

	(19) 대한민국특허청(KR) (12) 공개특허공보(A)	(11) 공개번호 10-2012-0020995 (43) 공개일자 2012년03월08일
(51) 국제특허분류(Int. Cl.) G06F 17/10 (2006.01) G06F 7/52 (2006.01) (21) 출원번호 10-2010-0084986 (22) 출원일자 2010년08월31일 심사청구일자 2010년08월31일		(71) 출원인 고려대학교 산학협력단 서울 성북구 안암동5가 1 (72) 발명자 홍석희 서울특별시 도봉구 마들로 859-19, 한신아파트 103동 107호 (도봉동) 조영인 서울특별시 강동구 올림픽로77길 46, 301호 (천호동) (뒷면에 계속) (74) 대리인 특허법인충현

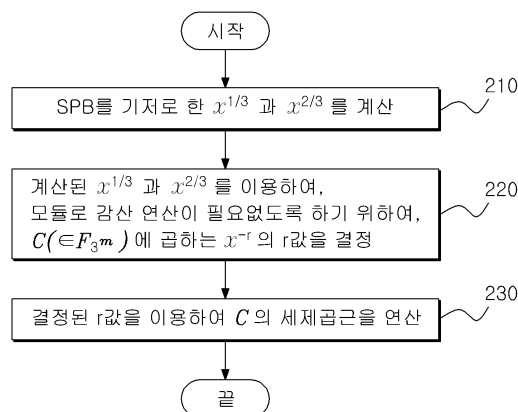
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 **페어링 암호 연산을 위한 세제곱근 연산 방법**

(57) 요약

본 발명은 F_{3^m} 에서의 세제곱근 연산방법에 관한 것으로서, $C \in F_{3^m}$ 에 대하여, SPB를 기저로 한 $C^{1/3}$ 의 $x^{1/3}$ 과 $x^{2/3}$ 를 계산하는 단계; 및 계산된 $x^{1/3}$ 과 $x^{2/3}$ 를 이용하여 $C^{1/3}$ 를 계산하는 경우, 모듈로 감산 연산이 필요없도록 SPB를 사용할 때 C에 곱해지는 x^{-r} 의 r값을 결정하여, C의 세제곱근을 연산하는 단계를 포함하는 것을 특징으로 하며, 세제곱근 연산의 효율성을 결정하는 $x^{1/3}$ 의 헤밍웨이트가 기존의 결과에 비해 거의 모든 경우에 대하여 감소하여 세제곱근 연산을 효율적으로 수행할 수 있고, SPB를 이용함으로써, F_{3^m} 에서의 세제곱근 연산 시 다항식 곱셈 횟수가 현저하게 줄어들었으며, 특정 SPB를 선정하여 모듈러 감산 연산을 제거하여 세제곱근 연산량이 더욱 줄어들도록 할 수 있다.

대표도 - 도2



(72) 발명자

장남수

서울특별시 마포구 월드컵북로27길 16, 2층 (성산동)

김창한

서울특별시 강남구 삼성로 212, 21동 507호 (대치동, 은마아파트)

특허청구의 범위

청구항 1

$f(x)=x^m+ax^k+b(a,b\in F_3)$ 가 $F_3[x]$ 의 삼항 기약다항식이고, $F_{3^m}=F_3[x]/(f(x))$ 이라 할 때, F_{3^m} 에서의 세제곱근 연산 방법에 있어서,

$C\in F_{3^m}$ 에 대하여, SPB(Shifted Polynomial Basis)를 기저로 한 $C^{1/3}$ 의 $x^{1/3}$ 과 $x^{2/3}$ 를 상기 m과 k에 따라 계산하는 단계; 및

상기 계산된 $x^{1/3}$ 과 $x^{2/3}$ 를 이용하여 상기 $C^{1/3}$ 를 계산하는 경우, 모듈로 감산 연산이 필요없도록 상기 SPB를 사용할 때 상기 C에 곱해지는 x^{-r} 의 r값을 결정하여, 상기 C의 세제곱근을 연산하는 단계를 포함하는 것을 특징으로 하는 F_{3^m} 에서의 세제곱근 연산방법.

청구항 2

제 1 항에 있어서,

상기 $m\equiv 0(\text{mod } 3)$, 상기 $k\equiv 1(\text{mod } 3)$ 이고, 임의의 양수 u와 v에 대하여($u>v$) $m=3u$ 이고, $k=3v+1$ 이라 하면, 상기 r값은 $3v$ 또는 $3v+1$ 인 것을 특징으로 하는 F_{3^m} 에서의 세제곱근 연산방법.

청구항 3

제 1 항에 있어서,

상기 $m\equiv 0(\text{mod } 3)$, 상기 $k\equiv -1(\text{mod } 3)$ 이고, 임의의 양수 u와 v에 대하여($u\geq v$) $m=3u$ 이고, $k=3v-1$ 이라 하면, 상기 r값은 $3v-2$ 또는 $3v-1$ 인 것을 특징으로 하는 F_{3^m} 에서의 세제곱근 연산방법.

청구항 4

제 1 항에 있어서,

상기 $m\equiv 1(\text{mod } 3)$, 상기 $k\equiv 0(\text{mod } 3)$ 이고, 임의의 양수 u와 v에 대하여($u\geq v$) $m=3u+1$ 이고, $k=3v$ 이라 하면, 상기 r값은 $3u$ 또는 $3u+1$ 인 것을 특징으로 하는 F_{3^m} 에서의 세제곱근 연산방법.

청구항 5

제 1 항에 있어서,

상기 $m\equiv -1(\text{mod } 3)$, 상기 $k\equiv 0(\text{mod } 3)$ 이고, 임의의 양수 u와 v에 대하여($u>v$) $m=3u-1$ 이고, $k=3v$ 이라 하면, 상기 r값은 $3u-2$ 또는 $3u-1$ 인 것을 특징으로 하는 F_{3^m} 에서의 세제곱근 연산방법.

청구항 6

$C\in F_{3^m}$ 에 대하여, SPB를 기저로 한 $C^{1/3}$ 의 $x^{1/3}$ 과 $x^{2/3}$ 를 계산하는 단계; 및

상기 계산된 $x^{1/3}$ 과 $x^{2/3}$ 를 이용하여 상기 $C^{1/3}$ 를 계산하는 경우, 모듈로 감산 연산이 필요없도록 상기 SPB를 사용할 때 상기 C에 곱해지는 x^{-r} 의 r값을 결정하여, 상기 C의 세제곱근을 연산하는 단계를 포함하는 것을 특징으로 하는 F_{3^m} 에서의 세제곱근 연산방법.

