情報保護學會論文誌
第12券 第2號, 2002. 4

타원곡선에서 스칼라 곱의 고속연산*

박 영 호**, 한 동 국***, 오 상 호***, 이 상 진***, 임 종 인***, 주 학 수****

A fast scalar multiplication on elliptic curves

Young-Ho Park**, Dong-Guk Han***, Sangho Oh***, Sangjin Lee***,
Jongin Lim***, Hak-Soo Ju****

요 약

Koblitz 타원곡선에서 스칼라 곱을 효율적으로 구현하기 위하여 프로베니우스 자기준동형 (Frobenius endomorphism)이 유용하게 사용된다. 스칼라 곱 연산시 스칼라를 이진 전개하는 대신에 프로베니우스 확장을 사용하여 고속연산을 가능하게 할 수 있으며 따라서 연산의 속도는 확장길이와 밀접한 관계가 있다. 본 논문은 스칼라의 프로베니우스 확장길이를 줄임으로써 스칼라 곱의 고속연산을 가능하게 하는 새로운 방법을 제안한다. 타원곡선의 위수를 노름(Norm)으로 갖는 원소대신 큰 소수 위수를 노름으로 갖는 원소를 사용하여 프로베니우스 확장길이를 최적화시키는 이 방법은 Solinas, Smart가 제안한 방법보다 프로베니우스 확장길이를 더 감소시킬 수 있다.[3,5]

ABSTRACT

For efficient implementation of scalar multiplication in Kobliz elliptic curves, Frobenius endomorphism is useful. Instead of binary expansion of scalar, using Frobenius expansion of scalar we can speed up scalar multiplication and so fast scalar multiplication is closely related to the expansion length of integral multipliers. In this paper we propose a new idea to reduce the length of Frobenius expansion of integral multipliers of scalar multiplication, which makes speed up scalar multiplication. By using the element whose norm is equal to a prime instead of that whose norm is equal to the order of a given elliptic curve we optimize the length of the Frobenius expansion. It can reduce more the length of the Frobenius expansion than that of Solinas, Smart.

Keyword : *Elliptic Curve, Scalar Multiplication, Public-key Cryptosystem*

Ⅰ. 서 론

타원곡선 암호시스템 구현의 주요한 쟁점들은 기본적으로 타원곡선 위에서 스칼라 곱의 속도를 높이는 것에 관심을 두고 있다. 유한체의 곱셈 군에서 사용되는 전통적인 '지수승 연산법'은 타원곡선의 스칼라 곱에서도 그대로 적용할 수 있다. 하지만 이 방법들은 곱셈 군에서의 제곱연산보다 계산복잡도가 높은 타원곡선 상의 점을 두 배하는 연산으로 이루어진다. 따라서 두 배하는 연산을 더 효율적으로 계산하는 방법들이 다양하게 연구되어왔다.

Koblitz는 [2]에서, anomalous 이진 곡선들을

* 본 연구는 한국정보보호진흥원 연구과제(2001-S-092) 지원으로 수행하였읍니다.
** 스팍스컴(Sparxcom) (youngho@cist.korea.ac.kr)
*** 정보보호기술연구센터(CIST) ({christa,gauss,sangin,jilim}@cist.korea.ac.kr)
**** 한국정보보호진흥원 (hsju@kisa.or.kr)

고려할 때, 두 배하는 연산을 프로베니우스 자기준동형으로 대체하여 고속연산이 가능함을 보여주었다. 또한 Müller는 표수(characteristic)가 2인 작은 유한체 위에서 정의된 non-supersingular 타원곡선에 대해 Koblitz 방법을 확장하였다.[2] 최근에 Smart는 Müller의 방법이 홀수 표수를 갖는 타원곡선에서도 사용될 수 있음을 보였다.[6] 게다가, 그는 타원곡선의 위수를 노름(Norm) 값으로 갖는 원소를 이용해 스칼라 곱의 정수를 나누는 방법으로 프로베니우스 확장길이를 50%나 감소시키는 알고리즘을 제안하였다.

암호학적 응용에서, 타원곡선 위의 모든 점에서의 스칼라 곱보다는, 큰 소수 위수를 갖는 점들의 스칼라 곱을 사용한다. 이런 측면에서, 타원곡선의 위수를 노름(Norm)으로 갖는 원소로 정수를 나누는 기존의 방법들은 몇몇 부수적인 계산을 지니고 있다.

본 논문에서는 스칼라인 정수의 프로베니우스 확장길이를 감소시킬 새로운 알고리즘을 제안한다. 이것은 타원곡선의 위수를 노름(Norm)으로 갖는 원소대신에 큰 소수 위수를 노름(Norm)으로 갖는 원소로 대체시키므로, 앞서 말한 부수적인 계산을 배제시키고 프로베니우스 확장길이를 최적화시킨다. 따라서 제안된 알고리즘은 줄어든 확장길이 만큼 스칼라 곱의 속도를 향상시킬 수 있게 한다.

