Regular paper http://dx.doi.org/10.13067/JKIECS.2014.9.8.867

특수한 정규기저를 이용한 유한체위에서의 역원 계산 알고리즘에 관한 연구

김용태*

Algorithms for Computing Inverses in Finite Fields using Special ONBs

Yong-Tae Kim*

요 약

유한체 연산에서 MONB를 사용하면 곱셈 역원 계산시에 대량의 제곱계산이 필요하므로 역원을 계산하는 데에 긴 시간이 필요하게 된다. 이에 본 논문에서는 바탕체 $GF(2^{2^n})$위의 확대체 $GF(2^{2^n m})^*$에서 특수한 정규기저를 사용하여 역원을 구하는 저 비용의 알고리즘을 제안한다. 제안하는 알고리즘을 사용하면 곱셈 역원 계산에는 $nb(2^n m-1)+w(2^n m-1)-2$ 번의 곱셈과 2^n-1 번의 제곱연산이 소요되며, H/W에서 구현한 결과 Itoh 등의 방법 보다 곱셈역원 계산속도가 빠르게 나타났다.

ABSTRACT

Since the computation of a multiplicative inverse using MONB includes many squarings and thus calculating inverse is expensive, we, in this paper, propose a low cost inverse algorithm requiring $nb(2^n m-1)+w(2^n m-1)-2$ multiplications and 2^n-1 squarings to compute an inverse in $GF(2^{2^n m})^*$ using special normal basis over $GF(2^{2^n})$, and give some implementation results using the algorithm and, show that the timing results of our implementation is faster than that of Itoh et al.'s method.

키워드

Finite Field, Modified Optimal Normal Basis(MONB), Inverse Element, Inverse Algorithm
유한체, 수정된 최적정규기저, 역원, 역원계산 알고리즘

I. 서 론

1987년에 Koblitz [1]에 의해서 타원곡선 암호법(Elliptic Curve Cryptosystem, ECC)이 제안된 후로 유한체 $GF(2^n)$위에서의 타원곡선 가법군 연산의 효율성이 중요한 문제가 되었다. 1992년에 Harper 등[2]은 유한체 $GF(2^n)$ 중에서 지수 n이 솟수인 경우보다 합성수인 경우인 유한체 $GF(2^k)^m$위에서의 연산이 더 효율적인 사실을 발표하였으며, 특히 H/W 구현시에는 $k=8,16$인 유한체가 가장 적절한 것으로 발표하였다. 그런데 이 경우에도 관용 다항식 기저 또는 정규기저를 사용하면 곱셈 연산시에 너무 긴 시간이 요구된다. 이러한 단점을 보완하기 위해서 Harper 등[2]은 수정된 다항식 기저를 사용하는 연산 알고리

* 교신저자(corresponding author) : 광주교육대학교 수학교육과(ytkim@gnue.ac.kr)
접수일자 : 2014. 06. 05 심사(수정)일자 : 2014. 07. 21 게재확정일자 : 2014. 08. 11

즘을 제안하였으며, Kim 등[3]은 수정된 최적 정규기저(Modified Optimal Normal Basis, MONB)를 사용하는 타원곡선 계산법을 발표하였고, 타원곡선위에서의 계산 알고리즘은 Cohen[4]에 의해서 일반화되었으며, 이차체의 구성에 필요한 이진수열을 생성하는 방법도 최근에 개발되었다[5-6]. 그런데 Kim 등[3]이 제안한 MONB를 사용하면 제곱연산이 한 번의 우측순환좌표이동(right cyclic shift)으로 되지 않기 때문에 많은 제곱연산이 필요한 곱셈역원 연산에는 효율성이 많이 떨어지게 된다. 따라서 본 논문에서는 이러한 단점을 보완하여 효율적인 역원 계산이 가능한 특수한 최적정규기저를 사용한 계산 알고리즘을 제안하였으며, 그 결과, 유한군 $GF(2^n)^*$의 원소 α의 곱셈에 대한 역원 α^{-1}의 계산에서 Itoh 등[7]이 제안한 알고리즘 보다 제안하는 알고리즘이 효율적임을 비교표를 통하여 제시하였다.

