타원곡선의 위수 계산 알고리듬의 구현

김영제*, 유영보**, 이민섭***

(*,**)(주)필크립, ***단국대학교 수학과

An Implementation of Elliptic Curve Point Counting

Young-Je Kim*, Young-Bo Yoo**, Min-Surp Rhee***

(*,**)PhilCrypt, Inc., ***Department of Mathematics, Dankook Univ.

요약

여러 가지 타원곡선을 이용한 암호 프로토콜을 위해서는 안전한 타원곡선의 선택이 필요하고 안전한 타원곡선의 조건은 그것의 크기와 밀접한 관계가 있다. 현재까지 알려진 타원곡선의 위수를 계산하는 알고리듬으로는 Schoof의 계산법, 이를 개선한 Schoof- Elkies-Atkin(SEA)방법, 그리고 Satoh-Fouquet-Gaudry-Harley(Satoh-FGH) 방법 등이 있다. 이 논문에서는 표수(characteristic) 2인 유한체 위의 타원곡선에 대한 SEA 방법에 대해서 설명하고 그 구현의 예를 보인다.

1. 서론

체 F를 $q=2^n$개(n은 홀수)의 원소를 가지는 유한체라고 할 때 F 위의 타원곡선은 동형의 관점에서 적당한 $a_2, a_6 \in F$ 에 대해서 다음 식으로 표현할 수 있다.

$$E(a_2, a_6) = \{(X, Y, Z) \in F^3 - \{(0,0,0)\}: Y^2Z + XYZ = X^3 + a_2X^2Z + a_6Z^3\}/\sim$$

(단, $\lambda \neq 0$일 때, $(X, Y, Z) \sim (\lambda X, \lambda Y, \lambda Z)$)

이를 달리 표현하면

$$E(a_2, a_6) = \{(x, y) \in F \times F: y^2 + xy = x^3 + a_2x^2 + a_6\} \cup \{O\}$$

이다. 이러한 타원곡선에서는 이항연산 " + "이 정의되어 이 연산에 대해 타원곡선은 가환군이 된다.([1]) 위와 같은 타원곡선 E가 있을 때, F의 algebraic closure $\overline{F}$에 대해

$$E(\overline{F}) = \{O\} \cup \{(x, y) \in \overline{F} \times \overline{F}: y^2 + xy = x^3 + a_2x^2 + a_6\}$$

으로 정의한다.

사상 $tr: F \to F_2$를 trace 라고 하면 $tr(a_2) = 0$, $tr(a_2') = 1$인 체 F의 임의의 원소 a_2, a_2 와 임의의 a_6 에 대하여

$$|E(a_2, a_6)| + |E(a_2', a_6)| = 2(q+1)$$

이 성립한다. 따라서 타원곡선의 위수를 구하는데 있어서는 $a_6 \in F$에 대해 $E(a_6) = E(0, a_6)$의 위수만 구하면 충분하다. $a_6 \neq 0$일 때 $E(a_6)$의 j-불

변자(j-invariant) $j(E)$를 $1/a_6(\in F)$로 정의한다. ($E(0)$는 supersingular curve로서 공격에 취약하여 논의에서 제외된다.) 앞으로는 F위의 모든 타원곡선을 $E(a_6), a_6\in F$의 형태라고 가정한다. 일반적으로 타원곡선 E는 다음 조건을 만족한다.

$$|E|=q+1-t,\ -2\sqrt{q}\le t\le 2\sqrt{q}$$

$$\phi^2(P)-[t]\phi(P)+[q]P=O\ \forall P\in E(\overline{F})$$

(단, $\phi:E(\overline{F})\to E(\overline{F})$ 는 q차 Frobenius 사상 ($(x,y)\mapsto(x^q,y^q), O\to O$), O는 E의 항등원이고, $m\in Z$에 대해서 $[m]:E(\overline{F})\to E(\overline{F})$는 연산 "+"의 m반복을 의미한다.) 여기서의 t는 E의 Frobenius trace이다. Schoof의 알고리듬은 충분한 수의 소수 l들(구체적으로 $\prod l>4\sqrt{q}$가 되도록)에 대하여 $x,y\in\overline{F}$에 관한 연립방정식

$$f_l(x)=0$$

$$y^2+xy=x^3+a_6$$

$$\phi^2(x,y)+[t_l]\phi(x,y)+[q_l](x,y)=O$$

(단, $q_l\equiv q(\bmod l)$이고 f_l은 타원곡선 $E(a_6)$의 l번째 나눔다항식(division polynomial)이다.([1]))

