情報保護學會論文誌
第 21 卷 第 2 號, 2011. 4

페어링 암호 연산을 위한 F_{3^m}에서의 효율적인 세제곱근 연산 방법*

조 영 인[1†], 장 남 수[2], 김 창 한[3], 박 영 호[2‡], 홍 석 희[1]
[1]고려대학교, [2]세종사이버대학교, [3]세명대학교

Efficient Formulas for Cube roots in F_{3^m} for Pairing Cryptography*

Young In Cho[1†], Nam Su Chang[2], Chang Han Kim[3], Young-Ho Park[2‡], Seokhie Hong[1]
[1]Korea University, [2]Sejong Cyber University, [3]Semyung University

요 약

F_{3^m} 에서의 Tate 페어링 또는 η_T 페어링 알고리즘 계산을 위하여 효율적인 세제곱근 계산은 매우 중요하다. $x^{1/3}$의 다항식 표현 중 0이 아닌 계수들의 개수를 $x^{1/3}$의 헤밍웨이트라 할 때, 이 헤밍웨이트가 세제곱근 연산의 효율성을 결정하게 된다. O. Ahmadi 등은 $f(x)=x^m+ax^k+b\ (a,\ b\in F_3)$가 $F_3[x]$의 삼항 기약다항식이라 할 때, $F_{3^m}=F_3[x]/(f)$을 생성하는 모든 삼항 기약다항식에 대하여 $x^{1/3}$의 헤밍웨이트를 계산하였다. 본 논문에서는 Shifted Polynomial Basis(SPB)가 기존의 결과보다 $x^{1/3}$의 헤밍웨이트를 낮출 수 있음을 보이며, 모듈로 감산 연산이 필요 없는 가장 적합한 SPB를 제공한다.

ABSTRACT

Evaluation of cube roots in characteristic three finite fields is required for Tate (or modified Tate) pairing computation. The Hamming weights (the number of nonzero coefficients) in the polynomial representations of $x^{1/3}$ and $x^{2/3}$ determine the efficiency of cube roots computation, where F_{3^m} is represented as $F_3[x]/(f)$ and $f(x)=x^m+ax^k+b\in F_3[x]\ \ (a,\ b\in F_3)$ is an irreducible trinomial. O. Ahmadi et al. determined the Hamming weights of $x^{1/3}$ and $x^{2/3}$ for all irreducible trinomials. In this paper, we present formulas for cube roots in F_{3^m} using the shifted polynomial basis(SPB). Moreover, we provide the suitable shifted polynomial basis bring no further modular reduction process.

Keywords: Cube root, Shifted polynomial basis, Finite field arithmetic

I. 서 론

페어링 암호 기반의 암호 프로토콜 구현을 위하여 F_{3^m}위의 초특이 타원곡선이 매우 적합한 것으로 연구되었고 이에따라 F_{3^m}에서의 효율적인 유한체 연산에 대한 연구가 최근 주목을 받고 있다[2][7]. 특히 초특이 타원곡선위의 페어링 암호 알고리즘 중 F_{3^m}위에서의 η_T 페어링의 계산을 위하여 세제곱근 연산이 필요하다[3][7]. $f(x)=x^m+ax^k+b\ (a,b\in F_3)$가 $F_3[x]$의 삼항 기약다항식(Irreducible trinomial)이라 할 때, $F_{3^m}=F_3[x]/(f)$라 하자. F_{3^m}에서의 세제곱근 연산

접수일(2010년 7월 9일), 게재확정일(2010년 11월 3일)
* 본 연구는 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업입니다. (No. 2010-0011511)
† 주저자, elowey@korea.ac.kr
‡ 교신저자, youngho@sjcu.ac.kr

을 살펴보도록 한다. 우선 임의의 자연수 u에 대하여 $m=3u$라 하자. ($m\equiv\pm1\pmod 3$인 경우도 유사하게 적용할 수 있다.) 그러면 $C\in F_{3^m}$에 대하여

$$C=\sum_{i=0}^{3u-1}c_ix^i=\sum_{i=0}^{u-1}c_{3i}x^{3i}+x\sum_{i=0}^{u-1}c_{3i+1}x^{3i}+x^2\sum_{i=0}^{u-1}c_{3i+2}x^{3i}$$

이고 이 식을 이용하여 C의 세제곱 연산식은 아래의 식 (1)과 같다.

$$C^{1/3}=\sum_{i=0}^{u-1}c_ix^i=\sum_{i=0}^{u-1}c_{3i}x^i+x^{1/3}\sum_{i=0}^{u-1}c_{3i+1}x^i+x^{2/3}\sum_{i=0}^{u-1}c_{3i+2}x^i. \quad (1)$$

$x^{1/3}$과 $x^{2/3}$가 사전계산 되었다면, 식 (1)을 이용하여 단지 두 번의 다항식 곱셈만으로 세제곱근을 계산할 수 있다. 이 다항식 곱셈을 할 때, $x^{1/3}$과 $x^{2/3}$의 다항식 표현이 작은 개수의 항을 갖는다면 보다 효율적으로 연산이 이루어진다. $m\equiv k\pmod 3$인 경우 $x^{1/3}$과 $x^{2/3}$의 다항식 표현이 매우 작은 개수의 항을 가지므로 가장 효율적으로 세제곱 연산을 할 수 있다 [5]. 그러나 $m\equiv k\pmod 3$인 형태의 삼항 기약다항식 $f(x)=x^m+ax^k+b$은 굉장히 드물게 존재한다. 따라서 $m\neq k\pmod 3$인 형태의 삼항 기약다항식에 대해서 세제곱근을 구할 수 있는 방법에 대한 연구가 필요하게 되었고 O. Ahmadi 등은 이 경우에 대하여 $x^{1/3}$의 다항식 표현 중 0 이 아닌 계수들의 개수를 $x^{1/3}$의 헤밍웨이트라 할 때, 이 헤밍웨이트가 세제곱근 연산의 효율성을 결정하게 된다. 세제곱근 연산식의 $x^{1/3}$과 $x^{2/3}$의 헤밍웨이트를 계산하였다[4].