본 논문은 다음과 같이 구성되어 있다. 2절에서는 표수 2인 유한체 위에 정의된 타원곡선의 일반적인 성질과 프로베니우스 자기준동형의 확장방법을 소개한다. 3절에서 프로베니우스의 확장길이를 줄이는 개선된 방법을 제안하고 효율적인 알고리즘을 제시한다. 4절에서 Koblitz, Solinas, Müller에 의한 기존의 결과들과 본 논문의 결과를 비교하고 5절에서 결론을 맺는다.

2. 타원곡선과 프로베니우스 확장

암호학적 응용의 관점에서, 표수가 2인 유한체 위에서 정의된 non-supersingular 타원곡선들이 많은 관심을 끌어왔으므로 본 논문에서는 표수 2인 유한체 위에서 정의된 곡선들만 고려할 것이다. F_q는 q개의 원소를 갖는 유한체이다. 여기서 $q=2^s(1\le s\le 5)$는 표수 2 의 지수승이다. 또한 $\overline{F_q}$를 F_q의 대수적 폐포(algebraic closure)라 하자. 다음과 같은 형태의 Weierstrass 방정식에 의해 주어진 non-supersingular 타원곡선 $E(F_q)$를 표현하면

$$y^2+xy=x^3+a_2x^2+a_6 \tag{1}$$

이다. 여기서 a_2, a_6는 F_q의 원소이고, $a_6\neq 0$ 이다. $E(F_q)$의 q-지수승 프로베니우스 자기준동형(Frobenius endomorphsim)은 다음같이 정의된다.

$$\Phi : E(\overline{F_q}) \to E(\overline{F_q}),\ (x,y)\mapsto (x^q, y^q).$$

유명한 Hasse의 결과로부터, $E(F_q)$의 위수는 다음 식에 의해 정수 t와 밀접하게 관련된다.

$$\#E(F_q)=q+1-t.$$

여기서 t는 다음 (2)식을 만족하는 프로베니우스 자기준동형 Φ의 자취(trace)이다.

$$\Phi^2-t\Phi+q=0. \tag{2}$$

t는 non-supersingular 타원곡선 $E(F_q)$에 대해서는 홀수여야 함에 주의하자. 이제 $Z[\Phi]$의 임의의 원소의 프로베니우스 확장 방법에 대해 간략하게 소개하겠다.[4]

[보조정리 1]

$\rho\in Z[\Phi]$로 놓자. 그러면 다음 식을 만족하는 정수 r과 $u\in Z$이 존재한다.

$$\rho=u\Phi+r,\quad -q/2\le r\le q/2$$

특별히 $r\in\{-q/2+1,\cdots,q/2\}$를 선택하면, r과 u는 유일하게 존재한다.

[보조정리 2]

$q\ge 4$에 대하여, $\rho\in Z[\Phi]$는 $N_{Z[\Phi]/Z}(\rho)\le(\sqrt{q}+1)^2$ 을 만족한다고 가정하자. 그러면 ρ는 많아야 4의 길이의 Φ-확장을 가지고 각 정수계수는 $q/2$로 경계되어지는 크기를 가진다.

[정리 3]

$q\ge 4$에 대하여, 임의의 $\rho\in Z[\Phi]$ 는 $\rho=\sum_{i=0}^{k} r_i\Phi^i$ 로 표현되어진다. 여기서 정수계수 $r_i\in\{-q/2+1, \cdots, q/2\}$이고, $k\le\lceil 2\log_q\|\rho\|\rceil+3$이다. 임의의 $\rho=a_1+a_2\Phi\in Z[\Phi]$에 대하여 확장길이 $k+1(\le$

$\lceil 2\log_q \|\rho\| \rceil + 4$)를 갖는 프로베니우스 확장을 효율적으로 계산하는 알고리즘 제시한다.

〔알고리즘 1〕

입력 : $\rho = a_1 + a_2\Phi \in Z[\Phi]$.

출력 : $\rho = \sum_{i=0}^{k} r_i \Phi^i$를 만족하는 정수 r_i들.

1. $x = a_1$, $y = a_2$, $i = 0$로 놓는다.
2. $|x| > q/2$ 또는 $|y| > q/2$를 만족하는 동안 다음을 실행한다.
   (a) $x_1 \equiv x \pmod q$를 계산한다.
   (b) $r_i = \begin{cases} x & \text{if } x \le q/2, \\ x - q & \text{otherwise.} \end{cases}$로 둔다.
   (c) $h = (r_i - x)/q$, $x = y - th$, $y = h$, 그리고 $i = i + 1$로 둔다.
3. $r_i = x$, $r_{i+1} = y$
4. r_i를 결과로 보낸다.

