

GF(2) 갈루아 필드 양자 게이트 설계 및 구현

대학원 세미나

최승주

2020.02.17

<https://youtu.be/49PMNr2AECw>

GF(2)

- 부호기반 내성 암호에서 사용되는 필드 GF(2)
 - Classic McEliece, NTS-KEM etc.
-
- 대학원 세미나 Finite Field
 - <https://www.youtube.com/watch?v=sX3FXujOMkk&t=595s>
-
- 장경배
 - https://www.youtube.com/channel/UCHXfXZtUSBDOoui_JPS_xwQ

GF(2)

- McEliece, NTS-KEM
- $GF(2^{12})$
- $f(x) = x^{12} + x^3 + 1$

GF(2)

$$\begin{aligned}
 1 &= 1 &= (1, 0, 0, 0)^T; \\
 \beta &= \beta &= (0, 1, 0, 0)^T; \\
 \beta^2 &= \beta^2 &= (0, 0, 1, 0)^T; \\
 \beta^3 &= \beta^3 &= (0, 0, 0, 1)^T; \\
 \beta^4 &= 1 + \beta^3 &= (1, 0, 0, 1)^T; \\
 \beta^5 &= 1 + \beta + \beta^3 &= (1, 1, 0, 1)^T; \\
 \beta^6 &= 1 + \beta + \beta^2 + \beta^3 &= (1, 1, 1, 1)^T; \\
 \beta^7 &= 1 + \beta + \beta^2 &= (1, 1, 1, 0)^T; \\
 \beta^8 &= \beta + \beta^2 + \beta^3 &= (0, 1, 1, 1)^T; \\
 \beta^9 &= 1 + \beta^2 &= (1, 0, 1, 0)^T; \\
 \beta^{10} &= \beta + \beta^3 &= (0, 1, 0, 1)^T; \\
 \beta^{11} &= 1 + \beta^2 + \beta^3 &= (1, 0, 1, 1)^T; \\
 \beta^{12} &= 1 + \beta &= (1, 1, 0, 0)^T; \\
 \beta^{13} &= \beta + \beta^2 &= (0, 1, 1, 0)^T; \\
 \beta^{14} &= \beta^2 + \beta^3 &= (0, 0, 1, 1)^T.
 \end{aligned}$$

$$*\beta^4 = \beta^3 + 1$$

$$\beta^5 = \beta^4 \cdot \beta$$

$$= (\beta^3 + 1) \cdot \beta$$

$$= \beta^4 + \beta$$

$$= 1 + \beta + \beta^3$$

• 위와 같이 순환 구조의 유한체 원소 형성

$$\text{GF}(2^{12}) = X^{12} + X^3 + 1$$

- $a_2X^{11} + \dots + a_{10}X^2 + a_{11}X + 1$
- $b_2X^{11} + \dots + b_{10}X^2 + b_{11}X + 1$

$$\text{GF}(2^{12}) = X^{12} + X^3 + 1$$

- Primitive element

- $f(a) = 0$
- $X^{12} + X^3 + 1 = 0$
- $X^3 + 1 = -X^{12}$
- $X^3 + 1 = X^{12}$

$$\text{GF}(2^{12}) \quad X^{12} = X^3 + 1$$

- $X^{10} * X^5$
 $= X^{15}$
 $= X^{12} * X^3$
 $= (X^3 + 1) * X^3$
 $= X^6 + X^3$

$$\text{GF}(2^{12}) \quad X^{12} = X^3 + 1$$

- Reduction이 필요한 값 계산 ($X^{12}, X^{13} \dots X^{21}, X^{22}$)
- Reduction 처리
- Reduction이 필요 없는 값 계산 ($X^0, X^1 \dots X^{10}, X^{11}$)

$$\text{GF}(2^{12}) \quad X^{12} = X^3 + 1$$

```
1 from projectq import MainEngine
2 from projectq.ops import H, CNOT, Swap, Measure, Toffoli
3 from projectq.backends import CircuitDrawer, ResourceCounter
4
5 #
6
7 def mul_con(eng):
8     a0 = eng.allocate_qubit()
9     a1 = eng.allocate_qubit()
10    a2 = eng.allocate_qubit()
11    a3 = eng.allocate_qubit()
12
13    a4 = eng.allocate_qubit()
14    a5 = eng.allocate_qubit()
15    a6 = eng.allocate_qubit()
16    a7 = eng.allocate_qubit()
17
18    a8 = eng.allocate_qubit()
19    a9 = eng.allocate_qubit()
20    a10 = eng.allocate_qubit()
21    a11 = eng.allocate_qubit()
22
23    b0 = eng.allocate_qubit()
24    b1 = eng.allocate_qubit()
25    b2 = eng.allocate_qubit()
26    b3 = eng.allocate_qubit()
27
28    b4 = eng.allocate_qubit()
29    b5 = eng.allocate_qubit()
30    b6 = eng.allocate_qubit()
31    b7 = eng.allocate_qubit()
32
33    b8 = eng.allocate_qubit()
34    b9 = eng.allocate_qubit()
35    b10 = eng.allocate_qubit()
36    b11 = eng.allocate_qubit()
37
38    c0 = eng.allocate_qubit()
39    c1 = eng.allocate_qubit()
40    c2 = eng.allocate_qubit()
41    c3 = eng.allocate_qubit()
42
43    c4 = eng.allocate_qubit()
44    c5 = eng.allocate_qubit()
45    c6 = eng.allocate_qubit()
46    c7 = eng.allocate_qubit()
47
48    c8 = eng.allocate_qubit()
49    c9 = eng.allocate_qubit()
50    c10 = eng.allocate_qubit()
51    c11 = eng.allocate_qubit()
52
```