본 논문에서는 효율적인 세제곱근 연산을 위하여 기존 결과보다도 $x^{1/3}$과 $x^{2/3}$의 헤밍웨이트를 낮추도록 한다. Polynomial Basis(PB)의 변형된 형태인 SPB는 2005년 $GF(2^n)$에서의 곱셈기 설계를 위하여 제안되었다[1]. 본 논문에서는 SPB를 기저로 한 $x^{1/3}$과 $x^{2/3}$의 다항식 표현이 작은 개수의 항을 갖는다는 것을 발견하였다. 따라서 SPB를 기저로 하여 $x^{1/3}$과 $x^{2/3}$의 헤밍웨이트를 계산한다. 또한, 본 논문에서는 가능한 모든 삼항 기약다항식에 대하여 모듈로 감산 연산이 필요없는 SPB를 제공한다. 따라서 본 논문의 방법으로 [4]의 방법보다 훨씬 효율적으로 세제곱근을 연산할 수 있다. 앞으로 $x^{1/3}$의 헤밍웨이트를 $wt(x^{1/3})$로 정의한다.

본 논문의 구성은 다음과 같다. 2 장에서는 기존 결과들을 살펴보고, 3 장에서 SPB를 기저로 하여 $wt(x^{1/3})$과 $wt(x^{2/3})$를 계산한 후, 가장 적합한 SPB를 찾는다. 4장에서 비교와 결론으로 끝을 맺는다.

II. 관련 연구

본 장에서는 관련 연구 결과를 설명한다. 관련 연구로는 [4, 5]가 유일하다.

정리 1. [5] $f(x)=x^m+ax^k+b$ ($a, b\in F_3$)가 F_3위의 삼항 기약다항식이고 $m\equiv k\pmod 3$이라 하면

$$wt(x^{1/3})=\begin{cases}3 & m\equiv k\equiv 1\pmod 3,\\ 2 & m\equiv k\equiv -1\pmod 3.\end{cases}$$

정리 1을 통하여 $m\equiv k\pmod 3$인 경우, $x^{1/3}$과 $x^{2/3}$의 다항식 표현이 매우 작은 개수의 항을 가지는 것을 알 수 있다.

정리 2. [4] $f(x)=x^m+ax^k+b$ ($a, b\in F_3$)가 F_3위의 삼항 기약다항식이고 $m\equiv -k\pmod 3$이라 하면 $wt(x^{1/3})\in\{(m/e)-2, (m/e)-1, m/e\}$. 이 때, $e=\gcd(m, k)$.

$m\equiv -k\pmod 3$인 경우, O. Ahmadi 등은 $x^{1/3}=\sum_{i=0}^{m-1}c_ix^i$ 라 할 때, $h(x)=\sum_{i=0}^{m-1}c_ix^{3i}-x=g(x)f(x)$를 만족하는 다항식 $g(x)$와 $h(x)$를 찾도록 하였다. 이로써 $x^{1/3}$의 다항식 표현을 찾고 $wt(x^{1/3})$을 계산하였다. SPB는 모듈로 감산 연산을 줄이기 위해 이용하는 것이기 때문에 이 경우에는 PB를 기저로 한 $wt(x^{1/3})$과 같은 결과를 갖는다. 아래의 정리들은 [4]의 결과들이며 본 논문에서는 아래의 정리들에 해당하는 경우에 대하여 보다 낮은 $wt(x^{1/3})$과 $wt(x^{2/3})$을 제공한다.

정리 3. [4] $f(x)=x^m+ax^k+b$ ($a, b\in F_3$)가 F_3위의 삼항 기약다항식이고 $m\equiv 0\pmod 3$, $k\equiv 1\pmod 3$이라 하면

$$wt(x^{1/3})=\begin{cases}3 & m\neq 3k,\ k\neq 1,\\ 1 & m=3k,\ a=1,\\ 2 & m=3k,\ a=-1,\\ 2 & k=1.\end{cases}$$

정리 4.[4] $f(x)=x^m+ax^k+b$ ($a,\ b\in F_3$)가 F_3위의 삼항 기약다항식이고 $m\equiv 0 \pmod 3$, $k\equiv -1 \pmod 3$이라 하면 $wt(x^{1/3})\le 5$ 이다.

정리 5.[4] $f(x)=x^m+ax^k+b$ ($a,\ b\in F_3$)가 F_3위의 삼항 기약다항식이라 하면

$$wt(x^{1/3})=\begin{cases}\in\{p,\ p+1,\ p+2\} & m\equiv 1,\ k\equiv 0 \pmod 3,\\ \in\{q,\ q+1,\ q+2,\ q+3\} & m\equiv -1,\ k\equiv 0 \pmod 3.\end{cases}$$

이 때, $p=\lceil (m-1)/3k\rceil+\lceil (m-1-k)/3k\rceil$, $q=\lceil (2m-1)/3k\rceil+\lceil (2m-1-k)/3k\rceil+\lceil (2m-1-2k)/3k\rceil$.

정리 5로부터 k가 클수록 낮은 $wt(x^{1/3})$를 얻을 수 있음을 알 수 있다. 그러나 큰 k를 갖는 삼항 기약다항식은 일반적으로 모듈러 감산 연산이 많이 필요하게 된다. 따라서 정리 5의 경우에 낮은 $wt(x^{1/3})$를 얻는다 해도 추가적인 모듈로 감산이 많아 질 수 있다.