〔알고리즘 1〕은 Müller가 제시한 알고리즘과 거의 같으며 단지 단계 3에서 Φ-확장의 계수 r_i는 $\pm q/2$까지 허용하는 것이 다르다.[4] 하지만 ρ에 대하여 Φ-확장이 유일하게 표현되지 않아도 되므로 아무런 문제가 발생하지 않으며 Müller의 알고리즘보다 확장길이를 조금이라도 줄일 수 있게끔 한다.

3. 프로베니우스 자기준동형의 확장길이

공개키 암호시스템에서는 $E(F_{q^n})$의 위수가 최소한 160비트 정도 길이의 큰 소수 인수 p을 가질 것을 요구한다. 따라서 타원곡선 $E(F_{q^n})$가 큰 소수 위수 p인 점 P를 갖는다 하자. 타원곡선 군의 위수를 $\#E(F_{q^n})$로 표시하면 $\#E(F_{q^n}) = hp$로 나타낼 수 있고, 이 때 h를 $E(F_{q^n})$의 cofactor라 부른다. 또한 Hasse와 Weil 정리에 의해 타원곡선의 위수는 $\Phi^n - 1$의 노름(Norm), $\#E(F_{q^n}) = N_{Z[\Phi]/Z}(\Phi^n - 1)$을 만족한다.

일반적으로, 타원곡선의 스칼라 곱은 큰 정수 $m \approx p \approx q^n$에 대하여 mP 계산을 해야한다. 〔정리 3〕이나 〔4, Theorem 1〕에 따르면, m의 프로베니우스 확장길이는 m의 노름에 달려 있다. 즉 m의 프로베니우스 확장은 〔알고리즘 1〕을 사용하여

$$m = \sum_{i=0}^{k} m_i \Phi^i$$

$m_i \in \{-q/2+1, \cdots, q/2\}$으로 표현할 수 있으며, 이때 확장길이 $k+1$은 기껏해야 $\lceil \log_q m^2 \rceil + 4$이 됨을 알 수 있다. 프로베니우스 확장방법을 이용하여 스칼라 곱을 할 때에는 프로베니우스 확장 길이가 짧으면 짧을수록 스칼라 곱의 속도는 빨라진다. 따라서 최근 Solinas와 Smart에 의해 프로베니우스 확장의 길이를 50% 정도 감소시키므로 스칼라 곱의 속도를 배나 빠르게 수행할 수 있는 방법을 제안했다.[3,6] 이 방법은 다음의 사실들을 사용한다:

1′) 임의의 점 $Q \in E(F_{q^n})$에 대해 $\Phi^n(Q) = Q$을 만족하며 이것은 $(\Phi^n - 1)Q = O$임을 만족시킨다.
2′) 따라서 $m \in Z[\Phi]$로 보아 m을 $\Phi^n - 1$로 나누어 나머지 $\rho' \in Z[\Phi]$를 얻는다. 이때 나머지 ρ'은 m의 노름에 절반정도인 q^{n+1} 크기의 노름을 갖는다.
   즉, $N_{Z[\Phi]/Q}(\rho') \approx q^{n+1}$.
3′) $mQ = \rho'(Q)$을 만족하기 때문에 m에 의한 스칼라 곱을 ρ'에 의한 곱으로 대체한다.
4′) 이때 ρ'의 프로베니우스 확장을 사용하면 그것의 확장길이는 거의 반으로 감소한다.

암호학적 응용을 고려할 때, 타원곡선 위의 모든 점 Q에서의 스칼라 곱보다는, 큰 소수 위수를 갖는 점 P들의 스칼라 곱을 이용하기를 원한다. 이런 측면에서 위에 제안된 방법은 타원곡선의 위수를 노름(Norm)으로 갖는 원소 $\Phi^n - 1$로 m을 나누므로 몇몇 부수적인 계산을 지니고 있다.

그러므로 우리는 본 절에서 $\Phi^n - 1$대신에 큰 소수 위수 p를 노름(Norm)으로 갖는 원소 α로 대체시키므로, 앞서 말한 부수적인 계산을 배제시키고 프로베니우스 확장길이를 최소화시키는 방법을 제안하다. 먼저 전체 타원곡선 군 $E(F_{q^n})$이 아니라 큰 소수 위수 p를 갖는 순환 부분군 $\langle P \rangle$를 고려하자. 프로베니우스 자기준동형 Φ는 순환군 $\langle P \rangle$에 스칼라 곱셈으로 작용하여

$$\Phi(P) = \mu P$$

을 만족한다. 이때 μ는 Φ의 법 p의 특성다항식, $\Phi^2 - t\Phi + q \bmod p$의 근이다. 작은 양의 정수 m_s와 원소 $\alpha = a + b\Phi \in Z[\Phi]$가 존재하여

