Regular paper

Journal of the KIECS. pp. 693-700, vol. 11, no. 7, Jul. 31 2016, t. 75, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2016.11.7.693

Weil 정리를 이용한 효율적인 타원곡선의 위수 계산법의 구현

김용태*

Efficient Implementations of Index Calculation Methods of Elliptic Curves using Weil's Theorem

Yong-Tae Kim*

요 약

현재 사용되고 있는 유한체 $GF(q)$ 위의 non-supersingular 타원곡선 이산대수문제에 기반한 공개키 암호법의 안전성을 보장하기 위해서는 타원곡선의 위수의 크기와 소인수의 크기를 계산하는 일이 매우 중요하다. 그런데 타원곡선의 위수를 구하는 전통적인 방법인 Schoof 알고리즘은 매우 복잡하여 지금도 개선작업이 진행 중이다. 본 논문에서는 복잡한 Schoof 알고리즘을 피하기 위하여, 표수가 2인 유한체의 합성체 $GF(2^m) = GF(2^{rs}) = GF((2^r)^s)$ 위에서 Weil 정리를 이용하여 타원곡선의 위수를 계산하는 방법을 제안한다. 또한, 그에 따른 알고리즘과 그 알고리즘을 적용한 프로그램을 실행하여 타원곡선 암호법에 사용될 수 있는 효율적인 곡선으로 $\#E(GF(2^5))$=36일 때의 합성체 $GF((2^5)^{31})$ 위에서 위수에 10^{40}이상인 소인수를 포함하는 non-supersingular 타원곡선을 찾을 수 있었다.

ABSTRACT

It is important that we can calculate the order of non-supersingular elliptic curves with large prime factors over the finite field $GF(q)$ to guarantee the security of public key cryptosystems based on discrete logarithm problem(DLP). Schoof algorithm, however, which is used to calculate the order of the non-supersingular elliptic curves currently is so complicated that many papers are appeared recently to update the algorithm. To avoid Schoof algorithm, in this paper, we propose an algorithm to calculate orders of elliptic curves over finite composite fields of the forms $GF(2^m) = GF(2^{rs}) = GF((2^r)^s)$ using Weil's theorem. Implementing the program based on the proposed algorithm, we find a efficient non-supersingular elliptic curve over the finite composite field $GF((2^5)^{31})$ of the order larger than 10^{40} with prime factor larger than 10^{40} using the elliptic curve $E(GF(2^5))$ of the order 36.

키워드

Order Of The Elliptic Curve, Non-Supersingular Elliptic Curve, Schoof Algorithm, Weil'S Theorem
타원 곡선 위수, non-supersingular 타원 곡선, Schoof 알고리즘, Weil 정리

* 교신저자: 광주교육대학교 수학교육과
• 접 수 일 : 2016. 05. 31
• 수정완료일 : 2016. 07. 13
• 게재확정일 : 2016. 07. 24
• Received : May. 31, 2016, Revised : Jul. 13, 2016, Accepted : Jul. 24, 2016
• Corresponding Author : Yong-Tae Kim
Dept. of Mathematics Education, Gwangju National University of Education
Email : ytkim@gnue.ac.kr