청구항 7

제 6 항에 있어서,

상기 $x^{1/3}$ 과 상기 $x^{2/3}$ 의 계수들의 개수를 각각의 해밍 웨이트라고 할 때, 상기 SPB를 기저로 하는 경우 상기 해밍 웨이트가 최소가 되는 것을 특징으로 하는 F_{3^m} 에서의 세제곱근 연산방법.

청구항 8

$C \in F_{3^m}$ 에 대하여, SPB를 기저로 한 $C^{1/3}$ 의 $x^{1/3}$ 과 $x^{2/3}$ 를 계산하는 단계; 및

상기 계산된 $x^{1/3}$ 과 $x^{2/3}$ 를 이용하여 상기 $C^{1/3}$ 를 계산하는 경우, 모듈로 감산 연산이 필요없도록 상기 SPB를 사용할 때, 상기 C에 곱해지는 x^{-r} 의 r값을 결정하여, 상기 C의 세제곱근을 연산하는 단계를 포함하는 것을 특징으로 하는 F_{3^m} 에서의 페어링 암호 연산 방법.

청구항 9

제 1 항 내지 제 8 항 중에 어느 한 항의 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 10

SPB를 기저로 한 F_{3^m} 에 속하는 다항식 C를 생성하는 SPB 기저 생성부;

상기 생성한 다항식 C에 대하여 세제곱근 식을 생성하는 세제곱근 생성부;

상기 세제곱근 식에 대하여 모듈로 감산 연산이 필요하지 않도록 하는 상기 SPB의 x^{-r} 을 결정하는 시프트 베이스 결정부; 및

상기 결정된 x^{-r} 을 이용하여 상기 C의 세제곱근을 연산하는 세제곱근 연산부를 포함하는 것을 특징으로 하는 F_{3^m} 에서의 세제곱근 연산장치.

명세서

기술분야

- [0001] 본 발명은 $F_{(3^m)}$ (이하 F_{3^m} 으로 표기한다)에서의 세제곱근 연산 방법에 관한 것으로, 더욱 상세하게는 $x^{1/3}$ 의 해밍웨이트가 기존의 결과에 비해 거의 모든 경우에 대하여 감소하고, 모듈로 감산 연산이 필요없는 F_{3^m} 에서의 세제곱근 연산 방법에 관한 것이다.

배경기술

- [0002] 페어링 암호 기반의 암호 프로토콜 구현을 위하여 F_{3^m} 위의 초특이 타원곡선이 매우 적합한 것으로 연구되었고 이에 따라 F_{3^m} 에서의 효율적인 유한체 연산에 대한 연구가 최근 주목을 받고 있다. 특히 초특이 타원곡선 위의 페어링 암호 알고리즘 중 F_{3^m} 위에서의 n_T 페어링의 계산을 위하여 F_{3^m} 위에서의 세제곱근 연산이 필요하다.

- [0003] <선행기술문헌>

- [0004] <비특허문헌>

- [0005] [문헌 1] O. Ahmadi, D. Hankerson and A. Menezes, "Formulas for cube roots in F_{3^m} ", Elsevier Discrete Applied Mathematics 155, pp.260-270, 2007.

발명의 내용

해결하려는 과제

- [0006] 따라서, 본 발명이 해결하고자 하는 첫 번째 과제는 $x^{1/3}$ 의 해밍웨이트가 감소하여 F_{3^m} 에서의 세제곱근 연산을 보다 효율적으로 할 수 있으며, 모듈로 감산 연산이 필요없는 F_{3^m} 에서의 세제곱근 연산방법을 제공하는 것이다.
- [0007] 본 발명이 해결하고자 하는 두 번째 과제는 $x^{1/3}$ 의 해밍웨이트가 감소하여 F_{3^m} 에서의 세제곱근 연산을 보다 효율적으로 할 수 있으며, 모듈로 감산 연산이 필요없는 F_{3^m} 에서의 세제곱근 연산장치를 제공하는 것이다.
- [0008] 또한, 상기된 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록 매체를 제공하는데 있다.

과제의 해결 수단

- [0009] 본 발명은 상기 첫 번째 과제를 달성하기 위하여, $f(x)=x^m+ax^k+b(a,b\in F_3)$ 가 $F_3[x]$ 의 삼항 기약다항식이고, $F_{3^m}=F_3[x]/(f(x))$ 이라 할 때, F_{3^m} 에서의 세제곱근 연산방법에 있어서, $C\in F_{3^m}$ 에 대하여, SPB(Shifted Polynomial Basis)를 기저로 한 $C^{1/3}$ 의 $x^{1/3}$ 과 $x^{2/3}$ 를 상기 m과 k에 따라 계산하는 단계; 및 상기 계산된 $x^{1/3}$ 과 $x^{2/3}$ 를 이용하여 상기 $C^{1/3}$ 를 계산하는 경우, 모듈로 감산 연산이 필요없도록 상기 SPB를 사용할 때 상기 C에 곱해지는 x^{-r} 의 r값을 결정하여, 상기 C의 세제곱근을 연산하는 단계를 포함하는 F_{3^m} 에서의 세제곱근 연산방법을 제공한다.
- [0010] 본 발명의 일 실시예에 의하면, 상기 $m\equiv 0(\text{mod } 3)$, 상기 $k\equiv 1(\text{mod } 3)$ 이고, 임의의 양수 u와 v에 대하여($u>v$) $m=3u$ 이고, $k=3v+1$ 이라 하면, 상기 r값은 $3v$ 또는 $3v+1$ 인 것이 바람직하다.
- [0011] 또한, 상기 $m\equiv 0(\text{mod } 3)$, 상기 $k\equiv -1(\text{mod } 3)$ 이고, 임의의 양수 u와 v에 대하여($u\geq v$) $m=3u$ 이고, $k=3v-1$ 이라 하면, 상기 r값은 $3v-2$ 또는 $3v-1$ 인 것이 바람직하다.
- [0012] 또한, 상기 $m\equiv 1(\text{mod } 3)$, 상기 $k\equiv 0(\text{mod } 3)$ 이고, 임의의 양수 u와 v에 대하여($u\geq v$) $m=3u+1$ 이고, $k=3v$ 이라 하면, 상기 r값은 $3u$ 또는 $3u+1$ 인 것이 바람직하다.
- [0013] 또한, 상기 $m\equiv -1(\text{mod } 3)$, 상기 $k\equiv 0(\text{mod } 3)$ 이고, 임의의 양수 u와 v에 대하여($u>v$) $m=3u-1$ 이고, $k=3v$ 이라 하면, 상기 r값은 $3u-2$ 또는 $3u-1$ 인 것이 바람직하다.
- [0014] 본 발명의 다른 실시예에 의하면, $C\in F_{3^m}$ 에 대하여, SPB를 기저로 한 $C^{1/3}$ 의 $x^{1/3}$ 과 $x^{2/3}$ 를 계산하는 단계; 및 상기 계산된 $x^{1/3}$ 과 $x^{2/3}$ 를 이용하여 상기 $C^{1/3}$ 를 계산하는 경우, 모듈로 감산 연산이 필요없도록 상기 SPB를 사용할 때 상기 C에 곱해지는 x^{-r} 의 r값을 결정하여, 상기 C의 세제곱근을 연산하는 단계를 포함하는 F_{3^m} 에서의 세제곱근 연산방법을 제공한다.
- [0015] 이때, 상기 $x^{1/3}$ 과 상기 $x^{2/3}$ 의 계수들의 개수를 각각의 해밍 웨이트라고 할 때, 상기 SPB를 기저로 하는 경우 상기 해밍 웨이트가 최소가 될 수 있다.
- [0016] 본 발명은 상기 두 번째 과제를 달성하기 위하여, SPB를 기저로 한 F_{3^m} 에 속하는 다항식 C를 생성하는 SPB 기저 생성부; 상기 생성한 다항식 C에 대하여 세제곱근 식을 생성하는 세제곱근 생성부; 상기 세제곱근 식에 대하여 모듈로 감산 연산이 필요하지 않도록 하는 상기 SPB의 x^{-r} 을 결정하는 시프트 베이스 결정부; 및 상기 결정된 x^{-r} 을 이용하여 상기 C의 세제곱근을 연산하는 세제곱근 연산부를 포함하는 F_{3^m} 에서의 세제곱근 연산장치를 제공한다.
- [0017] 상기 다른 기술적 과제를 해결하기 위하여, 본 발명은 상기된 F_{3^m} 에서의 세제곱근 연산방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록 매체를 제공한다.