$$N_{Z[\Phi]/Z}(a+b\Phi) = m_s p \quad (3)$$

$$(a+b\Phi)P = 0 \quad (4)$$

두 개의 식을 만족한다고 가정하자. 만일 노름 방정식 (3)만을 만족하는 $a+b\Phi \in Z[\Phi]$ 찾으면

$(a+b\Phi)(a+b\overline{\Phi}) = (a+b\Phi)(a+b(t-\Phi))$
$(a+b\Phi)(a+bt-b\Phi) = m_s p$를 만족하므로
$(a+b\mu)(a+bt-b\mu) \equiv 0 \mod p$이다.

따라서 $a+b\mu \equiv 0$ 또는 $a+bt-b\mu \equiv 0 \mod p$이므로 $(a+b\Phi)P = O$ 또는 $(a+b\overline{\Phi})P = O$를 만족한다. 그러므로 위 가정에서 (3)를 만족하는 노름방정식의 해를 구한다면 (4)의 식을 만족하는 α를 쉽게 구할 수 있다.

간략하게 요약해서, 본 방법의 주요 아이디어는 위의 가정에 기반해서 기존 방법 2') 에서 $\Phi^n - 1$ 대신 $\alpha = a+b\Phi$로 m을 나누는 방법을 사용하는 것이다. $Z[\Phi]$가 양의 실수 λ에 대해 λ-유클리안 (λ-Eulidean) 환이므로 m을 α로 나눌 수 있고 $N_{Z[\Phi]/Z}(\rho) < \lambda N_{Z[\Phi]/Z}(\alpha)$ 만족하는 나머지 ρ를 [정리 6]이나 [6]을 통해 얻을 수 있다. 따라서 앞에서 언급한 방법처럼 mP 의 계산을 ρP로 대체할 수 있다. 이 방법은 위수 p을 갖는 임의의 점들에 대한 스칼라 곱에 있어서 프로베니우스 확장길이를 최적화 할 수 있게 한다. 그러므로 우리는 이론상으로나 계산적인 실험을 통해서 이 방법이 기존의 가장 효율적인 방법보다 $\lfloor \log_q(\#E(F_{q^n})/m_s p) \rfloor$ $\lfloor \log_q(h/m_s) \rfloor$ 정도 확장길이를 줄일 수 있음을 자세히 보일 것이다. 다만 이 방법은 $E(F_{q^n})$의 모든 점에서가 아니라 위수 p의 모든 점들에서 작용함에 주의하자. 새로운 방법의 내용은 다음과 같이 요약할 수 있다.

1) $N_{Z[\Phi]/Z}(a+b\Phi) = m_s p$ 와 $(a+b\Phi)P = O$ 을 만족하는 아주 작은 양의 정수 m_s에 대하여 $a+b\Phi$을 찾는다. (정리 5 참조)
2) m을 $a+b\Phi$로 나누면 나머지 $\rho \in Z[\Phi]$ $N_{Z[\Phi]/Z}(\rho) < \lambda N_{Z[\Phi]/Z}(\alpha)$, $0 < \lambda \le \frac{9+4q}{16}$ 을 얻는다. (정리 6 참조)
3) $mP = \rho(P)$을 만족하기 때문에 m에 의한 스칼라 곱을 ρ에 의한 곱으로 대체한다.
4) 이때 ρ의 프로베니우스 확장을 사용하면 그것의 확장길이를 ρ'을 사용한 것보다 대략 $\lfloor \log_q(h/m_s) \rfloor$ 정도 줄일 수 있다. (정리1 참조)

[보조정리 4]

[7] $K = Q(\sqrt{D})$를 허수 이차체라 하자. 그리고 K의 영이 아닌 이데알(ideal) $\mathfrak{g}$는 K에서 정수환 O_K의 원소 α에 대해서 다음을 만족하는 이데알 ϑ를 갖는다:

$$\vartheta\mathfrak{g} = (\alpha), \quad N_{K/Q}(\vartheta) \le \frac{2}{\pi}\sqrt{|D|}. \quad (5)$$

[정리 5]

$\#E(F_{q^n})$는 큰 소수 p에 의해 나누어지고, $p^2 \nmid \#E(F_{q^n})$이라고 하자. 만약 $D = t^2 - 4q$가 제곱인 수를 갖지 않으면 $m_s < 1.28\sqrt{q}$인 어떤 양의 정수에 대하여 $N_{K/Q}(a+b\Phi) = m_s p$를 만족시키는 $\alpha = a+b\Phi \in Z[\Phi]$가 존재한다.