III. 적합한 SPB 계산

본 장에서는 SPB를 이용하여 효율적으로 세제곱근을 연산할 수 있는 방법을 제안한다. 또한, $m\neq \pm k \pmod 3$인 경우에 대하여 $wt(x^{1/3})$과 $wt(x^{2/3})$을 계산하고 모듈로 감산 연산이 필요없는 가장 적합한 SPB를 찾는다.

정의 1. r을 임의의 정수라 하고 집합 $S=\{x^i \mid 0\le i\le m-1\}$를 F_3위의 PB라 할 때, 집합 $x^{-r}S:=\{x^{i-r} \mid 0\le i\le m-1\}$을 S의 SPB라 한다.

기존 결과 [4]에서는 추가적인 모듈로 감산 연산이 필요했다. 예를 들어, 정리 2의 $m\equiv 0 \pmod 3$, $k\equiv 1 \pmod 3$인 삼항 기약다항식에 대하여 식 (1)에서 $x^{1/3}$의 다항식 표현은 $\sum_{i=0}^{u-1} c_{3i+1}x^i$와 곱해져야한다. 그러면 $x^{1/3}\cdot\sum_{i=0}^{u-1} c_{3i+1}x^i$의 최대 차수는 $4u-v-1$가 되고 $4u-v-1>3u(=m)$이므로 추가적인 모듈로 감산 연산이 필요하게 된다. 다른 모든 경우에 대해서도 같은 이유로 모듈로 감산 연산이 필요하다. 따라서 본 논문에서는 [4]에서와 달리 $C^{1/3}$ 계산 시 모듈로 감산 연산이 필요 없도록 정의 1의 r을 결정한다. 이와 같은 r을 γ로 정의하고 식 전개의 편의를 위하여 임의의 정수 t와 $\theta\in\{0,\ 1,\ 2\}$에 대하여 r 대신에 $3t+\theta$을 대입한다.

3.1 $m\equiv 0 \pmod 3$인 경우

SPB를 기저로 하여 C를 간결하게 표현하기 위하여 아래의 함수를 정의한다.

$$\sigma_j(j=1,\ 2)=\begin{cases}0 & [\theta+j]<3,\\ 1 & [\theta+j]\ge 3.\end{cases}$$

식 (1)과 정의 1로부터 SPB를 기저로 한 C의 다항식 표현은 다음과 같다.

$$\begin{aligned}C&=x^{-r}\sum_{i=0}^{3u-1}c_ix^i\\ &=\sum_{i=0}^{u-1}c_{3i+\theta}x^{3i+\theta-(3t+\theta)}+x\sum_{i=-\sigma_1}^{u-1-\sigma_1}c_{3i+[\theta+1]}x^{3i+\theta-(3t+\theta)}\\ &\quad+x^2\sum_{i=-\sigma_2}^{u-1-\sigma_2}c_{3i+[\theta+2]}x^{3i+\theta-(3t+\theta)}\\ &=\sum_{i=0}^{u-1}c_{3i+\theta}x^{3(i-t)}+x\sum_{i=-\sigma_1}^{u-1-\sigma_1}c_{3i+[\theta+1]}x^{3(i-t)}\\ &\quad+x^2\sum_{i=-\sigma_2}^{u-1-\sigma_2}c_{3i+[\theta+2]}x^{3(i-t)}.\end{aligned}\tag{2}$$

따라서 식 (2)로부터 C의 세제곱근 연산식은 아래와 같다.

$$\begin{aligned}C^{1/3}&=\sum_{i=0}^{u-1}c_{3i+\theta}x^{(i-t)}+x^{1/3}\sum_{i=-\sigma_1}^{u-1-\sigma_1}c_{3i+[\theta+1]}x^{(i-t)}\\ &\quad+x^{2/3}\sum_{i=-\sigma_2}^{u-1-\sigma_2}c_{3i+[\theta+2]}x^{(i-t)}.\end{aligned}$$

이제 SPB를 기저로 하여 $wt(x^{1/3})$과 $wt(x^{2/3})$을 계산하고 각 경우에 대하여 γ을 결정한다. 본 논문에서는 $wt(x^{1/3})$를 최소화 하는데 초점을 맞추고 있으므로 PB에 속하지 않는 항에 대하여 허용한다. 그리고 나서 결과적으로 모듈로 감산이 필요 없는 적합한 SPB를 찾는다.

정리 6. $f(x)=x^m+ax^k+b$ ($a,\ b\in F_3$)가 F_3위의 삼항 기약다항식이고 $m\equiv 0 \pmod 3$, $k\equiv 1 \pmod 3$이라 하면

$$\begin{cases}wt(x^{1/3})=2,\\ wt(x^{2/3})=3.\end{cases}$$

증명. 임의의 양수 u와 v에 대하여$(u>v)$ $m=3u$이고 $k=3v+1$라 하자. F_{3^m}에서 $x^{3u}+ax^{3v+1}+b=0$ 이므로 $ax^{3v}\cdot x=-x^{3u}-b$ 이다. 따라서

$$x^{1/3}=-ax^{u-v}-abx^{-v}=-a(x^{u-v}+bx^{-v}). \tag{3}$$

또한

$$x^{2/3}=(-a(x^{u-v}+bx^{-v}))^2=x^{2u-2v}+x^{-2v}-bx^{u-2v}. \tag{4}$$

따름정리 1. $f(x)=x^m+ax^k+b$ $(a,\ b\in F_3)$가 F_3위의 삼항 기약다항식이고 $m\equiv 0\pmod 3$, $k\equiv 1\pmod 3$이라 하면 $\gamma\in\{3v,\ 3v+1\}$.

