ B(x) & = & x^4 + x^2 + 1 \\ \hline C(x) & = & x^7 + x^6 + x^2 \end{array}$$

Multiplication in *GF(2^m)*

$$A(x)\cdot B(x) = (a_{m-1}x^{m-1}+\cdots+a_0)\cdot(b_{m-1}x^{m-1}+\cdots+b_0)$$
$$C'(x) = c'_{2m-2}x^{2m-2}+\cdots+c'_0,$$

where:

$$\begin{aligned}
c'_0 &= a_0b_0 \bmod 2\\
c'_1 &= a_0b_1+a_1b_0 \bmod 2\\
&\vdots\\
c'_{2m-2} &= a_{m-1}b_{m-1} \bmod 2.
\end{aligned}$$

Multiplication in *GF(2^m)*

Definition 4.3.4 Extension field multiplication
Let $A(x), B(x) \in GF(2^m)$ *and let*

$$P(x) \equiv \sum_{i=0}^{m} p_i x^i, \quad p_i \in GF(2)$$

be an irreducible polynomial. Multiplication of the two elements $A(x), B(x)$ *is performed as*

$$C(x) \equiv A(x) \cdot B(x) \bmod P(x).$$

- Note that the multiplication may create terms with degree more than (m-1), in which case the results need to be reduced using the irreducible polynomial in a modulo operation and keep only the remainder.

(Hint: you can use the extended Euclidean Algorithm)

Example: Extending GF(2) to GF(2^2)

- Find an irreducible polynomial f(x) *defined over your base finite field*.
- Irreducible equation means it cannot be factored, i.e., f(x) is reducible if it has a factor x + a and a ∈ GF(2) .
- Add an element α to the group that satisfies f(α) = 0
- Using what you know of your finite field already, plus this fact, you can create the rest of the field.
- Example, f(x) = x^2+X+1, obviously, X or X+1 cannot factor it. If X is a factor f(0) should be 0 also if X+1 is a factor f(1)should be 0 because we take mod2.
- To extend GF(2) to GF(2^2), we know the elements 0, 1 and α (the root of f(x)) how can we get the rest of the elements? We should have 4 elements.

f(α) = α^2+ α +1 = 0 or α^2 = α +1 if you multiply α by itself you get element in the field that is α +1.

- GF(2^2) = {0, 1, α, α +1}

- We can work with addition in GF(2^2) by just working with vectors
- The vectors are of the form (a_0, a_1), $a_i \in$ GF(2) which represents
- a_0+a_1α . You can add them by just adding like vectors with each element being in GF(2).

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

$.$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

Multiplication cannot be done simply by multiplying elements

Example

Example 7. Let $p = 2$ and $f(x) = x^3 + x + 1$. Then $f(x)$ is irreducible over GF(2). Let α be a root of $f(x)$, i.e., $f(\alpha) = 0$. The finite field GF(2^3) is defined by

$$GF(2^3) = \{a_0 + a_1\alpha + a_2\alpha^2 \mid a^i \in GF(2)\}.$$

Table 1. GF(2^3), defined by $f(x) = x^3 + x + 1$ and $f(\alpha) = 0$.

As a 3-tuple	As a polynomial	As a power of α
000 =	0	= 0
001 =	1	= 1
010 =	α	$= \alpha$
100 =	α^2	$= \alpha^2$
011 =	$1 + \alpha$	$= \alpha^3$
110 =	$\alpha + \alpha^2$	$= \alpha^4$
111 =	$1 + \alpha + \alpha^2$	$= \alpha^5$
101 =	$1 + \alpha^2$	$= \alpha^6$
	$\alpha^7 = 1$	

Irreducible Polynomial $P(x)$ for $GF(2^m)$

Table 4.9 *List of irreducible polynomials*

Degree	*Irreducible Polynomials*
1	$(x+1), (x)$
2	(x^2+x+1)
3	$(x^3+x^2+1), (x^3+x+1)$
4	$(x^4+x^3+x^2+x+1), (x^4+x^3+1), (x^4+x+1)$
5	$(x^5+x^2+1), (x^5+x^3+x^2+x+1), (x^5+x^4+x^3+x+1),$ $(x^5+x^4+x^3+x^2+1), (x^5+x^4+x^2+x+1)$

- Example: We can choose polynomials from this table for Linear Feedback Shift Registers (See Chapter 2 in the Understanding Cryptography Book, but we won't go into that here)

  e.g., for $GF(2^8)$: $P(x) = x^8 + x^4 + x^3 + x + 1$

Inversion in $GF(2^m)$

- Core operation for S-Boxes (byte substitution transformation).
- For a given finite field $GF(2^m)$ and the corresponding irreducible reduction polynomial $P(x)$, the inverse A^{-1} of a nonzero element $A \in GF(2^m)$ is defined as:

