

일반화된 쌍선형넘기기 거꿀계산을 위한 보다 빠른 방법

Lael Cellier

lael.cellier@laposte.net

2026년 10월 5일

요약

Satoh는 최근에 일반화된 쌍선형넘기기 거꿀계산문제(generalized pairing inversion, GPI)에 대하여 전수탐색이나 고정변수오라클이 아니라 Miller 함수의 구조를 리용하는 알고리즘을 내놓았다. 보통곡선에서 그 기대계산량은 차수가 $\Omega(\ell)$ 인 뿌리찾기부분프로그램을 $(q^k - 1)/\ell^2$ 번 정도 호출하는것, 즉 $\tilde{O}((q^k - 1)/\ell)$ 번의 연산이다. 필자는 같은 문제에 대하여 다른 방법을 제시한다. 이 방법은 끼워넣기차수가 짝수 $k > 2$ 이고 짝수차 $e \geq 4$ 의 꼬임을 가지는 보통곡선들에서 성립하며 그 기대계산량은 각각 쌍선형넘기기 몇번의 비용이 드는 후보 $q^{k/e}/2$ 개이다. $\mathbb{F}_{q^k}$ 에서의 곱하기회수로 재면 Satoh의 알고리즘에 비한 개선은 상수와 로그인자를 무시할 때 $q^{k-k/e}/\ell$ 배이다. 분석은 Tate 쌍선형넘기기에서처럼 길이가 ℓ 의 배수인 Miller 순환을 다루는데 Satoh의 순환은 길이가 $q^{k/2} \equiv -1 \pmod{\ell}$ 이다. 목표 쌍선형넘기기는 최종소속검사를 통해서만 들어오므로 알고리즘은 Satoh의 쌍선형넘기기에 대한 GPI를 직접 풀며 쌍선형넘기기들 사이의 변환도, 리산로그도 어디에서도 쓰지 않는다. 축약된 쌍선형넘기기값과 원시 Miller 값의 노름은 서로 독립인 자리표이며 이것은 $\gcd(\ell, q^{k/2} - 1) = 1$ 이기때문에 성립하는 중국나머지정리의 사실이다. 따라서 이 방법은 x자리표쌍에 대한 탐색에 최종 쌍선형넘기기검사를 불인것이며 필자는 그 이상을 주장하지 않는다. 기술적핵심 — 두 변수를 모두 모르는 경우 원시 Miller 값의 다항식시간 거꿀계산 — 은 그 탐색공간을 확정하고 이 경로에서는 아무것도 그것을 줄일수 없다는것을 보여주는데 쓰인다. 이 검사는 최종거듭제곱을 하기 전의 원시 Miller 값을 입력으로 받는다 — 이것은 Satoh 자신의 Miller 거꿀계산알고리즘과 같은 입력으로서 어떤 규약도 이를 드러내지 않으며, 축약값으로부터 이 값으로 넘어가는것은 Galbraith, Hess와 Vercauteren의 거듭제곱거꿀계산단계인데 제6-8절은 이를 탐색으로 처리하고 명제 6.2는 이것을 노름을 통하여 단축할수 없다는것을 보여준다. 그리고 이 검사는 Satoh의 이전 Miller 거꿀계산연구의 노름관계를, 모르는 두 x자리표를 분리하는 $\mathbb{F}_q$ -선형사영과 결합한다. 이 두 x자리표는 $\mathbb{F}_{q^{k/2}}$ 의 서로 보충하는 $\mathbb{F}_q$ -부분공간들에 놓여있다. 이 부분체구조의 리용은 Akagi와 Nogami에게로 거슬러올라가지만 그들의 환원은 한 변수를 알고있을것을 요구한다. BN254에서 기대계산량은 $\mathbb{F}_{q^k}$ 에서의 곱하기 약 2^{2800} 번으로부터 2^{518} 번으로, BLS12-381에서는 약 2^{4325} 번으로부터 2^{772} 번으로 줄어든다. 이 값들은 모두 $\mathbb{F}_{q^k}$ 에서의 지표계산법(index calculus)의 계산량보다 훨씬 높다. 이 결과는 구조적인것이며 암호해독적인것은 아니다.

1 머리말

Galbraith, Hess와 Vercauteren [3]은 쌍선형넘기기(pairing) $e: G_1 \times G_0 \rightarrow \mu_\ell$ 에 대한 세가지 거꿀 계산문제를 갈라내었다. 그것은 한 변수가 주어지는 두 고정변수문제 FAPI-1과 FAPI-2, 그리고 목표값 z 만이 주어지고 어떤 원상쌍이든 허용되는 일반화된 문제 GPI이다.

Satoh [7]는 군들중 하나를 탐색하는것이 아니라 쌍선형넘기기계산의 수학적구조를 리용하는 알고리즘이 알려져있지 않다는것을 지적하고 그러한 알고리즘을 제시하였다. 그는 ℓ 번째 Miller 함수를 인자계(factor system)로 써서 Ate 쌍선형넘기기의 분해를 얻고 이로부터 뿌리찾기단계를 통하여 GPI의 풀이를 조립한다. 그 결과로 얻어지는 절차([7, Alg. 6.1])는 $\gamma \in \mu_{\nu(s-1)}$ 에 대하여 순환하며(여기서 $s = q^{k/2}$, $\nu = (s+1)/N$) 매 단계마다 차수 $(N-1)/2$ 인 함수 φ 의 뿌리를 찾는다. 보통곡선에서는 $\nu(s-1) = (q^k - 1)/\ell$ 이고 단계당 성공확률은 많아야 $(\ell - 1)/((s-1)\nu)$ 이므로 [7, Rem. 6.5] 기대계산량은 차수 $\ell/2$ 의 뿌리찾기 약 $(q^k - 1)/\ell^2$ 번, 즉 $\tilde{O}((q^k - 1)/\ell)$ 번의 연산이다. Satoh는 이 경우를 《 q 가 작은 값일 때에도 수치실험을 하기에는 너무 비효율적》이라고 서술하였다.

이 논문은 같은 문제에 대하여 기대계산량이 더 작은 다른 방법을 제시한다. 이 방법은 Satoh 의것과 마찬가지로 최종 쌍선형넘기기검사를 가진 맹목탐색이며 — 여기서는 x 자리표쌍들에 대한 탐색이다 — 명제 6.2는 Miller 값의 노름우에 세워진 어떤 방법도 그밖의것으로 될수 없는 리유를 보여준다. 즉 축약된 쌍선형넘기기값과 그 노름은 서로 독립인 자리표이다. 문제설정에서 본질적인 두가지 점을 처음부터 밝혀둔다.