증명. 식 (3)과 (4)로부터 다음의 식 (5)를 얻을 수 있다.

$$\begin{aligned}C^{1/3}=&\sum_{i=0}^{u-1}c_{3i+\theta}x^{(i-t)}-a(x^{u-v}+bx^{-v})\\&\sum_{i=-\sigma_1}^{u-1-\sigma_1}c_{3i+[\theta+1]}x^{(i-t)}+(x^{2u-2v}+x^{-2v}-bx^{u-2v})\\&\sum_{i=-\sigma_2}^{u-1-\sigma_2}c_{3i+[\theta+2]}x^{(i-t)}.\end{aligned} \tag{5}$$

식 (5)로부터 $C^{1/3}$의 최소 차수는 $-2v-\sigma_2-t$이고 최대 차수는 $3u-2v-1-\sigma_2-t$임을 알 수 있다. 그러므로 식 (6)을 만족하면 식 (5)에서 더 이상의 모듈로 감산 연산은 필요하지 않게 된다.

$$\begin{cases}-2v-\sigma_2-t\ge -3t-\theta,\\3u-2v-1-\sigma_2-t\le 3u-1-(3t+\theta).\end{cases} \tag{6}$$

식 (6)으로부터 $t=(2v+\sigma_2-\theta)/2$를 구할 수 있고, 이 때, $(t,\ \theta)$ 쌍은 $(v,\ 0)$과 $(v,\ 1)$가 될 수 있다. 그러므로 γ은 $3v$나 $3v+1$이 된다.

정리 7. $f(x)=x^m+ax^k+b$ $(a,\ b\in F_3)$가 F_3위의 삼항 기약다항식이고 $m\equiv 0\pmod 3$, $k\equiv -1\pmod 3$이라 하면

$$\begin{cases}ut(x^{1/3})=3,\\ut(x^{2/3})=2.\end{cases}$$

증명. 임의의 양수 u와 v에 대하여$(u\ge v)$ $m=3u$이고 $k=3v-1$라 하자. F_{3^m}에서 $x^{3u}+ax^{3v-1}+b=0$이므로 $ax^{3v}\cdot x^{-1}=-x^{3u}-b$이다. 따라서

$$x^{-1/3}=-a(x^{u-v}+bx^{-v}).$$

그러므로

$$x^{2/3}=x^{-1/3}\cdot x=-a(x^{u-v+1}+bx^{-v+1}). \tag{7}$$

식 (7)로부터

$$\begin{aligned}x^{1/3}\cdot x&=(-a(x^{u-v+1}+bx^{-v+1}))^2\\&=x^{2u-2v+2}+x^{-2v+2}-bx^{u-2v+2}\end{aligned}$$

가 된다. 그러므로

$$x^{1/3}=x^{2u-2v+1}+x^{-2v+1}-bx^{u-2v+1}. \tag{8}$$

따름정리 2. $f(x)=x^m+ax^k+b$ $(a,\ b\in F_3)$가 F_3위의 삼항 기약다항식이고 $m\equiv 0\pmod 3$, $k\equiv -1\pmod 3$이라 하면 $\gamma\in\{3v-2,\ 3v-1\}$.

증명. 식 (7)과 (8)로부터 다음의 식 (9)를 얻을 수 있다.

$$\begin{aligned}C^{1/3}=&\sum_{i=0}^{u-1}c_{3i+\theta}x^{(i-t)}+(x^{2u-2v+1}+x^{-2v+1}\\&-bx^{u-2v+1})\sum_{i=-\sigma_1}^{u-1-\sigma_1}c_{3i+[\theta+1]}x^{(i-t)}\\&-a(x^{u-v+1}+bx^{-v+1})\sum_{i=-\sigma_2}^{u-1-\sigma_2}c_{3i+[\theta+2]}x^{(i-t)}.\end{aligned} \tag{9}$$

식 (9)로부터 $C^{1/3}$의 최소 차수는 $-2v+1+\sigma_1-t$이고 최대 차수는 $3u-2v-\sigma_1-t$임을 알 수 있다. 그러므로 식 (10)을 만족하면 식 (9)에서 더 이상의 모듈로 감산 연산은 필요하지 않게 된다.

$$\begin{cases}-2v+1-\sigma_1-t\ge -3t-\theta,\\3u-2v-\sigma_1-t\le 3u-1-(3t+\theta).\end{cases} \tag{10}$$

식 (10)으로부터 $t=(2v-1+\sigma_1-\theta)/2$를 구할 수 있고, 이 때, $(t,\ \theta)$ 쌍은 $(v-1,\ 1)$과 $(v-1,\ 2)$가 될 수 있다. 그러므로 γ은 $3v-2$나 $3v-1$이 된다.

3.2 $k \equiv 0 \pmod 3$인 경우

먼저 $m \equiv 1 \pmod 3$, $k \equiv 0 \pmod 3$인 경우를 고려해 보도록 한다. 임의의 양수 u에 대하여 $m = 3u+1$라 하면 $C \in F_{3^m}$는 다음과 같이 표현된다.

$$C = \sum_{i=0}^{3u} c_i x^i = \sum_{i=0}^{u} c_{3i} x^{3i} + x \sum_{i=0}^{u-1} c_{3i+1} x^{3i} + x^2 \sum_{i=0}^{u-1} c_{3i+2} x^{3i}.$$

C의 간략한 표현을 위하여 아래와 같이 정의한다.

$$\sigma_o = \begin{cases} 0 & \theta = 0, \\ 1 & \theta \in \{1, 2\}. \end{cases}$$

이를 이용하여 SPB를 기저로 한 C를 표현하면 식 (11)과 같이 쓸 수 있다.