발명의 효과

[0018] 본 발명에 따르면, 세제곱근 연산의 효율성을 결정하는 $x^{1/3}$ 의 해밍웨이트가 기존의 결과에 비해 거의 모든 경우에 대하여 감소하여 세제곱근 연산을 효율적으로 수행할 수 있다. 또한, 본 발명에 따르면, SPB를 이용함으로써, F_3^m 에서의 세제곱근 연산 시 다항식 곱셈 횟수가 현저하게 줄어들었으며, 특정 SPB를 선정하여 모듈로 감산 연산을 제거하여 세제곱근 연산량이 더욱 줄어들도록 할 수 있다.

도면의 간단한 설명

[0019] 도 1은 본 발명의 바람직한 일 실시예에 따른 F_3^m 에서의 세제곱근 연산장치의 구성도이다.

도 2는 본 발명의 바람직한 일 실시예에 따른 F_3^m 에서의 세제곱근 연산 방법의 흐름도이다.

도 3은 PB와 SPB에 대하여 $2 \leq m \leq 56$ 이고, $m \neq \pm k \pmod{3}$ 인 삼항 기약다항식의 $\text{wt}(x^{1/3})$ 비교표를 나타낸 것이다.

발명을 실시하기 위한 구체적인 내용

[0020] 본 발명에 관한 구체적인 내용의 설명에 앞서 이해의 편의를 위해 본 발명이 해결하고자 하는 과제의 해결 방안의 개요 혹은 기술적 사상의 핵심을 우선 제시한다.

[0021] 본 발명의 일 실시예에 따른 F_3^m 에서의 세제곱근 연산방법은 $C \in F_3^m$ 에 대하여, SPB를 기저로 한 $C^{1/3}$ 의 $x^{1/3}$ 과 $x^{2/3}$ 를 계산하는 단계; 및 상기 계산된 $x^{1/3}$ 과 $x^{2/3}$ 를 이용하여 상기 $C^{1/3}$ 를 계산하는 경우, 모듈로 감산 연산이 필요없도록 상기 SPB를 사용할 때 상기 C에 곱해지는 x^{-r} 의 r값을 결정하여, 상기 C의 세제곱근을 연산하는 단계를 포함한다.

[0022] 이하, 바람직한 실시예를 들어 본 발명을 더욱 상세하게 설명한다. 그러나 이들 실시예는 본 발명을 보다 구체적으로 설명하기 위한 것으로, 본 발명의 범위가 이에 의하여 제한되지 않는다는 것은 당업계의 통상의 지식을 가진 자에게 자명할 것이다. 본 발명이 해결하고자 하는 과제의 해결 방안을 명확하게 하기 위한 발명의 구성을 본 발명의 바람직한 실시예에 근거하여 첨부 도면을 참조하여 상세히 설명한다. 아울러 본 발명과 관련된 공지 기능 혹은 구성에 대한 구체적인 설명 그리고 그 이외의 제반 사항이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우, 그 상세한 설명을 생략한다.

[0023] F_3^m 에서의 Tate 페어링 또는 n_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 해밍웨이트라 할 때, 이 해밍웨이트가 세제곱근 연산의 효율성을 결정하게 된다. 문헌 1에서는 $f(x)=x^m+ax^k+b(a,b \in F_3)$ 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 해밍웨이트를 계산하였다. 본 발명에서는 Shifted Polynomial Basis(SPB)가 기존의 결과보다 $x^{1/3}$ 의 해밍웨이트를 낮출 수 있음을 보이며, 모듈로 감산 연산이 필요없는 가장 적합한 SPB를 제공한다.

[0024] $x^{1/3}$ 와 $x^{2/3}$ 의 해밍 웨이트는 $m \equiv k \pmod{3}$ 일 때 가장 작지만, $m \not\equiv k \pmod{3}$ 일 때는 비효율적이다. 따라서, $(m \pmod{3}, k \pmod{3}) \in \{(0,1), (0,-1), (1,0), (-1,0)\}$ 일 때, F_3^m 에서의 세제곱근 계산방법을 제시하기로 한다. $m \equiv k \pmod{3}$ 일 때의 $x^{1/3}$ 와 $x^{2/3}$ 의 해밍 웨이트와 같은 해밍 웨이트를 갖는 본 발명에서의 세제곱근 계산 방법은 종래 계산 방법보다 더 효과적임을 알 수 있다.