Ⅰ. 서 론

오늘날의 많은 공개키 암호법의 안전성은 이산대수문제(discrete logarithm problem)의 제어곤란성(intractability)에 기반으로 두고 있다. 또한 유한체 $GF(q)$위의 non-supersingular 타원곡선을 사용하는 이산대수문제에서 제곱근(square root)공격법을 피하기 위해서는 타원곡선의 위수는 10^{40}이상이어야 하며 10^{40}이상의 큰 소인수(prime factor)를 가져야 한다[1]. 따라서 이산대수문제에 기반한 공개키 암호법은 표수 2인 기초체위에서의 타원곡선을 사용하는 경우에는 크기가 2^{130} 이상이고 최적정규기저를 가져야 하며 타원곡선은 순환군(cyclic group)을 이루어야 안전한 것으로 알려져 있다. 이러한 이유로 non-supersingular 타원곡선을 사용하는 이산대수문제를 기반으로 하는 공개키 암호법에서는 우선 그 타원곡선의 위수(order) N을 계산하여 N이 큰 소인수를 가지는지의 여부를 알아야 한다. 주어진 타원곡선의 위수의 범위를 최초로 구한 사람은 Hasse[2]이다. 그러나 그의 방법은 확률적으로 다항식시간(polynomial time) 내에 타원곡선위의 점을 균등하고 임의적으로 알아낼 수 있다는 장점이 있으나 근사값만을 제시하는 한계가 있었으며, 실제로 유한체위에서 타원곡선의 정확한 점의 개수를 계산하는 방법은 1985년에 Schoof[3]가 처음으로 발표하였다. Koblitz[4]는 Schoof 알고리즘을 표수가 2인 유한체 $GF(2^m)$위에서 정의된 타원곡선에 적용하여 실행방법과 안전도를 제시하였으며 2진수열의 성질에 관한 연구는 현재[5-6]에도 꾸준히 진행 발전되고 있다. 그 후 2002년에는 p가 작은 소수이고 $q=p^m$일 때, 유한체 $GF(q)$위에서 Schoof 알고리즘보다 빠르게 타원곡선의 위수를 구하는 방법[7]이 제안되었으나 H/W 실행시간이 $\log p$에 관한 지수적(exponential)이었다. 또한 Schoof 알고리즘의 과정에서 시간이 많이 소모되는 중국인의 나머지 정리(chinese remainder theorem)의 실행속도를 높이는 가장 최근의 방법은 2013년에 개발[8]되었으나 그 역시 H/W 실행시간이 지수적이다. 본 논문에서는, 먼저 Schoof 알고리즘의 개요를 소개하고 그의 복잡성을 분석한 다음, Schoof 알고리즘을 사용하지 않고 Weil정리를 이용한 우리의 타원곡선의 위수계산 알고리즘을 제안하고 그에 따른 구체적인 수치실험결과를 알아본다.

Ⅱ. 표수가 2인 타원곡선

이 장에서는 Menezes[1], Koblitz[4]와 Washington[9]을 중심으로, 본 논문에서 사용되는 표수(characteristic)가 2인 유한체위에서의 몇 가지 타원곡선을 소개하도록 한다. 먼저, $q=2^m$이고 $K=GF(q)$를 q개의 원소를 갖는 유한체라고 하자. 그러면 $K-$유리수 점(rational point)으로 이루어진 종수(genus)가 1인 부드러운 사영곡선(smooth projective curve)을 유한체 K위에서의 타원곡선 $E=E(K)$라고 부른다. 즉, 그 곡선을 만족하는 $K\times K$상의 점들 (x,y)와 무한원점 O으로 이루어진 집합을 타원곡선이라 한다.

2.1 타원곡선의 개요

잘 알려진 바와 같이, Riemann-Roch 정리에 의해서 위의 타원곡선 E는 무한원점 O을 포함하며 계수가 모두 K의 원소인 곡선

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6, a_i \in K, \quad (1)$$

으로 표현할 수 있다. 여기에서 E/K의 판별식 Δ는 0이 아니라고 가정한다. 그러면 현-접선(cord-tangent)방법에 의해서 타원곡선 E는 가환군(abelian group)이 되며, 이러한 표수가 2인 타원곡선은 다음과 같이 두 가지 유형으로 분류된다.

① Non-supersingular 타원곡선:

$$y^2+xy=x^3+a_2x^2+a_6(a_6\neq 0), a_i \in K, \quad (2)$$

② Supersingular 타원곡선:

$$y^2+a_3y=x^3+a_4x+a_6(a_3\neq 0), a_i \in K. \quad (3)$$

이때, $q=2^m$에서의 m이 홀수인 경우에는 ②번의 타원곡선들은 3 종류의 동치류가 존재하게 되며, m이 짝수인 경우에는 7 종류의 동치류가 존재한다는 사실이 알려져 있다.

2.2 타원곡선의 표준형

E가 supersingular인 경우에는 E가 속하는 동치류를 찾아내서 유한체 K 위에서의 E의 점들의 개수 $\#E(K)$를 계산할 수 있다. 그런데 E가 non-supersingular인 경우에는, 유한체 K 위에서 $2q-2$ 종류의 동치류가 있으며, 각 동치류의 대표 곡선은 다음과 같다.