II. 수정된 정규기저를 이용한 유한체위에서의 연산

이 장에서는 Kim 등[3]이 발표한 수정된 정규기저(modified normal basis)와, 그 정규기저를 사용하여 유한체의 원소를 표현하고 역원 계산에 필요한 두 원소의 곱셈 과정을 소개하기로 한다.

2.1. 수정된 정규기저

p는 솟수이고 자연수 m에 대해서 $q=p^m$이라고 하면 유한체 $GF(q^n)$은 q^n 개의 원소를 갖는다. 그러면 임의의 0이 아닌 $\alpha \in GF(q^n)$에 대해서 부분집합 $A=\{\alpha,\alpha^q,\alpha^{q^2},\cdots,\alpha^{q^{n-1}}\}$이 $GF(q)$위에서 일차독립이면 A는 $GF(q)$위에서 $GF(q^n)$의 정규기저가 되며, 특히 $\gcd(m,n)=1$ 이고, 0이 아닌 $\beta \in GF(q^m)$에 대하여 $B=\{\beta,\beta^q,\beta^{q^2},\cdots,\beta^{q^{m-1}}\}$이 $GF(q)$위에서 $GF(q^m)$의 정규기저인 경우에는 B는 $GF(q^n)$위에서 확대체 $GF(q^{mn})$의 기저가 되는 것은 잘 알려진 사실이다[6].

정의 1. [3, Definition 4] $\gcd(m,n)=1$ 이고, 0이 아닌 $\beta \in GF(q^n)$에 대하여 $B=\{\beta,\beta^q,\beta^{q^2},\cdots,\beta^{q^{m-1}}\}$가 $GF(q)$위에서 $GF(q^m)$의 정규기저일 때, B를 $GF(q^n)$위에서 확대체 $GF(q^{mn})$의 수정된 정규기저라고 한다.

그러면 $x,y \in GF(q^{mn})$를 수정된 기저 B를 사용하면 다음과 같이 표현된다.

$$\begin{aligned} x &= a_0\beta + a_1\beta^q + a_2\beta^{q^2} + \cdots + a_{m-1}\beta^{q^{m-1}}, \\ y &= b_0\beta + b_1\beta^q + b_2\beta^{q^2} + \cdots + b_{m-1}\beta^{q^{m-1}}, \\ a_i, b_j &\in GF(q^n). \end{aligned} \tag{1}$$

그런데 $\beta^{q^m}=\beta$가 되는 사실을 이용하면,

$$\begin{aligned} x^q &= a_0^q\beta^q + a_1^q\beta^{q^2} + a_2^q\beta^{q^3} + \cdots + a_{m-1}^q\beta^{q^m} \\ &= a_{m-1}^q\beta + a_0^q\beta^q + a_1^q\beta^{q^2} + \cdots + a_{m-2}^q\beta^{q^{m-1}}, \\ y^q &= = b_0^q\beta^q + b_1^q\beta^{q^2} + b_2^q\beta^{q^3} + \cdots + b_{m-1}^q\beta^{q^m} \\ &= b_{m-1}^q\beta + b_0^q\beta^q + b_1^q\beta^{q^2} + \cdots + b_{m-2}^q\beta^{q^{m-1}} \end{aligned} \tag{2}$$

이므로, 이 사실을 이용하여 역원계산과정에서 꼭 필요한 두 원소 x와 y의 곱셈 방법을 알아보기로 한다.

2.2. 수정된 정규기저를 이용한 곱셈

$x,y \in GF(q^{mn})$를 수정된 기저 B를 사용하여 표현하여 곱하는 과정을 다음과 같다.

$$\begin{aligned} z &= x \cdot y \\ &= [a_0\beta + a_1\beta^q + a_2\beta^{q^2} + \cdots + a_{m-1}\beta^{q^{m-1}}] \cdot \\ &\quad [b_0\beta + b_1\beta^q + b_2\beta^{q^2} + \cdots + b_{m-1}\beta^{q^{m-1}}] \\ &= c_0\beta + c_1\beta^q + c_2\beta^{q^2} + \cdots + c_{m-1}\beta^{q^{m-1}} \end{aligned} \tag{3}$$

라고 놓고, 기저 B에 대한 z의 계수 $c_i, i=0,1,2,\cdots,m-1$, 사이에 나타나는 관계를 알아보자.

z의 계수 $c_i, i=0,1,2,\cdots,m-1$ 는 모두 x,y의 계수인 a_i와 $b_j, i,j=0,1,2,\cdots,m-1$ 들의 사칙연산으로 만들어지므로, 우선

$c_0=f(a_0,a_1,\cdots,a_{m-1},b_0,b_1,\cdots,b_{m-1})$ 로 놓자.