[0025] $f(x)=x^m+ax^k+b(a,b \in F_3)$ 가 $F_3[x]$ 의 삼항 기약다항식이라 할 때, $F_3^m=F_3[x]/(f)$ 라 하자. 이하에서 F_3^m 에서의 세제곱근 연산을 살펴보도록 한다.

[0026] 우선 임의의 자연수 u에 대하여 $m=3u$ 라 하자. ($m \equiv \pm 1 \pmod{3}$ 인 경우도 유사하게 적용할 수 있다.) 그러면 $C \in F_3^m$

에 대하여 다음의 수학적 식 1과 같이 표현된다.

수학적 식 1

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

수학적 식 1을 이용하여 C의 세제곱 연산식은 다음의 수학적 식 2와 같다.

수학적 식 2

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

$x^{1/3}$ 과 $x^{2/3}$ 가 사전계산되었다면, 수학적 식 2를 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.

$m \equiv k \pmod{3}$ 경우 $x^{1/3}$ 과 $x^{2/3}$ 의 다항식 표현이 매우 작은 개수의 항을 가지므로 가장 효율적으로 세제곱을 연산할 수 있다. 그러나 $m \equiv k \pmod{3}$ 인 형태의 삼항 기약다항식 $f(x) = x^m + ax^k + b$ 은 굉장히 드물게 존재한다. 따라서 $m \not\equiv k \pmod{3}$ 인 형태의 삼항 기약다항식에 대해서 세제곱근을 구할 수 있는 방법에 대한 연구가 필요하게 되었고 문헌 1에서는 이 경우에 대하여 세제곱근 연산식의 $x^{1/3}$ 과 $x^{2/3}$ 의 헤밍웨이트를 계산하였다.

본 발명은 효율적인 세제곱근 연산을 위하여 문헌 1에서의 결과보다도 $x^{1/3}$ 과 $x^{2/3}$ 의 헤밍웨이트를 낮추었다. Polynomial Basis(PB)의 변형된 형태인 SPB는 2005년 $GF(2^n)$ 에서의 곱셈기 설계를 위하여 제안되었다.

본 발명에서는 SPB를 기저로 한 $x^{1/3}$ 과 $x^{2/3}$ 의 다항식 표현이 작은 개수의 항을 갖는다는 것을 발견하여 SPB를 기저로 하여 $x^{1/3}$ 과 $x^{2/3}$ 의 헤밍웨이트를 계산하였다. 또한, 본 발명에서는 가능한 모든 삼항 기약다항식에 대하여 모듈로 감산 연산이 필요없는 SPB를 제공한다. 따라서 본 발명으로 문헌 1에서 제시된 방법보다 훨씬 효율적으로 세제곱근을 연산할 수 있다. 이하에서는 $x^{1/3}$ 의 헤밍 웨이트를 $wt(x^{1/3})$ 로 정의한다.

[$m \equiv k \pmod{3}$ 인 경우]

$f(x) = x^m + ax^k + b$ ($a, b \in F_3$)가 F_3 위의 삼항 기약다항식이고, $m \equiv k \pmod{3}$ 이라 하면, 다음의 수학적 식 3을 만족한다.

수학적 식 3

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

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

[$m \equiv -k \pmod{3}$ 인 경우]

[0039] $f(x)=x^m+ax^k+b(a,b\in F_3)$ 가 F_3 위의 삼약 기약다항식이고, $m\equiv -k(\bmod 3)$ 이라 하면, 다음의 수학식 4을 만족한다.

수학식 4

[0040] $wt(x^{1/3})\in\{(m/e)-2, (m/e)-1, m/e\}$

[0041] 여기서, $e=\gcd(m,k)$ 이고, $\gcd$ 는 최대공약수를 의미한다.

[0042] $m\equiv -k(\bmod 3)$ 인 경우, 문헌 1에서는 $x^{1/3}=\sum_{i=0}^{m-1}c_ix^i$ 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. 본 발명에서는 아래에 해당하는 경우에 대하여 보다 낮은 $wt(x^{1/3})$ 과 $wt(x^{2/3})$ 을 제공한다.

[0043] **[$m\equiv 0(\bmod 3)$, $k\equiv 1(\bmod 3)$ 인 경우]**

[0044] $f(x)=x^m+ax^k+b(a,b\in F_3)$ 가 F_3 위의 삼약 기약다항식이고, $m\equiv 0(\bmod 3)$, $k\equiv 1(\bmod 3)$ 이라 하면, 다음의 수학식 5를 만족한다.

수학식 5

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

[0046] **[$m\equiv 0(\bmod 3)$, $k\equiv -1(\bmod 3)$ 인 경우]**

[0047] $f(x)=x^m+ax^k+b(a,b\in F_3)$ 가 F_3 위의 삼약 기약다항식이고, $m\equiv 0(\bmod 3)$, $k\equiv -1(\bmod 3)$ 이라 하면, $wt(x^{1/3})\leq 5$ 이다.

[0048] $f(x)=x^m+ax^k+b(a,b\in F_3)$ 가 F_3 위의 삼약 기약다항식이라면, 다음의 수학식 6을 만족한다.

수학식 6

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

[0050] 이때, $p=\lceil (m-1)/3k \rceil + \lceil (m-1-k)/3k \rceil$ 이고, $q=\lceil (2m-1)/3k \rceil + \lceil (2m-1-k)/3k \rceil + \lceil (2m-1-2k)/3k \rceil$ 이다.

[0051] 수학식 6으로부터 k 가 클수록 낮은 $wt(x^{1/3})$ 를 얻을 수 있음을 알 수 있다. 그러나 큰 k 를 갖는 삼항 기약다항식은 일반적으로 모듈로 감산 연산이 많이 필요하게 된다. 따라서 수학식 6의 경우에 낮은 $wt(x^{1/3})$ 를 얻는다 해도 추가적인 모듈로 감산이 많아 질 수 있다.

[0052] 따라서, 이하에서는 $m\neq \pm k(\bmod 3)$ 인 경우에 대하여 $wt(x^{1/3})$ 과 $wt(x^{2/3})$ 을 계산하고 모듈로 감산 연산이 필요없

는 가장 적합한 SPB를 찾는다.

[0053] [정의 1]

[0054] r 을 임의의 정수라 하고 집합 $S=\{x^i \mid 0 \leq i \leq m-1\}$ 를 F_3 위의 PB라 할 때, 집합 $x^{-r}S:=\{x^{i-r} \mid 0 \leq i \leq m-1\}$ 을 S 의 SPB라 한다.