이 해를 갖게 되는 (유일한) $t_l\ (-l/2<t_l\le l/2)$을 계산하고 Chinese Remainder Theorem을 이용하여 $t(\bmod\prod l)$ 을 계산하여 결국 t와 $|E|=q+1-t$를 계산하는 것이다. Schoof 알고리듬의 단점은 계산에 쓰이는 많은 부분이 다항식환 $F[x]$에서의 modulo $f_l(x)$연산인데 비하여 $f_l(x)$의 차수($\sim l^2/2$) 가 너무 크다는 것이다. 이러한 단점을 극복하기 위한 것이 Schoof-Elkies-Atkin의 방법이다.

II. Schoof-Elkies-Atkin 알고리듬

타원곡선 $E=E(a_6)$와 소수 l에 대해 $E[l]$을 $\{P\in E(\overline{F}):[l]P=O\}$ 으로 정의하면 $E[l]$은 $E(\overline{F})$의 ϕ-불변부분군이고(즉, $\phi(E[l])=E[l]$이고) $l\neq 2$일 때, $E[l]\cong Z/lZ+Z/lZ$ 이다. ϕ의 $E[l]$에 대한 작용은 Z/lZ-선형이므로 다음의 두 가지 중 하나가 성립한다.

(1) ϕ가 Z/lZ에서 고유값을 가진다.

(2) ϕ가 Z/lZ에서 고유값을 가지지 않는다.

(1)의 경우 l을 E의 Elkies-소수라고 하고 (2)의 경우 Atkin-소수라고 한다.

1. Elkies-소수의 판별

l을 임의의 소수라고 하고 $\Phi_l(x,y)\in Z[x,y]$를 l번째 modular-다항식이라고 하자.([1])

$\Phi_l(x,y)$ 를 다항식환 $F[x,y]$의 원소로 보면 $\Phi_l(x,j(E))\in F[x]$인데 $\Phi_l(x,j(E))$를 $F[x]$에서 소인수분해하면 다음의 두 가지 성질 중 하나가 성립한다.

(1) 일차의 인수를 가진다.

(2) 일차가 아닌 같은 차수의 소인수들을 가진다.

(1)의 경우 즉, 일차인수를 가지는 경우가 정확히 l이 Elkies-소수인 경우이다.

2. l이 Atkin-소수일 경우

$\Phi_l(x,j(E))$의 소인수들의 차수를 r이라고 하면 $r|l+1$이고 t는 다음의 식을 만족한다.

$$t^2=q(\zeta+1/\zeta+2)(\bmod l)$$

(단, ζ는 F_{l^2}의 r차 원시근(r-th primitive root of unity) 중의 하나이다.)

$r=2$일 경우 $t\equiv 0(\bmod l)$이고 그렇지 않을 경우에는 $t\not\equiv 0(\bmod l)$임을 알 수 있다. 또한 F_{l^2}의 r차 원시근들은 다음 사실을 이용하여 구할 수 있다: u를 유한체 F_{l^2}의 임의의 (l^2-1)차 원시근 ((l^2-1)-th primitive root of unity)이라고 할 때, $\zeta\in F_{l^2}$가 r차 원시근일 필요충분조건은 $1<i<r, \gcd(i,r)=1$인 어떤 i에 대해서 $\zeta=u^{i(l^2-1)/r}$인 것이다. 결국 l이 Atkin-소수일 경우 $\phi_{Euler}(r)$개의 $t(\bmod l)$의 후보들을 구할 수 있다.(단, ϕ_{Euler}는 Euler ϕ-함수이다.)

3. l이 Elkies-소수일 경우

l이 E의 Elkies-소수라고 하자. 위에서 본 바와 같이 방정식 $\Phi_l(x,j(E))=0$는 F에서 해 j'를 가

진다. $a_6' = 1/j' \in F$ 라고 하면 E에서 $E(a_6')$로의 isogeny 사상 ϕ가 존재한다.([1]) ϕ를 이용하여 차수가 $(l-1)/2$인 적당한 $F_l(x) \in F[x]$를 정의할 수 있는데 정의에 의해 $F_l(x) | f_l(x)$이다. ($F_l(x)$의 계산은 다음 장에서 다룬다.) $F_l(x)$를 구한 후 다음의 연립방정식이 해를 가지는 $\lambda(-l/2 < \lambda \le l/2)$를 구한다.

$$F_l(x) = 0$$

$$y^2 + xy = x^3 + a_6$$

$$\phi(x,y) = [\lambda](x,y)$$

일단 $F_l(x)$가 결정되면 위의 λ는 유일하고 $t \equiv \lambda + q/\lambda \pmod{l}$이다.