그러면

$$z^q = x^q \bullet y^q$$
$$= c^q_{m-1}\beta + c^q_0\beta^q + c^q_1\beta^{q^2} + \cdots + c^q_{m-2}\beta^{q^{m-1}},$$
$$c^q_{m-1} = f(a^q_{m-1}, a^q_0, \cdots, a^q_{m-2}, b^q_{m-1}, b^q_0, \cdots, b^q_{m-2}) \quad (4)$$

가 되고,

$$\beta^{q^i} \bullet \beta^{q^j} = l^{(0)}_{ij}\beta + l^{(1)}_{ij}\beta^q + \cdots + l^{(m-1)}_{ij}\beta^{q^{m-1}},$$
$$l^{(t)}_{ij} \in GF(q), i,j,t = 0,1,2,\cdots,m-1 \quad (5)$$

로 놓으면,

$$c_0 = f(a_0, a_1, \cdots, a_{m-1}, b_0, b_1, \cdots, b_{m-1})$$
$$= \sum_{i=0}^{m-1}\sum_{j=0}^{m-1} a_i b_j l_{ij},\ l_{ij} = l^{(0)}_{ij} \in GF(q) \quad (6)$$

가 된다. 그런데

$$c^q_{m-1} = \sum_{i=0}^{m-1}\sum_{j=0}^{m-1} a^q_{m-1+i} b^q_{m-1+j} l_{ij}$$
$$= (\sum_{i=0}^{m-1}\sum_{j=0}^{m-1} a_{m-1+i} b_{m-1+j} l_{ij})^q \quad (7)$$

이고, $a^q = b^q$일 필요충분조건은 바탕체 $GF(q)$에서 $a = b$이므로

$$c_{m-1} = \sum_{i=0}^{m-1}\sum_{j=0}^{m-1} a_{m-1+i} b_{m-1+j} l_{ij} \quad (8)$$

이 된다. 그러므로 $0 \le k \le m-1$인 모든 k에 대하여

$$c_k = \sum_{i=0}^{m-1}\sum_{j=0}^{m-1} a_{i+k} b_{j+k} l_{ij} \quad (9)$$

단 $i+k, j+k$ 는 각각 m으로 나눈 나머지이다.

이때 생성되는 계수행렬 $L = (l_{ij})$을 유한체 $GF(q^n)$위에서 기저 B에 관한 확대체 $GF(q^{mn})$의 수정된 곱셈행렬이라고 하며, 특히 $n = 1$인 경우에는 $L = (l_{ij})$은 바탕체 $GF(q)$위에서 기저 B에 관한 유한체 $GF(q^m)$의 곱셈행렬이라고 부른다. 그러면 $\gcd(m,n) = 1$인 경우에는 식 (6)에 의해서 $GF(q^{mn})$의 수정된 곱셈행렬은 $GF(q^m)$의 곱셈행렬과 같아짐을 알 수 있다. 이때 C_m을 기저 B에 관한 곱셈행렬 L의 0이 아닌 성분의 개수라 하고, $C_m = 2m-1$이면 기저 B는 바탕체 $GF(q)$위에서 유한체 $GF(q^m)$의 최적정규기저라고 부르며[8], 정의 1에서 정규기저 대신 최적정규기저로 바꾸면 다음과 같은 정의를 얻는다.

정의 2. $\gcd(m,n) = 1$이고, 0이 아닌 $\beta \in GF(q^m)$에 대하여 $B = \{\beta, \beta^q, \beta^{q^2}, \cdots, \beta^{q^{m-1}}\}$가 $GF(q)$위에서 $GF(q^m)$의 최적정규기저일 때, B를 $GF(q^n)$위에서 확대체 $GF(q^{mn})$의 수정된 최적정규기저(MONB)라고 한다.