[0055] 문헌 1에서는 추가적인 모듈로 감산 연산이 필요했다. 예를 들어, 수학식 5의 $m \equiv 0 \pmod{3}$, $k \equiv 1 \pmod{3}$ 인 경우인 삼항 기약다항식에 대하여 수학식 2에서 $x^{1/3}$ 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 degree는 $4u-v-1$ 가 되고 $4u-v-1 > 3u(=m)$ 이므로 추가적인 모듈로 감산 연산이 필요하게 된다. 다른 모든 경우에 대해서도 같은 이유로 모듈로 감산 연산이 필요하다.

[0056] 따라서 본 발명에서는 문헌 1에서와 달리 $C^{1/3}$ 계산시 모듈로 감산 연산이 필요 없도록 정의 1의 r 을 결정한다. 이와 같은 r 을 γ 로 정의하고 식 전개 편의를 위하여 임의의 정수 t 와 $\theta \in \{0, 1, 2\}$ 에 대하여 r 대신에 $3t+\theta$ 을 대입한다.

[0057] 1. $m \equiv 0 \pmod{3}$ 인 경우

[0058] SPB를 기저로 하여 C 를 간결하게 표현하기 위하여 아래의 함수를 정의한다.

[0059]
$$\sigma_j(j=1, 2) = \begin{cases} 0 & [\theta+j] < 3 \\ 1 & [\theta+j] \geq 3 \end{cases}$$

[0060] 수학식 1와 정의 1로부터 SPB를 기저로 한 C 의 다항식 표현은 다음의 수학식 7과 같다.

수학식 7

[0061]
$$\begin{aligned} C &= x^{-r} \sum_{i=0}^{3u-1} c_i x^i \\ &= \sum_{i=0}^{u-1} c_{3i+\theta} x^{3i+\theta-(3t+\theta)} + x \sum_{i=-\sigma_1}^{u-1-\sigma_1} c_{3i+[\theta+1]} x^{3i+\theta-(3t+\theta)} + x^2 \sum_{i=-\sigma_2}^{u-1-\sigma_2} c_{3i+[\theta+2]} x^{3i+\theta-(3t+\theta)} \\ &= \sum_{i=0}^{u-1} c_{3i+\theta} x^{3(i-t)} + x \sum_{i=-\sigma_1}^{u-1-\sigma_1} c_{3i+[\theta+1]} x^{3(i-t)} + x^2 \sum_{i=-\sigma_2}^{u-1-\sigma_2} c_{3i+[\theta+2]} x^{3(i-t)} \end{aligned}$$

[0062] 따라서 수학식 7로부터 C 의 세제곱근 연산식은 다음의 수학식 8과 같다.

수학식 8

[0063]
$$C^{1/3} = \sum_{i=0}^{u-1} c_{3i+\theta} x^{(i-t)} + x^{1/3} \sum_{i=-\sigma_1}^{u-1-\sigma_1} c_{3i+[\theta+1]} x^{(i-t)} + x^{2/3} \sum_{i=-\sigma_2}^{u-1-\sigma_2} c_{3i+[\theta+2]} x^{(i-t)}$$

[0064] 이제 SPB를 기저로 하여 $wt(x^{1/3})$ 과 $wt(x^{2/3})$ 을 계산하고 각 경우에 대하여 γ 를 결정한다. 본 발명에서는 $wt(x^{1/3})$ 를 최소화하는데 초점을 맞추고 있으므로 PB에 속하지 않는 항에 대하여 허용한다. 그리고 나서 결과적으로 모듈로 감산이 필요 없는 적합한 SPB를 찾는다.

[0065] $f(x)=x^m+ax^k+b(a,b\in F_3)$ 가 F_3 위의 삼약 기약다항식이고, $m\equiv 0(\bmod 3)$, $k\equiv 1(\bmod 3)$ 이라 하면, $wt(x^{1/3})=2$, $wt(x^{2/3})=3$ 이다.

[0066] 이를 증명하면 다음과 같다.

[0067] 임의의 양수 u 와 v 에 대하여($u>v$) $m=3u$ 이고, $k=3v+1$ 이라 하자. F_{3^m} 에서 $x^{3u}+ax^{3v+1}+b=0$ 이므로 $ax^{3v}x=x^{3u}-b$ 이다.

[0068] 따라서, 다음의 수학적 9와 같다.

수학적 9

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

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

[0069]

[0070] $f(x)=x^m+ax^k+b(a,b\in F_3)$ 가 F_3 위의 삼약 기약다항식이고, $m\equiv 0(\bmod 3)$, $k\equiv 1(\bmod 3)$ 이라 하면, $y\in\{3v, 3v+1\}$ 이다.

[0071] 이를 증명하면 다음과 같다.

[0072] 수학적 9로부터 다음의 수학적 10을 얻을 수 있다.

수학적 10

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

$$+ (x^{2u-2v} + x^{-2v} - bx^{u-2v}) \sum_{i=-\sigma_2}^{u-1-\sigma_2} c_{3i+[\theta+2]} x^{(i-t)}$$

[0073]

[0074] 수학적 10으로부터 $C^{1/3}$ 의 최소 degree는 $-2v-\sigma_2-t$ 이고, 최대 degree는 $3u-2v-1-\sigma_2-t$ 임을 알 수 있다. 그러므로, 다음의 수학적 11을 만족하면, 수학적 10에서 더 이상의 모듈로 감산 연산은 필요하지 않게 된다.

수학적 11

$$\begin{cases} -2v-\sigma_2-t \geq -3t-\theta, \\ 3u-2v-1-\sigma_2-t \leq 3u-1-(3t+\theta) \end{cases}$$

[0075]

[0076] 수학적 11으로부터 $t=(2v+\sigma_2-\theta)/2$ 를 구할 수 있고, 이 때, (t, θ) 쌍은 $(v, 0)$ 과 $(v, 1)$ 가 될 수 있다. 그러므로 y 은 $3v$ 나 $3v+1$ 이 된다.

[0077] $f(x)=x^m+ax^k+b(a,b\in F_3)$ 가 F_3 위의 삼약 기약다항식이고, $m\equiv 0(\bmod 3)$, $k\equiv -1(\bmod 3)$ 이라 하면, $wt(x^{1/3})=3$, $wt(x^{2/3})=2$ 이다.

[0078] 이를 증명하면 다음과 같다.