순환길이. 이 방법은 $\mathbb{F}_q$ -유리변수 $A \in G_1$ 에서의 Miller 함수 $h_{d,A}$ 를 자취가 령인 변수 $Q \in G_0$ 에서 계산하며 순환길이 d 는 ℓ 의 배수이다 — 이것이 Tate 설정이다. Satoh의 알고리즘 6.1은 이 논문의 기호로 $h_{q^{k/2}, -Q}(A)$ 를 내놓는데(그의 문자 A 와 Q 는 필자의것과 반대이다. 즉 그의 A 는 G_0 에 속한다) 이것은 자취가 령인 변수에서의 Miller 함수이고 순환길이는 $s = q^{k/2}$ 이다. 중요한 구별은 방향이 아니라 순환길이를 ℓ 로 나눈 나머지이다. 이 논문이 기초하는 노름관계(명제 3.1)는 $d \equiv 0 \pmod{\ell}$ 일 때 $(\xi(Q) - \xi(A))^d$ 를 주고 $d \equiv -1 \pmod{\ell}$ 일 때 $(\xi(Q) - \xi(A))^{d-1}$ 을 주는데 후자는 $d = s$ 일 때 항등적으로 1이다 (주의 3.2). 그러므로 이 방법은 [7, Alg. 6.1]의 내부단계를 대신하는것이 아니며 필자도 그렇다고 주장하지 않는다. 옳은것은 목표 쌍선형넘기기가 최종소속 검사를 통해서만 이 방법에 들어온다는것이며 따라서 그것을 Satoh의 쌍선형넘기기 그자체로 잡을 수 있다는것이다(제 6절). 쌍선형넘기기들사이의 변환은, 특히 리산로그는 어디에서도 나타나지 않는다.

새로운 점. 이 방법의 핵심은 A 와 Q 를 모두 모르는 원시 Tate-Miller 값 $h_{d,A}(Q)$ 가 주어졌을 때 A 와 Q 를 복원하는 다항식시간절차이다(제 5절). 이 절차는 Satoh가 고정변수설정에서 리용한 노름관계 [6]를, 모르는 두 x 자리표를 분리하는 선형사영과 결합한다. 이 두 x 자리표는 $\mathbb{F}_{q^{k/2}}$ 의 서로 보충하는 $\mathbb{F}_q$ -부분공간들에 놓여있다(제 4절). 이 부분체구조를 처음으로 리용한것은 Akagi 와 Nogami [1]로서 그들은 주어진 x 자리표의 최소다항식을 만들어 FAPI-2에 대한 거듭제곱거꿀계 산문제를 어께수 $q - 1$ 의 경우으로 환원한다. 그들의 구성은 $\text{Tr}(\xi(Q)^3)$ 과 $N(\xi(Q))$ 를 필요로 하며 Q 를 모르는 경우으로는 옮겨지지 않는다. 《한개의 미지수, 최소다항식》으로부터 《두개의 미지수, 선형사영》에로의 이행이 기술적으로 새로운 점이다. 이것을 중심으로 이 논문은 다음의것들을

보충한다. 쌍선형넘기기값과 노름의 독립성(명제 6.2) — 이것은 탐색공간을 확정하고 이 경로에 서는 그것을 줄일수 없다는것을 보여준다. 순환길이 s 와 q 의 Miller 값을 축약 Tate 쌍선형넘기기의 거듭제곱으로 나타내는 명시적공식(보조정리 3.3, 주의 3.4) — 이것으로 하여 알고리즘은 Satoh 의 쌍선형넘기기들을 직접 목표로 할수 있다. 그리고 [7, Alg. 6.1]에 비한 개선을 네개의 인자로 나누어 각각을 이 결과들중 하나에 귀속시키는 계산(제 10절).

덧붙여 GPI가 암호학적결과를 가지지 않는것은 아니라는것을 지적해둔다. Groth16 증명 [5]은 단 하나의 쌍선형넘기기공방정식이 성립하기만 하면 받아들여지며, 그 세번째 원소를 $\mathcal{O}$ 로 놓으면 검증열식와 공개입력만으로 계산할수 있는 목표값이 남는다. 따라서 GPI의 임의의 풀이는 임의의 명제에 대한 위조증명을 준다. BN254와 BLS12-381우의 Groth16은 실지 운영되고있는 암호화폐 체계들을 보호하고있으므로 이러한 위조는 곧 자금의 절취로 된다. 이것은 제 10절의 계산량으로 보아 실현될수 없는것이지만 FAPI만이 아니라 GPI도 주시하여야 할 리유로 된다.

2 설정과 기호

q 를 홀수수의 거듭제곱, $E/\mathbb{F}_q$ 를 짧은 Weierstrass 모형 $Y^2 = X^3 + a_4X + a_6$ 을 가지는 보통타원 곡선이라고 하자. ℓ 을 $\ell \parallel \#E(\mathbb{F}_q)$ — 정확한 나누어짐, 즉 $\ell \mid \#E(\mathbb{F}_q)$ 이고 $\ell^2 \nmid \#E(\mathbb{F}_q)$ 이며 따라서 $h := \#E(\mathbb{F}_q)/\ell$ 은 ℓ 로 나누어지지 않는다(보조정리 6.1에서 이것이 필요하다) — 이고 끼워넣기차수(embedding degree)가 짝수 $k > 2$ 인 홀수수라고 하자. $k = \text{ord}_\ell(q)$ 는 $\ell - 1$ 을 나누므로 자동적으로 $\ell \nmid k$ 이다. [7, §5]에 따라 다음과 같이 놓는다.

$$s := q^{k/2}, \quad G_0 := \{P \in E[\ell] : \text{Fr}_q P = [q]P\}, \quad G_1 := E(\mathbb{F}_q) \cap E[\ell].$$

그러면 $G_0 \cong G_1 \cong \mathbb{Z}/\ell\mathbb{Z}$, $G_0 \cap G_1 = \{\mathcal{O}\}$ 이고 $E[\ell] = G_1 \oplus G_0$ 이다. $\ell \mid s + 1$ 이므로 $P \in G_0$ 에 대하여 $\text{Fr}_q^{k/2} P = -P$ 이다. 또한 $\ell \nmid s - 1$ 이므로 $E[\ell]$ 우에서 $\text{Fr}_q^{k/2}$ 의 고유값은 G_1 우에서 1, G_0 우에서 -1 뿐이며 따라서

$$E[\ell] \cap \ker(\text{Fr}_q^{k/2} - 1) = G_1, \quad E[\ell] \cap \ker(\text{Fr}_q^{k/2} + 1) = G_0. \quad (1)$$

ξ, η 는 자리표함수, $\tau := -\xi/\eta$ 는 $\mathcal{O}$ 에서의 국소매개변수(uniformizer), $h_{n,A}$ 는 A 에서의 정규화된 n 번째 Miller 함수, 즉 $\text{div } h_{n,A} = n[A] - [nA] - (n-1)[\mathcal{O}]$ 이고 τ 에 관하여 $\text{lc}_{\mathcal{O}}(h_{n,A}) = 1$ 인 함수를 나타낸다.

이하 언제나 $A \in G_1$, $Q \in G_0$ 이고 d 는 다음을 만족시키는 옹근수이다.

$$\ell \mid d; \quad (2)$$

d 제곱뿌리를 구해야 할 때(보조정리 3.5)에는 [6, Alg. 4.1]의 두번째 조건인 $d \mid s+1$ 을 더 가정한다. 원시 Miller 값은 $v := h_{d,A}(Q) \in \mathbb{F}_{q^k}^\times$ 이고 축약 Tate 쌍선형넘기기는 $t(A, Q) := h_{\ell,A}(Q)^{(q^k-1)/\ell} \in \mu_\ell$ 인데 이것은 $G_1 \times G_0$ 우에서 쌍선형이고 비퇴화이다.

