通信情報保護學會論文誌
第 9 券 第 3 號, 1999. 09

GF(2^n) 위에서의 다항식 인수분해

김 창 한*, 서 광 석**

The polynomial factorization over $GF(2^n)$

Chang Han Kim*, Kwang Suk Suh**

요약

공개키 암호법은 정수 인수분해의 어려움에 바탕을 둔 RSA와 이산대수문제의 어려움에 근거한 ElGamal 암호법으로 대표된다. $GF(q^n)^*$에서 index-calculus 이산대수 알고리즘은 다항식 인수분해를 필요로 한다. 최근에 Niederreiter에 의하여 유한체위에서의 다항식 인수분해 알고리즘이 제안되었다. 이 논문에서는 정규기저(normal basis)를 이용한 유한체의 연산을 C-언어로 구현하고, 이것을 이용한 Niederreiter의 알고리즘을 기반으로 유한체위에서의 다항식 인수분해 알고리즘과 구현한 결과를 제시한다.

ABSTRACT

The public key cryptosystem is represented by RSA based on the difficulty of integer factorization and ElGamal cryptosystem based on the intractability of the discrete logarithm problem in a cyclic group G. The index-calculus algorithm for discrete logarithms in $GF(q^n)^*$ requires an polynomial factorization. The Niederreiter recently developed deterministic facorization algorithm for polynomial over $GF(q^n)$. In this paper we implemented the arithmetic of finite field with c-language and give an implementation of the Niederreiter's algorithm over $GF(2^n)$ using normal bases.

---

* 세명대학교 컴퓨터응용수학과(chkim@venus.semyung.ac.kr)
** 서남대학교 수학과(suh0415@chollian.net)

이 논문은 1997년도 세명대학교 교내학술연구비 지원에 의해 수행된 연구임

Ⅰ. 서 론

암호론은 역사적으로 오래된 흥미있는 문제로 1976년 Diffie 와 Hellman에 의하여 공개키 암호법이 제안된 이후, 정보통신의 시대를 맞이하여 암호학의 이용 가치가 증대되고 있다. 특히 전자상거래의 활성화와 관련하여 공개키 암호시스템의 수요가 증대되고 있다. 공개키 암호법은 일방향 함수(one way function)에 근거를 두고 있으며 RSA와 ElGamal 암호법으로 대표된다. RSA는 큰 수의 소인수분해의 어려움에 바탕을 두고있는 암호법이고 ElGamal 암호법은 순환군(cyclic groups)의 이산대수(discrete logarithm) 문제의 어려움에 근거한 암호법이다. ElGamal 암호법의 순환군은 Z_p^* 와 $GF(q^n)^*$가 주로 사용된다. 또한 타원곡선 암호법(Elliptic curve cryptosystem)은 1985년 Kobliz[2]와 Miller[7]에 의하여 각각 독자적으로 제안된 것으로 유한체 $GF(q^n)$ 위에서 덧셈에 대한 타원곡선군의 이산대수 문제의 어려움에 바탕을 둔 암호법이다. 유한체 $GF(2^n)$를 구성하기 위하여 $GF(2)[x]$에 있는 n 차의 기약다항식이 필요하고, 그리고 이산대문제를 푸는 가장 효율적인 방법으로 알려진 index-calculus 알고리즘에는 다항식의 인수분해 과정이 필요하다[6].

이와 같이 최근 들어 암호학과 관련하여 유한체 위에서의 다항식의 인수분해와 기약다항식의 판정 문제가 중요한 문제로 재기되고 있으며 또한 오래된 수학문제 중 하나로, 이 문제를 푸는 알고리즘은 Berlekamp의 알고리즘[3,4]으로 대표되었으나, 최근에 Niederreiter의 알고리즘[8,9]이 제안되었다. Characteristic이 2인 유한체 위에서는 Niederreiter의 알고리즘이 더 효율적이다. 유한체의 표현에는 몇 가지 방법이 있으나 대표적인 것으로 다항식기저(polynomial basis) 표현법과 정규기저(normal basis) 표현법이 주로 사용된다. 그리고 Niederreiter의 알고리즘은 $GF(2^n)[x]$에서 미분방정식 $(fh)' = h^2$ 를 이용한 것으로 이 방정식은 정규기저를 사용하면 일차 연립방정식으로 쉽게 변환할 수 있으나 다항식기저를 사용하여서는 구현하기 어렵다.

