홀수 표수 확장체위의 타원곡선 고속연산

김용호*, 박영호*, 이상진*, 임종인*

*고려대학교

An improved method of multiplication on Elliptic Curve Cryptosystems over Small Fields of Odd Characteristic

Yong Ho Kim * , Young-Ho Park * , Sangjin Lee * , Jongin Lim *

*Korea Univ.

요 약

본 논문은 작은 홀수 표수를 갖는 유한체에서 정의된 타원곡선의 스칼라 곱 연산속도를 향상시키는 새로운 방법을 소개한다. 본 논문에서 제안하는 알고리즘은 스칼라의 프로베니우스 자기준동형 (Frobenius endomorphsim) 확장길이를 줄이는 최근의 방법들을 개선한 방법이다.

I. 서론

타원곡선 공개키 암호법은 이산대수를 기반으로 하는 다양한 암호 시스템에 효율적으로 적용 가능하므로 타원곡선 암호시스템 구현에서 효율성을 높이는 연구는 중요한 문제이다. 특히, 타원곡선 위에서 스칼라 곱 연산을 효율적으로 하는 다양한 방법들이 연구되어 왔다.

처음에 Koblitz[3]는 anomalous 이진 타원곡선 위에서 두 배 연산 대신에 프로베니우스 자기준동형을 사용하였다. 그리고 Müller[2]는 이 방법을 확장하여 표수(characteristic)가 2인 작은 유한체 위의 확장체에서 정의된 타원곡선에 적용하였다. 또한 Smart[1]는 이 방법이 홀수 표수를 갖는 확장체위의 타원곡선에서도 적용 가능함을 보인 동시에, 프로베니우스 확장길이를 반으로 감소시키므로 스칼라 곱의 고속연산을 가능하게 하였다. 본 논문에서는 Smart의 방법을 개선하여 스칼라 곱의 프로베니우스 확장길이를 보다 더 감소시킬 새로운 알고리즘을 제안한다.

본 논문의 구성은 다음과 같다. 2절에서 타원곡선의 기본성질과 프로베니우스 확장을 이용한 스칼라 곱 연산 방법을 간략하게 소개한다. 3절에서는 홀수 표수 확장체위의 타원곡선에서 프로베니우스 자기준동형 확장길이를 줄이는 알고리즘을 제시한다. 그리고 4절에서는 제안된 방법과 기존의 방법들과의 확장길이를 비교하고, 5절에서 결론을 맺는다.

II. 프로베니우스 확장을 이용한 스칼라 곱 연산 방법

본 논문에서는 아래와 같은 형태의 Weierstrass 방정식에 의해 정의된 표수가 홀수인 타원곡선 $E(F_{q^n})$만 고려한다.

$$E: y^2 = x^3 + ax + b$$

여기서 $p \geq 5$ 인 소수이고 $q = p^s$, $a, b \in F_q$. q-지수승 프로베니우스 자기준동형(Frobenius endomorphsim)은 다음과 같이 정의된다.

$$\Phi : E(F_{q^n}) \to E(F_{q^n}), \ by\ (x, y) \mapsto (x^q, y^q).$$

함수 Φ는 아래의 방정식을 만족한다.

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

또한 Hasse의 정리에 의해 $|t| \le 2\sqrt{q}$ 임을 알 수 있다. 암호학적 관점에서 non-supersingular 곡선만 다루므로, $4a^3 + 27b^2 \ne 0$이라 가정하고, p는 Φ의 자취(trace) $t = q + 1 - \#E(F_q)$를 나누지 않는다고 가정한다.

정리 1 $S \in Z[\Phi]$ 로 놓자. 그러면 S를 다음과 같이 표현할 수 있다.

$$S = \sum_{i=0}^{k} r_i \Phi^i$$

여기서 $r_i \in \{-(q+1)/2+1, \cdots, (q+1)/2\}$ 이고, $k \le \lceil \log_q 4N_{Z[\Phi]/Z}(S) \rceil + 3$ 이다.