[증명]

$N_{K/Q}(\Phi^n - 1) = \#E(F_{q^n})$과 $p^2 \nmid \#E(F_{q^n})$이므로 p는 K/Q에서 쪼개(split)진다. $\mathfrak{g}$를 $N_{K/Q}(\mathfrak{g}) = p$를 만족하는 K의 prime ideal이라 하자. [보조정리 4]에 의해, 어떤 $\alpha \in O_K$에 대해 $\vartheta\mathfrak{g} = (\alpha)$를 만족하는 $N_{K/Q}(\vartheta) \le \frac{2}{\pi}\sqrt{|D|}$인 이데알 ϑ가 존재한다. 따라서 $m_s = N_{K/Q}(\vartheta)$라 놓으면

$$m_s \le \frac{2}{\pi}\sqrt{|D|} = \frac{2}{\pi}\sqrt{|t^2-4q|}$$
$$\le \frac{2}{\pi}2\sqrt{q} < 1.28\sqrt{q}\text{이다.}$$

그러므로 $m_s < 1.28\sqrt{q}$ 과 $\alpha \in O_K$이 존재하여 $N_{K/Q}(\alpha) = N_{K/Q}(\vartheta\mathfrak{g}) = m_s p$를 만족한다. 이제 $\alpha \in Z[\Phi]$임을 보여야 한다. t가 홀수이고 $D \equiv 1 \pmod 4$이므로 $\omega = (1+\sqrt{D})/2$인 $O_K = Z[\omega]$이다.
$\Phi^2 - t\Phi + q = 0$이므로 $\Phi = (t \pm \sqrt{D})/2$ 와

$$\omega = \begin{cases} \Phi + (t-1)/2 & \text{if } \Phi = (t+\sqrt{D})/2, \\ -\Phi + (t+1)/2 & \text{if } \Phi = (t-\sqrt{D})/2. \end{cases}$$

를 얻는다. 따라서 $\alpha \in Z[\Phi]$일 필요충분조건이 $\alpha \in O_K$가 되고, 증명은 완성된다. □

[정리 5]에서 $N_{K/Q}(\alpha) = m_s p$를 만족하는 $\alpha = a+b\Phi$을 찾는 것은 Cornacchia 알고리즘을 사용하여 쉽게 구할 수 있다.[1] 사실상 이 과정은 타원곡선 $E(F_{q^n})$의 파라미터의 구성 준비단계에서 수행되므로 스칼라 곱의 연산속도와는 무관하다.

〔정리 6〕

$\alpha = a + b\Phi \neq 0 \in Z[\Phi]$로 놓자. 임의의 $\beta \in Z[\Phi]$에 대해, $\beta = \delta\alpha + \rho$ 와 $N_{Z[\Phi]/Z}(\rho) < \lambda N_{Z[\Phi]/Z}(\alpha)$, $0 < \lambda \leq \frac{(9+4q)}{16}$ 를 만족하는 $\delta, \rho \in Z[\Phi]$가 존재한다.

〔증명〕

$\Phi^2 - t\Phi + q$ 이므로 $D = t^2 - 4q$ 이고 $\Phi = (t + \sqrt{D})/2$이라 하자.
또한 $N_\alpha = N_{Z[\Phi]/Z}(\alpha)$와 $c = -\lfloor t/2 \rfloor$로 놓자. $\Phi' = \Phi + c$로 놓아, Z-기저 $\{1, \Phi\}$를 $\{1, \Phi'\}$로 바꾼다. 그러면 이 새로운 기저로 $\alpha = a_1 + b_1\Phi'$로 표현할 수 있다. 주어진 피제수 β에대해, $\gamma = \beta/\alpha$로 놓고 $\gamma = \beta/\alpha = \beta\bar{\alpha}/N_\alpha = \frac{c_1 + c_2\Phi'}{N_\alpha}$를 얻는다. 여기서 $\bar{\alpha}$는 α의 켤레 복소수(complex conjugate)를 나타낸다. 이제 $d_i = \lfloor c_i/N_\alpha \rceil$ $(i = 1, 2)$인 $d = d_1 + d_2\Phi'$를 택한다. $\lfloor x \rceil$ 는 x에 가장 가까운 정수를 의미한다.