4. $t \pmod{2^c}$ 의 계산

다음과 같이 $F[x]$의 원소들 $\{g_i(x)\}_{0 \le i \le c-1}$을 정의한다.

$$g_0(x) = x,\ g_1(x) = x + \sqrt[4]{a_6},\ \cdots,$$
$$g_i(x) = (g_{i-1}(x))^2 + \sqrt[2^{i+1}]{a_6} \prod_{j=1}^{i-2} (g_j(x))^2,\ (i \ge 2)$$

그러면 $g_{c-1}(x)$는 $f_{2^c}(x)$의 2^{c-2}차의 인수이고 다음의 연립방정식이 해를 가지는 $\lambda(-2^{c-1} < \lambda \le 2^{c-1})$가 $t \pmod{2^c}$이다.

$$g_{c-1}(x) = 0$$

$$y^2 + xy = x^3 + a_6$$

$$\phi(x,y) = [\lambda](x,y)$$

III. Elkies-소수 $l(\neq 2)$에 대해서 다항식 $F_l(x)$의 계산 : Lercier의 방법

이제 $d = (l-1)/2$라고 하자. 다음의 관계식들을 만족시키는 d차 다항식 $P(x) = \sum_{i=0}^{d} p_i^2 x^i \in F[x]$를 구한다.

$$p_0 = \sqrt[4]{a^{2d} + a^{2d-1} p_{d-1}},\quad p_d = 1,\ p_{d-1} = \alpha + \beta \qquad (0.1)$$

$$p_{d-2} = \begin{cases} p_{d-1}^4 + \alpha p_{d-1} + \alpha^2 & (d: \text{홀수}) \\ p_{d-1}^4 + \alpha p_{d-1} & (d: \text{짝수}) \end{cases} \qquad (0.2)$$

$$\sqrt[4]{\alpha} \sum_{i=0}^{k} p_i^2 p_{d-k+i}^2 \alpha^{2i} = \sqrt[4]{\beta}\sqrt{\alpha}^{d+2k} \sum_{i=0}^{\lfloor k/2 \rfloor} p_{k-2i} \varepsilon_{d-k+2i,i} \qquad (1)$$
$$(\forall k = 0, \cdots, d)$$

$$p_k^4 = \alpha^{2d-4k-1} \sum_{i=0}^{k} p_{d-2k-1+2i} \varepsilon_{d-2k-1+2i,i} \alpha^{2i} + \alpha^{2d-4k} \sum_{i=0}^{k} p_{d-2k+2i} \varepsilon_{d-2k+2i,i} \alpha^{2i} \qquad (2)$$
$$(\forall k = 0, \cdots, \lfloor \frac{d-1}{2} \rfloor)$$

$$p_{d-k}^4 = \alpha \sum_{i=0}^{k-1} p_{d-2k+1+2i} \varepsilon_{d-2k+1+2i,i} \alpha^{2i} + \sum_{i=0}^{k} p_{d-2k+2i} \varepsilon_{d-2k+2i,i} \alpha^{2i} \qquad (3)$$
$$(\forall k = 0, \cdots, \lfloor \frac{d}{2} \rfloor)$$

(단, $\alpha = \sqrt[4]{a_6}$, $\beta = \sqrt[4]{a_6'}$, $a_6' = 1/j'$, $\Phi_l(j', j(E)) = 0$ 이고, $\varepsilon_{k,i}$는 이항계수 $\binom{k}{i} \pmod 2$이다.) 이 때,

$F_l(x) = x^d + \sum_{i=0}^{d-1} \sqrt{\alpha/\beta}\, \alpha^{d-2i} p_{d-i}^2 x^i$이다.

1. $P(x)$의 계산

$K = 1, K_1 = 0, K_2 = 0$ 으로 초기화한다.