그러면 정의 2와 Kim[8, 따름정리 4]에 의해서 다음의 정리를 얻게 된다.

정리 1. $\gcd(m,n) = 1$ 이고, 0이 아닌 $\beta \in GF(q^n)$에 대하여 $B = \{\beta, \beta^q, \beta^{q^2}, \cdots, \beta^{q^{m-1}}\}$이 $GF(q)$위에서 $GF(q^m)$의 최적정규기저이면, B는 $GF(q^n)$위에서 확대체 $GF(q^{mn})$의 MONB 이다.

특히 m이 홀수이고 B가 $GF(2)$위에서 $GF(2^m)$의 최적정규기저이면, $B = \{\beta, \beta^2, \beta^{2^2}, \cdots, \beta^{2^{m-1}}\}$는 $GF(2^n)$위에서 $GF(2^{2^n m})$의 MONB 이고, B에 대한 $GF(2^{2^n m})$의 곱셈행렬의 모든 성분은 0 또는 1이 된다.

III. 유한체 $GF(2^{2^n m})$에서의 효율적인 역원 계산 알고리즘

이 절에서는 $n > 0, m$이 홀수인 경우, Agnew 등[9]과 Kim[10]을 참고하여 0이 아닌 $\alpha \in GF(2^{2^n m})$의 역원 α^{-1}을 효율적으로 계산하는 알고리즘을 단계적으로 제안하기로 한다. 유한체의 성질에 의하여 $\alpha \in GF(2^{2^n m})$에 대하여 $\alpha^{2^{2^n m}} = \alpha$ 이므로,

$$\alpha^{-1}=\alpha^{2^{2^n}m-2}$$
$$=\alpha^{2+2^2+\cdots+2^{2^n}m-1}$$
$$=\alpha^{2^{2^n}m-2^n+2^n-2}$$
$$=\alpha^{(2^n-1)(2^{2^n}+2^{2^n2}+\cdots+2^{2^n(m-1)})}\cdot\alpha^{2+2^2+\cdots+2^{n-1}} \quad (10)$$

이다. 따라서 α^{-1}의 계산방법을 두 단계로 나누어서 알아보기로 한다. 우선 식 (10)에서 $\alpha^{2+2^2+\cdots+2^{n-1}}$ 형태의 원소를 계산하기 위하여 개발한 알고리즘은 다음과 같다.

3.1. 부분계산 알고리즘

이 절에서는 역원계산과정에서 발생하는 특수한 형태의 원소를 계산하는 알고리즘을 먼저 소개하기로 한다.

Algorithm 1.

Input : integer $n>0$, $\alpha\in GF(2^{n+1})^*$.

Output : $x=\alpha^{2+2^2+\cdots+2^n}$

1. Set $t\leftarrow m$, $x\leftarrow 1$, $u\leftarrow\alpha^2$.
2. While $t>0$ do
   2.1 While $t_0=0$ and $t>1$ do
   ($(t_i)_2$ is the binary representation of t)
   2.1.1 $t\leftarrow t\gg 1$(1 right shift)
   2.1.2 Set $u\leftarrow u\cdot u^{2^t}$.
   2.2 Set $x\leftarrow x\cdot u$.
   2.3 If $t=1$, then stop.
   2.4 else set $u\leftarrow u^2$.
   2.5 Set $t_0\leftarrow 0$.

이제 앞으로의 계산과정을 용이하게 설명하기 위해서 자연수 n의 함수를 정의하기로 한다.

정의 3. 자연수 n에 대하여 $tw(n)$을 Algorithm 1의 2.1.2와 2.2 단계에서 사용되는 제곱을 포함한 곱셈 횟수라고 한다.

그러면 $tw(n)$은 Itoh 등[7]이 제안한 $\alpha\in GF(2^{n+1})$의 역원 계산에 필요한 곱셈 횟수와 같다.