$$\begin{aligned} C &= x^{-r} \sum_{i=0}^{3u} c_i x^i \\ &= \sum_{i=0}^{u-\sigma_o} c_{3i+\theta} x^{3i+\theta-(3t+\theta)} + x \sum_{i=-\sigma_1}^{u-1} c_{3i+[\theta+1]} x^{3i+\theta-(3t+\theta)} \\ &\quad + x^2 \sum_{i=-\sigma_2}^{u-1-\sigma_1} c_{3i+[\theta+2]} x^{3i+\theta-(3t+\theta)} \\ &= \sum_{i=0}^{u-\sigma_o} c_{3i+\theta} x^{3(i-t)} + x \sum_{i=-\sigma_1}^{u-1} c_{3i+[\theta+1]} x^{3(i-t)} \\ &\quad + x^2 \sum_{i=-\sigma_2}^{u-1-\sigma_1} c_{3i+[\theta+2]} x^{3(i-t)}. \end{aligned} \tag{11}$$

식 (11)로부터 아래와 같이 $C^{1/3}$을 구할 수 있다.

$$\begin{aligned} C^{1/3} &= \sum_{i=0}^{u-\sigma_o} c_{3i+\theta} x^{(i-t)} + x^{1/3} \sum_{i=-\sigma_1}^{u-1} c_{3i+[\theta+1]} x^{(i-t)} \\ &\quad + x^{2/3} \sum_{i=-\sigma_2}^{u-1-\sigma_1} c_{3i+[\theta+2]} x^{(i-t)}. \end{aligned}$$

정리 8. $f(x) = x^m + ax^k + b$ (a, $b \in F_3$)가 F_3위의 삼항 기약다항식이고 $m \equiv 1 \pmod 3$, $k \equiv 0 \pmod 3$이라 하면

$$\begin{cases} wt(x^{1/3}) = 2, \\ wt(x^{2/3}) = 3. \end{cases}$$

증명. 임의의 양수 u와 v에 대하여($u \geq v$) $m = 3u+1$이고 $k = 3v$라 하자. F_{3^m}에서 $x^{3u+1} + ax^{3v} + b = 0$ 이므로 $-x^{3u} \bullet x = ax^{3v} + b$ 이다. 따라서

$$x^{1/3} = -ax^{v-u} - bx^{-u}. \tag{12}$$

또한

$$x^{2/3} = (-ax^{v-u} - bx^{-u})^2 = x^{2v-2u} + x^{-2u} - abx^{v-2u}. \tag{13}$$

따름정리 3. $f(x) = x^m + ax^k + b$ (a, $b \in F_3$)가 F_3위의 삼항 기약다항식이고 $m \equiv 1 \pmod 3$, $k \equiv 0 \pmod 3$이라 하면 $\gamma \in \{3u, 3u+1\}$.

증명. 식 (12)과 (13)로부터 다음의 식 (14)를 얻을 수 있다.

$$\begin{aligned} C^{1/3} &= \sum_{i=0}^{u-\sigma_o} c_{3i+\theta} x^{(i-t)} - (ax^{v-u} + bx^{-u}) \\ &\quad \sum_{i=-\sigma_1}^{u-1} c_{3i+[\theta+1]} x^{(i-t)} + (x^{2v-2u} + x^{-2u} - bx^{v-2u}) \\ &\quad \sum_{i=-\sigma_2}^{u-1-\sigma_1} c_{3i+[\theta+2]} x^{(i-t)}. \end{aligned} \tag{14}$$

식 (14)로부터 $C^{1/3}$의 최소 차수는 $-2u-\sigma_2-t$이고 최대 차수는 $u-\sigma_o-t$임을 알 수 있다. 그러므로 식 (15)을 만족하면 식 (14)에서 더 이상의 모듈로 감산 연산은 필요하지 않게 된다.

$$\begin{cases} -2u-\sigma_2-t \geq -3t-\theta, \\ u-\sigma_o-t \leq 3u-(3t+\theta). \end{cases} \tag{15}$$

식 (15)으로부터 $(2u+\sigma_2-\theta)/2 \leq t \leq (2u+\sigma_o-\theta)/2$를 구할 수 있고, 이 때, (t, θ) 쌍은 $(u, 0)$과 $(u, 1)$가 될 수 있다. 그러므로 γ은 $3u$나 $3u+1$ 된다.

다음으로 $m \equiv -1 \pmod 3$, $k \equiv 0 \pmod 3$인 경우를 고려해보도록 한다. 임의의 양수 u에 대하여 $m = 3u-1$라 하면 $C \in F_{3^m}$는 다음과 같이 표현된다.

$$C = \sum_{i=0}^{3u-2} c_i x^i = \sum_{i=0}^{u-1} c_{3i} x^{3i} + x \sum_{i=0}^{u-1} c_{3i+1} x^{3i} + x^2 \sum_{i=0}^{u-2} c_{3i+2} x^{3i}.$$

이를 이용하여 SPB를 기저로 한 C를 표현하면 식 (16)과 같이 쓸 수 있다.

$$\begin{aligned} C &= x^{-r} \sum_{i=0}^{3u-2} c_i x^i = \sum_{i=0}^{u-1-\sigma_1} c_{3i+\theta} x^{3i+\theta-(3t+\theta)} \\ &\quad + x \sum_{i=-\sigma_1}^{u-1-\sigma_2} c_{3i+[\theta+1]} x^{3i+\theta-(3t+\theta)} \\ &\quad + x^2 \sum_{i=-\sigma_2}^{u-2} c_{3i+[\theta+2]} x^{3i+\theta-(3t+\theta)} \\ &= \sum_{i=0}^{u-1-\sigma_1} c_{3i+\theta} x^{3(i-t)} + x \sum_{i=-\sigma_1}^{u-1-\sigma_2} c_{3i+[\theta+1]} x^{3(i-t)} \\ &\quad + x^2 \sum_{i=-\sigma_2}^{u-2} c_{3i+[\theta+2]} x^{3(i-t)}. \end{aligned} \tag{16}$$