$$A^{-1}(x) \cdot A(x) = 1 \bmod P(x)$$

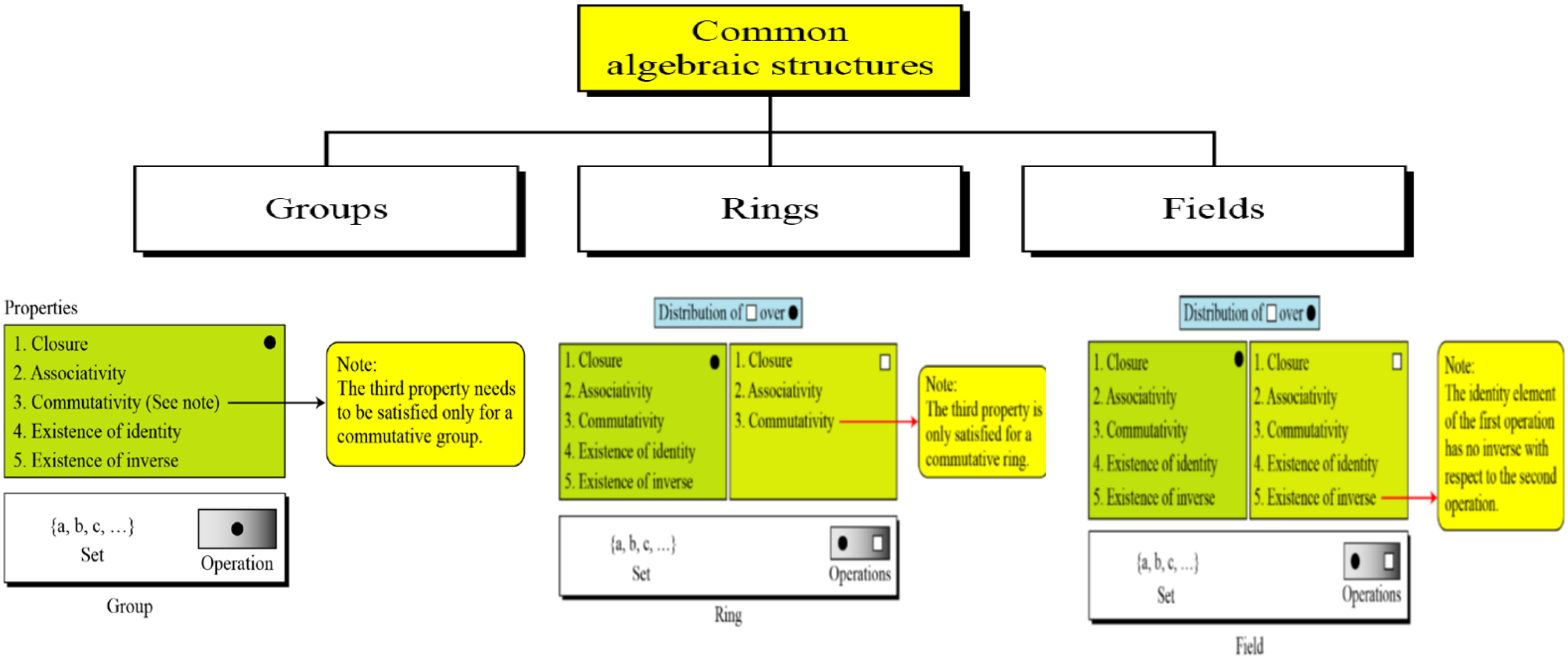
- Lookup tables with precomputed inverses of all field elements exist for small fields ($\leq 2^{16}$ elements)

Multicative Inverse Table for GF(2^8)

- X and Y are bytes used within the AES S-Box operation

X \ Y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	00	01	8D	F6	CB	52	7B	D1	E8	4F	29	C0	B0	E1	E5	C7
1	74	B4	AA	4B	99	2B	60	5F	58	3F	FD	CC	FF	40	EE	B2
2	3A	6E	5A	F1	55	4D	A8	C9	C1	0A	98	15	30	44	A2	C2
3	2C	45	92	6C	F3	39	66	42	F2	35	20	6F	77	BB	59	19
4	1D	FE	37	67	2D	31	F5	69	A7	64	AB	13	54	25	E9	09
5	ED	5C	05	CA	4C	24	87	BF	18	3E	22	F0	51	EC	61	17
6	16	5E	AF	D3	49	A6	36	43	F4	47	91	DF	33	93	21	3B
7	79	B7	97	85	10	B5	BA	3C	B6	70	D0	06	A1	FA	81	82
8	83	7E	7F	80	96	73	BE	56	9B	9E	95	D9	F7	02	B9	A4
9	DE	6A	32	6D	D8	8A	84	72	2A	14	9F	88	F9	DC	89	9A
A	FB	7C	2E	C3	8F	B8	65	48	26	C8	12	4A	CE	E7	D2	62
B	0C	E0	1F	EF	11	75	78	71	A5	8E	76	3D	BD	BC	86	57
C	0B	28	2F	A3	DA	D4	E4	0F	A9	27	53	04	1B	FC	AC	E6
D	7A	07	AE	63	C5	DB	E2	EA	94	8B	C4	D5	9D	F8	90	6B
E	B1	0D	D6	EB	C6	0E	CF	AD	08	4E	D7	E3	5D	50	1E	B3
F	5B	23	38	34	68	46	03	8C	DD	9C	7D	A0	CD	1A	41	1C

To Summarize...



Thank you