[0079] 임의의 양수 u 와 v 에 대하여($u\geq v$) $m=3u$ 이고, $k=3v-1$ 이라 하자. F_{3^m} 에서 $x^{3u}+ax^{3v-1}+b=0$ 이므로 $ax^{3v}x^{-1}=x^{3u}-b$ 이다.

[0080] 따라서, $x^{-1/3} = -a(x^{u-v} + bx^{-v})$ 이고, $x^{2/3}$ 는 다음의 수학적 식 12와 같다.

수학적 식 12

$$[0081] \quad x^{2/3} = x^{-1/3} \cdot x = -a(x^{u-v+1} + bx^{-v+1})$$

[0082] 수학적 식 12로부터

[0083] $x^{1/3} \cdot x = (-a(x^{u-v+1} + bx^{-v+1}))^2 = x^{2u-2v+2} + x^{-2v+2} - bx^{u-2v+2}$ 가 유도되고, $x^{1/3}$ 는 다음의 수학적 식 13과 같이 표현된다.

수학적 식 13

$$[0084] \quad x^{1/3} = x^{2u-2v+1} + x^{-2v+1} - bx^{u-2v+1}$$

[0085] $f(x) = x^m + ax^k + b$ ($a, b \in F_3$)가 F_3 위의 삼항 기약다항식이고, $m \equiv 0 \pmod{3}$, $k \equiv -1 \pmod{3}$ 이라 하면, $\gamma \in \{3v-2, 3v-1\}$ 이 된다.

[0086] 이를 증명하면 다음과 같다.

[0087] 수학적 식 12, 13으로부터 다음의 수학적 식 14를 얻을 수 있다.

수학적 식 14

$$[0088] \quad C^{1/3} = \sum_{i=0}^{u-1} c_{3i+\theta} x^{(i-t)} + (x^{2u-2v+1} + x^{-2v+1} - bx^{u-2v+1}) \sum_{i=-\sigma_1}^{u-1-\sigma_1} c_{3i+[\theta+1]} x^{(i-t)} \\ - a(x^{u-v+1} + bx^{-v+1}) \sum_{i=-\sigma_2}^{u-1-\sigma_2} c_{3i+[\theta+2]} x^{(i-t)}$$

[0089] 수학적 식 14로부터 $C^{1/3}$ 의 최소 degree는 $-2v+1+\sigma_1-t$ 이고, 최대 degree는 $3u-2v-\sigma_1-t$ 임을 알 수 있다. 그러므로, 다음의 수학적 식 15를 만족하면, 수학적 식 14에서 더 이상의 모듈로 감산 연산은 필요하지 않게 된다.

수학적 식 15

$$[0090] \quad \begin{cases} -2v+1-\sigma_1-t \geq -3t-\theta, \\ 3u-2v-\sigma_1-t \leq 3u-1-(3t+\theta) \end{cases}$$

[0091] 수학적 식 15로부터 $t = (2v-1+\sigma_1-\theta)/2$ 를 구할 수 있고, 이때, (t, θ) 쌍은 $(v-1, 1)$ 과 $(v-1, 2)$ 가 될 수 있다. 그러므로 γ 은 $3v-2$ 나 $3v-1$ 이 된다.

[0092] 2. $k \equiv 0 \pmod{3}$ 인 경우

[0093] 먼저 $m \equiv 1 \pmod{3}$, $k \equiv 0 \pmod{3}$ 인 경우를 고려해 보도록 한다. 임의의 양수 u 에 대하여 $m=3u+1$ 이라 하면, $C \in F_{3^m}$ 는 다음과 같이 표현된다.

수학식 16

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

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 다음의 수학식 17과 같이 표현할 수 있다.

수학식 17

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

수학식 17로부터 아래와 수학식 18과 같이 $C^{1/3}$ 을 구할 수 있다.

수학식 18

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

$f(x) = x^m + ax^k + b$ ($a, b \in F_3$)가 F_3 위의 삼약 기약다항식이고, $m \equiv 1 \pmod{3}$, $k \equiv 0 \pmod{3}$ 이라 하면, $\text{wt}(x^{1/3}) = 2$, $\text{wt}(x^{2/3}) = 3$ 이다.

이를 증명하면 다음과 같다.

임의의 양수 u 와 v 에 대하여 ($u \geq v$) $m = 3u + 1$ 이고, $k = 3v$ 이라 하자. F_{3^m} 에서 $x^{3u+1} + ax^{3v} + b = 0$ 이므로 $-x^{3u} = ax^{3v} + b$ 이다.

따라서, $x^{1/3}$ 와 $x^{2/3}$ 는 다음의 수학식 19와 같다.

수학식 19

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

$f(x) = x^m + ax^k + b$ ($a, b \in F_3$)가 F_3 위의 삼약 기약다항식이고, $m \equiv 1 \pmod{3}$, $k \equiv 0 \pmod{3}$ 이라 하면, $y \in \{3u, 3u+1\}$ 이다.

이를 증명하면 다음과 같다.

수학식 19로부터 다음의 수학식 20을 얻을 수 있다.

수학식 20

$$C^{1/3} = \sum_{i=0}^{u-\sigma_0} c_{3i+\theta} x^{(i-t)} - (ax^{v-u} + bx^{-u}) \sum_{i=-\sigma_1}^{u-1} c_{3i+[\theta+1]} x^{(i-t)} \\ + (x^{2v-2u} + x^{-2u} - bx^{v-2u}) \sum_{i=-\sigma_2}^{u-1-\sigma_1} c_{3i+[\theta+2]} x^{(i-t)}$$

[0109]

[0110] 수학식 20으로부터 $C^{1/3}$ 의 최소 degree는 $-2u-\sigma_2-t$ 이고, 최대 degree는 $u-\sigma_0-t$ 임을 알 수 있다. 그러므로, 다음의 수학식 21을 만족하면, 수학식 20에서 더 이상의 모듈로 감산 연산은 필요하지 않게 된다.

수학식 21

$$\begin{cases} -2u-\sigma_2-t \geq -3t-\theta \\ u-\sigma_0-t \leq 3u-(3t+\theta) \end{cases}$$

[0111]

[0112] 수학식 21로부터 $(2u+\sigma_2-\theta)/2 \leq t \leq (2u+\sigma_0-\theta)/2$ 를 구할 수 있고, 이때, (t, θ) 쌍은 $(u, 0)$ 과 $(u, 1)$ 가 될 수 있다. 그러므로 γ 은 $3u$ 나 $3u+1$ 이 된다.