3 노름관계

명제 3.1. 우의 기호에서 $\ell \mid d$ 만을 리용하면

$$v^{s+1} = (-1)^d (\xi(Q) - \xi(A))^d \quad (3)$$

이다. 특히 $d = \ell$ 이면 $v^{s+1} = -(\xi(Q) - \xi(A))^\ell$ 이다.

증명. $\ell \mid d$ 이고 $A \in E[\ell]$ 이므로 $[d]A = \mathcal{O}$ 이고 $\text{div } h_{d,A} = d([A] - [\mathcal{O}])$ 이다. 마찬가지로 $\text{div } h_{d,-A} = d([-A] - [\mathcal{O}])$ 이다. 그러므로 $h_{d,A}h_{d,-A}$ 와 $(\xi - \xi(A))^d$ 는 같은 인자(divisor) $d([A] + [-A] - 2[\mathcal{O}])$ 를 가지며 $\xi = \tau^{-2} + O(\tau^{-1})$ 이므로 두 함수 모두 $\mathcal{O}$ 에서 선두결수(leading coefficient)가 1이다. 따라서

$$h_{d,A} h_{d,-A} = (\xi - \xi(A))^d. \quad (4)$$

다음으로 $h_{d,A} \circ [-1]$ 과 $h_{d,-A}$ 는 같은 인자를 가진다. 짧은 Weierstrass 모형에서는 $\tau \circ [-1] = -\tau$ 이고 $\text{ord}_{\mathcal{O}} h_{d,A} = -d$ 이므로 $\text{lc}_{\mathcal{O}}(h_{d,A} \circ [-1]) = (-1)^d$ 이며 이로부터

$$h_{d,A} \circ [-1] = (-1)^d h_{d,-A}. \quad (5)$$

끝으로 $h_{d,A}$ 는 $\mathbb{F}_q$ 위에서 정의되고 $\text{Fr}_q^{k/2} Q = -Q$ 이므로 (5)에 의하여 $v^s = h_{d,A}(\text{Fr}_q^{k/2} Q) = h_{d,A}(-Q) = (-1)^d h_{d,-A}(Q)$ 이고 $v^{s+1} = v \cdot v^s = (-1)^d (h_{d,A} h_{d,-A})(Q)$ 인데 이것은 (4)에 의하여 (3)이다. $\square$

(3)의 오른변에는 Miller 값이 들어있지 않다. [6, Alg. 4.1]의 기초로 되는 인수분해 $h_{s+1,A} = (\xi - \xi(A)) h_{s,A}$ 와 비교해보라. 거기서는 인수 $h_{s,A}(Q)$ 가 $(s+1)$ 제곱에 의하여 소거된다. 그 정확한 구조는 보조정리 3.3이 준다. 즉 $h_{s,A}(Q) = -t(A, Q)^{-1/2}$ 이며 이것은 위수가 정확히 2ℓ 이고 그 위수가 $s+1$ 을 나누는 원소이다. μ_ℓ 에 속하는것은 그 부호를 바꾼 $-h_{s,A}(Q) = t(A, Q)^{-1/2}$ 이다. 자취가 려인 변수에서의 Miller 함수를 쓰면 그대신 $h_{s,Q}(A) = t(Q, A)^{-1/2} \in \mu_\ell$ 이 얻어지는데 이것은 이 설정에서의 [4]의 주장을 명시적공식과 함께 표현한것이다. 이것이 Satoh가 《(최종거듭제곱 전의 값) = (단순한 함수) $\times$ (다른 쌍선형넉기기)》라고 서술한 현상이다. 상수에 대하여 두가지를 지적한다. 첫째로, 그것은 이미 알려진 부호이며 미리 계산해두어야 할 량이 아니다. 둘째로, Miller 함수를 $\mathcal{O}$ 에서 정규화하지 않는 프로그램들(PARI/GP의 `elltatepairing`이 그 실례이다)은 그것을 다른 상수로 바꾼다. 그 상수가 역시 A 와 Q 에 무관하다는것은 제 9절의 시험곡선(toy curve)에서 얻은 PARI의 직선함수정규화에 대한 경험적관찰이며 그 경우 상수는 알려진 쌍 하나로부터 읽어낼수 있다.

주의 3.2 (방향이 아니라 순환길이). $[n]P \neq \mathcal{O}$ 인 임의의 순환길이 n 에 대하여 같은 인자계산은 부호없이 정확하게 다음을 준다.

$$h_{n,P} h_{n,-P} = \frac{(\xi - \xi(P))^n}{\xi - \xi([n]P)} \quad (6)$$

여기서 량변은 $\mathcal{O}$ 에서 선두결수가 1이다. (6)은 어느 군에 속하는 P 에 대해서도 성립한다. ((5)의 부호는 $(-1)^{\text{ord}_{\mathcal{O}} h_{n,P}}$ 이며 이것은 $[n]P \neq \mathcal{O}$ 일 때 $(-1)^{n-1}$, $\ell \mid n$ 일 때 $(-1)^n$ 이다. 이 부호는 $h_{n,-P}$

를 R 에서 계산하는 대신 $h_{n,P}$ 를 $-R$ 에서 계산할 때에만 나타난다.) n 을 ℓ 로 나눈 나머지에서 세가지가 문제로 된다.

$n \equiv 0 \pmod{\ell}$ 이면 분모는 1이고 노름관계는 $(\xi - \xi(P))^n$ 을 복원한다. 이것이 명제 3.1이며 이 관계는 두 방향에서 모두 성립한다. Ate 방향에서는 $\text{Fr}_q^{k/2}$ 가 $h_{n,Q}$ 의 곱수들에 작용하여 그것을 $h_{n,-Q}$ 로 보내는데 부호를 바꾼 점에서의 계산이 없으므로 부호도 생기지 않는다. 따라서

$$h_{\ell,Q}(A)^{s+1} = (\xi(A) - \xi(Q))^\ell = -(\xi(Q) - \xi(A))^\ell = h_{\ell,A}(Q)^{s+1} \quad (Q \in G_0, A \in G_1) : \quad (7)$$

두 노름은 일치한다.