- a[12] a0 ~ a11

- b[12] b0 ~ b11

- c[12] c0 ~ c11

$$\text{GF}(2^{12}) \quad X^{12} = X^3 + 1$$

```

56 Toffoli (a11, b1, c0)
57 Toffoli (a10, b2, c0)
58 Toffoli (a9, b3, c0)
59 Toffoli (a8, b4, c0)
60 Toffoli (a7, b5, c0)
61 Toffoli (a6, b6, c0)
62 Toffoli (a5, b7, c0)
63 Toffoli (a4, b8, c0)
64 Toffoli (a3, b9, c0)
65 Toffoli (a2, b10, c0)
66 Toffoli (a1, b11, c0)
67
68 Toffoli (a11, b2, c1)
69 Toffoli (a10, b3, c1)
70 Toffoli (a9, b4, c1)
71 Toffoli (a8, b5, c1)
72 Toffoli (a7, b6, c1)
73 Toffoli (a6, b7, c1)
74 Toffoli (a5, b8, c1)
75 Toffoli (a4, b9, c1)
76 Toffoli (a3, b10, c1)
77 Toffoli (a2, b11, c1)
78
79 Toffoli (a11, b3, c2)
80 Toffoli (a10, b4, c2)
81 Toffoli (a9, b5, c2)
82 Toffoli (a8, b6, c2)
83 Toffoli (a7, b7, c2)
84 Toffoli (a6, b8, c2)
85 Toffoli (a5, b9, c2)
86 Toffoli (a4, b10, c2)
87 Toffoli (a3, b11, c2)

```

- Reduction이 필요한 값 계산

$$X^{12} \rightarrow c0$$

$$X^{13} \rightarrow c1$$

...

$$X^{21} \rightarrow c9$$

$$X^{22} \rightarrow c10 \quad (x^{11} * x^{11})$$

*c11은 여기서 사용하지 않고 비워둠

$$\text{GF}(2^{12}) \quad X^{12} = X^3 + 1$$

- Toffoli(x, y, **z**)

x, y가 1이면 z 반전

1 0 1 \rightarrow 1 0 1

1 1 1 \rightarrow 1 1 0

- CNOT(x, **y**)

x가 1이면 y 반전

$$\text{GF}(2^{12}) \quad X^{12} = X^3 + 1$$

0	1	0	0	0	0	0	0	0	0	1	0
1	0	1	0	0	0	0	0	0	0	0	1
2	0	0	1	0	0	0	0	0	0	0	0
3	1	0	0	1	0	0	0	0	0	1	0
4	0	1	0	0	1	0	0	0	0	0	1
5	0	0	1	0	0	1	0	0	0	0	0
6	0	0	0	1	0	0	1	0	0	0	0
7	0	0	0	0	1	0	0	1	0	0	0
8	0	0	0	0	0	1	0	0	1	0	0
9	0	0	0	0	0	0	1	0	0	1	0
10	0	0	0	0	0	0	0	1	0	0	1
11	0	0	0	0	0	0	0	0	1	0	0
	c0	c1	c2	c3	c4	c5	c6	c7	c8	c9	c10
	x^{12}	x^{13}	x^{14}	x^{15}	x^{16}	x^{17}	x^{18}	x^{19}	x^{20}	x^{21}	x^{22}

$$\text{GF}(2^{12}) \quad X^{12} = X^3 + 1$$

0	1	0	0	0	0	0	0	0	0	1	0		e0
1	0	1	0	0	0	0	0	0	0	0	1		e1
2	0	0	1	0	0	0	0	0	0	0	0		e2
3	1	0	0	1	0	0	0	0	0	1	0		e3
4	0	1	0	0	1	0	0	0	0	0	1		e4
5	0	0	1	0	0	1	0	0	0	0	0		e5
6	0	0	0	1	0	0	1	0	0	0	0		e6
7	0	0	0	0	1	0	0	1	0	0	0		e7
8	0	0	0	0	0	1	0	0	1	0	0		e8
9	0	0	0	0	0	0	1	0	0	1	0		e9
10	0	0	0	0	0	0	0	1	0	0	1		e10
11	0	0	0	0	0	0	0	0	1	0	0		
	c0	c1	c2	c3	c4	c5	c6	c7	c8	c9	c10		
	x^{12}	x^{13}	x^{14}	x^{15}	x^{16}	x^{17}	x^{18}	x^{19}	x^{20}	x^{21}	x^{22}		

$$\text{GF}(2^{12}) \quad X^{12} = X^3 + 1$$

0	1	0	0	0	0	0	0	0	0	1	0		e0
1	0	1	0	0	0	0	0	0	0	0	1		e1
2	0	0	1	0	0	0	0	0	0	0	0		e2
3	1	0	0	1	0	0	0	0	0	1	0		e3 + e0
4	0	1	0	0	1	0	0	0	0	0	1		e4 + e1
5	0	0	1	0	0	1	0	0	0	0	0		e5 + e2
6	0	0	0	1	0	0	1	0	0	0	0		e6 + e3
7	0	0	0	0	1	0	0	1	0	0	0		e7 + e4
8	0	0	0	0	0	1	0	0	1	0	0		e8 + e5
9	0	0	0	0	0	0	1	0	0	1	0		e9 + e6
10	0	0	0	0	0	0	0	1	0	0	1		e10 + e7
11	0	0	0	0	0	0	0	0	1	0	0		e8
	c0	c1	c2	c3	c4	c5	c6	c7	c8	c9	c10		
	x ¹²	x ¹³	x ¹⁴	x ¹⁵	x ¹⁶	x ¹⁷	x ¹⁸	x ¹⁹	x ²⁰	x ²¹	x ²²		

$$\text{GF}(2^{12}) \quad X^{12} = X^3 + 1$$

0	1	0	0	0	0	0	0	0	0	1	0		e0 + e9
1	0	1	0	0	0	0	0	0	0	0	1		e1 + e10
2	0	0	1	0	0	0	0	0	0	0	0		e2
3	1	0	0	1	0	0	0	0	0	1	0		e3 + e0
4	0	1	0	0	1	0	0	0	0	0	1		e4 + e1
5	0	0	1	0	0	1	0	0	0	0	0		e5 + e2
6	0	0	0	1	0	0	1	0	0	0	0		e6 + e3
7	0	0	0	0	1	0	0	1	0	0	0		e7 + e4
8	0	0	0	0	0	1	0	0	1	0	0		e8 + e5
9	0	0	0	0	0	0	1	0	0	1	0		e9 + e6
10	0	0	0	0	0	0	0	1	0	0	1		e10 + e7
11	0	0	0	0	0	0	0	0	1	0	0		e8
	c0	c1	c2	c3	c4	c5	c6	c7	c8	c9	c10		
	x^{12}	x^{13}	x^{14}	x^{15}	x^{16}	x^{17}	x^{18}	x^{19}	x^{20}	x^{21}	x^{22}		