[0113] 다음으로 $m \equiv -1 \pmod{3}$, $k \equiv 0 \pmod{3}$ 인 경우를 고려해 보도록 한다. 임의의 양수 u 에 대하여 $m=3u-1$ 이라 하면, $C \in F_{3^m}$ 는 다음과 같이 표현된다.

수학식 22

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

[0114]

[0115] 이를 이용하여 SPB를 기저로 한 C 를 표현하면, 다음의 수학식 23과 같다.

수학식 23

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

[0116]

[0117] 수학식 23으로부터 다음의 수학식 24와 같이 $C^{1/3}$ 을 구할 수 있다.

수학식 24

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

[0118]

[0119] $f(x)=x^m+ax^k+b(a,b\in F_3)$ 가 F_3 위의 삼약 기약다항식이고, $m\equiv -1(\bmod 3)$, $k\equiv 0(\bmod 3)$ 이라 하면, $\text{wt}(x^{1/3})=3$, $\text{wt}(x^{2/3})=2$ 이다.

[0120] 이를 증명하면 다음과 같다.

[0121] 임의의 양수 u 와 v 에 대하여($u>v$) $m=3u-1$ 이고, $k=3v$ 이라 하자. F_{3^m} 에서 $x^{3u-1}+ax^{3v}+b=0$ 이므로 $x^{3u}x^{-1}=-ax^{3v}-b$ 이다.

[0122] 따라서, $x^{-1/3}=-ax^{v-u}-bx^{-u}$ 이고, $x^{2/3}$ 는 다음의 수학적 식 25와 같다.

수학적 식 25

[0123]
$$x^{2/3} = x^{-1/3} \cdot x = -a(x^{v-u+1} + bx^{-u+1})$$

[0124] 수학적 식 25로부터

[0125] $x^{1/3}x=(-a(x^{v-u+1}+bx^{-u+1}))^2=x^{2v-2u+2}+x^{-2u+2}-bx^{v-2u+2}$ 가 유도되고, $x^{1/3}$ 는 다음의 수학적 식 26과 같이 표현된다.

수학적 식 26

[0126]
$$x^{1/3} = x^{2v-2u+1} + x^{-2u+1} - bx^{v-2u+1}$$

[0127] $f(x)=x^m+ax^k+b(a,b\in F_3)$ 가 F_3 위의 삼약 기약다항식이고, $m\equiv -1(\bmod 3)$, $k\equiv 0(\bmod 3)$ 이라 하면, $y\in\{3u-2, 3u-1\}$ 이다.

[0128] 이를 증명하면 다음과 같다.

[0129] 수학적 식 25, 26으로부터 다음의 수학적 식 27을 얻을 수 있다.

수학적 식 27

[0130]
$$C^{1/3} = \sum_{i=0}^{u-1-\sigma_1} c_{3i+\theta} x^{(i-t)} + (x^{2v-2u+1} + x^{-2u+1} - bx^{v-2u+1}) \sum_{i=-\sigma_1}^{u-1-\sigma_2} c_{3i+[\theta+1]} x^{(i-t)} - a(x^{v-u+1} + bx^{-u+1}) \sum_{i=-\sigma_2}^{u-2} c_{3i+[\theta+2]} x^{(i-t)}$$

[0131] 수학적 식 27로부터 $C^{1/3}$ 의 최소 degree는 $-2u+1-\sigma_1-t$ 이고, 최대 degree는 $u-1-\sigma_1-t$ 임을 알 수 있다. 그러므로, 다음의 수학적 식 28을 만족하면, 수학적 식 27에서 더 이상의 모듈로 감산 연산은 필요하지 않게 된다.

수학적 식 28

[0132]
$$\begin{cases} -2u+1-\sigma_1-t \geq -3t-\theta \\ u-1-\sigma_1-t \leq 3u-2-(3t+\theta) \end{cases}$$

[0133] 수학적 식 28으로부터 $t=(2u+1+\sigma_1-\theta)/2$ 를 구할 수 있고, 이때, (t, θ) 쌍은 $(u-1, 1)$ 과 $(u-1, 2)$ 가 될 수 있다. 그러므로 y 은 $3u-1$ 나 $3u-2$ 이 된다.

- [0134] 도 1은 본 발명의 바람직한 일 실시예에 따른 F_{3^m} 에서의 세제곱근 연산장치의 구성도이다.
- [0135] 도 1을 참조하면, 본 실시예에 따른 세제곱근 연산장치는 SPB 기저 생성부(100), 세제곱근 생성부(110), 시프트 베이스 결정부(120), 및 세제곱근 연산부(130)으로 구성된다.
- [0136] SPB 기저 생성부(100)는 SPB를 기저로 하여 F_{3^m} 에 속하는 다항식 C를 생성한다. 일반적으로 F_{3^m} 에 속하는 다항식 C는 수학적 1과 같이 나타낼 수 있는데, SPB를 기저로 한 F_{3^m} 에 속하는 다항식 C는 수학적 1에 x^{-r} 을 곱함으로써, 생성할 수 있다.
- [0137] 세제곱근 생성부(110)는 SPB 기저 생성부(100)가 생성한 SPB를 기저로 하는 다항식 C에 대하여 세제곱근 식을 생성한다.
- [0138] 시프트 베이스 결정부(120)는 $C^{1/3}$ 의 최소 degree와 최대 degree를 이용하여 모듈로 감산 연산이 필요하지 않도록 하는 x^{-r} 을 결정한다.
- [0139] 세제곱근 연산부(130)는 시프트 베이스 결정부(120)가 결정한 x^{-r} 을 이용하여 C의 세제곱근을 연산한다.
- [0140] 도 2는 본 발명의 바람직한 일 실시예에 따른 F_{3^m} 에서의 세제곱근 연산 방법의 흐름도이다.
- [0141] 도 2를 참조하면, 본 실시예에 따른 F_{3^m} 에서의 세제곱근 연산 방법은 도 1에 도시된 F_{3^m} 에서의 세제곱근 연산 장치에서 시계열적으로 처리되는 단계들로 구성된다. 따라서, 이하 생략된 내용이라 하더라도 도 1에 도시된 F_{3^m} 에서의 세제곱근 연산 장치에 관하여 이상에서 기술된 내용은 본 실시예에 따른 F_{3^m} 에서의 세제곱근 연산 방법에도 적용된다.
- [0142] 210 단계에서 세제곱근 연산 장치는 SPB를 기저로 한 $x^{1/3}$ 과 $x^{2/3}$ 를 계산한다.
- [0143] 본 발명의 일 실시예에 따른 세제곱근 연산 장치는 SPB를 기저로 하여 F_{3^m} 에 속하는 C의 다항식을 생성하고, 상기 생성된 C의 다항식에 대하여 세제곱근 식을 생성하면, SPB를 기저로 한 $x^{1/3}$ 과 $x^{2/3}$ 를 계산할 수 있다.
- [0144] 220 단계에서 세제곱근 연산 장치는 계산된 $x^{1/3}$ 과 $x^{2/3}$ 를 이용하여 모듈로 감산 연산이 필요없도록 하기 위해 C ($\in F_{3^m}$)에 곱하는 x^{-r} 의 r값을 결정하여 $C^{1/3}$ 를 계산한다.
- [0145] 본 발명의 일 실시예에 따른 세제곱근 연산 장치는 210 단계에서 계산된 $x^{1/3}$ 과 $x^{2/3}$ 를 이용하여 $C^{1/3}$ 의 최소 degree와 최대 degree를 구한다. $C^{1/3}$ 의 최소 degree와 최대 degree로부터 모듈로 감산 연산이 필요하지 않도록 하는 x^{-r} 을 결정한다.
- [0146] 230 단계에서 세제곱근 연산 장치는 220 단계에서 결정한 x^{-r} 을 이용하여 C의 세제곱근을 연산한다.
- [0147] 본 발명에서는 SPB를 기저로 하여 $wt(x^{1/3})$ 와 $wt(x^{2/3})$ 를 낮출 수 있다.