$n \equiv -1 \pmod{\ell}$ 이면 $[n]P = -P$ 이고 (6)은 $(\xi - \xi(P))^{n-1}$ 로 된다. $n = s$ 이면 어깨수 $s-1$ 이 $\mathbb{F}_{q^{k/2}}^\times$ 를 소멸시키므로 항등적으로 $h_{s,P}(R)^{s+1} = 1$ 이며 x자리표에 관한 정보는 아무것도 남지 않는다. 이것이 보통곡선의 경우에 [7, Alg. 6.1]이 리용하는 순환이며 그 알고리즘에 이 논문의 검사를 넣을수 없는 리유이다. 다른 $n \equiv -1 \pmod{\ell}$, 실제로 $n = 2\ell - 1$ 에 대해서는 노름이 자명하지 않지만 그것은 ζ 를 $\gcd(n-1, s-1)$ 개의 후보까지밖에 결정하지 못한다. 그 수는 시험곡선에서 48, BN254에서 $48u \approx 2^{67.7}$ 이다(이 값은 그 곡선에 대하여 계산한것이다. 일반적으로 $\gcd(2\ell-2, s-1)$ 은 $\gcd(\ell-1, q-1) = 6u$ 의 배수인데 보조인수 $6u^3 + 6u^2 + 3u + 1$ 과 $6u^3 + 6u^2 + 4u + 1$ 은 서로 1 이외의 공약수를 가지지 않으며 인수 8은 $s-1$ 의 다른 인수들에서 나온다). 뿌리의 유일성이 바로 $\ell \mid d \mid s+1$ 이 $\gcd(d, s-1) = \gcd(d, 2)$ 를 통하여 얻어주는것이며(보조정리 3.5) 또한 바로 $n \equiv -1 \pmod{\ell}$ 이 잃는것이다.

$P = Q \in G_0$ 인 Ate 순환 $T = t - 1$ 에서처럼 $n \equiv q \pmod{\ell}$ 이면 $[n]Q = \text{Fr}_q Q$ 이고

$$h_{T,Q}(A)^{s+1} = \frac{(\xi(A) - \xi(Q))^T}{\xi(A) - \xi(Q)^q} \quad (8)$$

이며 여기서도 부호는 없다. $\xi(A) \in \mathbb{F}_q$ 이므로 분모는 $(\xi(A) - \xi(Q))^q$ 이고 따라서 (8)은 $h = \#E(\mathbb{F}_q)/\ell$ 에 대하여 $(\xi(A) - \xi(Q))^{T-q} = (\xi(A) - \xi(Q))^{-h\ell}$ 로 줄어든다. 즉 그것은 (7)의 $(-h)$ 제곱이며 — 부호가 아니라 거꿀수를 취한것이다 — $\ell \mid d$ 만을 필요로 하는 $d = h\ell$ 인 명제 3.1과 같은 정보를 담고있다. (이와 일치하게 정규화된 함수로서 $h_{q,Q} = h_{T,Q} h_{\ell,Q}^h$ 이고 $h_{q,Q}(A)^{s+1} = 1$ 이다.) 이 주의의 모든 항등식은 수값적으로 검사되었다(제 9절).

보조정리 3.3. $P \in E[\ell]$ 에 대하여 유리함수로서

$$h_{s,P}^\ell = \frac{h_{\ell,P}^s}{h_{\ell,-P}} \quad (9)$$

이 성립한다. 또한 령이 아닌 두 점 $A \in G_1, Q \in G_0$ 에 대하여, $t(\cdot, \cdot)$ 를 어느 변수순서로든 축약 Tate 쌍선형넘기기라고 하면

$$t(A, Q) = h_{s,A}(Q)^{-2}, \quad t(Q, A) = h_{s,Q}(A)^{-2} \quad (10)$$

이며 따라서 $h_{s,A}(Q) = -t(A, Q)^{-1/2}$ 이고 $h_{s,Q}(A) = t(Q, A)^{-1/2}$ 이다. 여기서 두제곱뿌리는 μ_ℓ 에서의 유일한것을 취한다. 특히 $h_{s,Q}(A) \in \mu_\ell$ 의 위수는 정확히 ℓ 이며 $h_{s,A}(Q)$ 의 위수는 정확히 2ℓ 이고 $2\ell \mid s+1$ 이다.

증명. 합성규칙 $h_{mn,P} = h_{m,P}^n h_{n,[m]P}$ (량변의 인자가 같고 양변이 정규화되어있다)로 $h_{\ell s,P}$ 를 두 가지 방법으로 계산하면 $h_{s,P}^\ell h_{\ell,[s]P} = h_{\ell,P}^s h_{s,[\ell]P}$ 를 얻는다. $[s]P = -P$ 이고 $h_{s,\mathcal{O}} = 1$ 이므로 이것이 (9)이다. 값을 계산하면, Ate 방향에서는 곱수들의 공액에 의하여 $h_{\ell,Q}(A)^s = \text{Fr}_q^{k/2}(h_{\ell,Q}(A)) = h_{\ell,-Q}(A)$ 이므로 $h_{s,Q}(A)^\ell = 1$ 이고, Tate 방향에서는 ℓ 이 홀수이므로 (5)에 의하여 $h_{\ell,A}(Q)^s = h_{\ell,A}(-Q) = -h_{\ell,-A}(Q)$ 이며 따라서 $h_{s,A}(Q)^\ell = -1$ 이다.

(10)에 대해서는 $[\ell]A = [s+1]A = \mathcal{O}$ 일 때 같은 규칙이 모든 c 에 대하여 $h_{\ell,A}^c = h_{\ell c,A}$ 와 $h_{(s+1)(s-1),A} = h_{s+1,A}^{s-1}$ 을 주며 인자들로부터 $h_{s+1,A} = (\xi - \xi(A)) h_{s,A}$ 가 나온다. 따라서 $\zeta = \xi(Q) - \xi(A) \in \mathbb{F}_{q^{k/2}}^\times$ 로 놓으면

$$\begin{aligned} t(A, Q) &= h_{\ell,A}(Q)^{(q^k-1)/\ell} = h_{q^k-1,A}(Q) = h_{s+1,A}(Q)^{s-1} \\ &= \zeta^{s-1} h_{s,A}(Q)^{s-1} = h_{s,A}(Q)^{s-1} = h_{s,A}(Q)^{-2} \end{aligned}$$

이다. 마지막 단계는 $h_{s,A}(Q)^{2\ell} = 1$ 이고 $2\ell \mid s+1$ 이기 때문이다. Ate 경우는 A 와 Q 를 바꾸어놓으면 똑같다. ℓ 이 홀수이므로 두제곱하기는 μ_ℓ 의 일대일대응이며 이것이 두제곱뿌리를 확정한다. $h_{s,A}(Q)$ 의 부호는 $h_{s,A}(Q)^\ell = -1$ 에 의하여 정해진다. 끝으로 비퇴화성에 의하여 $t(A, Q) \neq 1$ 이므로 $h_{s,A}(Q)^2 \neq 1$ 이고 그 위수는 2가 아니라 정확히 2ℓ 이다. 마찬가지로 $h_{s,Q}(A) \neq 1$ 이고 그 위수는 정확히 ℓ 이다. $\square$

네가지 결과가 나온다. 첫째로, 순환길이 s 의 Miller 값은 최종거듭제곱이 없이 축약 Tate 쌍선형 넘기기의 $-1/2$ 제곱 그자체이다. Satoh가 말한 《다른 쌍선형 넘기기》는 문자 그대로이다. 그것은 원시 Miller 값으로서 두 변수에 관하여 쌍선형이며 이것은 직접 검사되었다(제 9절). 둘째로, 부호는 다시 (5)의 $(-1)^\ell$ 이며 이것은 (7)의 기구이다. (9)는 [4]의 Ate 방향의 주장을 두줄로 준다. 셋째로, $d = \ell$ 일 때의 명제 3.1은 같은 항등식을 다시 읽은것이다. 즉 $h_{\ell,A}(Q)^{s+1} = h_{s+1,A}(Q)^\ell = \zeta^\ell h_{s,A}(Q)^\ell = -\zeta^\ell$ 이다. 넷째로, 같은 규칙이 순환길이 q 일 때의 값을 준다(주의 3.4).