$$\text{GF}(2^{12}) \quad X^{12} = X^3 + 1$$

0	1	0	0	0	0	0	0	0	0	1	0		e0 + e9
1	0	1	0	0	0	0	0	0	0	0	1		e1 + e10
2	0	0	1	0	0	0	0	0	0	0	0		e2
3	1	0	0	1	0	0	0	0	0	1	0		e3 + e0 + e9
4	0	1	0	0	1	0	0	0	0	0	1		e4 + e1 + e10
5	0	0	1	0	0	1	0	0	0	0	0		e5 + e2
6	0	0	0	1	0	0	1	0	0	0	0		e6 + e3
7	0	0	0	0	1	0	0	1	0	0	0		e7 + e4
8	0	0	0	0	0	1	0	0	1	0	0		e8 + e5
9	0	0	0	0	0	0	1	0	0	1	0		e9 + e6
10	0	0	0	0	0	0	0	1	0	0	1		e10 + e7
11	0	0	0	0	0	0	0	0	1	0	0		e8
	c0	c1	c2	c3	c4	c5	c6	c7	c8	c9	c10		
	x^{12}	x^{13}	x^{14}	x^{15}	x^{16}	x^{17}	x^{18}	x^{19}	x^{20}	x^{21}	x^{22}		

$$\text{GF}(2^{12}) \quad X^{12} = X^3 + 1$$

0	1	0	0	0	0	0	0	0	0	1	0		e0 + e9
1	0	1	0	0	0	0	0	0	0	0	1		e1 + e10
2	0	0	1	0	0	0	0	0	0	0	0		e2
3	1	0	0	1	0	0	0	0	0	1	0		e0 + e3 + e9
4	0	1	0	0	1	0	0	0	0	0	1		e1 + e4 + e10
5	0	0	1	0	0	1	0	0	0	0	0		e2 + e5
6	0	0	0	1	0	0	1	0	0	0	0		e3 + e6
7	0	0	0	0	1	0	0	1	0	0	0		e4 + e7
8	0	0	0	0	0	1	0	0	1	0	0		e5 + e8
9	0	0	0	0	0	0	1	0	0	1	0		e6 + e9
10	0	0	0	0	0	0	0	1	0	0	1		e7 + e10
11	0	0	0	0	0	0	0	0	1	0	0		e8
	c0	c1	c2	c3	c4	c5	c6	c7	c8	c9	c10		
	x^{12}	x^{13}	x^{14}	x^{15}	x^{16}	x^{17}	x^{18}	x^{19}	x^{20}	x^{21}	x^{22}		

$$\text{GF}(2^{12}) \quad X^{12} = X^3 + 1$$

0	1	0	0	0	0	0	0	0	0	1	0	e0	e0 + e9
1	0	1	0	0	0	0	0	0	0	0	1	e1	e1 + e10
2	0	0	1	0	0	0	0	0	0	0	0	e2	e2
3	1	0	0	1	0	0	0	0	0	1	0	e3	e0 + e3 + e9
4	0	1	0	0	1	0	0	0	0	0	1	e4	e1 + e4 + e10
5	0	0	1	0	0	1	0	0	0	0	0	e5	e2 + e5
6	0	0	0	1	0	0	1	0	0	0	0	e6	e3 + e6
7	0	0	0	0	1	0	0	1	0	0	0	e7	e4 + e7
8	0	0	0	0	0	1	0	0	1	0	0	e8	e5 + e8
9	0	0	0	0	0	0	1	0	0	1	0	e9	e6 + e9
10	0	0	0	0	0	0	0	1	0	0	1	e10	e7 + e10
11	0	0	0	0	0	0	0	0	1	0	0	e11	e8
	c0	c1	c2	c3	c4	c5	c6	c7	c8	c9	c10		
	x ¹²	x ¹³	x ¹⁴	x ¹⁵	x ¹⁶	x ¹⁷	x ¹⁸	x ¹⁹	x ²⁰	x ²¹	x ²²		

$$\text{GF}(2^{12}) \quad X^{12} = X^3 + 1$$

e0 + e9
e1 + e10
e2
e0 + e3 + e9
e1 + e4 + e10
e2 + e5
e3 + e6
e4 + e7
e5 + e8
e6 + e9
e7 + e10
e8

$$\text{GF}(2^{12}) \quad X^{12} = X^3 + 1$$

$e0 + e9$

$e1 + e10$

$e2$

$e0 = \text{CNOT}(e9, e0) \rightarrow e0' (e9+e0)$

$e1 = \text{CNOT}(e10, e1) \rightarrow e1' (e10+e1)$

$e2 =$

$$\text{GF}(2^{12}) \quad X^{12} = X^3 + 1$$

e0 + e9
e1 + e10
e2
e0 + e3 + e9
e1 + e4 + e10
e2 + e5
e3 + e6
e4 + e7
e5 + e8
e6 + e9
e7 + e10
e8

- e0 + e9 값을 중복해서 다시 사용할 수 있음
- e1 + e10 값을 중복해서 다시 사용할 수 있음

$$e0 = \text{CNOT}(e9, \text{e0}) \rightarrow e0' (e9+e0)$$

$$e1 = \text{CNOT}(e10, \text{e1}) \rightarrow e1' (e10+e1)$$

$$\text{GF}(2^{12}) \quad X^{12} = X^3 + 1$$

0	1	0	0	0	0	0	0	0	0	1	0	e0	e0 + e9
1	0	1	0	0	0	0	0	0	0	0	1	e1	e1 + e10
2	0	0	1	0	0	0	0	0	0	0	0	e2	e2
3	1	0	0	1	0	0	0	0	0	1	0	e3	e0 + e3 + e9
4	0	1	0	0	1	0	0	0	0	0	1	e4	e1 + e4 + e10
5	0	0	1	0	0	1	0	0	0	0	0	e5	e2 + e5
6	0	0	0	1	0	0	1	0	0	0	0	e6	e3 + e6
7	0	0	0	0	1	0	0	1	0	0	0	e7	e4 + e7
8	0	0	0	0	0	1	0	0	1	0	0	e8	e5 + e8
9	0	0	0	0	0	0	1	0	0	1	0	e9	e6 + e9
10	0	0	0	0	0	0	0	1	0	0	1	e10	e7 + e10
11	0	0	0	0	0	0	0	0	1	0	0	e11	e8
	c0	c1	c2	c3	c4	c5	c6	c7	c8	c9	c10		
	x ¹²	x ¹³	x ¹⁴	x ¹⁵	x ¹⁶	x ¹⁷	x ¹⁸	x ¹⁹	x ²⁰	x ²¹	x ²²		