--1단계--

가) 귀납적으로 $p_0, \cdots, p_{K-1}$ 과 $p_{d-2K}, \cdots, p_d$가 Boole 변수들(즉, 0 또는 1의 값을 가질 수 있는 변수들) $\pi_0, \cdots, \pi_{K-2}$ 의 다항식으로 구해져 있음을 가정한다.

수식 (1)에서 $k = K$를 대입하면 다음 이차방정식을 얻는다.

$$p_K^2 + b_K p_K + c_K = 0$$

단, $b_K = \sqrt[4]{\beta}\sqrt{\alpha}^{d+2K} / (\alpha^{2K} \sqrt[4]{\alpha}) \in F$ 이고,

$$c_K=(\sqrt[4]{\alpha}\sum_{i=0}^{K-1}p_i^2p_{d-K+i}^2\alpha^{2i}+\sqrt[4]{\beta}\sqrt{\alpha}^{d+2K}\sum_{i=1}^{\lfloor K/2\rfloor}p_{K-2i}\varepsilon_{d-K+2i,i})/(\alpha^{2K}\sqrt[4]{\alpha})$$

이다. 이때, c_K 는 $\pi_0,\cdots,\pi_{K-2}$ 의 다항식임을 알 수 있는데,

$c_K/b_K^2=\sum_{\mu\in\{0,1\}^{K-1}}C_\mu\pi_0^{\mu_0}\cdots\pi_{K-2}^{\mu_{K-2}}(\ C_\mu\in F)$ 라 고 하고 $TS=\sum_{\{\mu:Tr_{F/F_2}(C_\mu)=0\}}\pi_0^{\mu_0}\cdots\pi_{K-2}^{\mu_{K-2}}$ 라고 하자. (단, $Tr_{F/F_2}:F\to F_2$ 는 trace함수이다.)

(a) 모든 μ에 대해 $Tr_{F/F_2}(C_\mu)=0$일 경우:

각각의 μ에 대해 $P_\mu\in F$ 를 방정식 $x^2+x+C_\mu=0$의 하나의 해라고 할 때,

$$p_K=b_K\pi_{K-1}+b_K\sum_{\mu=(\mu_0,\cdots,\mu_{K-2})\in\{0,1\}^{K-1}}P_\mu\pi_0^{\mu_0}\cdots\pi_{K-2}^{\mu_{K-2}}$$ 이다.

(b) 그렇지 않을 경우:

방정식 $TS=0$으로부터 $\pi_0,\cdots,\pi_{K-2}$에 관한 단항식 하나를 다른 것들의 적당한 합으로 표현할 수 있는데, 이를 다시 c_K/b_K^2 에 대입하고 새로운 TS를 구하면 (a) 의 경우로 돌아간다. 만약 특히 원래의 방정식 $TS=0$로부터 어떤 변수 π_i 를 다른 것들의 다항식으로 표현할 수 있으면 이를 이용하고 또한 미리 구한 $p_0,\cdots,p_{K-1}$ 과 $p_{d-2K},\cdots,p_d$들에 이 식을 대입하여 π_i를 제거한다. 만약 $K>d-2K-2$이면 2단계로 넘어간다.

나) 그렇지 않으면 K_1을 1만큼 증가시킨다. 수식 (2)에 $k=K$를 대입하면 다음을 얻는다.

$$p_{d-2K-1}=\alpha^{-(2d-4K-1)}p_K^4+\sum_{i=1}^{K}p_{d-2K-1+2i}\varepsilon_{d-2K-1+2i,i}\alpha^{2i}+\alpha\sum_{i=0}^{K}p_{d-2K+2i}\varepsilon_{d-2K+2i,i}\alpha^{2i}$$

만약 $K>d-2K-3$이면 2단계로 넘어간다.

다) 그렇지 않으면 K_2를 1만큼 증가시킨다. 수식 (3)에 $k=K+1$을 대입하면 다음을 얻는다.

$$p_{d-2K-2}=p_{d-K-1}^4+\sum_{i=1}^{K+1}p_{d-2K-2+2i}\varepsilon_{d-2K-2+2i,i}\alpha^{2i}+\alpha\sum_{i=0}^{K}p_{d-2K-1+2i}\varepsilon_{d-2K-1+2i,i}\alpha^{2i}$$

$K=d-2K-3$이면 2단계로 가고 그렇지 않으면 K를 1만큼 증가시키고 1단계를 계속한다.