주의 3.4 (순환길이 q). 같은 합성규칙을 $h_{q^k,Q}$ 에 적용하면 $h_{q^k,Q} = \prod_{i=0}^{k-1} h_{q,[q^i]Q}^{q^{k-1-i}}$ 를 얻으며, $[q^i]Q = \text{Fr}_q^i Q$ 이고 A 가 유리점이므로 $h_{q,\text{Fr}_q^i Q}(A) = h_{q,Q}(A)^{q^i}$ 이고 따라서 $h_{q^k,Q}(A) = h_{q,Q}(A)^{kq^{k-1}}$ 이다. 한편 $\text{div } h_{q^k,Q} = (q^k - 1)([Q] - [\mathcal{O}]) = \text{div } h_{\ell,Q}^{(q^k-1)/\ell}$ 이므로 $h_{q^k,Q}(A) = t(Q, A)$ 이다. 이것만으로는 $h_{q,Q}(A) \in \mu_{k\ell}$ 이 나온다. 그것이 μ_ℓ 에 속한다는것은 같은 규칙을 $h_{q\ell,Q}$ 에 적용한 $h_{q,Q}^\ell h_{\ell,[q]Q} = h_{\ell,Q}^q$ 로부터 나오는데 $h_{\ell,Q}(A)^q = h_{\ell,\text{Fr}_q Q}(A)$ 이고 $[q]Q = \text{Fr}_q Q$ 이므로 $h_{q,Q}(A)^\ell = 1$ 이기 때문이다. 따라서 μ_ℓ 에서 뿌리가 유일하므로

$$h_{q,Q}(A) = t(Q, A)^{1/(kq^{k-1})} = t(Q, A)^{-1/(kq^{k/2-1})} \in \mu_\ell$$

이다. 마지막 형태는 $q^{k-1} = s q^{k/2-1} \equiv -q^{k/2-1} \pmod{\ell}$ 이기 때문이다 (그리고 $\ell \nmid k$ 이다. 제 2절). 그의 알고리즘 6.1을 순환길이 q 로 감싼 [7, Alg. 6.6]의 목표는 이 논문의 기호로 $h_{q,-Q}(A) = t(Q, A)^{1/(kq^{k/2-1})}$ 이다($h_{q,Q}(A)$ 는 t 의 고정된 거듭제곱이므로 Q 에 관하여 쌍선형이다). 따라서 제 8절의 15행에서 최종검사를 $t(Q, A) = z^{-kq^{k-1}}$ 로 하면 그 문제도 직접 풀린다. (수값적으로 검사되었다. 제 9절.)

보조정리 3.5. $d \mid s + 1$ 이라고 하자. 그러면 $\gcd(d, s - 1) = \gcd(d, 2)$ 이고 $u \in \mathbb{F}_{q^{k/2}}^\times$ 에 대하여 방정식 $\zeta^d = u$ 는 $\mathbb{F}_{q^{k/2}}^\times$ 에서 풀이를 가지지 않거나 정확히 $\gcd(d, 2)$ 개의 풀이를 가진다. 풀이가 있을 때

1. d 가 홀수이면 풀이는 유일하며 $u^{d^{-1} \bmod (s-1)}$ 이다.
2. d 가 짝수이면 풀이는 $\pm \zeta_0$ 이다. 여기서 ζ_0 은 하나의 풀이로서, d 를 $d = 2^a d'$ (d' : 홀수) 형태로 쓰고 $u_1 := u^{d'^{-1} \bmod (s-1)}$ 로 놓은 다음 임의의 표준적인 뿌리구하기 알고리즘으로 $\mathbb{F}_{q^{k/2}}$ 에서 u_1 의 두제곱뿌리를 a 번 연속 구하여 얻을 수 있다.

증명. 표준적이다. s 가 홀수이므로 $\gcd(s + 1, s - 1) = 2$ 이고 $\gcd(d, s - 1) \mid 2$ 이며 나머지는 [6, Thm. 4.2]의 증명에서처럼 순환군에서 $\zeta^d = u$ 의 풀이의 개수를 세는 것이다. 아래에서는 d 가 언제나 홀수이므로 경우 (i)만 쓰인다. $\square$

홀수인 $d = \ell$ 에 대해서는 경우 (i)이 적용된다. 경우 (ii)는 [6, Alg. 4.1, 단계 3–4]에서 볼 수 있는 부호의 모호성이며 거기서는 두개의 x자리표 $\xi(A) \pm u$ 가 만들어진다. 이것은 계산량을 두배로 할뿐이다.

4 분리보조정리

E 의 꼬임(twist) E' (차수 $e \mid k$)가 존재한다고 가정하고 $m := k/e$ 로 놓는다. k 가 짝수이므로 $e \geq 3$ 은 $e \in \{4, 6\}$ 을 뜻한다. $e = 3$ 인 꼬임은 $j(E) = 0$ 과 $6 \mid k$ 를 강요하므로 6차꼬임이 존재하며 따라서 $e = 3$ 은 결코 최대꼬임차수가 아니다. 그러므로 이하 e 는 언제나 짝수로 잡는다. 꼬임은 $\mathbb{F}_{q^m}$ 위에서 파라미터 $\theta \in \mathbb{F}_{q^m}^\times$ 에 의하여 정의되는데 그 류는 $\mathbb{F}_{q^m}^\times / (\mathbb{F}_{q^m}^\times)^e$ 를 생성하며 그러한 $\varphi(e)$ 개의 류가운데서 $\ell \mid \#E'(\mathbb{F}_{q^m})$ 인 것(통상적인 용어로 D형 또는 M형 꼬임)을 택한다. 꼬임동형넘기기 $\psi: E' \rightarrow E$ 는 $\omega := \theta^{2/e}$ 에 대하여 (x', y') 를 $(\omega x', \omega^{3/2} y')$ 로 보낸다. $G_0 = \psi(E'(\mathbb{F}_{q^m})[\ell])$ 이므로

$$\xi(P) \in W := \omega \mathbb{F}_{q^m} \quad (\text{모든 } P \in G_0 \setminus \{\mathcal{O}\} \text{에 대하여}) \quad (11)$$

이며 W 는 차원이 $m = k/e$ 인 $\mathbb{F}_q$ -부분공간이고 e 가 짝수이므로 $\mathbb{F}_{q^{k/2}}$ 에 포함된다. (이와 일치하게 ξ 가 짝함수이고 $\text{Fr}_q^{k/2}$ 가 G_0 우에서 $[-1]$ 로 작용하므로 $\xi(P) \in \mathbb{F}_{q^{k/2}}$ 이다. [7, Lem. 5.2].) 다른 한편 $A \in G_1$ 에 대해서는 $\xi(A) \in \mathbb{F}_q$ 이다.