〔표 1〕 $x^{1/3}$와 $x^{2/3}$의 헤밍웨이트 비교표

$m \pmod 3$	$k \pmod 3$	PB〔4〕		SPB	
		$wt(x^{1/3})$	$wt(x^{2/3})$	$wt(x^{1/3})$	$wt(x^{2/3})$
0	1	3	2	2	3
0	-1	≤ 5	2	3	2
1	0	$\in\{p^{\alpha}, p+1, p+2\}$	-	2	3
-1	0	$\in\{q^{\beta}, q+1, q+2, q+3\}$	-	3	2

α: $p = \lceil (m-1)/3k \rceil + \lceil (m-1-k)/3k \rceil$, β: $q = \lceil (2m-1)/3k \rceil + \lceil (2m-1-k)/3k \rceil + \lceil (2m-1-2k)/3k \rceil$.

식 (16)로부터 아래와 같이 $C^{1/3}$을 구할 수 있다.

$$C^{1/3} = \sum_{i=0}^{u-1-\sigma_1} c_{3i+\theta} x^{(i-t)} + x^{1/3} \sum_{i=-\sigma_1}^{u-1-\sigma_2} c_{3i+[\theta+1]} x^{(i-t)} + x^{2/3} \sum_{i=-\sigma_2}^{u-2} c_{3i+[\theta+2]} x^{(i-t)}.$$

정리 9. $f(x) = x^m + ax^k + b$ ($a, b \in F_3$)가 F_3위의 삼항 기약다항식이고 $m \equiv -1 \pmod 3$, $k \equiv 0 \pmod 3$ 이라 하면

$$\begin{cases} wt(x^{1/3}) = 3, \\ wt(x^{2/3}) = 2. \end{cases}$$

증명. 임의의 양수 u와 v에 대하여$(u > v)$ $m = 3u-1$이고 $k = 3v$라 하자. F_{3^m}에서 $x^{3u-1} + ax^{3v} + b = 0$이므로

$$x^{3u} \cdot x^{-1} = -ax^{3v} - b$$

이다. 따라서 $x^{-1/3} = -ax^{v-u} - bx^{-u}$.

그러므로

$$x^{2/3} = x^{-1/3} \cdot x = -a(x^{v-u+1} + bx^{-u+1}). \quad (17)$$

식 (17)로부터

$$x^{1/3} \cdot x = (-a(x^{v-u+1} + bx^{-u+1}))^2 = x^{2v-2u+2} + x^{-2u+2} - bx^{v-2u+2}$$

가 된다. 그러므로

$$x^{1/3} = x^{2v-2u+1} + x^{-2u+1} - bx^{v-2u+1}. \quad (18)$$

따름정리 4. $f(x) = x^m + ax^k + b$ ($a, b \in F_3$)가 F_3위의 삼항 기약다항식이고 $m \equiv -1 \pmod 3$, $k \equiv 0 \pmod 3$ 이라 하면 $\gamma \in \{3u-2, 3u-1\}$.

증명. 식 (17)과 (18)로부터 다음의 식 (19)를 얻을 수 있다.

$$C^{1/3} = \sum_{i=0}^{u-1-\sigma_1} c_{3i+\theta} x^{(i-t)} + (x^{2v-2u+1} + x^{-2u+1} - bx^{v-2u+1}) \sum_{i=-\sigma_1}^{u-1-\sigma_2} c_{3i+[\theta+1]} x^{(i-t)} - a(x^{v-u+1} + bx^{-u+1}) \sum_{i=-\sigma_2}^{u-2} c_{3i+[\theta+2]} x^{(i-t)}. \quad (19)$$

식 (19)로부터 $C^{1/3}$의 최소 차수는 $-2u+1-\sigma_1-t$이고 최대 차수는 $u-1-\sigma_1-t$임을 알 수 있다. 그러므로 식 (20)을 만족하면 식 (19)에서 더 이상의 모듈로 감산 연산은 필요하지 않게 된다.

$$\begin{cases} -2u+1-\sigma_1-t \geq -3t-\theta, \\ u-1-\sigma_1-t \leq 3u-2-(3t+\theta). \end{cases} \quad (20)$$

식 (20)으로부터 $t = (2u+1+\sigma_1-\theta)/2$를 구할 수 있고, 이 때, (t, θ) 쌍은 $(u-1, 1)$과 $(u-1, 2)$가 될 수 있다. 그러므로 γ은 $3u-1$나 $3u-2$이 된다.

IV. 비교 및 결론

본 논문에서는 SPB를 기저로 하여 $wt(x^{1/3})$와 $wt(x^{2/3})$를 낮출 수 있음을 보였다. 〔표 1〕은 기존 결과 〔4〕와 본 논문의 결과를 비교한 표이다. 〔표 2〕만으로는 PB를 기저로 한 $wt(x^{1/3})$와 SPB를 기저로 한 $wt(x^{1/3})$를 비교하는 것이 쉽지 않으므로, $m \in [2, 56]$인 삼항 기약다항식에 대하여 이들을 비교하여 〔표 2〕에 표현하였다. PB를 기저로 한 $wt(x^{1/3})$와 비교하여 보다 좋은 결과를 굵게 표현하였다. 〔표 2〕를 통하여 기존 결과 〔4〕 보다 SPB를 기저로 한 $wt(x^{1/3})$가 훨씬 효율적임을 알 수 있다. 또한, 3장의 따름정리에서