3.2. 제안하는 알고리즘

이제 m은 홀수, n은 짝수, $\alpha\in GF(2^{mn})^*$이고 $B=\{\beta,\beta^2,\beta^{2^2},\cdots,\beta^{2^{m-1}}\}$가 $GF(2)$위에서 $GF(2^m)$의 정규기저라고 하자. 그러면 정리 1에 의해서 B는 $GF(2^n)$위에서 확대체 $GF(2^{mn})$의 MONB 가 된다는 사실과, $\alpha^{2+2^2+\cdots+2^{n-1}}$ 형태의 원소 계산 알고리즘인 Algorithm 1을 적용하여, 제안하는 역원계산 알고리즘은 다음과 같다.

Algorithm 2.

Input : m odd integer, n positive integer
and $\alpha\in GF(2^{2^n}m)^*$.

Output : $x=\alpha^{-1}$

1. Set $t\leftarrow 2^n-1$, $x\leftarrow 1$, $u\leftarrow\alpha^{2.}$
2. While $t>0$ do
   2.1 While $t_0=0$ and $t>1$ do
   ($(t_i)_2$ is the binary representation of t)
   2.1.1 $t\leftarrow t\gg 1$(1 right shift)
   2.1.1 Set $u\leftarrow u\cdot u^{2^t}$.
   2.2 Set $x\leftarrow x\cdot u$.
   2.3 If $t=1$, then go to 3.
   2.4 else set $u\leftarrow u^2$.
   2.5 Set $t_0\leftarrow 0$.
3. Set $t\leftarrow m-1$, $u\leftarrow(x\cdot\alpha)^{2^{2^n}}$, $y\leftarrow 1$.
4. While $t>0$ do
   4.1 While $t_0=0$ and $t>1$ do
   ($(t_i)_2$ is the binary representation of t)
   4.1.1 $t\leftarrow t\gg 1$(1 right shift)
   4.1.2 Set $u\leftarrow u^{2^{2^n t}}$.
   4.2 Set $y\leftarrow y\cdot u$.
   4.3 If $t=1$, then go to 5.
   4.4 else set $u\leftarrow u^{2^{2^n}}$.
   4.5 Set $t_0\leftarrow 0$.
5.. $x\leftarrow x\cdot y$.

그러면 $\alpha\in GF(2^{mn})^*$의 역원 α^{-1}을 구할 때, 제안하는 Algorithm 2 의 계산 복잡도는 다음과 같다.

정리 2. $\alpha \in GF(2^{2^n m})^*$를 $GF(2^{2^n})$위에서 MONB B를 사용하여 표현하면 역원 α^{-1}는 $tw(m-1)+tw(2^n-1)+2$ 번의 곱셈과 2^n-1 번의 제곱으로 계산된다.

(증명) 0이 아닌 임의의 $\alpha \in GF(2^{2^n m})$를 $GF(2)$위에서 $GF(2^m)$의 정규기저 $B=\{\beta,\beta^2,\beta^{2^2},\cdots,\beta^{2^{m-1}}\}$를 이용하면 $GF(2^{2^n})$위에서 다음과 같이 표현된다.

$$\alpha = a_0\beta + a_1\beta^q + a_2\beta^{q^2} + \cdots + a_{m-1}\beta^{q^{m-1}},$$
$$a_i \in GF(2^{2^n}). \tag{11}$$

그런데

$$\alpha^{2^{2^r}} = a_0\beta^{2^{2^r}} + a_1\beta^{2^{2^r+1}} + a_2\beta^{2^{m-2+2^r}} + \cdots + a_{m-1}\beta^{2^{m-1+2^r}}$$
$$= a_{m-2^n}\beta + a_{m-2^n+1}\beta^q + a_2\beta^{q^2} + \cdots + a_{m-1-2^n}\beta^{q^{m-1}},$$
$$\text{단, 계수 } a_i\text{의 첨자 } i \equiv i \bmod m, \tag{12}$$

이므로 $\alpha^{2^{2^n}}$는 2^n번의 우측 순환좌표이동으로 계산된다. 따라서 Algorithm 2의 2.1.2 단계에서의 $u^{2^{2^n t}}$는 $2^n t$번의 우측 순환좌표이동으로 계산된다. 그런데 식 (10)에서

$$\alpha^{-1} = \alpha^{(2^n-1)(2^{2^n}+2^{2^{n+2}}+\cdots+2^{2^n(m-1)})} \cdot \alpha^{2+2^2+\cdots+2^{n-1}}$$