--2단계--

1단계가 끝났으므로 각각의 $p_i,\ i=0,\cdots,d$가 많아야 K개의 Boole 변수들 $\pi_0,\cdots,\pi_{K-1}$에 관한 다항식으로 구해져 있다. 반면에 수식 (2)와 수식 (3)의 d개의 관계식 중 K_1+K_2개가 쓰였으므로 적어도 K개의 관계식이 남아있는데 이를 이용하여 $\pi_0,\cdots,\pi_{K-1}$의 값을 구한다.([1],[3])

IV. 모든 정보의 결합

이제, 앞에서의 결과들과 다음과 같은 Baby Step-Giant Step 방법에 의해 타원곡선 E의 Frobenius Trace t 를 구할 수 있다.

III장 4절의 내용에서 각각의 c에 대하여 $t(\mathrm{mod}2^c)$의 값을 구할 수 있는데 c의 값이 커짐에 따라 $t(\mathrm{mod}2^c)$의 값을 구하는 시간이 급격하게 늘어나고 이를 감안하여 $c=2^{\lfloor\log_2 n\rfloor}$으로 한다. 앞에서 구한 모든 홀수인 Elkies-소수들과 $2^{\lfloor\log_2 n\rfloor}$의 곱을 M_3라고 하자. II장 3절과 II장 4절에서의 결과와 Chinese Remainder Theorem을 이용하여 $t_3\equiv t(\mathrm{mod}M_3)$인 $t_3(0\le t_3<M_3)$를 구한다. Atkin-소수들을 두 개의 집합으로 나누어 각각의 집합의 원소들의 곱을 M_1 과 M_2 로 할 때 II장 2절의 내용에 의해 구할 수 있는 가능한 $t(\mathrm{mod}M_1)$의 개수와 $t(\mathrm{mod}M_2)$의 개수가 비슷하게 한다. 각각의 $t_1\equiv t(\mathrm{mod}M_1)$ 과 $t_2\equiv t(\mathrm{mod}M_2)$의 후보들에 대해 다음과 같은 r_1 과 r_2를 구한다.

$$r_1=(t_1-t_3)/M_2M_3(\mathrm{mod}M_1),|r_1|\le\lfloor M_1/2\rfloor$$

$$r_2=(t_2-t_3)/M_1M_3(\mathrm{mod}M_2),\ |r_2|<M_2$$

E위의 random한 점 P를 잡고 각각의 r_1에 대해 $Q_{r_1}=[q+1-t_3]P-[r_1M_2M_3]P$를 계산하고

순서쌍들의 집합 $\{(Q_{r_1}, r_1)\}$을 미리 정의해둔 E 위의 적당한 선형순서구조(linear partial ordering)에 따라 정렬한다. 그 후 각각의 r_2에 대해 $Q_{r_1} = [r_2 M_1 M_3]P$를 만족하는 r_1이 있는지를 검색한다. 일단 집합 $\{(Q_{r_1}, r_1)\}$가 정렬되어 있기 때문에 여러 가지 빠른 검색알고리듬을 적용할 수 있다. 만약 그러한 r_1이 있다면 $t = t_3 + M_3(M_1 r_2 + M_2 r_1)$이 구하려는 Frobenius Trace 일 가능성이 크다. (실제로 거의 항상 이것이 성립한다.) 이 t 가 정말로 올바른 값인지 확인하기 위해서는 E위의 random한 점 P'에 대해 $[q+1-t]P' = O$인지를 확인한다.

V. 구현

우리의 알고리듬은 임의의 홀수 n이 주어졌을 때, F_{2^n} 의 난수 $a_6(\neq 0)$ 를 생성하여 $E(a_6)$의 위수를 구한다. 유한체상의 사칙연산, 다항식들에 관한 알고리듬(Karatsuba 등), 그리고 큰 정수의 계산을 위해 V. Shoup의 NTL library를 이용하였고 modular-다항식 $\Phi_l(X, Y)$들은 미리 구해둔 것을 이용했다. 다음의 예들에서 base polynomial 이란 $F = F_2[T]/\langle f(T)\rangle$가 되도록 하는 n차 다항식 $f(T)$를 의미하는데 0차의 계수부터 오름차순으로 표현하였다. F의 난수는 $n-1$차 이하의 다항식으로 역시 오름차순으로 표현하되 뒷부분의 0들은 생략하였다.