마지막으로 $\rho = \alpha(\gamma - \delta) \in Z[\Phi'] = Z[\Phi]$를 취한다. 그러면

$$N_{Z[\Phi]/Z}(\rho)/N_{Z[\Phi]/Z}(\alpha) = N_{Z[\Phi]/Z}(\gamma - \delta)$$
$$\leq N_{Z[\Phi]/Z}\left(\frac{1}{2} + \frac{1}{2}\frac{1+\sqrt{D}}{2}\right)$$
$$= \frac{1}{4}N_{Z[\Phi]/Z}\left(\frac{3+\sqrt{D}}{2}\right) = \frac{1}{4}\left(\frac{9-D}{4}\right)$$
$$\leq \frac{1}{4}((9+4q)/4) \qquad \square$$

〔정리 6〕은 $Z[\Phi]$ 가 $0 < \lambda \leq (9+4q)/16$인 λ에 대해 λ-Euclidean 환임을 보이고 있다. 이것은 〔6, 정리5〕의 결과에 비하면 λ의 경계를 1/4 배 줄인 셈이다. 〔정리 6〕의 증명을 사용하여, m, t, q, $\alpha = a + b\Phi$로부터 나머지 ρ를 계산하는 효율적인 알고리즘을 제안한다.

〔알고리즘 2〕 (m를 $\alpha = a + b\Phi$로 나누기)
입력 : $m \in Z$, $\alpha = a + b\Phi$
출력 : $\rho = r_1 + r_2\Phi$ ($N_{Z[\Phi]/Z}(\rho) < \lambda N_{Z[\Phi]/Z}(\alpha)$)

Ⅰ. 사전계산

1. $N_\alpha = N_{Z[\Phi]/Z}(\alpha)$, $c = -\lfloor t/2 \rfloor$
2. $\Phi' = \Phi + c$, $N = N_{Z[\Phi]/Z}(\Phi')$.
3. $a_1 = a - bc$, $b_1 = b$, $(\alpha = a_1 + b_1\Phi')$

Ⅱ. 본 알고리즘

4. $x_1 = m(a_1 + b_1)$ 그리고 $x_2 = -mb_1$
5. $y_i = \lfloor \frac{x_i}{N_\alpha} \rceil$ $(i = 1, 2)$.
6. $r'_1 = m - (a_1y_1 - Nb_1y_2)$,
   $r'_2 = -(a_1y_2 + b_1y_1 + b_1y_2)$.
7. $r_1 = (r'_1 + r'_2c)$, $r_2 = r'_2$.
8. r_1, r_2 결과를 보낸다.

〔알고리즘 2〕의 I 사전계산은 타원곡선의 구성과정에서 한번만 계산하면 되므로 스칼라 곱 mP를 계산하는 데에는 직접 필요한 계산량은 아니다. m이 주어졌을 때 나머지 ρ를 구하는 본 알고리즘은 2번의 라운드 계산($\lfloor \cdot \rceil$)과 7번의 큰 정수 곱셈이 필요하다. 여기서 $c = -\lfloor t/2 \rfloor$는 작은 수이므로 계산량을 무시할 수 있다.

〔정리 7〕

임의의 정수 m를 〔알고리즘 2〕를 통하여 α로 나눈 나머지를 ρ라 하자. 그러면 ρ의 확장 길이는 기껏해야 $\lceil \log_q(\lambda m_s p) \rceil + 4$이다.

〔증명〕

〔정리 3〕으로부터 ρ의 프로베니우스 확장길이 $k+1$은 기껏해야 $\lceil 2\log_q \mathrm{LEFT}\|\rho\| \rceil + 4 = \lceil \log_q N_{Z[\Phi]/Z}(\rho) \rceil + 4 \leq \lceil \log_q(\lambda m_s p) \rceil + 4$ 이다. $\square$

4. 기존의 방법들과의 비교

본 절에서는 표수가 2인 작은 유한체 위에서 정의된 non-supersingular 타원곡선에서 스칼라 곱의 고속연산을 위해 사용되는 기존의 방법들과 본 논문에서 제안된 방법을 비교하기 위해서, 암호학적 응용에 사용하기 적합한 다양한 타원곡선들에 대한 구현 결과를 제시한다.[3,4] 여기서 암호학적으로 적합한 타원곡선이라는 것은 non-supersingular 곡선이고, Pohlig-Hellman 공격에 견디기 위해서 타원곡선 군의 위수가 적어도 155 비트 이상의 큰 소인수 p를 갖고, 구현관점에서 cofactor의 크기가 작아야한다.[5] 따라서 적합한 타원곡선 $E(F_{q^n})$를 찾

기 위해서 먼저 위수를 계산하여야 한다. 일반적으로 주어진 타원곡선의 위수를 계산하는 문제는 쉽지 않다. 그러나 다행히도 작은체 위에 정의된 타원곡선 $E(F_q)$의 위수는 쉽게 알 수 있으므로 다음과 같이 잘 알려진 방법으로 $E(F_{q^n})$의 위수를 쉽게 구할 수 있다:

$$t_0=2,\ t_1=t=q+1-\#E(F_q),$$

$n \geq 2$에 대하여, $t_n=t_1t_{n-1}-qt_{n-2}$이다.

그러면 $\#E(F_{q^n})=q^n+1-t_n$이다.