$$\text{GF}(2^{12}) \quad X^{12} = X^3 + 1$$

e0	e0 + e9	3
e1	e1 + e10	4
e2	e2	(12)
e3	e0 + e3 + e9	10
e4	e1 + e4 + e10	11
e5	e2 + e5	7
e6	e3 + e6	8
e7	e4 + e7	9
e8	e5 + e8	2
e9	e6 + e9	5
e10	e7 + e10	6
e11	e8	1

#

CNOT | (c8, c11)
CNOT | (c5, c8)

CNOT | (c9, c0)
CNOT | (c10, c1)

CNOT | (c6, c9)
CNOT | (c7, c10)

CNOT | (c2, c5)
CNOT | (c3, c6)
CNOT | (c4, c7)

CNOT | (c0, c3)
CNOT | (c1, c4)

$$\text{GF}(2^{12}) \quad X^{12} = X^3 + 1$$

e0	e0 + e9	
e1	e1 + e10	
e2	e2	
e3	e0 + e3 + e9	
e4	e1 + e4 + e10	
e5	e2 + e5	
e6	e3 + e6	
e7	e4 + e7	
e8	e5 + e8	2
e9	e6 + e9	
e10	e7 + e10	
e11	e8	1

CNOT | (c8, c11)
CNOT | (c5, c8)

C8 → 1번에 의해 공간이 생겼음

C11 → 비어있던 공간

$$\text{GF}(2^{12}) \quad X^{12} = X^3 + 1$$

e0	e0 + e9	3
e1	e1 + e10	4
e2	e2	
e3	e0 + e3 + e9	
e4	e1 + e4 + e10	
e5	e2 + e5	
e6	e3 + e6	
e7	e4 + e7	
e8	e5 + e8	2
e9	e6 + e9	
e10	e7 + e10	
e11	e8	1

 CNOT | (c8, c11)
 CNOT | (c5, c8)

 CNOT | (c9, c0)
 CNOT | (c10, c1)

- e0과 e1의 연산이자 e3와 e4에서 사용될 값 미리 연산

$$\text{GF}(2^{12}) \quad X^{12} = X^3 + 1$$

e0	e0 + e9	3
e1	e1 + e10	4
e2	e2	
e3	e0 + e3 + e9	
e4	e1 + e4 + e10	
e5	e2 + e5	7
e6	e3 + e6	8
e7	e4 + e7	9
e8	e5 + e8	2
e9	e6 + e9	5
e10	e7 + e10	6
e11	e8	1

#

CNOT		(c8, c11)
CNOT		(c5, c8)
CNOT		(c9, c0)
CNOT		(c10, c1)
CNOT		(c6, c9)
CNOT		(c7, c10)
CNOT		(c2, c5)
CNOT		(c3, c6)
CNOT		(c4, c7)

- 연산되는 값들은 **변경**이 된 값들이 아니기에 가능
ex) e0, e1, e8의 값은 현재 CNOT에 의해 변경됨

$$\text{GF}(2^{12}) \quad X^{12} = X^3 + 1$$

e0	e0 + e9	
e1	e1 + e10	
e2	e2	
e3	e0 + e3 + e9	
e4	e1 + e4 + e10	
e5	e2 + e5	1
e6	e3 + e6	
e7	e4 + e7	
e8	e5 + e8	2
e9	e6 + e9	
e10	e7 + e10	
e11	e8	

- 연산되는 값들은 **변경**이 된 값들이 아니기에 가능
ex) e0, e1, e8의 값은 현재 CNOT에 의해 변경됨
- Ex) e5 → e8 순서로 연산을 하게 되는 경우
- e5는 정상적으로 값이 입력 되지만
- e8 같은 경우 $e5 + e8 \rightarrow (e2 + e5) + e8$ 이 되어 연산이 꼬이게 된다.

$$\text{GF}(2^{12}) \quad X^{12} = X^3 + 1$$

e0	e0 + e9	3
e1	e1 + e10	4
e2	e2	
e3	e0 + e3 + e9	10
e4	e1 + e4 + e10	11
e5	e2 + e5	7
e6	e3 + e6	8
e7	e4 + e7	9
e8	e5 + e8	2
e9	e6 + e9	5
e10	e7 + e10	6
e11	e8	1

#

CNOT | (c8, c11)
CNOT | (c5, c8)

CNOT | (c9, c0)
CNOT | (c10, c1)

CNOT | (c6, c9)
CNOT | (c7, c10)

CNOT | (c2, c5)
CNOT | (c3, c6)
CNOT | (c4, c7)

CNOT | (c0, c3)
CNOT | (c1, c4)

→ 연산 절감

$$\text{GF}(2^{12}) \quad X^{12} = X^3 + 1$$

- Reduction이 필요 없는 부분 Multiplication

$$X^0 \rightarrow c0$$

$$X^1 \rightarrow c1$$

...