표 1

$m \pmod 3$	$k \pmod 3$	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	$\in \{p^a, p+1, p+2\}$	-	2	3
-1	0	$\in \{q^b, q+1, q+2, q+3\}$	-	3	2

$$\alpha : p = \lceil (m-1)/3k \rceil + \lceil (m-1-k)/3k \rceil$$

$$\beta : q = \lceil (2m-1)/3k \rceil + \lceil (2m-1-k)/3k \rceil + \lceil (2m-1-2k)/3k \rceil$$

[0148]

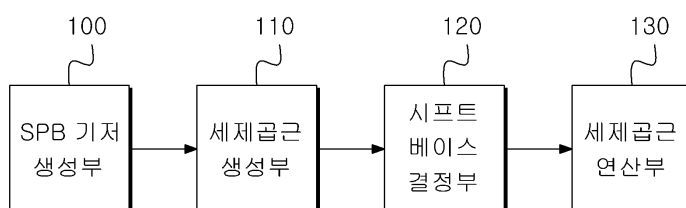
- [0149] 표 1은 문헌 1의 $wt(x^{1/3})$ 와 $wt(x^{2/3})$ 결과와 본 발명의 $wt(x^{1/3})$ 와 $wt(x^{2/3})$ 결과를 비교한 표이다. 표 1만으로는 PB를 기저로 한 $wt(x^{1/3})$ 와 SPB를 기저로 한 $wt(x^{1/3})$ 를 비교하는 것이 쉽지 않으므로, $m \in [2, 56]$ 인 삼항 기약다항식에 대하여 이들을 비교하여 도 3에 표현하였다.
- [0150] 도 3은 PB와 SPB에 대하여 $2 \leq m \leq 56$ 이고, $m \neq \pm k \pmod{3}$ 인 삼항 기약다항식의 $wt(x^{1/3})$ 비교표를 나타낸 것이다.
- [0151] 도 3에서 $wt(x^{1/3})$ 은 세제곱근 연산의 효율성을 결정하는 $x^{1/3}$ 의 해밍웨이트를 의미하며 $wt(x^{1/3})$ 가 낮을수록 세제곱근을 효율적으로 수행할 수 있다. 굵게 표시된 결과가 비교적 좋은 결과이며 본 발명으로 구한 $wt(x^{1/3})$ 가 거의 모든 경우에 대하여 낮은 $wt(x^{1/3})$ 를 제공하는 것을 알 수 있다.
- [0152] 도 3을 통하여 문헌 1의 결과보다 SPB를 기저로 한 $wt(x^{1/3})$ 가 훨씬 효율적임을 알 수 있다. 또한, 이상에서 살펴본 각각의 y 를 적용한 SPB를 기저로 하면 더 이상의 모듈로 감산 연산은 필요없게 된다.
- [0153] 본 발명의 실시예들은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.
- [0154] 이상과 같이 본 발명에서는 구체적인 구성 요소 등과 같은 특정 사항들과 한정된 실시예 및 도면에 의해 설명되었으나 이는 본 발명의 보다 전반적인 이해를 돕기 위해서 제공된 것일 뿐, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상적인 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다.
- [0155] 따라서, 본 발명의 사상은 설명된 실시예에 국한되어 정해져서는 아니되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

산업상 이용가능성

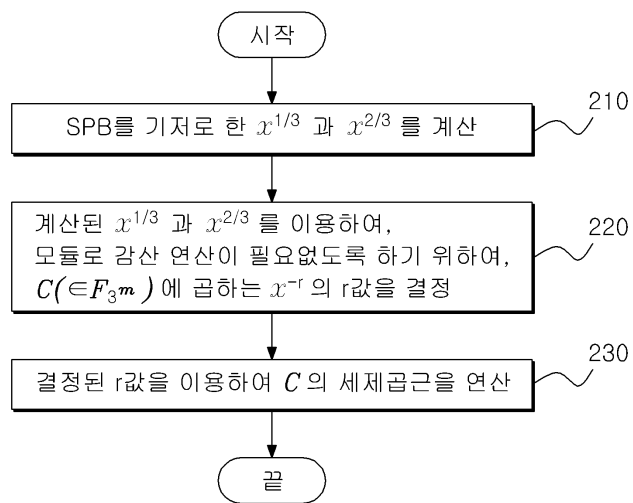
- [0156] 본 발명의 일 실시예에 따른 F_{3^m} 에서의 세제곱근 연산방법을 이용하여 페어링 암호 연산 특히, F_{3^m} 위에서의 n_T 페어링 연산을 훨씬 효율적으로 수행할 수 있으며 이는 장치의 개발과 시장으로의 진입을 더욱 빠르게 할 수 있어 산업, 기술 측면에서 많은 이점을 갖는다.

도면

도면1



도면2



도면3

Irreducible trinomial	PB	SPB	Irreducible trinomial	PB	SPB	Irreducible trinomial	PB	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	$x^{37} + x^{15} - 1$	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			