〔표 2〕 $2 \le m \le 56$이고 $m \neq \pm k \pmod 3$인 삼항 기약다항식의 $wt(x^{1/3})$ 비교표

Irreducible trinomial	PB[4]	SPB	Irreducible trinomial	PB[4]	SPB	Irreducible trinomial	PB[4]	SPB
$x^3 - x^1 \pm 1$	2	2	$x^{23} - x^{15} + 1$	6	**3**	$x^{39} + x^{26} - 1$	3	3
$x^3 - x^2 + 1$	3	3	$x^{23} - x^{18} + 1$	6	**3**	$x^{39} - x^{32} + 1$	5	**3**
$x^3 + x^2 - 1$	3	3	$x^{23} + x^{18} - 1$	6	**3**	$x^{39} + x^{32} - 1$	5	**3**
$x^4 \pm x^3 - 1$	3	**2**	$x^{24} \pm x^4 - 1$	3	**2**	$x^{40} \pm x^3 - 1$	11	**2**
$x^6 \pm x^1 - 1$	2	2	$x^{24} \pm x^{20} - 1$	5	**3**	$x^{40} \pm x^{15} - 1$	4	**2**
$x^6 - x^2 + 1$	**2**	3	$x^{25} - x^3 \pm 1$	8	**2**	$x^{40} \pm x^{27} - 1$	4	**2**
$x^6 - x^4 + 1$	3	**2**	$x^{25} - x^6 + 1$	5	**2**	$x^{40} \pm x^{30} - 1$	2	2
$x^6 \pm x^5 - 1$	5	**3**	$x^{25} - x^6 + 1$	5	**2**	$x^{40} \pm x^{39} - 1$	3	**2**
$x^8 \pm x^3 - 1$	8	**3**	$x^{26} - x^{12} + 1$	8	**3**	$x^{42} \pm x^7 - 1$	3	**2**
$x^8 \pm x^6 - 1$	4	**3**	$x^{26} - x^{18} + 1$	6	**3**	$x^{42} - x^{10} + 1$	3	**2**
$x^9 - x^4 + 1$	3	**2**	$x^{26} - x^{24} + 1$	6	**3**	$x^{42} - x^{32} + 1$	5	**3**
$x^9 + x^4 - 1$	3	**2**	$x^{27} - x^7 \pm 1$	3	**2**	$x^{42} \pm x^{35} - 1$	5	**3**
$x^9 - x^5 \pm 1$	4	**3**	$x^{27} + x^{20} - 1$	5	**3**	$x^{44} \pm x^3 - 1$	32	**3**
$x^{11} - x^3 \pm 1$	10	**3**	$x^{27} - x^{20} + 1$	5	**3**	$x^{45} - x^{17} \pm 1$	4	**3**
$x^{11} - x^9 \pm 1$	6	**3**	$x^{28} \pm x^{15} - 1$	4	**2**	$x^{45} - x^{28} + 1$	3	**2**
$x^{12} \pm x^2 - 1$	4	**3**	$x^{30} \pm x^1 - 1$	2	2	$x^{45} + x^{28} - 1$	3	**2**
$x^{12} \pm x^{10} - 1$	3	**2**	$x^{30} - x^4 + 1$	3	**2**	$x^{46} - x^6 + 1$	8	**2**
$x^{13} - x^6 + 1$	4	**2**	$x^{30} - x^{14} + 1$	4	**3**	$x^{46} - x^{30} + 1$	4	**2**
$x^{13} + x^6 - 1$	4	**2**	$x^{30} - x^{16} + 1$	3	**2**	$x^{46} - x^{36} + 1$	4	**2**
$x^{13} - x^9 \pm 1$	4	**2**	$x^{30} - x^{26} + 1$	5	**3**	$x^{47} - x^{15} \pm 1$	10	**3**
$x^{13} + x^{12} - 1$	3	**2**	$x^{30} \pm x^{29} - 1$	5	**3**	$x^{48} \pm x^8 - 1$	4	**3**
$x^{13} - x^{12} + 1$	3	**2**	$x^{32} \pm x^{12} - 1$	8	**3**	$x^{48} \pm x^{40} - 1$	3	**2**
$x^{15} - x^2 + 1$	4	**3**	$x^{32} \pm x^{18} - 1$	7	**3**	$x^{50} - x^6 + 1$	20	**3**
$x^{15} + x^2 - 1$	4	**3**	$x^{32} \pm x^{24} - 1$	4	**3**	$x^{50} - x^{12} + 1$	12	**3**
$x^{15} - x^7 \pm 1$	3	**2**	$x^{32} \pm x^{27} - 1$	6	**3**	$x^{51} - x^1 \pm 1$	2	2
$x^{15} - x^8 + 1$	4	**3**	$x^{33} - x^{28} + 1$	3	**2**	$x^{51} - x^{50} + 1$	5	**3**
$x^{15} + x^8 - 1$	4	**3**	$x^{35} - x^{18} + 1$	7	**3**	$x^{51} + x^{50} - 1$	5	**3**
$x^{15} - x^{13} \pm 1$	3	**2**	$x^{35} + x^{18} - 1$	7	**3**	$x^{52} \pm x^9 - 1$	6	**2**
$x^{16} \pm x^9 - 1$	4	**2**	$x^{35} - x^{33} \pm 1$	6	**3**	$x^{52} \pm x^{15} - 1$	5	**2**
$x^{16} \pm x^{12} - 1$	2	**2**	$x^{36} \pm x^{14} - 1$	4	**3**	$x^{52} \pm x^{27} - 1$	4	**2**
$x^{18} \pm x^7 - 1$	3	**2**	$x^{36} \pm x^{22} - 1$	3	**2**	$x^{52} \pm x^{45} - 1$	4	**2**
$x^{18} - x^8 + 1$	4	**3**	$x^{37} - x^6 + 1$	6	**2**	$x^{54} \pm x^1 - 1$	2	2
$x^{18} - x^{10} + 1$	3	**2**	$x^{37} + x^6 - 1$	6	**2**	$x^{54} \pm x^{13} - 1$	3	**2**
$x^{18} \pm x^{11} - 1$	5	**3**	$x^{37} - x^{12} + 1$	4	**2**	$x^{54} - x^{14} + 1$	4	**3**
$x^{20} \pm x^{15} - 1$	4	**3**	$x^{37} + x^{12} - 1$	4	**2**	$x^{54} - x^{40} + 1$	3	**2**
$x^{21} - x^5 \pm 1$	4	**3**	$x^{37} - x^{15} \pm 1$	4	**2**	$x^{54} \pm x^{41} - 1$	5	**3**
$x^{21} - x^{16} + 1$	3	**2**	$x^{37} - x^{24} + 1$	4	**2**	$x^{54} \pm x^{53} - 1$	5	**3**
$x^{21} + x^{16} - 1$	3	**2**	$x^{37} + x^{24} - 1$	4	**2**	$x^{56} \pm x^3 - 1$	40	**3**
$x^{22} - x^6 + 1$	5	**2**	$x^{39} - x^7 \pm 1$	3	**2**	$x^{56} \pm x^{30} - 1$	7	**3**
$x^{22} - x^{18} + 1$	4	**2**	$x^{39} - x^{13} \pm 1$	2	2	$x^{56} \pm x^{51} - 1$	6	**3**
$x^{23} - x^3 \pm 1$	18	**3**	$x^{39} - x^{26} + 1$	3	3			