$\{y^2+xy=x^3+a_2x^2+a_6 | a_6 \in K^*, a_2 \in \{0,\alpha\}\}$, (4)

단, $\alpha \in K$는 trace가 1인 고정된 원소이다. 만일 두 타원곡선 E, E'이 각각

$y^2+xy=x^3+a_6(a_6 \neq 0)$, (5)

$y^2+xy=x^3+\alpha x^2+a_6(a_6 \neq 0)$ (6)

인 경우에는 $\#E(K)+\#E'(K)=2q+2$ 이므로, 타원곡선 $y^2+xy=x^3+a_6(a_6 \neq 0)$의 위수를 구하면 타원곡선 $y^2+xy=x^3+\alpha x^2+a_6(a_6 \neq 0)$의 위수는 자동적으로 구할 수 있다. 따라서 통상 non-supersingular 타원곡선 E를

$y^2+xy=x^3+a_6(a_6 \neq 0)$ (7)

형태로 사용하고 있으며,

$y^2+xy=x^3+\alpha x^2+a_6(a_6 \neq 0)$를

$y^2+xy=x^3+a_6(a_6 \neq 0)$의 대응곡선이라고 한다. 또한 대부분의 타원곡선은 순환군(cyclic group)을 이루고 있음이 알려져 있다.

III. 타원곡선의 위수

주어진 타원곡선의 위수(order)의 범위를 최초로 아래의 정리와 같음을 증명한 사람은 Hasse[2]이다.

정리 1.([1, 정리 2.8])

p는 소수, $q=p^m$이고 $K=GF(q)$를 q개의 원소를 갖는 유한체라고 하자. 그러면

$\#E(K)=q+1-t, |t| \leq 2\sqrt{q}$ (8)

정리 1은 확률적으로 다항식시간 내에 타원곡선위의 점을 균등하고 임의적으로 알아낼 수 있다는 장점이 있으나 근사값만을 제시하는 한계가 있었으며, 실제로 유한체위에서 타원곡선의 정확한 점의 개수를 계산하는 방법은 1985년에 Schoof[3]가 처음으로 발표하였다.

3.1 $GF(2^m)$위의 타원곡선의 위수

1985년에 Schoof[3]는 홀수 q일 때의 일반적인 유한체 $GF(q)$상에서 정의된 타원곡선 E위에 있는 $GF(q)$-유리수 점의 개수 $\#E(GF(q))$를 다항식 시간 내에 계산하는 알고리즘을 제안하였다.

그런데 H/W의 실행시간을 단축하기 위해서는 표수가 2인 유한체위에서의 암호법이 더 선호되기 때문에, Koblitz[4]는 Schoof 알고리즘을 표수가 2인 유한체 $GF(2^m)$위에서 정의된 타원곡선에 적용하여 실행방법과 안전도를 제시하였으며, 그 이후에는 대부분의 타원곡선 암호법에서는 표수가 2인 유한체 $GF(2^m)$위에서 정의된 타원곡선을 사용하고 있다. 또한 II장에서 언급한바와 같이 타원곡선이 supersingular인 경우에는 곡선의 유형이 거의 밝혀져 있으며, non-supersingular 타원곡선의 위수를 계산하는 빠른 알고리즘이 존재하지 않기 때문에 안전한 암호법을 수행하기 위해서 non-supersingular 타원곡선위에서의 암호법을 선택하고 있다. 타원곡선 암호법을 구축하고 구현하기 위해서는, 먼저 타원곡선의 위수 N을 계산하여 N의 약수 중에 큰 소수가 존재하는지를 확인해야 한다. 특히 암호법의 안전을 위해서는 non-supersingular 타원곡선의 위수가 최소한 40자리 정수인 소인수를 가져야 한다[1]. 즉, 유한체 $GF(2^m)$의 크기는 $m \geq 130$이어야 한다. 이 절에서는 표수가 2인 유한체 $GF(2^m)$위에서 정의된 non-supersingular 타원곡선위에서의 위수를 계산하는 데에 현재까지 사용되고 있는 Schoof 알고리즘[3]을 개관하고 그의 복잡성을 분석하기로 한다.