이 논문에서는 정규기저(normal basis)를 이용한 유한체의 연산을 C-언어로 구현하고, 이것을 이용한 Niederreiter의 알고리즘을 기반으로 유한체위에서의 다항식인수분해 알고리즘과 구현한 결과를 제시한다.

Ⅱ. 유한체의 표현

p를 소수, $q=p^n$, $n \in Z^+$ 라 하자. q개의 원소를 갖는 유한체를 GF(q) 라 하면 GF(q)는 다음과 같이 구성할 수 있다. $f(x) \in Z_p[x]$ ($GF(p)[x]$)를 n차의 monic인 기약다항식 이라 하면 $GF(q) \cong Z_p[x]/(f(x))$.

즉,

$$GF(q)=\{a_0+a_1x+\cdots+a_{n-1}x^{n-1}|a_i\in GF(p)\}$$

이다. 한편 $f(\alpha) = 0$ 라 하면

$$GF(q) = \{a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1} \mid a_i\in Z_p\}$$

와 같이 표현할 수 있다. 이와 같이 표현하는 것을 다항식기저를 사용한 표현이라 한다.

정의1. $GF(2^n)$의 부분집합 $B = \{ \alpha, \alpha^2, \alpha^{2^2}, \cdots, \alpha^{2^{n-1}} \}$가 GF(2) 위에서 일차독립일 때 B를 $GF(2^n)$의 정규기저(normal basis) 라 한다.

유한체 $GF(2^n)$의 원소 x, y를 정규기저 B를 사용하여 나타내면 다음과 같다.

$$x = a_0\alpha + a_1\alpha^2 + \cdots + a_{n-1}\alpha^{2^{n-1}},$$
$$a_i \in GF(2)$$
$$y = b_0\alpha + b_1\alpha^2 + \cdots + b_{n-1}\alpha^{2^{n-1}},$$
$$b_i \in GF(2)$$

이때 x를 제곱하면 $\alpha^{2^n} = \alpha$을 이용하여

$$x^2 = \{a_0\alpha + a_1\alpha^2 + \cdots + a_{n-1}\alpha^{2^{n-1}}\}^2$$
$$= a_0^2\alpha^2 + a_1^2(\alpha^2)^2 + \cdots + a_{n-1}^2(\alpha^{2^{n-1}})^2$$
$$= a_{n-1}\alpha + a_0\alpha^2 + \cdots + a_{n-2}\alpha^{2^{n-1}}$$

를 구할 수 있다. 즉,

$x = (a_0, a_1, \cdots, a_{n-1})$ 로 표현하면 x를 제곱하는 것은 x를 오른쪽으로 한번 쉬프팅한

$x^2 = (a_{n-1}, a_0, \cdots, a_{n-2})$이다. 그리고 xy 곱의 경우

$$z = xy = c_0\alpha + c_1\alpha^2 + \cdots + c_{n-1}\alpha^{2^{n-1}}$$

라 하고 $c_0 = f(a_0, \cdots, a_{n-1}, b_0, \cdots, b_{n-1})$ 라 하면

$$c_i = f(a_{n-i}, \cdots, a_{n-i-1}, b_{n-i}, \cdots, b_{n-i-1}),$$
$$a_k = a_r, \quad b_k = b_r, \quad k \equiv r \mod n$$

이다. 즉

$$c_0 = f(a_0, \cdots, a_{n-1}, b_0, \cdots, b_{n-1})$$
$$= \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} a_i b_j l_{ij}, \quad l_{ij} = 0 \text{ or } 1$$

로 놓으면

$$c_k = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} a_{i+k} b_{j+k} l_{ij}$$

이다. 이때 $M = (l_{ij})$를 곱의 행렬이라 한다.

III. $GF(2^n)$ 위에서의 다항식 인수분해 알고리즘

f를 $GF(2^n)[x]$의 degree $d \geq 1$인 monic 다항식이라 하고, $GF(2^n)[x]$에서

$$f = \prod_{i=1}^{m} g_i^{e_i}, \quad g_i : \text{기약다항식}, \quad e_i \geq 1 \qquad (1)$$

과 같이 표준분해 된다고 하자.