제공한 γ를 적용한 SPB를 기저로 하면 더 이상의 모듈로 감산 연산은 필요없게 된다.

참고문헌

〔1〕 H. Fan and Y. Dai, "Fast Bit-Parallel $GF(2^n)$ Multiplier for All Trinomials," *IEEE Transactions on Computers*, vol.54, no. 4, pp.485-490, April 2005.

〔2〕 I. Duursma and H. S. Lee, "Tate pairing implementation for hyperelliptic curves $y^2 = x^p - x + d$," *Advances in Cryptology. ASIACRYPT 2003, Lecture Notes in Computer Science*, vol. 2894, Springer, Berlin, pp. 111-123, 2003.

〔3〕 J. Beuchat, N. Brisebarre, J. Detrey, E. Okamoto, M. Shirase and T. Takagi. "Algorithms and arithmetic operators for computing the η_T pairing in characteristic three," *IEEE Transactions on Computers, Special Section on Special-Purpose Hardware for Cryptography and Cryptanalysis*,

vol. 57, no. 11, IEEE Computer Society, November 2008.

〔4〕 O. Ahmadi, D. Hankerson and A. Menezes, "Formulas for cube roots in F_{3^m}," *Elsevier Discrete Applied Mathematics* 155, pp.260-270, 2007.

〔5〕 P. S. L. M. Barreto, "A note on efficient computation of cube roots in characteristic 3," *Cryptology ePrint Archive: Report 2004/305*, 2004.

〔6〕 P. S. L. M. Barreto, H. Y. Kim, B. Lynn and M. Scott, "Efficient algorithms for pairing-based cryptosystems," *Advances in Cryptology. CRYPTO 2002, Lecture Notes in Computer Science*, vol. 2442, Springer, Berlin, pp. 354-368, 2002.

〔7〕 P. S. L. M. Barreto, S. D. Galbraith, C. Ó hÉigeartaigh and M. Scott, "Efficient pairing computation on supersingular abelian varieties," *Des. Codes Cryptography 42*, pp. 239-271, 2007.

〈著者紹介〉

조 영 인 (Young In Cho) 학생회원
2006년 2월: 한양대학교 수학과 이학사
2009년 2월: 고려대학교 정보보호 대학원 공학석사
2009년 9월 ~ 현재: 고려대학교 정보보호 대학원 박사과정
〈관심분야〉 페어링 암호, 암호칩 설계 기술, 부채널 공격, 공개키 암호 알고리즘

장 남 수 (Nam Su Chang) 학생회원
2002년 2월: 서울 시립대학교 수학과 이학사
2004년 8월: 고려대학교 정보보호 대학원 공학석사
2009년 8월: 고려대학교 정보경영공학전문대학원 공학박사
〈관심분야〉 암호칩 설계 기술, 부채널 공격, 공개키 암호 알고리즘, 공개키 암호 암호분석

김 창 한 (Chang Han Kim) 종신회원
1985년 2월: 고려대학교 수학과 학사
1987년 2월: 고려대학교 수학과 석사
1992년 2월: 고려대학교 수학과 박사
1992년 3월 ~ 현재: 세명대학교 정보통신학부 교수
〈관심분야〉 정수론, 공개키암호, 암호프로토콜

박 영 호 (Young-Ho Park) 종신회원
1990년 2월: 고려대학교 수학과 이학사
1993년 2월: 고려대학교 수학과 이학석사
1997년 2월: 고려대학교 수학과 이학박사
2002년 3월 ~ 현재: 세종 사이버 대학교 부교수
〈관심분야〉 정수론, 공개키 암호, 암호 프로토콜, 부채널 공격

홍 석 희 (Seokhie Hong) 종신회원
1995년 2월: 고려대학교 수학과 학사
1997년 2월: 고려대학교 수학과 석사
2001년 2월: 고려대학교 수학과 박사
1999년 8월 ~ 2004년 2월: (주)시큐리티 테크놀로지스 선임연구원
2003년 3월 ~ 2004년 2월: 고려대학교 시간강사
2004년 4월 ~ 2005년 2월: K.U. Leuven 박사후연구원
2005년 3월 ~ 현재: 고려대학교 정보경영전문대학원 부교수
〈관심분야〉 대칭키 암호 알고리즘, 공개키 암호 알고리즘, 포렌식