(예 1) $n = 71$

The base polynomial : [1 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1]

Random number in F: [0 1 1 1 0 0 0 1 1 0 1 0 0 1 1 1 1 0 1 1 1 0 0 1 0 1 0 0 0 0 0 0 1 0 1 0 1 1 0 0 0 1 1 0 0 0 1 0 1 1 1 0 0 0 1 1 0 1 0 0 0 1 1 0 0 1 1 1]

Trace modulo 2^6: 45

3:Elkies ; Trace: 0.

5:Atkin ; Possible Traces: 0.

7:Atkin ; Possible Traces: 0.

11:Elkies ; Trace: 0.

13:Atkin ; Possible Traces: 2 11 3 10 6 7.

17:Elkies ; Trace: 15.

19:Atkin ; Possible Traces: 2 17 9 10 4 15 6 13.

23:Elkies ; Trace: 4.

29:Elkies ; Trace: 18.

Number of Possible Traces: 48

Trace: -54520639635

Order of the Curve: 2361183241489343246484.

(예 2) $n = 139$

The base polynomial :

[1 0 0 1 0 1 0 0 1 0 1]

Random number in F:

[0 0 0 0 0 1 1 0 1 0 0 1 1 0 0 0 1 1 1 0 1 0 1 1 1 1 1 1 0 0 1 0 1 1 1 0 1 0 1 1 0 1 1 0 1 1 1 1 0 1 1 1 1 0 0 0 0 0 1 1 0 1 1 0 0 1 1 0 1 1 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 1 1 0 1 0 0 0 0 1 0 0 0 0 0 0 0 1 0 0 0 1 0 1 0 0 1 0 1 0 0 1 1 0 1 1 1 1 0 1 0 0 1 0 1 1 1 0 1 1 1 0 1 1]

Trace modulo 2^7: 37

3:Atkin ; Possible Traces: 1 2.

5:Atkin ; Possible Traces: 2 3.

7:Atkin ; Possible Traces: 2 5.

11:Atkin ; Possible Traces: 2 9 3 8.

13:Elkies ; Trace: 10.

17:Atkin ; Possible Traces: 3 14 2 15 1 16.

19:Atkin ; Possible Traces: 9 10 7 12 1 18 8 11.

23:Atkin ; Possible Traces: 5 18 2 21.

29:Atkin ; Possible Traces: 4 25.

31:Elkies ; Trace: 23.

41:Elkies ; Trace: 31.

59:Atkin ; Possible Traces: 13 46 9 50 15 44 14 45.

71:Atkin ; Possible Traces: 7 64 4 67 3 68.

109:Atkin ; Possible Traces: 17 92 13 96 12 97 3 106 40 69.

Number of Possible Traces: 5898240

numtraces2: 960

numtraces1: 6144

Trace: 1289413116069810194213

Order of the Curve:

6968982874540819731717017829041914868676 76

VI. 맺음말

현재까지 알려진 여러 가지 공격법(anomalous attack, MOV attack, Weil Descent 등)에 안전하기 위해서는 선택된 타원곡선이 정의된 유한체 F_{2^n}을 n이 소수가 되도록 하며 그 타원곡선의 위수가 매우 큰 소수를 약수로 가져야 한다. 이러한 면에서 적은 시간에 곡선의 위수를 구하는 알고리듬이 필요하다. 현재 ECPC 알고리듬 중에서 Satoh-FGH의 알고리듬 등이 SEA알고리듬보다 훨씬 뛰어난 결과를 보인다고 알려져 있다. ([2]) 안전한 곡선을 구하는 데 있어서는 SEA 알고리듬의 일부분을 이용한 조기중단(Early-Abort)방법 등 SEA알고리듬에서는 아직도 많은 활용의 여지가 있다.

참고문헌

[1] I. Blake, G. Seroussi, and N. Smart, *Elliptic Curves in Cryptography*, LMS Lecture Note Series. 265 ,Cambridge University Press, 1999

[2] M. Fouquet, P. Gaudry, and R. Harley, "An extension of Satoh's algorithm and its implementation", J. Ramanujan Math. Soc. vol. 15 , pp. 281-318, 2000

[3] R. Lercier, "Computing Isogenies in F_{2^n}", LNCS 1122, pp. 197-212 , 1996