Φ를 사용하여 타원곡선 $E(F_{q^n})$의 점 P 에 대한 스칼라 곱 mP 를 효율적으로 계산할 수 있다. 우선 $m \in Z[\Phi]$로 보아, 정리 1를 사용하여 $m = \sum_{i=0}^{k} r_i \Phi^i$ 으로 표현할 수 있다. 여기서 $k \le \lceil \log_q 4m^2 \rceil + 3$ 이다. 그래서

$$\begin{aligned} mP &= \sum_{i=0}^{k} r_i \Phi^i(P) \\ &= \Phi(\cdots\Phi(r_k\Phi(P) + r_{k-1}P) + \cdots + r_1P) + r_0P \end{aligned}$$

로 계산된다.

mP 계산 속도는 확장 길이에 밀접한 관계가 있다. 즉, Φ의 확장 길이 $k+1$가 줄어들면 연산 속도는 빨라진다. 따라서 다음절에서 프로베니우스 확장길이를 줄이는 새로운 방법을 설명할 것이다.

Ⅲ. 프로베니우스 자기준동형 확장 길이를 줄이는 방법

암호학적 응용에 있어 타원곡선 $E(F_{q^n})$의 위수는 큰 소인수 p를 가져야 한다. 타원곡선의 위수를 $\#E(F_{q^n}) = hp$ 라 하자 여기서 h는 작은 정수 값을 갖는다. 타원곡선 암호시스템에서는 전체 군 $E(F_{q^n})$보다 큰 소수 p를 위수로 갖는 점 P 로 생성되는 순환 부분군 $\langle P \rangle$를 사용한다. 따라서 전체 군이 아닌 순환 부분군 $\langle P \rangle$에서 스칼라 곱의 연산을 고려할 것이다.

본 절에서는 Smart[1]의 방법을 개선하여 프로베니우스 확장 길이 $(k+1)$를 줄이는 방법에 대하여 설명한다. 우선, 작은 정수 m_s에 대하여

$$N_{Z[\Phi]/Z}(\alpha) = m_s p\,,\ \alpha P = O \qquad (1)$$

을 만족하는 $\alpha = a + b\Phi \in Z[\Phi]$ 를 찾고자 한다. 이는 Cornacchia 알고리즘[4]을 사용하여 쉽게 찾을 수 있으며 m_s의 존재성과 작은 상한 값을 갖음을 다음의 정리에서 알 수 있다.

보조정리 1. ([5] 참조) $K = Q(\sqrt{D})$를 허수 이차체라 하자. K의 영이 아닌 이데알(ideal) I 에 대하여 이데알 J 와 K의 정수 환 O_K의 어떤 원소 α가 존재하여 다음을 만족한다:

$$N_{K/Q}(J) \le \frac{2}{\pi}\sqrt{|D|},\ I \cdot J = (\alpha).$$

정리 2. $p \| \#E(F_{q^n}), p^2 \nmid \#E(F_{q^n})$이라고 하자. 만약 $D = t^2 - 4q$가 제곱인수를 갖지 않으면 어떤 양의 정수 $m_s < 1.28\sqrt{q}$ 에 대하여 $N_{Z[\Phi]/Z}(a + b\Phi) = m_s p$를 만족하는 $\alpha \in Z[\Phi]$가 존재한다.

증명. $\#E(F_{q^n}) = hp$, $K = Q(\sqrt{D})$라 하자.

$N_{K/Q}(\Phi^n - 1) = \#E(F_{q^n}) = hp$ 이므로 p는 K/Q에서 쪼개(split)진다. I를 $N_{K/Q}(I) = p$인 K의 소수 이데알이라 하자. 보조정리 1에 의해, 어떤 $\alpha \in O_K$에 대해 $I \cdot J = (\alpha)$를 만족하는 $N_{K/Q}(J) \le \frac{2}{\pi}\sqrt{|D|}$인 이데알 J가 존재한다. 그래서

$$\begin{aligned} m_s &= N_{K/Q}(J) \le \frac{2}{\pi}\sqrt{|t^2 - 4q|} \\ &\le \frac{2}{\pi}\sqrt{4q} < 1.28\sqrt{q}. \end{aligned}$$

가 된다. 이제 $\alpha \in Z[\Phi]$임을 보이자. Φ의 자취(trace)에 따라

$$\theta = \begin{cases} (1+\sqrt{D})/2 & \text{if } t \text{ 홀수} \\ \sqrt{D}/2 & \text{if } t \text{ 짝수} \end{cases}$$ 이고,