이고

$$\alpha^{2^n-1} = \alpha \cdot \alpha^{2+2^2+\cdots+2^{n-1}} \tag{13}$$

이므로, Algorithm 2에서 $\alpha^{(2^n-1)(2^{2^n}+2^{2^{n+2}}+\cdots+2^{2^n(m-1)})}$과 $\alpha^{2+2^2+\cdots+2^{n-1}}$의 계산에 소요되는 곱셈횟수는 각각 $tw(m-1)$과 $tw(n-1)$이므로 α^{-1}는 $tw(m-1)+tw(2^n-1)+2$ 번의 곱셈과 2^n-1 번의 제곱연산으로 계산된다.

[참고] Itoh 등[7]이 제안한 역원계산 방법을 사용하면, $\alpha \in GF(2^{2^n m})^*$를 $GF(2^{2^n})$위에서 MONB B를 사용하여 표현할 때, 역원 α^{-1}는 $tw(2^n m-1)$ 번의 곱셈과 $2^n m-1$ 번의 제곱으로 계산된다.

이제 Itoh 등[7]이 제안한 역원계산 방법과 제안하는 알고리즘과의 효율성을 비교하기 위해서 다음의 정리를 증명하기로 한다.

정리 3. m은 홀수, n은 자연수일 때, 등식

$$tw(2^n m-1) = tw(m-1) + tw(2^n-1) + 2 \tag{14}$$

가 성립한다.

(증명) m을 내림차순 이진법 표현을 $(a_l, a_{l-1}, \cdots, a_1, 1)_2$라고 하자. 그러면

$m-1 = (a_l, a_{l-1}, \cdots, a_1, 0)_2$ 이고,

$$2^n m = (a_l, a_{l-1}, \cdots, 0, \underbrace{1, \cdots, 1}_{n\text{번}})_2. \tag{15}$$

그런데 정의 3과 Kim 등[3]에 의해서,

$$\begin{aligned} tw(2^n-1) &= w(2^n-1) + nb(n)(2^n-1) - 2 \\ &= 2n-2, \\ tw(m-1) &= w(m-1) + nb(m-1) \\ &= (w(m)-1) + (l+1) - 2 \\ &= w(m) + l - 2 \end{aligned} \tag{16}$$

이므로

$$tw(m-1) + tw(2^n-1) = w(m) + 2n + l - 4 \tag{17}$$

가 된다. 따라서

$$\begin{aligned} & tw(2^n m-1) \\ &= w(2^n m-1) + nb(2^n m-1) - 2 \\ &= (w(m)+n-1) + (l+n+1) - 2 \\ &= w(m) + 2n + l - 2 \\ &= tw(m-1) + tw(2^n-1) + 2 \end{aligned} \tag{18}$$

이므로 식 (14)가 증명되었다.

정리 3에 의하면 제안하는 Algorithm 2를 적용하여 역원 α^{-1}를 계산할 때, Itoh 등[7]이 제안한 역원 계산 방법과 곱셈횟수는 동일하고 제곱횟수는 적다는 사실을 알 수 있다.

IV. 계산 복잡도

이 장에서는 바탕체 $GF(2^8)$위의 $m=23$, 33일 때의 유한확대체 $GF((2^8)^{23}=GF(2^{184})$와 $GF((2^8)^{33}=GF(2^{264})$에 대해서, 제안하는 Algorithm 2와 Itoh 등[7]의 역원계산 방법과의 복잡도를 Pentium 166 MHZ CPU에서 10,000번의 곱셈, 제곱, 역원계산을 실행하여 실행시간을 초(second)로 계산하여 비교한 결과를 표 1에 정리하였다.

표 1. 정규기저를 갖는 유한체의 곱셈 연산기의 복잡도 비교
Table 1. Comparison of normal basis multipliers.(seconds)

curve	$GF(2^{184})$		$GF(2^{264})$	
Multiplier	Itoh	Alg.2	Itoh	Alg.2
Multi.	2.90		6.01	
Square	0.031	0.024	0.042	0.035
Inverse	47.07	41.01	83.95	71.96

표 1에서 보는 바와 같이 제안하는 알고리즘은 유한체 $GF(2^{184})$와 $GF(2^{264})$위에서 Itoh 등의 알고리즘과 곱셈속도는 같으나 제곱계산 속도가 22% 빠르기 때문에 곱셈역원의 계산속도가 13% 빠르게 나타났다.