보조정리 4.1 (분리). $e \in \{4, 6\}$ 이라고 가정하고 $\lambda := \omega^{q^m - 1}$ 로 놓는다. 그러면 $\omega \notin \mathbb{F}_{q^m}$ 이므로 $\lambda \neq 1$ 이고 $\mathbb{F}_q \cap W = \{0\}$ 이다. 또한 임의의 $Q_0 \in G_0 \setminus \{\mathcal{O}\}$ 에 대하여 $\lambda = \xi(Q_0)^{q^m} / \xi(Q_0)$ 이고 $\xi(Q_0) \in \mathbb{F}_{q^{k/2}}$ 이므로 $\lambda \in \mathbb{F}_{q^{k/2}}$ 이며 따라서 $\mathbb{F}_q$ -선형넘기기

$$L: \mathbb{F}_{q^{k/2}} \longrightarrow \mathbb{F}_{q^{k/2}}, \quad L(u) := u^{q^m} - \lambda u$$

는 잘 정의되고 $\ker L = W$, $L|_{\mathbb{F}_q} = (1 - \lambda) \text{id}$ 를 만족시킨다. 그리고 $\xi(Q) \in W$, $\xi(A) \in \mathbb{F}_q$ 인 $\zeta := \xi(Q) - \xi(A)$ 에 대하여

$$\xi(A) = \frac{L(\zeta)}{\lambda - 1}, \quad \xi(Q) = \zeta + \xi(A) \quad (12)$$

이다.

증명. 만일 $\omega \in \mathbb{F}_{q^m}$ 이면 $\theta^2 = \omega^e \in (\mathbb{F}_{q^m}^\times)^e$ 이므로 θ 의 류는 위수 e 인 순환군에서 위수가 2의 약수인데 그 군에서 그 위수는 e 이다. 따라서 $e \mid 2$ 로 되어 $e \geq 4$ 에 모순된다. 그러므로 $\omega \notin \mathbb{F}_{q^m}$, 즉 $\lambda \neq 1$ 이다. $a \neq 0$ 인 $a \in \mathbb{F}_q \cap W$ 가 있다면 $x' \in \mathbb{F}_{q^m}^\times$ 에 대하여 $a = \omega x'$ 이고 $\omega = a/x' \in \mathbb{F}_{q^m}$ 으로 되어 모순이다. 따라서 $\mathbb{F}_q \cap W = \{0\}$ 이다. $u \mapsto u^{q^m}$ 이 $\mathbb{F}_q$ -선형이므로 L 도 $\mathbb{F}_q$ -선형이다. $u = \omega x' \in W$ 에 대하여 $u^{q^m} = \omega^{q^m} x' = \lambda u$ 이므로 $L(u) = 0$, 즉 $W \subseteq \ker L$ 이다. 거꾸로 $\omega^{e/2} = \theta$ 이며 $X^{e/2} - \theta$ 는 $\mathbb{F}_{q^m}$ 위에서 기약이다. 그 차수 $e/2 \in \{2, 3\}$ 은 짝수이고 θ 는 $(e/2)$ 제곱이 아니기 때문이다. 만일 그렇다면 θ^2 도 e 제곱으로 되어 θ 의 류의 위수가 2의 약수로 될것이다. 따라서 $1, \omega, \dots, \omega^{e/2-1}$ 은 $\mathbb{F}_{q^{k/2}}$ 의 $\mathbb{F}_{q^m}$ -기저이며 $([\mathbb{F}_{q^{k/2}} : \mathbb{F}_{q^m}] = e/2$ 에 주의) 고유값이 $\lambda^j (0 \leq j < e/2)$ 인 $u \mapsto u^{q^m}$ 의 고유벡터들로 이루어진다. 이 고유값들은 $\lambda \neq 1$ 이고 $e/2$ 가 짝수인 조건에서 $\lambda^{e/2} = \theta^{q^m-1} = 1$ 이므로 서로 다르다. 그러므로 $u \mapsto u^{q^m}$ 은 대각화가능하며 $\ker L$ 은 그것의 λ -고유공간인데 이것은 $\omega \mathbb{F}_{q^m} = W$ 이다. $a \in \mathbb{F}_q$ 에 대하여 $a^{q^m} = a$ 이므로 $L(a) = (1 - \lambda)a$ 이다. L 을 ζ 에 적용하면 $L(\zeta) = -(1 - \lambda)\xi(A)$ 를 얻는데 이것이 (12)이다. $\square$

주의 4.2. $e = 2$ 이면 $m = k/2$ 이고 $W = \omega \mathbb{F}_{q^{k/2}} = \mathbb{F}_{q^{k/2}}$ 이다. 사영은 퇴화되지만($\lambda = 1, L = 0$) 아무것도 무너지지 않는다 — $\xi(A) \in \mathbb{F}_q$ 는 여전히 q 개의 가능한 값만을 가지므로 알고리즘 5.1의 3단계는 $x_Q = \zeta + x_A$ 로 하는 $x_A \in \mathbb{F}_q$ 에 대한 순환으로 되며 그 계산량은 $O(1)$ 대신 $O(q)$ 이다. 그리고 제 8절의 알고리즘은 일반공식의 계산량 $q^{k/e}/2 = q^{k/2}/2$ 로 $\mathbb{F}_q \times \mathbb{F}_{q^{k/2}}$ 를 돈다. 따라서 $O(1)$ 의 복호에는 4차 또는 6차 꼬임이 필요하며 — BN과 BLS12($e = 6$), KSS16($e = 4$), [1]의 Brezing–Weng 곡선들 — 2차꼬임만을 가지는 곡선들로는 안된다.

주의 4.3. $k = 2$ 이면, 특히 $t = 0$ 이 $k \leq 2$ 를 강요하는 [7, §4]의 초특이곡선들에서는 $s = q$ 이고 두 x 자리표가 모두 $\mathbb{F}_q$ 에 놓인다. 따라서 그것들을 분리하는 $\mathbb{F}_q$ -선형넘기기는 없다. 필자의 견해로는 이것이 [6](FAPI, 한 변수를 앞, 다항식시간)과 [7](GPI, 두 변수를 모름, 지수시간)의 쓸모있는 영역이 서로 겹치지 않는 구조적리유이다.

BN 곡선에서는 $e = 6, m = 2, L(u) = u^{q^2} - \lambda u$ 이고 $\lambda^3 = \theta^{q^2-1} = 1$ 이다. 즉 λ 는 1의 원시세제곱뿌리이다. 일반적으로 $\lambda^{e/2} = 1$ 이다. 이것은 곡선의 상수이며 알려진 임의의 G_0 -생성원으로부터 얻어진다.