보조정리2. f(x)를 양의 차수를 갖는 $GF(2^n)[x]$의 monic 다항식이라 하자. 그러면 $h \in GF(2^n)[x]$인 미분방정식

$$(fh)' = h^2 \qquad (2)$$

은 f의 모든 square free monic factor인 b에 대해

$$h = \frac{f}{b} b' \qquad (3)$$

는 (2)의 해이다. 그러므로 g가 (1)과 같이 표현되면 (2)의 서로 다른 해는 2^m개이다.[8]

참고 3. 만약 f의 인수 g_i가 mutiple root를 가지면 $g_i' = 0$이므로, $b = g_i$와 $b = 1$ 일때 $h = 0$ 인 (2)의 해가 된다. 그러나 유한체는 완전체(perfect field)이므로 이런 경우는 없다.

$$f(x) = \sum_{i=0}^{d} f_i x^i, \quad h(x) = \sum_{j=0}^{d-1} h_j x^j \in GF(2^n)[x] \qquad (4)$$

라 하자. $(x^{2j})' = 0$ 이므로 미분방정식 (2)의 해가 성립하기 위한 필요충분 조건은 $j=0, \cdots, d-1$에 대해

$$\sum_{l=\max(2j+1-d,\ 0)}^{\min(2j+1,\ d-1)} f_{2j+1-l} h_l = h_j^2 \qquad (5)$$

이다. N(f)를 (5)의 좌변의 계수행렬이라 하자. 먼저 n=1이면 $h_j^2 = h_j$ 이므로 (5)식은

$$(N(f)-I_d)H^T = 0, \quad H^T = (h_0, \cdots, h_{d-1}) \in GF(2)^d$$

이다.

다음으로 n>1인 경우를 살펴보자. $GF(2^n)$의 최적 정규기저를 $B = \{ \beta, \beta^2, \cdots, \beta^{2^{n-1}} \}$라 하자. $GF(2^n)$의 원소

$$f_i = \sum_{s=0}^{n-1} f_i^{(s)} \beta^{2^s}, \qquad f_i^{(s)} \in GF(2)$$

$$h_i = \sum_{x=0}^{n-1} h_j^{(t)} \beta^{2^t}, \qquad h_j^{(t)} \in GF(2)$$

와 같이 표현한다. (5)식에 f_i , h_i 를 대입하여, 미지수 $h_i^{(s)}$에 관하여 basis B를 이용하여 정리하면

$$K(f,\ B)H^T = 0,$$
$$H^T = (h_0^{(0)}, \cdots, h_0^{(n-1)}, h_1^{(0)}, \cdots, h_{d-1}^{(n-1)})^T,$$
$$h_i^{(s)} \in GF(2) \qquad (6)$$

와 같다.

참고 4. 미분방정식 (2)의 해가 2^m 개이므로 (6)의 해도 2^m개이다. 그러므로
rank K(f, B) = dn-m 이다.

참고 5. (f, f′)=1이고, rank K(f, B) = dn-1 이면 f는 기약다항식이다.

연립방정식 (6)의 해들은 $GF(2)^{dn}$의 m차원 부분공간을 형성하므로 basis C = {h_1, ⋯, h_m }를 갖는다. 그러면 h_i들을 $GF(2^n)[x]$의 원소로 표현하고 i=1,⋯, m에 대해 $b_i = \frac{f}{(f, h_i)}$라 하면 다음의 성질을 얻을 수 있다.

보조정리 6. b_i는 f의 square free monic factor이다.
증명. h_i는 (2)의 해이므로

$$h_i = \frac{f}{b} b', \quad b = \prod_{j=1}^{m} g_j^{r_j}, \quad 0 \le r_j \le 1$$

이다. 그러므로

$$(f,\ h_i) = \prod_{j=1}^{m} g_j^{e_j - r_j}(b,\ b') = \prod_{j=1}^{m} g_j^{e_j - r_j}$$

이다. 따라서

$$b_i = \frac{f}{(f, h_i)} = \prod_{j=1}^{m} g_j^{r_j}.$$

결국 b_i는 f의 square free monic factor이다.

다음은 아래와 같이 m개의 행벡터 A_i를 만들자.

i) A_1은 b_1으로 되어 있다.

ii) A_2는 (b_2, b_1), $\frac{b_1}{(b_2, b_1)}$, $\frac{b_2}{(b_2, b_1)}$ 중 상수가 아닌 것으로 되어 있다.

iii) A_{k-1}이 $r_1, r_2, \cdots, r_s$로 되어 있으면 j=1, ⋯, s에 대해 $d_j = (b_k, r_j)$ 로 놓고

$$d_1, \frac{r_1}{d_1}, \cdots, \frac{r_s}{d_s}, \frac{b_k}{d_1 \cdots d_s}$$ 중 상수가 아닌 것으로 A_k를 만든다.