그러므로 우리는 위 방법을 사용하여 작은체 F_q, $(2\leq q=2^s\leq 32)$에서 정의된 타원곡선과 암호학적으로 적합한 이들의 확장체 $E(F_{q^n})$들을 찾아보았다. 여기서 우리는 $q^n\leq 2^{550}$이며, 위수는 155 비트 이상의 큰 소인수를 가지고, 너무 크지 않은 cofactor h ($\#E(F_q)<h<2^{36}$)를 갖는 타원곡선 $E(F_{q^n})$을 고려하였다. (Cofactor 가 $\#E(F_q)$인 Koblitz 곡선은 본 Table에서는 생략하였다.)

이제 Table에 주어진 타원곡선 $E(F_{q^n})$에서의 스칼라 곱 mP를 고려하자. 여기서 P는 위수가 p인 점이라 하자. [4]에서 Müller는 m의 프로베니우스 확장길이를 줄이는 방법을 사용하지 않았고, Solinas 와 Smart는 m을 Φ^n-1로 나누어 나머지 ρ'를 사용하여 프로베니우스 확장의 길이를 50% 정도 감소시키는 방법을 제안했다.[3,6] 마지막으로 본 논문에서 제안된 방법은 (3),(4)를 만족하는 $a=a+b\Phi$로 m을 나누는 방법을 사용한다. 이 세 가지 방법을 사용하여 얻어지는 m에 관한 프로베니우스 확장길이는 기껏해야 각각 $\lceil \log_q m^2 \rceil+4$,

〔표 1〕 $q=2$ 인 경우

n	t	$\log_2 p$	h	m_s
	λ	확장길이 no reduction	확장길이 by Φ^n-1	확장길이 by a
277	1	264	15514	1
	0.25	523	274	260
307	-1	289	351212	1
	0.25	575	305	287

〔표 2〕 $q=4$ 인 경우

n	t	$\log_2 p$	h	m_s
	λ	확장길이 no reduction	확장길이 by Φ^n-1	확장길이 by a
97	1	179	58204	1
	0.42	176	96	88
139	1	266	6676	1
	0.42	264	138	131
163	3	316	1306	1
	0.25	315	162	157
181	1	349	13036	1
	0.42	347	180	173
191	-1	363	880134	1
	0.42	361	190	180
239	-1	464	20082	2
	0.42	462	238	231
251	-1	482	1518054	1
	0.42	480	250	240
271	1	522	1645516	1
	0.42	519	270	259

〔표 3〕 $q=8$ 인 경우

n	t	$\log_2 p$	h	m_s
	λ	확장길이 no reduction	확장길이 by Φ^n-1	확장길이 by a
71	-3	199	30684	2
	0.58	131	71	66
71	-1	200	12790	2
	0.74	131	70	66
89	3	257	1074	2
	0.58	170	88	86
101	-1	288	62630	1
	0.75	190	100	95
107	1	309	6856	1
	0.74	204	106	102
157	1	440	2603655352	1
	0.74	292	156	146

〔표 4〕 $q=16$ 인 경우

n	t	$\log_2 p$	h	m_s
	λ	확장길이 no reduction	확장길이 by Φ^n-1	확장길이 by a
47	-1	166	5042178	9
	1.42	82	46	42
73	3	257	57048553058	2
	1.25	127	72	64
83	5	305	226317108	3
	0.92	151	82	76
97	3	367	2118494	3
	1.27	183	96	91

〔표 5〕 $q=32$ 인 경우

n	t	$\log_2 p$	h	m_s
	λ	확장길이 no reduction	확장길이 by Φ^n-1	확장길이 by α
37	-5	163	7491206	4
	2.25	64	37	33
41	-5	181	29486746	2
	2.27	71	40	36
41	3	183	8297610	5
	2.60	72	40	37
41	9	195	1992	1
	1.07	77	41	38
47	-1	220	57562	4
	2.73	87	46	44
73	-3	349	120924	6
	2.60	138	72	70
101	-7	491	32360	2
	1.76	195	101	98
101	-3	473	5588277516	3
	2.56	188	101	95
101	1	491	19424	2
	2.72	195	100	98

$\lceil \log_q(\lambda \#E(F_{q^n})) \rceil + 4$, $\lceil \log_q(\lambda m_s p) \rceil + 4$이 된다. 다음 Table의 테이터 값들($\lambda$, 프로베니우스 확장길이)은 10^5개의 난수 $m \leq p$에 대한 실험결과를 평균한 것이다.