주의 4.4 (G_0 에 대한 Legendre 검사). $\beta := x_Q^3 + a_4 x_Q + a_6 \neq 0$ 인 $x_Q \in \mathbb{F}_{q^{k/2}}$ 에 대하여 $y_Q \in \mathbb{F}_{q^k}, y_Q^2 = \beta$ 인 $Q = (x_Q, y_Q)$ 를 잡자. 그러면 $\text{Fr}_q^{k/2} Q = -Q$ 일 필요충분조건은 β 가 $\mathbb{F}_{q^{k/2}}$ 에서 두제곱이 아닌것이다. 실제로 $\text{Fr}_q^{k/2} Q = (x_Q, y_Q^s)$ 이고 $y_Q^s = -y_Q$ 일 필요충분조건은 $y_Q^{s-1} = \beta^{(s-1)/2} = -1$ 이다. 따라서 Q 가 $\ker(\text{Fr}_q^{k/2} + 1)$ 에 속하는가 하는것은 두제곱뿌리를 구하기 전에 $\mathbb{F}_{q^{k/2}}$ 에서의 Legendre 기호 하나로 판정되며 $\beta \neq 0$ 인 $x_Q \in \mathbb{F}_{q^{k/2}}$ 의 약 절반이 이 검사를 통과한다. $\beta(x)$ 가 두제곱이 아닌 $x \in \mathbb{F}_{q^{k/2}}$ 의 개수는 $(s + t_s - N_0)/2$ 이며 여기서 t_s 는 $\mathbb{F}_{q^{k/2}}$ 에서의 E 의 Frobenius 자취이고 $N_0 = \#\{\beta = 0\}$ 이다. 부분공간 $W = \omega \mathbb{F}_{q^m}$ 에서는 두 꼬임차수가 서로 다르게 행동한다. $e = 6(a_4 = 0)$ 일 때 $x_Q = \omega u$ 에 대하여 $\beta = \theta u^3 + a_6 \in \mathbb{F}_{q^m}$ 이고 $[\mathbb{F}_{q^{k/2}} : \mathbb{F}_{q^m}] = 3$ 이 홀수이므로 β 가 $\mathbb{F}_{q^{k/2}}$ 에서 두제곱이 아닐 필요충분조건은 그것이 $\mathbb{F}_{q^m}$ 에서 두제곱이 아닌것이다.

따라서 $x_Q \in W$ 의 약 절반이 살아남으며 기호를 $\mathbb{F}_{q^m}$ 에서 직접 계산할 수 있다. $e = 4(a_6 = 0)$ 일 때는 $\beta = \omega u(\theta u^2 + a_4)$ 이고 $u(\theta u^2 + a_4) \in \mathbb{F}_{q^m}$ 은 2차확대체 $\mathbb{F}_{q^{k/2}}$ 에서 두제곱인 반면 ω 는 $\mathbb{F}_{q^{k/2}}$ 에서 두제곱이 아니다(θ 가 $\mathbb{F}_{q^m}$ 에서 두제곱이 아니고 $(q^m + 1)/2$ 가 홀수이므로 $\omega^{(s-1)/2} = \theta^{(q^m-1)/2 \cdot (q^m+1)/2} = -1$). 따라서 $\beta \neq 0$ 인 모든 $x_Q \in W$ 가 살아남으며 검사는 아무런 역할도 하지 못하고 $[\ell]Q = \mathcal{O}$ 가 모든 걸러내기를 맡는다. 기호를 $\log_2 s$ 비트의 거듭제곱으로 계산해서는 안되는데 그렇게 하면 절약되는 비용의 약 절반이 들기 때문이다. $\beta^{(s-1)/2} = N_{\mathbb{F}_{q^{k/2}/\mathbb{F}_q}}(\beta)^{(q-1)/2}$ 이므로 그 비용은 $\mathbb{F}_{q^{k/2}}$ 에서 Frobenius $k/2 - 1$ 번과 곱하기 $k/2 - 1$ 번, 그리고 그뒤의 $\mathbb{F}_q$ 에서의 Jacobi 기호 하나인데 Jacobi 기호의 비용은 $\mathbb{F}_{q^k}$ 에서의 곱하기 한번보다 훨씬 작다. (제 9절에서 검사되었다.)

5 두 변수를 모두 모르는 경우의 Miller 거꿀계산

이 절은 실제의 결과, 즉 원시 Tate–Miller 값을 받아 그 두 변수를 모두 돌려주는 다항식시간절차를 담고있다. 그것은 알려진 A 에서 $h_{d,A}$ 를 거꿀계산하는 [6, Alg. 4.1]에 두가지 변경을 가한것이다. 하나는 방향이 Ate가 아니라 Tate이며 따라서 노름이 ζ^2 가 아니라 ζ^d 를 주고(명제 3.1과 [6, eq. (4.3)]의 대비) d 제곱뿌리가 유일하다는것이다(보조정리 3.5). 다른 하나는 그의 3단계 $\xi(Q) = \xi(A) \pm u$ 를 보조정리 4.1의 사영으로 바꾼것이다. 아래의 1–2단계와 5–8단계는 그의것이다.

명제 5.1. 알고리즘 5.1은 옳게 동작하며 $O((k \log q)^3)$ 번의 비트연산으로 끝난다.

증명. 어떤 $(A_0, Q_0) \in G_1 \times G_0$ 에 대하여 $w = h_{d,A_0}(Q_0)$ 이면 명제 3.1에 의하여 $u = (\xi(Q_0) - \xi(A_0))^d$ 이므로 $\zeta = \xi(Q_0) - \xi(A_0)$ 이고(경우 (ii)의 부호를 제외하면, 그 부호는 시험된다) 보조정리 4.1은 $x_A = \xi(A_0)$, $x_Q = \xi(Q_0)$ 을 준다. 그러면 5–7단계는 부호를 모르는 $A = \pm A_0$, $Q = \pm Q_0$ 을 만든다. (5)와 명제 3.1의 증명에 의하여 네개의 원시값은 $h_{d,A_0}(Q_0) = w$, $h_{d,-A_0}(-Q_0) = -w$, $h_{d,A_0}(-Q_0) = w^s$, $h_{d,-A_0}(Q_0) = -w^s$ 이므로 (d 가 홀수일 때) 8단계는 부호를 식별하고 Miller 값이 정확히 w 인 쌍을 돌려준다. 거꾸로 알고리즘이 쌍을 돌려준다면 5단계와 7단계에 의하여 $A \in E(\mathbb{F}_q)[\ell] = G_1$ 이고, 6–7단계와 주의 4.4, (1)에 의하여 $Q \in E[\ell] \cap \ker(\text{Fr}_q^{k/2} + 1) = G_0$ 이며, 8단계에 의하여 그 Miller 값은 w 이다. 8단계가 없다면 알고리즘은 전혀 Miller 값이 아닌 w 에 대해서도 유효한 쌍을 돌려줄 수 있다. 계산량에 대해서는 [6, Thm. 4.2]에서처럼 $\mathbb{F}_{q^k}$ 에서의 곱하기를 센다. 교과서식 산법으로 곱하기 한번은 $O((k \log q)^2)$ 번의 비트연산이다. $\mathbb{F}_{q^{k/2}}$ 나 $\mathbb{F}_q$ 에서의 곱하기는 이보다 더 들지 않으며 어깨수 $d^{-1} \bmod (s-1)$, 상수 λ , $(\lambda-1)^{-1}$ 과 보조정리 4.1의 기저는 곡선마다 한번 계산된다. 단계별로 보면 다음과 같다.