그러면 다음과 같은 보조정리가 성립한다.

보조정리 7. 위와 같이 $A_1, \cdots, A_m$을 만들면 각 행의 다항식은 서로소이고 f의 인수이며 적어도 m번째의 행 A_m은 m개로 되어 있다[1].

알고리즘 8. (The polynomial factorization algorithm over $GF(2^n)$)

Input. $GF(2^n)[x]$의 monic 다항식 f(x)

Output. $f = \prod_{i=1}^{m} g_i^{e_i}$, g_i는 기약다항식, e_i는 양의 정수.

1. 최적 정규기저를 이용한 유한체를 구성한다.
2. 최적 정규기저를 이용하여 (6)의 dn차 행렬 K(f, B)를 구성한다.
4. Gauss 소거법을 활용하여 K(f, B)의 null space 의 basis C = { h_1, ⋯, h_m }를 구한다.
5. i = 1, ⋯, m에 대해 $b_i = \frac{f}{(f, h_i)}$를 구한다.
6. i = 1부터 A_i의 요소가 m개가 될 때까지 A_i를 구한다.
7. A_i의 원소 g_1, ⋯, g_m 를 이용하여 $f = \prod_{i=1}^{m} g_i^{e_i}$ 인 e_i 를 구한다.

예제. $F_{2^3} = F_2[x]/(x^3 + x^2 + 1)$이면

$\alpha^3+\alpha^2+1 = 0$을 만족하는 α는 정규기저를 형성한다. F_{2^3} 의 원소

$$a = (a_0, a_1, a_2) \equiv a_0\alpha + a_1\alpha^2 + a_2\alpha^{2^2}$$

이다.

$$f(x) = x^3+(1,1,0)x^2+(0,0,1) \in F_{2^3}[x]$$

라 하자. 그러면

$$K(f,B) = \begin{pmatrix} 0&0&1&0&1&1&0&0&0\\ 1&0&0&1&1&0&0&0&0\\ 0&1&0&1&0&0&0&0&0\\ 1&0&0&1&1&0&0&0&0\\ 0&1&0&0&0&0&0&0&0\\ 0&0&1&1&1&1&0&0&0\\ 0&0&0&0&0&0&1&0&1\\ 0&0&0&0&0&0&1&1&0\\ 0&0&0&0&0&0&0&1&1 \end{pmatrix} \text{이고}$$

해들의 기저는

$$\begin{aligned} h_1 &= (1,0,1)+(0,1,0)x \\ &= (0,1,0)\{(1,0,0)+(1,1,1)x\}, \\ h_2 &= (0,0,1)+(0,0,1)x \\ &= (0,0,1)\{(1,1,1)+(1,1,1)x\}, \end{aligned}$$

$h_3 = (1,1,1)x^2$ 이므로 monic인 것으로 선택하면

$(1,0,0)+(1,1,1)x$, $(1,1,0)+(1,1,1)x$, $(1,1,1)x^2$ 이다. 따라서

$$A_2 = \{(1,0,1)+x,\ (1,1,1)+x,\ (1,0,0)+x\}$$

이므로 $f(x)$는 이 3개의 일차식으로 인수분해된다.

Ⅳ. 구현한 결과

최적 정규기저는 Ⅰ, Ⅱ 타입이 있고 각각 구성하는 방법이 알려져 있다.[5] $GF(2^{105})$는 Ⅱ타입 형태이고 $GF(2^{162})$는 Ⅰ 타입 형태이다.

1)

$$\begin{aligned} f(x) &= x^{73}+(\alpha+\alpha^2+\alpha^{2^2})x^{23} \\ &\quad +(\alpha+\alpha^{2^2})x^{14}+(\alpha+\alpha^{2^2}) \\ &\in GF(2^{105})[x] \end{aligned}$$

를 인수분해하면 다음과 같다.