$$X^{10} \rightarrow c10$$

$$X^{11} \rightarrow c11 \quad (X^{11} * X^0)$$

```

160 Toffoli | (a0, b0, c0)
161
162 Toffoli | (a1, b0, c1)
163 Toffoli | (a0, b1, c1)
164
165 Toffoli | (a2, b0, c2)
166 Toffoli | (a1, b1, c2)
167 Toffoli | (a0, b2, c2)
168
169 Toffoli | (a3, b0, c3)
170 Toffoli | (a2, b1, c3)
171 Toffoli | (a1, b2, c3)
172 Toffoli | (a0, b3, c3)
173
174 Toffoli | (a4, b0, c4)
175 Toffoli | (a3, b1, c4)
176 Toffoli | (a2, b2, c4)
177 Toffoli | (a1, b3, c4)
178 Toffoli | (a0, b4, c4)
179
180 Toffoli | (a5, b0, c5)
181 Toffoli | (a4, b1, c5)
182 Toffoli | (a3, b2, c5)
183 Toffoli | (a2, b3, c5)
184 Toffoli | (a1, b4, c5)
185 Toffoli | (a0, b5, c5)
186
187 Toffoli | (a6, b0, c6)
188 Toffoli | (a5, b1, c6)
189 Toffoli | (a4, b2, c6)
190 Toffoli | (a3, b3, c6)
191 Toffoli | (a2, b4, c6)
192 Toffoli | (a1, b5, c6)
193 Toffoli | (a0, b6, c6)
...
```

$$\text{GF}(2^{13}) \quad X^{13} = X^4 + X^3 + X + 1$$

- Reduction이 필요한 값 계산 ($X^{13}, X^{14} \dots X^{23}, X^{24}$)
- Reduction 처리
- Reduction이 필요 없는 값 계산 ($X^0, X^1 \dots X^{10}, X^{12}$)

$$\text{GF}(2^{13}) \quad X^{13} = X^4 + X^3 + X + 1$$

0	1	0	0	0	0	0	0	0	0	0	1	1	0
1	1	1	0	0	0	0	0	0	0	0	1	0	1
2	0	1	1	0	0	0	0	0	0	0	0	1	0
3	1	0	1	1	0	0	0	0	0	0	1	1	1
4	1	1	0	1	1	0	0	0	0	0	1	0	1
5	0	1	1	0	1	1	0	0	0	0	0	1	0
6	0	0	1	1	0	1	1	0	0	0	0	0	1
7	0	0	0	1	1	0	1	1	0	0	0	0	0
8	0	0	0	0	1	1	0	1	1	0	0	0	0
9	0	0	0	0	0	1	1	0	1	1	0	0	0
10	0	0	0	0	0	0	1	1	0	1	1	0	0
11	0	0	0	0	0	0	0	1	1	0	1	1	0
12	0	0	0	0	0	0	0	0	1	1	0	1	0
	c0	c1	c2	c3	c4	c5	c6	c7	c8	c9	c10	c11	
	x^{13}	x^{14}	x^{15}	x^{16}	x^{17}	x^{18}	x^{19}	x^{20}	x^{21}	x^{22}	x^{23}	x^{24}	

$$\text{GF}(2^{13}) \quad X^{13} = X^4 + X^3 + X + 1$$

0	1	0	0	0	0	0	0	0	0	0	1	1	0
1	1	1	0	0	0	0	0	0	0	0	1	0	1
2	0	1	1	0	0	0	0	0	0	0	0	1	0
3	1	0	1	1	0	0	0	0	0	0	1	1	1
4	1	1	0	1	1	0	0	0	0	0	1	0	1
5	0	1	1	0	1	1	0	0	0	0	0	1	0
6	0	0	1	1	0	1	1	0	0	0	0	0	1
7	0	0	0	1	1	0	1	1	0	0	0	0	0
8	0	0	0	0	1	1	0	1	1	0	0	0	0
9	0	0	0	0	0	1	1	0	1	1	0	0	0
10	0	0	0	0	0	0	1	1	0	1	1	0	0
11	0	0	0	0	0	0	0	1	1	0	1	1	0
12	0	0	0	0	0	0	0	0	1	1	0	1	0
	c0	c1	c2	c3	c4	c5	c6	c7	c8	c9	c10	c11	
	x^{13}	x^{14}	x^{15}	x^{16}	x^{17}	x^{18}	x^{19}	x^{20}	x^{21}	x^{22}	x^{23}	x^{24}	

$$\text{GF}(2^{13}) \quad X^{13} = X^4 + X^3 + X + 1$$

0
1
0
1
1
0
1
0
0
0
0
1
1
c11
X^{24}

$$X^{24}$$

$$= X^{13} * X^{11}$$

$$= (X^4 + X^3 + X + 1) * X^{11}$$

$$= X^{15} + X^{14} + X^{12} + X^{11}$$

$$= (X^{13} * X^2) + (X^{13} * X^1) + X^{12} + X^{11}$$

$$= (X^4 + X^3 + X + 1) * X^2 + (X^4 + X^3 + X + 1) * X^1 + X^{12} + X^{11}$$

$$= X^6 + X^5 + X^3 + X^2 + X^5 + X^4 + X^2 + X^1 + X^{12} + X^{11}$$

$$= X^{12} + X^{11} + X^6 + 2X^5 + X^4 + X^3 + 2X^2 + X^1$$

$$= X^{12} + X^{11} + X^6 + X^4 + X^3 + X$$

$$\text{GF}(2^{13}) \quad X^{13} = X^4 + X^3 + X + 1$$

0	1	0	0	0	0	0	0	0	0	1	1	0	e0	
1	1	1	0	0	0	0	0	0	0	1	0	1	e1	
2	0	1	1	0	0	0	0	0	0	0	1	0	e2	
3	1	0	1	1	0	0	0	0	0	1	1	1	e3	
4	1	1	0	1	1	0	0	0	0	1	0	1	e4	
5	0	1	1	0	1	1	0	0	0	0	1	0	e5	
6	0	0	1	1	0	1	1	0	0	0	0	1	e6	
7	0	0	0	1	1	0	1	1	0	0	0	0	e7	
8	0	0	0	0	1	1	0	1	1	0	0	0	e8	
9	0	0	0	0	0	1	1	0	1	1	0	0	e9	
10	0	0	0	0	0	0	1	1	0	1	1	0	e10	
11	0	0	0	0	0	0	0	1	1	0	1	1	e11	
12	0	0	0	0	0	0	0	0	1	1	0	1	e12	
	c0	c1	c2	c3	c4	c5	c6	c7	c8	c9	c10	c11		
	x^{13}	x^{14}	x^{15}	x^{16}	x^{17}	x^{18}	x^{19}	x^{20}	x^{21}	x^{22}	x^{23}	x^{24}		