3.2 $GF(2^m)$위에서 Schoof 알고리즘의 개요

Schoof 알고리즘은 $q=2^m$, $K=GF(q)$이고 $\#E(K)=q+1-t$라고 놓은 다음 t값을 구하는 다음과 같은 방법이다.

먼저, 임의의 자연수 L'을 선택하여, 3과 L'사이의 모든 소수(prime number) l의 곱이 다음 식이 성립하도록 한다.

$\Pi l > 4\sqrt{q}$. (9)

이러한 조건하에서, 각각의 홀수인 소수 $l \leq L'$에 대하여 $t \bmod l$을 계산한 다음, $|t| \leq 2\sqrt{q}$이므로 초등정수론의 내용인 중국인의 나머지 정리를 적용하여 t값을 계산한다.

$P=(\bar{x},\bar{y}) \in E[l]^*$, $E[l] \cong \mathbb{Z}_l \bigoplus \mathbb{Z}_l$이고 $k \equiv q \bmod l, 0 \leq k \leq l-1$인 경우에, 타원곡선 E의 Frobenius endomorphism ϕ에 대하여, 다음 식을 만족하는 정수 $\tau, 0 \leq \tau \leq l-1$를 찾는다.

$\phi^2(P)+kP=\tau\phi(P)$. (10)

그러면 $(t-\tau)\phi(P)=O$(무한원점)이고 $\phi(P)$는 위수 l인 점이므로, $t\equiv\tau \bmod l$이 되므로 t값을 구하게 된다.

3.3 $GF(2^m)$위에서의 Schoof 알고리즘 분석

Schoof 알고리즘은 이론적인 실행시간은 $O(\log^8 q)$-비트 연산이지만, 다음과 같은 어려움 때문에 실제로 적용하기가 매우 복잡하고 지루한 방법이다.

3.3.1 식 (9)가 성립하는 자연수 L'의 선택

자연수 L'을 선택할 때마다 식 (9)가 성립하는지를 검증해야하며 3과 L'사이의 모든 소수 l을 찾아야 한다. 그러나 잘 알려진 바와 같이 어떤 정수가 소수인지를 판명하는 소수 판정법(primality testing)은 대단히 어려운 문제이다.

3.3.2 중국인의 나머지 정리의 실행 시간

모든 소수 l에 대하여 중국인의 나머지정리를 적용하여 t값을 계산해야 한다. 그러나 중국인의 나머지 정리 알고리즘의 실행시간이 비교적 길기 때문에, Schoof 알고리즘을 적용하는 많은 연구에서 중국인의 나머지 정리의 실행시간을 줄이는 연구가 지금도 진행되고 있다[8].

3.3.3 식 (10)을 만족하는 $P\in E[l]^*$의 선택

점 $P=(\overline{x},\overline{y})\in E[l]^*$가 식 (10)을 만족하는지를 검증하기 위해서는, 먼저 나눗셈 다항식(division polynomial) $f_l(x)\in K[x]$을 찾아서 $f_l(\overline{x})=0$이 되는지를 확인한 다음, 두 점 $\phi^2(P)+kP$와 $\tau\phi(P)$의 x좌표를 등식으로 표현한 다음, 분모와 y좌표를 소거한 x에 관한 등식 $h_1(x)=0$ 을 찾아서 등식

$$H_1(x)=\gcd(h_1(x),f_l(x)) \tag{11}$$

를 계산한다. 만일 $H_1(x)=1$ 이면 식 (10)을 만족하는 점 $P\in E[l]^*$는 없으며, $H_1(x)\neq 1$ 인 경우에는 $\phi^2(P)+kP=\pm\tau\phi(P)$가 되는 점 $P\in E[l]^*$을 찾을 수 있다. 그러나 식 (10)을 만족하는 점 $P\in E[l]^*$을 찾기 위해서는 두 점 $\phi^2(P)+kP$와 $\tau\phi(P)$의 y좌표끼리의 등식에서 분모와 y를 소거하여 만든 x에 관한 등식 $h_2(x)=0$ 을 찾아서 등식

$$H_2(x)=\gcd(h_2(x),f_l(x)) \tag{12}$$

를 계산한다. 이때 만일 $H_2(x)=1$ 이면 $\phi^2(P)+kP=-\tau\phi(P)$이 되며, $H_2(x)\neq 1$ 이면 $P\in E[l]^*$는 식 (10)을 만족하므로 $t\equiv\tau \bmod l$이 된다는 복잡한 과정을 거쳐야한다. .