{(11111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111)x
+
(000100111010011111010000101000100010011111100111110010
0000011111111111100001100111010011001101101111001100) }

{(11111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111) x^7
+
(100011101100000010110010101110011111101111001001110001
1100110001000001011000001110011000111111011001100100) x^6
+
(1011110000010110010011110011001000100011001000100101000
1000101000101110001101101011010000000000111100010110) x^5
+
(010000110011101011010001000000110111001100011011110001
110000101111111101111101010111010110110111000111001) x^4
+
(100100100001101001100000011010001000101111111010110100
0101101111011110100000110000100111011001100110011001101) x^3
+
(100011101111110101101000001111011110100010011001 10100
011010011010001000010000001001111010110100100010000) x^2
+
(10010110101101001110111101001111110111011001001 0001000
0010110101111111011110001100110111101011001010000101) x
+
(101110101000100101000011101010101110101000010110001100
1100001000100111111000111011001000010101001010 10000) }

{(11111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111) x^4
+
(101101110101010101001001101110001001010110110011111001
1001110100001110000001000000001110010010100110101001) x^3
+
(100111101100110100110100111110111110010010100110001110
010100010101101001000101001101011100111000001101110) x^2
+
(0000110111101111101111011010111000000110100100110111010
111001110100111011110111110111010010110011000100001) x
+
(10111100000011000100100100000011100010011000010001100100
101110110011001100111100011101100111000110100110101) }

{(11111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111) x
+
(100111100110010100011011010000111001101100100100001111
011010010111110110100100001010110000000010001001100) }

{(11111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111)

x^{47}

+

(010111111001000010011000010111101110011001000111000111010101010100000001111010101101000101100110000110010) x^{46}

+

(111000110001011111010100000111110101100010111010001101011101110011101100000101001001000100011100100010001) x^{45}

+

(111100111111111011100100111100100101101001101111010101101100000111111110101010100010011110001011001110111) x^{34}

+

(110010001110010111111010001111110100010000101110100101011010011101110011110100000110000110111110000011101) x^{43}

+

(011111101010011110110101111111010001011010101011001101110111110011011101000011010101100010110111010011000) x^{42}

+

(11000000111010010100100101000111110000011111001110101110011001111011000011011001001100101011110000011100001) x^{41}

+

(1011001111110010110011001011100000111010100010110011111110110100001000101011011101100010100011011000100001) x^{40}

+

(11011100100001111110011111101101011001100001011011111111100101010111001011011100001000101100010100100001) x^{39}

+

(011000000100100000011110010001101010001100110011100101010000011111011000000001011000111000001110011010111110) x^{38}

+

(0010001101110011001000101001010010000111100100001001111110010111111101000110101001011111111001110110110110) x^{37}

+

(010001100001110001000010010111110011101000100011110001101010001001110010101100011001011101011011011101110) x^{36}

+

(001001000101101100000110111011010011100011101111110001111111000010101111000111000010111101100011101100100) x^{35}

+

(11111111010101011111010000010000101110011100110001100011101100111000000110110011000111100000000000101000100) x^{34}

+

(110001001111001011000111101110100010011011111011110101010000110101110110000111011010100111101110111001001) x^{33}

+

(11011100110111001011010101111011111010010000000111010110001011011010110000001101111011110110100000000011011) x^{32}

+

(1010001001010111101100001100110011011100101000001011001111001011111100010110110100101011011000111100011101) x^{31}

+

(101010110011111110000001011011011010111001101011011111001010001101111000100111110001000001010111011010110110) x^{30}

+

(0010111010101001001011000001000111100101010000001000100111010100110011110101000101100101001101010101100001) x^{29}

+

(0000001101011001000111110101000101100111100111000101110010011101100110000000011001101111001011011110101010) x^{28}

+

(111111000011110000100110100010100011011110010111000001011100001011110111011101110110001001111111011010100) x^{27}

+

(100101010000100011101011000001000100110110110111100100111110000011011110101110000000110010010110100101001) x^{26}

+

(0000101111011110001010010111000111101100000010011010001111000100100000010111010011100001111000011010010101) x^{25}

+

(000001110010101110100000110000000110010011111110110001100010100010001110100100101110110101101111110100001) x^{24}

+

(1000000101001001110011110000000000010000100101101000011110110110000001111101100010101101011000001101010100) x^{23}

+

(0000000100101000101011110001111100011001001000100110111100000011001101100111001011011001101011100101100001) x^{22}

+

(0111010101010010110001011001101111111001010000010110011011110101111100100101101101000101110001111101111101) x^{21}

+

(1010100000010001110010010000100100101100110111100011010100100000010111001000011001100010110001001010101101101) x^{20}

+

(0101001011101011111101101101001010010110000100101111100011101001001001111001001011100110010000000110011110) x^{19}

+

(101010100110101011110001110000100000001010110001010100000011010100101110110101011110100110000100101001001) x^{18}

+

(101001110101011010001011101110100011001011101001111101101001111001110000001011010111011000000100001000000010) x^{17}