V. 결 론

MONB를 사용하면 제곱연산이 한 번의 우측순환 좌표이동(right cyclic shift)으로 되지 않기 때문에, 많은 제곱연산이 필요한 곱셈 역원 연산에는 효율성이 떨어지게 된다. 본 논문에서는 이러한 단점을 보완하고 이진수열의 생성[11]에도 활용될 수 있도록, 특수한 최적정규기저를 사용하여 곱셈 역원 계산에 2^n-1 번의 제곱연산 $nb(2^nm-1)+w(2^nm-1)-2$ 번의 곱셈이 소요되는 역원 계산 알고리즘을 제안하였으며, H/W상에서 구현하여 Itoh 등[7]의 방법 보다 역원계산속도가 13% 빠르다는 결과를 얻었다.

감사의 글

본 논문은 광주교육대학교 2014년도 학술연구비 지원에 의한 것임

References

[1] N. Koblitz, “Elliptic Curve cryptosystems,” *Math. Comp.* 48, 1987, pp. 203-209.

[2] G. Harper, A. Menezes, and S. Vanstone, “Public-key Cryptosystems with very small key length,” *Eurocrypto 92, Springer-Verlag.* Balatonfured, Hungary, May 1992, pp. 163-172.

[3] C.-H. Kim, S.-H. Oh, J.-I. Lim, K.-S. Suh, and J.-C. Yoon, “Operations in finite fields using modified method,” *J. Korea Institute of Information Security and Cryptography,* vol. 8, no. 2, 1998, pp. 27-36.

[4] H. Cohen, *A Course in Computational Algebraic Number Theory.* New York : Springer-Verlag, 2000.

[5] U.-S. Choi and S.-J. Cho, “Design of Binary Sequence with optimal Cross-correlation Values,” *J. of The Korea Institute of Electronic Communication Sciences,* vol. 6, no. 4, 2011, pp. 539-544,

[6] H.-D. Kim, S.-J. Cho, M.-J. Kwon, and H.-J. An, "A study on the cross-correlation function of extended Zeng sequences,” *The J. of The Korea Institute of Electronic Communication Sciences,* vol. 7, no. 1, 2012, pp. 61-67.

[7] T. Itoh, O. Teechal, and S. Tsujii, "A fast algorithm for computing multiplicative inverse in $GF(2^n)$ using normal bases,“ *J. Soc. Electro. Comm.(Japan),* vol. 44, 1986, pp. 31-36.

[8] Y. Kim, “A Fast Multiplier of Composite fields over finite fields,” *J. of The Korea Institute of Electronic Communication Sciences,* vol. 6, no. 3, 2011, pp. 389-395.

[9] G. Agnew, T. Beth, B. Mullin, and S. Vanstone,

"Arithmetic Operations in $GF(2^n)$," *J. Cryptology*, vol. 6, 1993, pp. 3-13.

[10] Y. Kim, "Fast Sequential Optimal normal Bases Multipliers over finite fields," *J. of The Korea Institute of Electronic Communication Sciences,* vol. 8, no. 8, 2013, pp. 1207-1212.

[11] U.-S. Choi, S.-J. Cho, and S.-H. Kwon, "Analysis of Cross Correlation of Extended Non-linear Binary Sequences," *J. of The Korea Institute of Electronic Communication Sciences,* vol. 7, no. 2, 2012, pp. 263-269.

저자 소개

김용태(Yong-Tae Kim)

1976년 공주사범대학 수학교육과 (이학사)
1986년 고려대학교 대학원 수학과 (이학석사)
1991년 고려대학교대학원 수학과(이학박사)
2000년 서울대학교 대학원 수학교육과(교육학석사)
2008년 서울대학교 대학원 수학교육과(박사과정수료)
1992년~현재 광주교육대학교 수학교육과 교수
※ 관심분야 : ECC, 정수론적 암호학, 공개키암호학