$$\text{GF}(2^{13}) \quad X^{13} = X^4 + X^3 + X + 1$$

0	1	0	0	0	0	0	0	0	0	1	1	0	e0	e0 + e9 + e10
1	1	1	0	0	0	0	0	0	0	1	0	1	e1	e0 + e1 + e9 + e11
2	0	1	1	0	0	0	0	0	0	0	1	0	e2	e1 + e2 + e10
3	1	0	1	1	0	0	0	0	0	1	1	1	e3	e0 + e2 + e3 + e9 + e10 + e11
4	1	1	0	1	1	0	0	0	0	1	0	1	e4	e0 + e1 + e3 + e4 + e9 + e11
5	0	1	1	0	1	1	0	0	0	0	1	0	e5	e1 + e2 + e4 + e5 + e10
6	0	0	1	1	0	1	1	0	0	0	0	1	e6	e2 + e3 + e5 + e6 + e11
7	0	0	0	1	1	0	1	1	0	0	0	0	e7	e3 + e4 + e6 + e7
8	0	0	0	0	1	1	0	1	1	0	0	0	e8	e4 + e5 + e7 + e8
9	0	0	0	0	0	1	1	0	1	1	0	0	e9	e5 + e6 + e8 + e9
10	0	0	0	0	0	0	1	1	0	1	1	0	e10	e6 + e7 + e9 + e10
11	0	0	0	0	0	0	0	1	1	0	1	1	e11	e7 + e8 + e10 + e11
12	0	0	0	0	0	0	0	0	1	1	0	1	e12	e8 + e9 + e11
	c0	c1	c2	c3	c4	c5	c6	c7	c8	c9	c10	c11		
	x^{13}	x^{14}	x^{15}	x^{16}	x^{17}	x^{18}	x^{19}	x^{20}	x^{21}	x^{22}	x^{23}	x^{24}		

$$\text{GF}(2^{13}) \quad X^{13} = X^4 + X^3 + X + 1$$

0	1	0	0	0	0	0	0	0	0	1	1	0	e0	e0 + e9 + e10
1	1	1	0	0	0	0	0	0	0	1	0	1	e1	e0 + e1 + e9 + e11
2	0	1	1	0	0	0	0	0	0	0	1	0	e2	e1 + e2 + e10
3	1	0	1	1	0	0	0	0	0	1	1	1	e3	e0 + e2 + e3 + e9 + e10 + e11
4	1	1	0	1	1	0	0	0	0	1	0	1	e4	e0 + e1 + e3 + e4 + e9 + e11
5	0	1	1	0	1	1	0	0	0	0	1	0	e5	e1 + e2 + e4 + e5 + e10
6	0	0	1	1	0	1	1	0	0	0	0	1	e6	e2 + e3 + e5 + e6 + e11
7	0	0	0	1	1	0	1	1	0	0	0	0	e7	e3 + e4 + e6 + e7
8	0	0	0	0	1	1	0	1	1	0	0	0	e8	e4 + e5 + e7 + e8
9	0	0	0	0	0	1	1	0	1	1	0	0	e9	e5 + e6 + e8 + e9
10	0	0	0	0	0	0	1	1	0	1	1	0	e10	e6 + e7 + e9 + e10
11	0	0	0	0	0	0	0	1	1	0	1	1	e11	e7 + e8 + e10 + e11
12	0	0	0	0	0	0	0	0	1	1	0	1	e12	e8 + e9 + e11
	c0	c1	c2	c3	c4	c5	c6	c7	c8	c9	c10	c11		
	x ¹³	x ¹⁴	x ¹⁵	x ¹⁶	x ¹⁷	x ¹⁸	x ¹⁹	x ²⁰	x ²¹	x ²²	x ²³	x ²⁴		

$$\text{GF}(2^{13}) \quad X^{13} = X^4 + X^3 + X + 1$$

e0	e0 + e9 + e10	3
e1	e0 + e1 + e9 + e11	4
e2	e1 + e2 + e10	5
e3	e0 + e2 + e3 + e9 + e10 + e11	
e4	e0 + e1 + e3 + e4 + e9 + e11	
e5	e1 + e2 + e4 + e5 + e10	
e6	e2 + e3 + e5 + e6 + e11	
e7	e3 + e4 + e6 + e7	
e8	e4 + e5 + e7 + e8	2
e9	e5 + e6 + e8 + e9	
e10	e6 + e7 + e9 + e10	
e11	e7 + e8 + e10 + e11	
e12	e8 + e9 + e11	1

$$\text{GF}(2^{13}) \quad X^{13} = X^4 + X^3 + X + 1$$

e0	e0 + e9 + e10	3
e1	e0 + e1 + e9 + e11	4
e2	e1 + e2 + e10	5
e3	e0 + e2 + e3 + e9 + e10 + e11	
e4	e0 + e1 + e3 + e4 + e9 + e11	
e5	e1 + e2 + e4 + e5 + e10	
e6	e2 + e3 + e5 + e6 + e11	
e7	e3 + e4 + e6 + e7	
e8	e4 + e5 + e7 + e8	2
e9	e5 + e6 + e8 + e9	
e10	e6 + e7 + e9 + e10	
e11	e7 + e8 + e10 + e11	
e12	e8 + e9 + e11	1

- 연산되는 값들은 **변경**이 된 값들이 아니기에 가능

$$\text{GF}(2^{13}) \quad X^{13} = X^4 + X^3 + X + 1$$

e0	e0 + e9 + e10	5
e1	e0 + e1 + e9 + e11	4
e2	e1 + e2 + e10	3
e3	e0 + e2 + e3 + e9 + e10 + e11	
e4	e0 + e1 + e3 + e4 + e9 + e11	
e5	e1 + e2 + e4 + e5 + e10	
e6	e2 + e3 + e5 + e6 + e11	
e7	e3 + e4 + e6 + e7	
e8	e4 + e5 + e7 + e8	2
e9	e5 + e6 + e8 + e9	
e10	e6 + e7 + e9 + e10	
e11	e7 + e8 + e10 + e11	
e12	e8 + e9 + e11	1

- 연산되는 값들은 **변경**이 된 값들이 아니기에 가능

$$\text{GF}(2^{13}) \quad X^{13} = X^4 + X^3 + X + 1$$

e0	e0 + e9 + e10	5
e1	e0 + e1 + e9 + e11	4
e2	e1 + e2 + e10	3
e3	e0 + e2 + e3 + e9 + e10 + e11	6
e4	e0 + e1 + e3 + e4 + e9 + e11	
e5	e1 + e2 + e4 + e5 + e10	
e6	e2 + e3 + e5 + e6 + e11	
e7	e3 + e4 + e6 + e7	
e8	e4 + e5 + e7 + e8	2
e9	e5 + e6 + e8 + e9	
e10	e6 + e7 + e9 + e10	
e11	e7 + e8 + e10 + e11	
e12	e8 + e9 + e11	1