$O_K = Z[\theta]$이다. 따라서 $\Phi = (t \pm \sqrt{D})/2$이므로,

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

이고, $O_K=Z[\Phi]=Z[\theta]$이다. □

Remark. 정리 2에서 $D=t^2-4q$가 $s^2|D$이고, $D'=D/s^2$ 가 제곱인수를 갖지 않으면 $m_s < s^2 1.28\sqrt{q}$ 조건을 만족하는 m_s을 찾을 수 있다. 그래서 일반적인 $D=t^2-4q$에 대하여도 m_s는 작은 정수 값으로 잡을 수 있다.

작은 정수 m_s에 대하여 (1)를 만족하는 $\alpha\in Z[\Phi]$를 찾는 과정은 사전계산으로 이루어지므로 스칼라 곱의 연산 속도에 영향을 주지 않는다.

다음은, 정리 2 에서 사용된 θ를 세분화하여 다시 정의하자.

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

그러면, $\theta=\Phi-\lfloor t/2 \rfloor$, $Z[\Phi]=Z[\theta]$ 가 된다.

정리 3에서 $Z[\Phi]$가 양의 실수 λ에 대해 λ-유클리안(λ-Euclidean) 환이 됨을 보이고, 특히 θ를 사용하여 Smart[1]가 제시한 λ의 상한 값을 1/4 줄일 수 있음을 보인다.

정리 3. $\alpha=a+b\Phi\neq 0\in Z[\Phi]$로 놓자.

만약 $\beta\in Z[\Phi]$ 일 때, 다음을 만족하는 $\delta,\rho\in Z[\Phi]$ 가 존재한다.

$$\beta=\delta\alpha+\rho,\quad N_{Z[\Phi]/Z}(\rho)\le\lambda N_{Z[\Phi]/Z}(\alpha)$$

$$0<\lambda\le\begin{cases}(9+4q)/16 & \text{if } t \text{ 홀수}\\ (1+q)/4 & \text{if } t \text{ 짝수}.\end{cases}$$

증명. $Z[\Phi]=Z[\theta]$이므로 Z-기저 $\{1,\Phi\}$를 $\{1,\theta\}$로 바꾼다. 그리고 Z-기저 $\{1,\theta\}$에 대하여 $\rho\in Z[\Phi]$를 계산하는 과정을 살펴본다.

$$\gamma=\beta/\alpha=\beta\bar{\alpha}/\alpha\bar{\alpha}=(x_1+x_2\theta)/N_{Z[\Phi]/Z}(\alpha)$$

$$\delta=\left\lfloor \frac{x_1}{N_{Z[\Phi]/Z}(\alpha)}\right\rceil+\left\lfloor \frac{x_2}{N_{Z[\Phi]/Z}(\alpha)}\right\rceil\theta$$

여기서 $\bar{\alpha}$는 α의 켤레복소수(complex conjugate)이고, $\lfloor x \rceil$는 x에 가장 가까운 정수이다.

그래서 $\rho=\beta-\delta\alpha=\alpha(\gamma-\delta)$ 가 되고,

$$N_{Z[\Phi]/Z}(\rho)/N_{Z[\Phi]/Z}(\alpha)=N_{Z[\Phi]/Z}(\gamma-\delta)$$

$$\le N_{Z[\Phi]/Z}\left(\frac{1}{2}+\frac{1}{2}\theta\right)=\frac{1}{4}N_{Z[\Phi]/Z}(1+\theta)$$

$$=\begin{cases}\frac{1}{4}N_{Z[\Phi]/Z}\frac{(3\pm\sqrt{D})}{2} & \text{if } t \text{ 홀수}\\ \frac{1}{4}N_{Z[\Phi]/Z}\frac{(2\pm\sqrt{D})}{2} & \text{if } t \text{ 짝수}\end{cases}$$

$$=\begin{cases}\frac{(9-D)}{16}\le\frac{(9+4q)}{16} & \text{if } t \text{ 홀수}\\ \frac{(4-D)}{4}\le\frac{(1+q)}{4} & \text{if } t \text{ 짝수}\end{cases}$$