5. 결 론

본 논문에서는 표수가 2인 작은 유한체 위에서 정의된 non-supersingular 타원곡선에서 스칼라 곱의 고속연산을 위한 효율적인 방법을 제안하였다. 이 방법은 스칼라 곱의 정수 multiplier의 프로베니우스 확장길이를 기존의 가장 효율적인 방법보다 $\lfloor \log_q(\#E(F_{q^n})/m_s p) \rfloor = \lfloor \log_q(h/m_s) \rfloor$ 정도 줄일 수 있음을 보였다. 또한 4절에서 제시된 암호학적으로 적합한 타원곡선들에 대한 구체적인 구현을 통해 이론의 타당성을 입증했으며 실험결과로서 약 5% 향상된 결과를 얻었다. 그러므로 본 논문에서 제안된 방법은 Koblitz, Solinas, Müller, Smart의 기존 방법들보다 향상된 방법으로 이론적으로나 실험적으로 그 이유의 타당성을 논하였다.[2,3,4,6]

참 고 문 헌

〔1〕 G. Cornacchia, "Su di un metodo per la risoluzione in numeri interi dell' equazione $\sum_{h=0}^{n} C_h x^{n-h} y^h = P$", *Giornale di Matematiche di Battaglini*, 46, pp. 33~90, 1908.

〔2〕 N.Koblitz, "CM-curves with good cryptographic properties", *In Advances in Cryptology*, CRYPTO 91, LNCS 576, Springer-Verlag, Berlin, pp. 279~287,1992.

〔3〕 J.A. Solinas, "An improved algorithm for arithmetic on a family of elliptic curves", *In Advances in Cryptology*, CRYPTO 97, LNCS 1294, Springer-Verlag, Berlin, pp. 357~371, 1997.

〔4〕 V.Müller, "Fast multication on elliptic curves over small fields of characteristic two", *Journal of Cryptology*, 11, pp. 219~234 (1998).

〔5〕 S. Pohlig, M. Hellman, "An improved algorithm for computing logarithms over $GF(p)$ its cryptographic significance", *IEEE Trans. Inform. Theory*, 24, pp. 106~110, 1978.

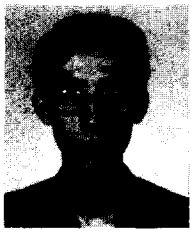
〔6〕 N.P. Smart, "Elliptic curve cryptosystems over small fields of odd characteristic", *Journal of Cryptology*, 12, pp. 141~151, 1998.

〔7〕 I. Stewart, D. Tall, "Algebraic Number Theory", *Chapman and Hall*, Halsted Press, 1979.

〈著者紹介〉

박 영 호 (Young-Ho Park) 정회원
1990년 2월 : 고려대학교 수학과 학사
1993년 2월 : 고려대학교 수학과 석사
1997년 2월 : 고려대학교 수학과 박사
2001년~현재 : 고려대 정보보호기술연구센터 객원조교수
〈관심분야〉 정수론, 공개키 암호, 암호 프로토콜.

한 동 국 (Dong-Guk Han) 정회원
1999년 2월 : 고려대학교 수학과 학사
1999년 3월~현재 : 고려대학교 수학과 석사 과정
2002년 3월~현재 : 고려대학교 정보보호대학원 박사 과정
〈관심분야〉 정수론, 공개키 암호 ,CMVP.



오 상 호 (Sang-Ho Oh) 정회원
1993년 2월 : 고려대학교 수학과 학사
현재 : 이노바시스 책임연구원
〈관심분야〉 Computational Number Theory, Cryptography.

이 상 진 (Samg-jin Lee) 정회원
1987년 2월 : 고려대학교 수학과 학사
1989년 2월 : 고려대학교 수학과 석사
1994년 2월 : 고려대학교 수학과 박사
1989년 2월~1999년 2월 : 한국전자통신연구원 선임 연구원,
1999년 2월~현재 : 고려대학교 자연과학대학 부교수, 고려대학교 정보보호대학원 겸임교수, 고려대학교 정보보호기술연구센터 연구실장
〈관심분야〉 블록 암호 및 스트림 암호의 분석 및 설계, 암호 프로토콜, 공개키 암호 알고리즘의 분석

임 종 인 (Jong-in Lim) 정회원
1980년 2월 : 고려대학교 수학과 학사
1982년 2월 : 고려대학교 수학과 석사
1986년 2월 : 고려대학교 수학과 박사
1999년 2월~현재 : 고려대학교 자연과학대학 정교수, 한국통신정보보호학회 편집위원장고려대학교 정보보호대학원 원장, 고려대학교 정보보호기술연구센터 센터장
〈관심분야〉 블록 암호 및 스트림 암호의 분석 및 설계, 암호 프로토콜, 공개키 암호 분석

주 학 수 (Hak-Soo Ju)
1997년 8월 : 고려대학교 수학과 학사
1999년 8월 : 고려대학교 수학과 이학석사
2001년 8월 : 고려대학교 수학과 박사과정 수료
2001년 9월~현재 : 한국정보보호진흥원 연구원