+

(000111011110001111011100011011010100011101000010010011101011101001110011000010101001010101110100010001011) x^{16}

+

(1010110000000000010011110001110010111000100100010100011000000001111000101010011011100101100111000010110010) x^{15}

+

(00000110010100111011111100111101111111000110000111111010001110000000100011001100011000101000000001100110001) x^{14}

+

(10111111111000011000111101110101000101110010110001111001111101110110011111111110011111001010011010110111010) x^{13}

+

(0101000000011011011001100010110011001100011101100000001110111011001010000011010000001100101010000000011010) x^{12}

+
(1110001011010101011110111101011111111100101010110110110
000011110100011001101010001100110011010000001110001) x^{11}
+
(011110001100110001110000110101100111001110010111000010
101011110111001100011000110010010110100100011011000) x^{10}
+
(010101110110010101000010110001001010010001101111110110
1001100001000000001010100100000001100100101010100001) x^9
+
(000110111010001010110011110000101001100011101111000010
1010011111001000011001100000110000000001000101110101) x^8
+
(110011110101001110111100011011011001001100001011010101
000011011001110110101000111101001101001100100111010) x^7
+
(1010100001111101011100010001110010000001001010011110001
101000100100001111010110111100001001001100111010000) x^6
+
(00010000001110100010001100001001101000000011001111010101
0100000001100100010011101101101011011110000100100001) x^5
+
(1110001101100001010010101000000001011010110111011001001
110101110010110110000111011100110111110111000011111) x^4
+
(101110000100101111101110001001101010100111101100011001
101011000001010101101010100010101010100110101000111) x^3
+
(100010001011000001001011001110010110000000100111101011
000000101000001110100010101111111011001101110100111) x^2
+
(010110111101100111001011111010101110010100001111110100
0110100101101011100101000000000001100101101000000010) x

(01111111111100001010110001110111111000000110101100110011
110011110100010101001000101001111000010001010100100) }

{(111111111111111111111111111111111111111111111111111111
111111111111111111111111111111111111111111111111111) x
+
(011011010100001100100001010111100010111101000001001000
110111010001100001000011001010011001001001111100000) }

{(111111111111111111111111111111111111111111111111111111
111111111111111111111111111111111111111111111111111)
x^{12}
+
(100001101000010010001001111000000001101110111111111010
101101111001011001011000100101000000101111110011111) x^{11}
+
(100011000111010000110111111011001011111000010100101000
101001000110101011010111111010000111011110100011010) x^{10}
+
(001010110101001101001111010110010010111111000000010001
011001100101011111010111110001101101101011010011011) x^9
+
(001101000010100100111110100101110011101101101101000110
001011111010011101011010000011101001100001000010110) x^8
+
(110111111000001000001100101111110011010100110110101110
000101001000101101000101111010111011100011010100000) x^7
+
(101101000111010100000010000011100110001010111000110101
010100011001101001111001111000011100011101101000110) x^6
+
(11000000111101001110000111111111000100110010110011110
100100011101100000001011110001111110001111101101101) x^5
+
(1101000100110010110011011000111101111110110011000100110
011111000011101110111010110101111100000100101100101) x^4
+
(000010100010010111110011110010100101100110011011101000
110011110110001110110101000001011110101111010110010) x^3
+
(1000001011011111110010011110101000110100001111001101110
000011110010110010000101100110010100111010110001111) x^2
+
(010110100011011110001000001011101101101111001001101000
001110101110101011001000000100111110100011000011110) x
+
(001000010101011101100100111010100001100100010000001010
011100000101011100100010001110110011001101110011010) }

2)

$$
\begin{aligned}
f(x) \quad = \quad & x^{35}+(\alpha+\alpha^{2^{13}}+\alpha^{2^{97}})x^{25} \\
& +(\alpha+\alpha^{2^{114}})x^{14}+(\alpha+\alpha^{2^{32}})x^{3} \\
& +(\alpha+\alpha^{2^{15}}) \in GF(2^{162})[x]
\end{aligned}
$$

를 인수분해하면 다음과 같다.