가 된다. □

알고리즘 1 (m를 α로 나눈 나머지 구하기)

입력 : $m\in N$, $\alpha=a+b\Phi\in Z[\Phi]$

출력 : $\rho=r_1+r_2\Phi$ ($N_{K/Q}(\rho)\le\lambda N_{K/Q}(\alpha)$)

[사전계산]

1 . $c=-\lfloor t/2 \rfloor=\begin{cases}-(t-1)/2 & \text{if } t \text{ 홀수},\\ -t/2 & \text{if } t \text{ 짝수},\end{cases}$

2. $T=\begin{cases}1 & \text{if } t \text{ 홀수},\\ 0 & \text{if } t \text{ 짝수},\end{cases}$

3. $N=\begin{cases}q+c(c-1) & \text{if } t \text{ 홀수},\\ q+c^2 & \text{if } t \text{ 짝수},\end{cases}$

4. $a_1=a-bc$, $b_1=b$, ($\alpha=a_1+b_1\theta$)

[본계산]

1. $x_1=m(a_1+b_1T)$, 그리고 $x_2=-mb_1$.

2. $y_i=\left\lfloor \frac{x_i}{m_s p}\right\rceil$, $(i=1,2)$.

3. $r'_1=m-(a_1y_1-Nb_1y_2)$,

$r'_2=-(a_1y_2+b_1y_1+Tb_1y_2)$,

4. $r_1=(r'_1+r'_2c)$, $r_2=r'_2$,

5. r_1, r_2 결과를 보낸다.

증명. 알고리즘 1의 증명은 정리 3에서 쉽게 유도된다. 다만,

$$T = Tr(\theta) = \theta + \overline{\theta} = \Phi + \overline{\Phi} + 2c = t - 2\lfloor t/2 \rfloor$$

이고, $N = \theta\overline{\theta} = (\Phi + c)(\overline{\Phi} + c) = q - tc - c^2$이다. 그리고 $\theta^2 = T\theta - N$ 이므로,

$$\begin{aligned}\rho &= m - (y_1 + y_2\theta)(a_1 + a_2\theta) \\ &= m - (a_1y_1 - Nb_1y_2) - (a_1y_2 + b_1y_1 + Tb_1y_2)\theta\end{aligned}$$

가 된다. □

알고리즘의 [사전계산]은 타원곡선의 구성단계에서 한번만 계산하면 되므로 ρ를 구하는 계산량에 포함되지 않는다. 그리고 T, N, c들은 q 보다 작은 수이므로 이들의 계산 량은 무시한다. 따라서 이 알고리즘은 2번의 라운드 계산과 6번의 큰 정수 곱셈이 필요하다.

최종적으로, 스칼라 곱의 고속연산을 위한 새로운 방법을 요약하면 다음과 같다.

< 스칼라 곱을 위한 새로운 방법 >

[Step 1] $N_{Z[\Phi]/Z}(\alpha) = m_s p$, $\alpha P = O$ 조건를 만족하는 $\alpha = a + b\Phi \in Z[\Phi]$를 결정.

[Step 2] 알고리즘 1 사용하여 m을 α로 나눈 나머지 $\rho \in Z[\Phi]$구하기.

[Step 3] $mP = \rho(P) = \sum_{i=0}^{k} r_i \Phi^i(P)$ 를 계산.

Ⅳ. 구현한 결과값 비교

적절한 타원곡선 $E(F_{q^n})$을 선택하기 위해서는 먼저 타원곡선의 위수를 계산하여야 한다. 작은체위의 $E(F_q) = q + 1 - t$ 의 위수는 쉽게 계산이 가능하고 $\#E(F_{q^n}) = q^n + 1 - t_n$ 의 위수는 다음의 방법으로 쉽게 구할 수 있다.

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

$$t_n = t_1 t_{n-1} - q t_{n-2}$$

Smart는 프로베니우스의 확장길이를 줄이기 위해 $\Phi^n - 1$를 사용하여 m를 나누었다. 하지만 본 논문에서 제안한 방법은 $\Phi^n - 1$ 대신 (1)를 만족하는 α를 사용하여 Φ의 확장길이를 더욱 줄였다. 그러나 Smart 방법은 타원곡선의 모든 점에 적용 가능하지만 본 논문에서 제안된 새로운 방법은 타원곡선 군 전체가 아니라 큰 소수 p를 위수로 갖는 순환 부분 군 $\langle P \rangle$에만 적용됨에 주의하자.