IV. 제안하는 타원곡선의 위수 계산법

지금까지 우리는 현재에도 타원곡선의 위수를 계산하는 방법으로 사용되고 있는 $GF(2^m)$위에서의 Schoof 알고리즘을 분석하여 H/W에 적용할 때 야기되는 복잡성을 알아보았다. 이 장에서는 위에서 알아본 Schoof 알고리즘 대신, 유한체$GF(2^m)$의 확대체인 $GF(2^{mk})$위에서의 새로운 타원곡선 위수계산법을 제안하기로 한다.

4.1 Weil 정리

타원곡선 E를 유한체 $GF(q)$의 확대체 $GF(q^k)$위에서의 타원곡선으로 간주할 수도 있다. 이 경우에는 Weil이 예상하고 1934년에 Hasse가 증명한 다음의 정리를 기반으로, $\#E(GF(q))$를 이용하여 $\#E(GF(q^k)), k\geq 2$를 계산한다.

정리 2.(Weil 정리[1, 정리 2.15])

E를 유한체 $GF(q)$위에서 정의된 타원곡선, $t=q+1-\#E(GF(q))$라고 하자. 그러면 α,β가 T에 관한 이차방정식

$$1-tT+qT^2=(1-\alpha T)(1-\beta T) \tag{13}$$

를 만족하는 복소수일 때,

$$\#E(GF(q^k))=q^k+1-\alpha^k-\beta^k. \tag{14}$$

4.2 Weil 정리를 이용한 타원곡선의 위수계산알고리즘

III장에서, 안전한 타원곡선 암호법을 실행하기 위해서는 non-supersingular 타원곡선의 기초체(underlying field) $GF(2^m)$의 크기는 $m\geq 130$이어야 하며, 타원곡선의 위수는 아주 큰 소인수를 가져야 하는 이유를 알아보았다. 이 절에서는 Weil 정리를 이용하여 간편하고 안전한 위수계산 알고리즘을 제안하기로 한다.

Step 1. 자연수 m의 선택

$m \geq 130,\ m = rs,\ r << s.$

Step 2. 기초체의 선택

기초체는 유한체 $GF(2^m) = GF(2^{rs}) = GF((2^r)^s)$ 이다.

Step 3. 위수 $\# E(GF(2^r))$의 계산

r는 아주 작은 자연수이므로 타원곡선 $E(GF(2^r))$의 위수는 Schoof 알고리즘을 사용하지 않고 다음과 같은 시행착오 법(method of trial-error)으로 쉽게 계산할 수 있다.

먼저 trace가 1인 유한체 $GF(2^r)$인 원소 τ을 선택한다. 그러면 2.2절의 식 (4),(5),(6)에 의해서 두 개의 non-supersingular 타원곡선 $y^2+xy=x^3+a_6$와 $y^2+xy=x^3+\tau x^2+a_6(a_6 \neq 0)$ 의 위수의 합은 $2 \cdot 2^r+2$ 이다. 따라서 만일 타원곡선 $y^2+xy=x^3+a_6$의 위수를 알게 되면 타원곡선 $y^2+xy=x^3+\tau x^2+a_6(a_6 \neq 0)$의 위수도 알 수 있게 된다. 이때, 타원곡선 $y^2+xy=x^3+\tau x^2+a_6(a_6 \neq 0)$을 대응곡선이라고 부른다. 그 다음에 유한체 $GF(2)$위에서의 r차 원시다항식 $f(z)$을 선택하면 유한체 $GF(2^r)$은 $GF(2^r) \cong GF(2)(z)/f(z)$이다. 이 관계식을 이용하여, 각 $a_6 = z^i\,(i=0,\cdots,2^r-2)$에 대하여,

타원곡선 $y^2+xy=x^3+a_6$과 대응곡선 $y^2+xy=x^3+\tau x^2+a_6(a_6 \neq 0)$의 위수를 구한다.