{(111111111111111111111111111111111111111111111111111111
111111111111111111111111111111111111111111111111111111
111111111111111111111111111111111111111111111111111111)
x^2
+(101011010111001010110000000101010111011000011111111100
1001011000111000111110010100000111011101101100111101001
1110000000010001011011111100011000100011101110110011011)
x
+(010101101001111100110001001000100000001011010010100000
01100000010010111010100001100001100010010110100001000011
100101110111000011011011111111110001010101110011001011)
}

{(111111111111111111111111111111111111111111111111111111
111111111111111111111111111111111111111111111111111111
111111111111111111111111111111111111111111111111111111)
x^4
+(010000000001111111101101100011011000100010110000011100

101000110000001011100110001100110100110001101001011001 10
0110110000110000011001000000110010000001000110111100011)

x^3

+(0011110101110101011010001000011010111011100010100001 0
0011110100101010110010011010111001111101101011010111111
1111110110110011000111100100000111111000010010001000 10)

x^2

+(000000000010011001001000000000000110010010001000000011
1000101111011010010101010110100110111011000101101001010
1111101100110111000010001111010011010111111101010111 00)

x

+(110010110110101111010011111110000000110101100100001 10
0110000101010100101010001111011001110111010100000101011
000111000100010010001010101100110011010101001011011010)

}

{(11111111111111111111111111111111111111111111111111111
11111111111111111111111111111111111111111111111111111
11111111111111111111111111111111111111111111111111111)

x^6

+(1000010101100111010010011000010010000111001011110011 0
0100000110000111011111010010110001001010100000111110011
001001100001110110010011101000110100111010001011111101)

x^5

+(1101011101101100110000100101111111110111101100101110 1
0110111011010111100010100111110111100011010100001110011
1010100101000111100000000101110010110100100000011010 10)

x^4

+(0100110011001100000011011111000011111110101100001101 0
0110000101100010000000101010001000100111011001010011111
01100011110001000011000110110000011001000000001110111 10)

x^3

+(1110100101001011010011010111101111111010101101011111 1
0000010100110111001001100101110000110100110010001101110
011111101000111100010110110100111010101011001110100001)

x^2

+(1110010100101100011110110111111001101000110101110101 0
0100001000100001110000010101100011001010101100000000101
110001010001010100011101001000011010000011001001000011)

x

+(1100000011001010000000100101001001101000101001001101 00
0100100110000011011110100101110010010010010000111010001
1001111100110010011001000000010111011010010011001111000)

}

{(11111111111111111111111111111111111111111111111111111
11111111111111111111111111111111111111111111111111111
11111111111111111111111111111111111111111111111111111)

x^{22}

+(1101100011101001010010001010100011100111000111101100 0
1001001111001011110010111111110111110000001101101100 1100
0001111111101100110011110111000100100111011101010 1011)

x^{21}

+(000001100100000011111111010010001100111010100000001100
1111111001101010111000000010000011001110111000101100100011
101110101011011110111001100010000100010111100110100010)

x^{20}

+(000000111100010100110110011011110000010100101100000 11
1101011001000000111011000101000000110010111100001110100
0011101010111110010101010000100011001100100101000011 01)

x^{19}

+(0010101011110110001011101101110100010101011100111000 0
1000011011011000111000100010010011100100100011111101000
0111101111101001011101101001101011110110011111010100 10)

x^{18}

+(0110010111110000000101001111000110010101100011001101 1
0001100110110100111011101110000010100011111110001110111
0000111100010110011000011111001001111110111111001000)

x^{17}

+(0011000010101110101111000100010111011101110100110110 1
0111011000110001101000111010001110011001100100001110001
1101011100110001000010101101001010101000100111101100 11)

x^{16}

+(1101111001100110011100001011001001101011101101100001 1
0000011101101110011100100010101101000001011010000010111
0010101011100011000111011111110001101001111101001010 00)

x^{15}

+(1010100000010100100111100101111110010000110100101100 01
1011000011010110011010011000110110111100110001101110111
0111011101000001111011000011111101000000001111010111101)

x^{14}

+(0010101101110011101001111010010011010000101001101101 1
0010111011000001101110100001101010001010100010000001010
000011001100000000111100001011101011100000111101000011 1)

x^{13}

+(1100111110101110101111110110001011101111100101001011 1
1111101111000100011011001011101101101010011000001101101
1001101011001110010110000011110000011010110001010100 00)

x^{12}

+(1001101100010000101001011101101110110011101000001111 1
1111101100010000100000011011100100111001000000010000111 0
1000000001110100110011010111111001011001010000111010 10)

x^{11}

+(1000011010100111011001111011110000111010001011010110 0
1000010001011111000100000110011111111100000011101011110 1
0000010110111011100101111001100111101001110011100110 11)