Reduction을 사용하지 않은 [방법 1], $\Phi^n - 1$을 사용한 [방법 2] 와 $\alpha = a + b\Phi \in Z[\Phi]$를 사용한 [방법 3] 의 확장길이를 비교하면 다음과 같다.

[방법 1]	$\lceil \log_q m^2 \rceil + 4$
[방법 2]	$\lceil \log_q(\lambda \# E(F_{q^n})) \rceil + 4$
[방법 3]	$\lceil \log_q(\lambda m_s p) \rceil + 4$

[표 1] 확장길이 비교

이와 같이 새로운 방법은 기존의 방법보다 확장길이를 약 $\lfloor \log_q(h/m_s) \rfloor$ 정도 줄일 수 있다. 다음 [표 2]는 각 방법의 결과를 비교한 실험 값이다. 특히, λ 와 프로베니우스 확장길이는 10^5개의 난수 $m \le p$에 대한 평균값이다. 여기서 다루는 F_q의 q는 $5 \le q \le 23$인 소수이다. 그리고 확장체 q^n의 크기는 130비트에서 220비트로 제한한다. 또한 타원곡선의 위수는 155비트 이상의 큰 소인수를 가지고, cofactor h는 $\#E(F_q) < h < 10^5$ 를 만족하는 타원곡선만 고려하였다.

q	n	t	$\lceil \log_2 p \rceil$	h
m_s	λ	확장길이 no reduction	확장길이 by $\Phi^n - 1$	확장길이 by α
5	79	-1	168	63049
1	0.497	142	78	71
7	61	-2	156	46370
2	0.590	109	60	55
7	67	3	174	29485
1	0.494	122	66	61
11	53	4	167	91592
1	0.673	95	52	48

[표 2] 확장길이 실험값 비교

q	n	t	$\lceil \log_2 p \rceil$	h
m_s	λ	확장길이 no reduction	확장길이 by Φ^n-1	확장길이 by α
11	53	6	168	68694
1	0.252	97	53	48
11	59	-1	189	36829
1	1.02	108	58	54
11	59	1	191	9097
1	1.000	109	58	54
11	61	4	199	7816
1	0.664	113	60	57
13	47	-3	162	4811
1	0.992	86	46	43
13	59	-3	205	12053
1	1.004	110	58	55
13	59	7	204	22309
1	0.167	110	59	55
17	47	-6	180	6792
3	0.746	87	47	44
17	47	-1	177	39311
1	1.486	85	46	43
19	41	2	164	1494
2	1.570	76	40	38
23	37	5	156	2831
1	1.509	68	37	34
23	41	-7	171	25451
1	1.001	75	41	37
23	41	-4	170	71204
4	1.663	74	40	37

[표 2] 확장길이 실험값 비교 (계속)

V. 결론

본 논문은 작은 홀수 표수를 갖는 유한체 위에서 정의된 non-supersingular 타원곡선에서 프로베니우스 자기준동형 (Frobenius endomorphsim)를 이용한 기존의 스칼라 고속연산을 개선하는 방법을 제안하였다. 이 방법은 Smart의 방법 보다 프로베니우스 자기준동형 (Frobenius endomorphsim) 확장길이를 약 $\lfloor \log_q(h/m_s) \rfloor$ 정도 줄일 수 있다.

참고문헌

[1] N. Smart,"Elliptic curve cryptosystems over small fields of odd characteristic", Journal of Cryptology, 1999, pp.141-145.

[2] V. Müller, " Fast multiplication in elliptic curves over small fields of characteristic two", Journal of Cryptology, 1998, pp.219-234.

[3] N. Koblitz, "CM-curves with good cryptographic properties", Advances in Cryptology-Crypto '91, 1992,279-287.

[4] 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, 33-90,1908.

[5] I. Stewart, D. Tall, "Algebraic Number Theory" Chapman and Hall, Halsted Press, 1979.