Step 4. Weil정리를 적용하여 $\# E(GF(2^m))$를 계산

Step 3에서 계산한 타원곡선 $E(GF(2^r))$의 위수를 Weil정리의 식 (14)에 대입하여 타원곡선의 위수 $\# E(GF((2^r)^s) = (2^r)^s+1-\alpha^s-\beta^s$를 계산한다.

Step 5. 타원곡선의 위수가 큰 소인수를 가지지 않으면 Step 1으로 환원하여 다른 타원곡선을 선택한다.

V. 수치실험 및 프로그램

이장에서는 우리의 타원곡선 위수계산법을 적용하기 위하여, $155 \geq 130,\ 155 = 5 \times 31$이므로 기초체를 합성체인 $GF(2^{155}) = GF((2^5)^{31})$으로 선택하고, $GF(2)$위에서의 5차 원시다항식은 $f(z) = 1+z^2+z^5$으로 선택한다. 이때 기초체 $GF((2^5)^{31})$위에서의 non-supersingular 타원곡선의 위수를 Pentium 166 MHZ CPU에서 Mathematica 4.0[10]을 이용한 프로그램을 사용하여 얻은 수치 실험결과와 프로그램은 다음과 같다.

5.1 수치실험의 예

$GF(2)(z)/(1+z^2+z^5)$위에서, $a_6 = z^i$ $(i=0,\cdots,30)$에 대한 타원곡선 $y^2+xy=x^3+a_6$와 대응곡선 $y^2+xy=x^3+\tau x^2+a_6(a_6 \neq 0)$ 위수는 표 1과 같다.

표 1. 타원곡선과 대응곡선의 위수

Table 1. Orders of elliptic ccurves and corresponding curves

i	order	Order of the corresponding curve
0	44	22
1,2,4,8,16	32	34
3,6,11,11,13,17, 21,22,24,26	36	30
5,9,10,18,20	28	38
7,14,19,25,28	24	42
15,23,27,29,30	40	26

표 1을 이용하여 non-supersingular 타원곡선 $E(GF(2^{155})) = E(GF((2^5)^{31}))$의 위수의 계산결과는 다음과 같다.

order=36

$t = -3x^{31}+y^{31}$ =381913138055676294829941

order=4567192616659071619386476910924578858795306202 8={{2,2},{3,2},{1268664615738631005385132752568274635542517 23,1}}

order=28

$t = 5x^{31}+y^{31}$ =4268092196884283247849 15

order=4567192616659071619386557783160343279257267688 4={{2.2},{7,1},{4217,1},{1108313,1},{3489998

724380075989872139757717710 43,1}}

order=22

$t = 11x^{31} + y^{31} = 2185642807449162564586 17$

order=4567192616659071619386493245810309944799143342={{2,1},{11,1},{26041,1},{41231,1},{19335042072015356797942560696891732 91,1}}

order=38

$t = -5x^{31} + y^{31} = 4268092195884283247849 15$

order=45671926166590716193864724213164255935923107054={{2,1},{19,1},{4093,1},{475169,1}{6179820875908641641659266709096800 49,1}}

5.2 결과 분석

$GF(2)(z)/(1+z^2+z^5)$ 위에서, $a_6 = z^i$ $(i=0,\cdots,30)$에 대한 서로 다른 타원곡선과 대응곡선은 12개이었으며, Weil 정리를 적용하여 각 곡선에 대한 합성체 $GF((2^5)^{31})$ 위에서의 non-supersingular 타원곡선의 위수를 계산한 결과, 그 중에서 30자리 이상의 소인수를 갖는 곡선은 위에 열거한 4개이었으며 특히, 40자리(10^{40}) 이상의 소인수를 갖는 곡선은 타원곡선 $y^2+xy=x^3+a_6$ 의 위수가 36인 경우이므로, 타원곡선 암호법에 사용될 수 있는 효율적인 곡선은 $\#E(GF(2^5))$=36일 때의 합성체 $GF((2^5)^{31})$ 위에서의 non-supersingular 타원곡선임을 알 수 있다.