x^{10}

+(1001111001111000010010000000011111111101000000100101100
1000001000000110011010110111010110101110011000101100101
1001000111100110010110011101011100100110000010110010 11)

x^9

+(0001000011100000101110000000110001011110100011001110011
1001100110000000011011011111000100000111011101101000110
1100000001110111110100110000000111001011110101100101110)

x^8

+(0100001001101010010000000110101110100111100101110000 11
1011101111010100101000101001100101101111111101010001101
1000111110110101000010101001111110001001101101001011 11)

x^7

+(100010110001111100010001110001001100101110001101111101
101101011101110011011100010010110101011110111111010101 0
111101111111111110111100100101110100001111001110110110)

x^6

+(101010000101011010011000011110010010001011110100111 10
000110000011101010011011110000111001111111010100111010 0
001001000100111010011001011111110111111110001101100101)

x^5

+(100100100000111111001111101010001010011110011000001 00
010001111110001011000000010011000101000000010101111110 0
101101110101101010111000110101101010011110110111111010)

x^4

+(111111110011100101010111001010010110110001001111011 01
101111011000110010111001010110011011101111111010100000 00
110000000101001111000010000000100111110101010001001101 0)

x^3

+(100001100100011010110111101001110011011000000101011110
000011010000100100110011110000000100001110000011101011 01
101011010010011011100101000100111111001001000101110110)

x^2

+(111000100001001000011011101110011100001000010000101 01
001001000011010110001000000011100011101111000110111001 10
100101010011101100010100111110110110010101011000000110)

x

+(110110100010000010011000111001001010100111101100111 01
111100111100100000000010010011100100000101010000110000 00
101001111100010000101011100100010101100100001100110000)

}

{(111111111111111111111111111111111111111111111111111111
111111111111111111111111111111111111111111111111111111
111111111111111111111111111111111111111111111111111111)

x

+(101100001100001101101010001000100000001110100111011110
111001110111000110000011111101101110111100011110110000
101101011110001111100111100110110001100001110000101110)

}

V. 결론

표수가 2인 유한체 $GF(2^n)$에서 정규기저를 이용한 유한체의 연산을 C-언어로 구현하고 $GF(2^n)$ 위에서의 다항식 인수분해 알고리즘을 구현함으로 유한체 구성에 필요한 기약다항식의 구성, 검증, index-calculus 알고리즘을 이용한 이산대수 문제, 기타 다항식의 인수분해를 필요로 하는 분야에 응용할 수 있을 것이다.

참고 문헌

[1] R. Göttfert, "An accelleration of the Niederreiter's factorization algorithm in characteristic 2", Math. Comp. 62, pp. 831-839(1994).

[2] N. Koblitz, "Elliptic curve cryptosystem", Math. of Computation, 48, pp. 203-209, 1987.

[3] A.K. Lenstra, "Factorization of polynomials", Computational method in number theory, part1, Mathematical Centre Tracts, 154, pp. 169-198(1992).

[4] R. Lidl and H. Niederreiter, " Introduction to finite fields and their applications ", Revised edition, Cambridge University press, Cambridge, 1994.

[5] A.J. Menezes, "Applications of finite fields", Kluwer academic publishers, Boston, 1993

[6] A.J. Menezes, "Handbook of applied cryptography ", CRC Press, New York, 1997.

[7] V.S. Miller, " Use of elliptic curve in cryptography", CRYPTO' 85, LNCS218, Springer-Verlag, pp. 417-426(1986).

[8] H. Niederreiter, "Factorization of polynomials and linear-algebra problems over finite fields", Linear Algebra Appl. 192, pp.301-328(1993).

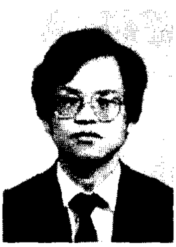
[9] H. Niederreiter, "Factoring polynomials over finite fields using differential equations and normal bases", Math. Comp. 62, pp.819-830(1994).

著者紹介----------------------------

김창한 Chang Han Kim 정회원

85년 고려대학교 수학과 졸업
92년 고려대학교 대학원졸업(이학박사)
92년 - 현재 세명대학교 조교수
관심분야 : 암호학, 응용대수학, 정보이론

서광석 : Kwang Suk Suh 정회원



82년 고려대학교 수학과 졸업
89년 고려대학교 대학원졸업(이학박사)
91년 - 현재 서남대학교 수학과 부교수
관심분야 : 전산수론, 암호학, 응용대수학