- 연산되는 값들은 **변경**이 된 값들이 아니기에 가능
- e0 + e2 + e3 + e9 + e10 + e11**
- e2가 이미 CNOT(e1, e2) CNOT(e10, e2)에 의해 변경

$$\text{GF}(2^{13}) \quad X^{13} = X^4 + X^3 + X + 1$$

e0	e0 + e9 + e10	
e1	e0 + e1 + e9 + e11	
e2	e1 + e2 + e10	3
e3	e0 + e2 + e3 + e9 + e10 + e11	
e4	e0 + e1 + e3 + e4 + e9 + e11	
e5	e1 + e2 + e4 + e5 + e10	4
e6	e2 + e3 + e5 + e6 + e11	
e7	e3 + e4 + e6 + e7	
e8	e4 + e5 + e7 + e8	2
e9	e5 + e6 + e8 + e9	
e10	e6 + e7 + e9 + e10	
e11	e7 + e8 + e10 + e11	
e12	e8 + e9 + e11	1

- 연산되는 값들은 **변경**이 된 값들이 아니기에 가능

$$\text{GF}(2^{13}) \quad X^{13} = X^4 + X^3 + X + 1$$

e0	e0 + e9 + e10	
e1	e0 + e1 + e9 + e11	5
e2	e1 + e2 + e10	3
e3	e0 + e2 + e3 + e9 + e10 + e11	
e4	e0 + e1 + e3 + e4 + e9 + e11	6
e5	e1 + e2 + e4 + e5 + e10	4
e6	e2 + e3 + e5 + e6 + e11	
e7	e3 + e4 + e6 + e7	
e8	e4 + e5 + e7 + e8	2
e9	e5 + e6 + e8 + e9	
e10	e6 + e7 + e9 + e10	
e11	e7 + e8 + e10 + e11	
e12	e8 + e9 + e11	1

- 연산되는 값들은 **변경**이 된 값들이 아니기에 가능

$$\text{GF}(2^{13}) \quad X^{13} = X^4 + X^3 + X + 1$$

e0	e0 + e9 + e10	7
e1	e0 + e1 + e9 + e11	5
e2	e1 + e2 + e10	3
e3	e0 + e2 + e3 + e9 + e10 + e11	8
e4	e0 + e1 + e3 + e4 + e9 + e11	6
e5	e1 + e2 + e4 + e5 + e10	4
e6	e2 + e3 + e5 + e6 + e11	
e7	e3 + e4 + e6 + e7	
e8	e4 + e5 + e7 + e8	2
e9	e5 + e6 + e8 + e9	
e10	e6 + e7 + e9 + e10	
e11	e7 + e8 + e10 + e11	
e12	e8 + e9 + e11	1

- 연산되는 값들은 **변경**이 된 값들이 아니기에 가능
- e0 + e2 + e3 + e9 + e10 + e11**
- e2가 이미 CNOT(e1, e2) CNOT(e10, e2)에 의해 변경

$$\text{GF}(2^{13}) \quad X^{13} = X^4 + X^3 + X + 1$$

e0	e0 + e9 + e10	
e1	e0 + e1 + e9 + e11	
e2	e1 + e2 + e10	
e3	e0 + e2 + e3 + e9 + e10 + e11	
e4	e0 + e1 + e3 + e4 + e9 + e11	
e5	e1 + e2 + e4 + e5 + e10	
e6	e2 + e3 + e5 + e6 + e11	
e7	e3 + e4 + e6 + e7	
e8	e4 + e5 + e7 + e8	
e9	e5 + e6 + e8 + e9	
e10	e6 + e7 + e9 + e10	
e11	e7 + e8 + e10 + e11	
e12	e8 + e9 + e11	

$$\text{GF}(2^{13}) \quad X^{13} = X^4 + X^3 + X + 1$$

e0	e0 + e9 + e10	
e1	e0 + e1 + e9 + e11	
e2	e1 + e2 + e10	
e3	e0 + e2 + e3 + e9 + e10 + e11	
e4	e0 + e1 + e3 + e4 + e9 + e11	
e5	e1 + e2 + e4 + e5 + e10	
e6	e2 + e3 + e5 + e6 + e11	
e7	e3 + e4 + e6 + e7	
e8	e4 + e5 + e7 + e8	
e9	e5 + e6 + e8 + e9	
e10	e6 + e7 + e9 + e10	
e11	e7 + e8 + e10 + e11	
e12	e8 + e9 + e11	

- 몇몇 변경되지 않은 값을 따로 저장해둘 공간이 더 필요

$$\text{GF}(2^{13}) \quad X^{13} = X^4 + X^3 + X + 1$$

- $\text{GF}(2^{12}) \quad X^{12} = X^3 + 1$

a0~a11 → 12 공간

b0~b11 → 12 공간

c0~c11 → 12 공간

➔ c11은 reduction에서 c8의 값을 담아줬던 임시로 비어져 있었던 공간

$$\text{GF}(2^{13}) \quad X^{13} = X^4 + X^3 + X + 1$$

- $\text{GF}(2^{13}) \quad X^{13} = X^4 + X^3 + X + 1$

$a_0 \sim a_{12} \rightarrow 13$ 공간

$b_0 \sim b_{12} \rightarrow 13$ 공간

$c_0 \sim c_{12} \rightarrow 13$ 공간 + **6개의 추가 공간**

➔ 변경되기 전의 값들을 담아줄 임시 공간들

$a_0 \sim a_{12} \rightarrow 13$ 공간

$b_0 \sim b_{12} \rightarrow 13$ 공간

$c_0 \sim c_{18} \rightarrow 19$ 공간

$$\text{GF}(2^{13}) \quad X^{13} = X^4 + X^3 + X + 1$$

e0	e0 + e9 + e10	6
e1	e0 + e1 + e9 + e11	4
e2	e1 + e2 + e10	2
e3	e0 + e2 + e3 + e9 + e10 + e11	7
e4	e0 + e1 + e3 + e4 + e9 + e11	5
e5	e1 + e2 + e4 + e5 + e10	3
e6	e2 + e3 + e5 + e6 + e11	13
e7	e3 + e4 + e6 + e7	12
e8	e4 + e5 + e7 + e8	11
e9	e5 + e6 + e8 + e9	10
e10	e6 + e7 + e9 + e10	9
e11	e7 + e8 + e10 + e11	8
e12	e8 + e9 + e11	1