5.3 프로그램

```
G[hh_]=Block[{ },
  Table[a[i]=(x+y)^i-Expand[(x+y)^i-x^i-
    y^i],{i,1,41}];
     Table[b[i]=0,{i,1,41}];
       For[i=1,i<42,i++,
        If[Mod[i,2]===1,
       For[j=1,j<(i+1)/2,j++,
      b[i]=b[i]+Coefficient[a[i],x^(i-j)*y^j]*(x*y)^j*
      (x^(i-2j)+y^(i-2j))
     ];
    b[i]=b[i]+(x+y)^i+Coefficient[a[i],x^(i/2)*y^(j/2)]*
  x^(i/2)*y^(j/2)
    ]
   ]
 ];

Z[u_]=Block[{ },G[1];
t=2^5+1-u;
  Do[b[i]/.(x+y)->t,{i,31}];
   For[i=1,i<(31+1),i++,
     Do[b[i]/. (x*y)^j->32^j,{j,1,i-1}];
     Do[b[i]/. (x^j+y^j)->b[j],{j,1,i-1}]
    ];
   Print["baseorder=",u,"t=",t,"x^31+y^31=",b[31],"
  "extensionorder=",
  2^155+1-b[31],
 "Factorization=",FactorInteger[2^155+1-b[31]]]
];
```

VI. 결 론

현재 사용되고 있는 유한체 $GF(q)$ 위의 non-supersingular 타원곡선 이산대수문제에 기반한 공개키 암호법의 안전성을 보장하기 위해서는 타원곡선의 위수의 크기와 소인수의 크기를 계산하는 일이 매우 중요하다. 그런데 타원곡선의 위수를 구하는 전통적인 방법인 Schoof알고리즘은 매우 복잡하여 지금도 개선작업이 진행 중이다. 본 논문에서는 복잡한 Schoof알고리즘을 피하기 위하여, 지금도 연구[11]가 진행되고 있는 표수가 2인 유한체의 합성체 $GF(2^{rs}) = GF((2^r)^s)$ 위에서 Weil 정리를 이용하여 타원곡선의 위수를 계산하는 방법을 제안하였다. 또한, 그에 따른 알고리즘과 그 알고리즘을 적용한 프로그램을 실행하여 타원곡선 암호법에 사용될 수 있는 효율적인 곡선인 $\#E(GF(2^5))$=36일 때의 합성체 $GF((2^5)^{31})$ 위에서 위수가 10^{40}이상인 소인수를 포함하는 non-supersingular 타원곡선을 찾을 수 있었다.

감사의 글

본 논문은 2016년도 광주교육대학교 학술연구비 지원에 의한 것임

References

[1] A. Menezes, *Elliptic Curve Public Key Cryptosystems.* Kluber Academic Publishers, Dordrecht, 1993.

[2] H. Hasse, "Zur Theorie der abstrakten elliptischen Funktionenkörper, I,II&III," *Crelle* 174, 1936, pp. 173-177.

[3] R. Schoof, "Elliptic curves over finite fields and the computation of square roots mod p," *Mathematics of Computation,* vol. 44, no. 170, 1985, pp. 483-494.

[4] N. Koblitz, "Constructing elliptic curve cryptosystems in characteristic 2," *Advances in Cryptography-CRYPTO'90,* Proc., LNCS 537, Springer, Santa Barbara, USA, Aug., 1991, pp. 156-167.

[5] U. Choi and S. 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] S. Cho, J. Kim, U. Choi, and S. Kim, "Cross-correlation of linear and nonlinear GMW-sequences generated by the same primitive polynomial on $GF(2^p)$," *The Korea Institute of Electronic Communication Sciences 2011 Spring Conf.* Busan, Korea, vol. 5, no. 1, June 2011, pp. 155-158.

[7] T. Satoh, "On p-adic point counting algorithms for elliptic curves over finite fields," *Algorithmic Number Theory, 5th Int. Symp., ANTS-V, Lecture Notes on Computer Science 2369,* Springer, Berlin, July, 2002, pp. 43-66.

[8] J. von zur Gathen and J. Garhard, *Modern Computer Algebra.* 3rd Ed., Cambridge University Press, Cambridge, 2013.

[9] L. C. Washington, "*Elliptic Curves; Number Theory and Cryptography,*" New York: Chapman&Hall/CRC, 2003.

[10] S. Wolfram, *Mathematica.* 4th Ed., Wolfram Champaign Research, Inc., New York, 1999.

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

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