e13 - e2

e14 - e3

e15 - e4

e16 - e5

e17 - e11



$$\text{GF}(2^{13}) \quad X^{13} = X^4 + X^3 + X + 1$$

e0	e0 + e9 + e10	6	e0 = e9 + e10
e1	e0 + e1 + e9 + e11	4	e1 = e0 + e9 + e11
e2	e1 + e2 + e10	2	e2 = e1 + e10
e3	e0 + e2 + e3 + e9 + e10 + e11	7	e3 = e0 + c[13] + e11
e4	e0 + e1 + e3 + e4 + e9 + e11	5	e4 = e1 + e3
e5	e1 + e2 + e4 + e5 + e10	3	e5 = e2 + e4
e6	e2 + e3 + e5 + e6 + e11	13	e6 = c[13] + c[14] + c[16] + c[17]
e7	e3 + e4 + e6 + e7	12	e7 = c[14] + c[15] + e6
e8	e4 + e5 + e7 + e8	11	e8 = c[15] + c[16] + e7
e9	e5 + e6 + e8 + e9	10	e9 = c[16] + e6 + e8
e10	e6 + e7 + e9 + e10	9	e10 = e6 + e7 + e9
e11	e7 + e8 + e10 + e11	8	e11 = e7 + e8 + e10
e12	e8 + e9 + e11	1	e12 = e8 + e9 + e11

e13 - e2

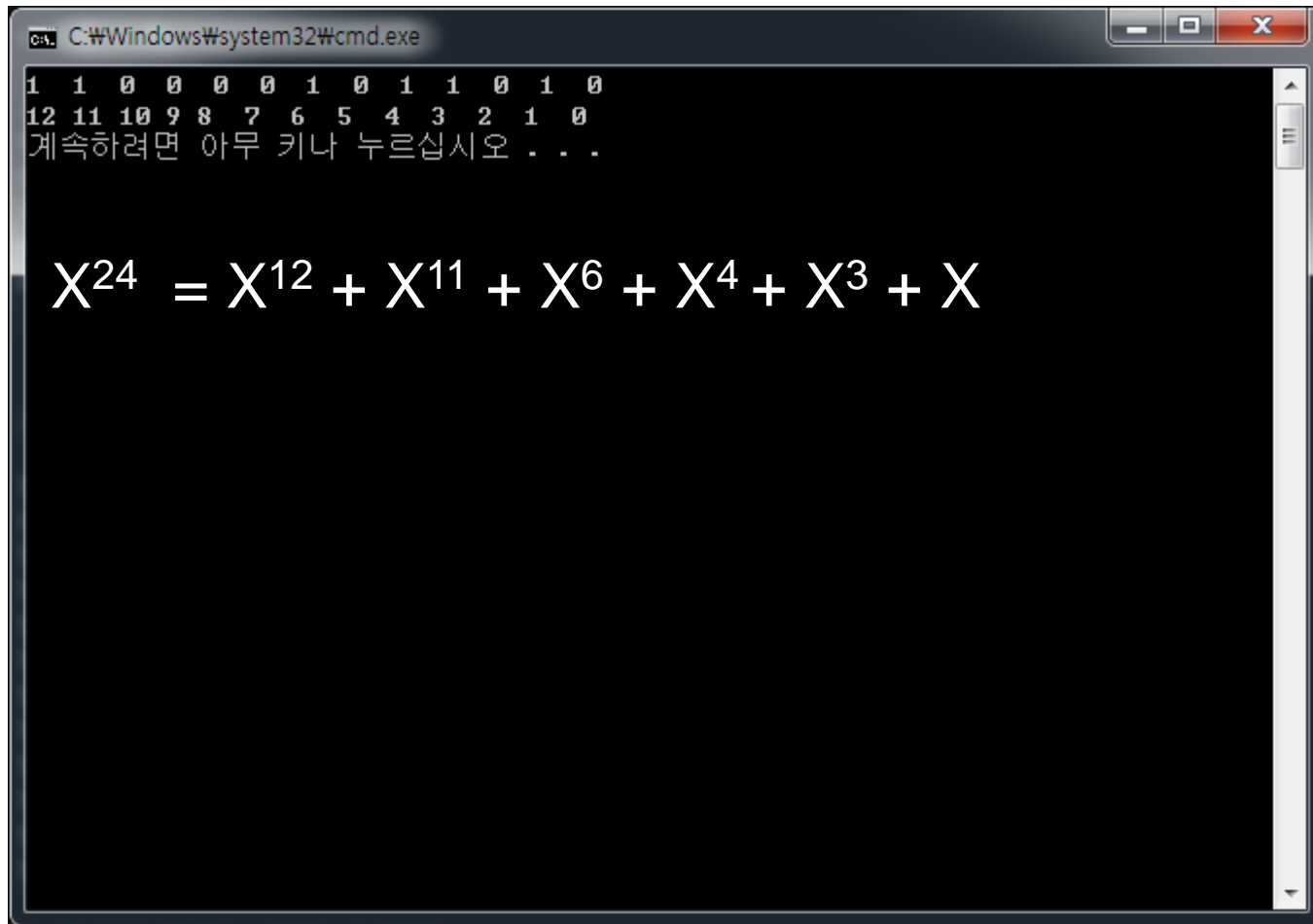
e14 - e3

e15 - e4

e16 - e5

e17 - e11

$$\text{GF}(2^{13}) \quad X^{13} = X^4 + X^3 + X + 1$$



```
C:\Windows\system32\cmd.exe
1 1 0 0 0 0 1 0 1 1 0 1 0
12 11 10 9 8 7 6 5 4 3 2 1 0
계속하려면 아무 키나 누르십시오 . . .

X24 = X12 + X11 + X6 + X4 + X3 + X
```

Q & A