1. $w^{s+1} = w^s \cdot w$: Frobenius 거듭제곱 한번과 곱하기 한번으로 $O(k \log q)$ 번의 곱하기이며 $\mathbb{F}_{q^k}$ 를 $\mathbb{F}_{q^{k/2}}$ 의 2차확대체로 표현하면 $w \mapsto w^s$ 가 공액이므로 $O(1)$ 이다.
2. 어깨수가 s 보다 작은 $\mathbb{F}_{q^{k/2}}$ 에서의 거듭제곱 한번: $O(k \log q)$ 번의 곱하기.
3. ζ^{q^m} 은 Frobenius 거듭제곱이고($O(k \log q)$ 번의 곱하기, 또는 미리 계산한 행렬을 쓰면 $\mathbb{F}_q$ 에서 $O(k^2)$ 번의 곱하기) 그뒤에 곱하기가 한번 따른다. 검사 $x_A \in \mathbb{F}_q$ 는 1을 포함하는 $\mathbb{F}_{q^{k/2}}$ 의 $\mathbb{F}_q$ -기저에서는 비용이 들지 않는다.

알고리즘 5.1 두 변수를 모두 모르는 Miller 거꿀계산

입력: $w \in \mathbb{F}_{q^k}^\times$; 여기서 $d \mid s+1$; 상수 $\lambda, (\lambda-1)^{-1}$ 과 보조정리 4.1의 기저는 곡선마다 한번 사전계산

출력: $h_{d,A}(Q) = w$ 인 $(A, Q) \in G_1 \times G_0$ 또는 $\perp$

1: $u \leftarrow (-1)^d w^{s+1}$

2: $\zeta \leftarrow \mathbb{F}_{q^{k/2}}^\times$ 에서 u 의 d 제곱뿌리 $\triangleright$ 보조정리 3.5; 없으면 $\perp$ 반환, 두개이면 두 부호를 다 시험

3: $x_A \leftarrow L(\zeta)/(\lambda-1)$

만일 $x_A^q \neq x_A$ **이면 반환** $\perp$

4: $x_Q \leftarrow \zeta + x_A$ $\triangleright$ 이때 $L(x_Q) = L(\zeta) + (1-\lambda)x_A = 0$ 은 자동적으로 성립

5: $\alpha \leftarrow x_A^3 + a_4 x_A + a_6$

만일 α 가 $\mathbb{F}_q$ 에서 두제곱이 **아니면 반환** $\perp$

$A \leftarrow (x_A, \sqrt{\alpha})$

6: $\beta \leftarrow x_Q^3 + a_4 x_Q + a_6$

만일 $N_{\mathbb{F}_{q^{k/2}}/\mathbb{F}_q}(\beta)^{(q-1)/2} \neq -1$ **이면 반환** $\perp$

$\triangleright$ 즉 $\text{Fr}_q^{k/2} Q \neq -Q$, 주의 4.4

$Q \leftarrow (x_Q, y_Q)$, 여기서 $y_Q \in \mathbb{F}_{q^k}, y_Q^2 = \beta$

7: **만일** $[\ell]A \neq \mathcal{O}$ 또는 $[\ell]Q \neq \mathcal{O}$ **이면 반환** $\perp$

8: $h \leftarrow h_{d,A}(Q)$

만일 $w = h$ **이면 반환** (A, Q)

만일 $w = -h$ **이면 반환** $(-A, -Q)$

만일 $w = h^s$ **이면 반환** $(A, -Q)$

만일 $w = -h^s$ **이면 반환** $(-A, Q)$

9: **반환** $\perp$

4. 더하기 한번.

5. $\mathbb{F}_q$ 에서의 Legendre 기호 하나와 두제곱뿌리 하나: $\mathbb{F}_q$ 에서 $O(\log q)$ 번의 곱하기.

6. 노름을 통한 $\mathbb{F}_{q^{k/2}}$ 에서의 Legendre 기호: $\mathbb{F}_{q^{k/2}}$ 에서 Frobenius 거듭제곱 $k/2 - 1$ 번과 곱하기 $k/2 - 1$ 번, 그리고 $\mathbb{F}_q$ 에서의 Jacobi 기호 하나(주의 4.4). $\mathbb{F}_{q^k}$ 에서의 두제곱뿌리 하나: $O(k \log q)$ 번의 곱하기 — 실은 $\mathbb{F}_{q^{k/2}}$ 에서의 두제곱뿌리이다. ν 를 $\mathbb{F}_{q^{k/2}}$ 의 두제곱이 아닌 원소로 하여 $\mathbb{F}_{q^k} = \mathbb{F}_{q^{k/2}}(\sqrt{\nu})$ 로 표현하면 원소 β/ν 는 $\mathbb{F}_{q^{k/2}}$ 의 두제곱이고 $\sqrt{\beta} = \sqrt{\nu} \sqrt{\beta/\nu}$ 이다.

7. $E(\mathbb{F}_q)$ 우에서의 $[\ell]A$ 와 $E(\mathbb{F}_{q^k})$ 우에서의 $[\ell]Q$: 각각 $O(\log \ell) = O(\log q)$ 번의 군연산이며 매 연산은 유계인 회수의 곱하기이다.

8. 길이 $d \leq s+1$ 인 Miller 순환 한번: 각각 유계인 회수의 곱하기로 이루어진 두배하기 또는 더하기 단계 $O(\log d) = O(k \log q)$ 번, 그리고 Frobenius 거듭제곱 한번의 비용이 드는 비교 네번.

매 단계는 $\mathbb{F}_{q^k}$ 에서 $O(k \log q)$ 번의 곱하기, 즉 $O((k \log q)^3)$ 번의 비트연산이며 1, 2, 6, 8 단계가

이 한계에 도달한다. 두제곱뿌리는 [6]에서 가정한 사전계산(2-Sylow 부분군의 생성원) 밑에서는 결정론적이며 그렇지 않으면 Cipolla 알고리즘으로 기대시간안에 계산된다. $\square$

두가지 특징을 지적할 필요가 있다. 첫째로, u 만을 보는 검사는 어느것도 판별력이 없다. w^{s+1} 은 노름이므로 모든 w 에 대하여 $\mathbb{F}_{q^{k/2}}$ 에 속하며 $\mathbb{F}_{q^{k/2}}$ 의 모든 원소는 $\mathbb{F}_{q^k}$ 에서 두제곱이다. 이것이 6단계가 β 를 $\mathbb{F}_{q^k}$ 가 아니라 $\mathbb{F}_{q^{k/2}}$ 에서 검사하는 리유이며 — 유용한 조건은 β 가 $\mathbb{F}_{q^{k/2}}$ 에서 두제곱이 아니라는것이다(주의 4.4) — 4단계가 단순한 대입인 리유이며($x_A \in \mathbb{F}_q$ 이기만 하면 $L(x_Q) = L(\zeta) + (1 - \lambda)x_A = 0$ 은 자동적으로 성립한다) 3, 6, 7단계의 검사가 모든 무계를 지는 리유이다. 제 9절의 시험곡선에서 고정된 목표값의 우연적인 ℓ 제곱뿌리 3000개는 모두 노름조건과 두제곱조건을 통과하였으나 모두 3단계에서 기각되었다. 둘째로, 이 절차는 두 변수를 모두 돌려준다. 그것은 탐색이 뒤따르는 소속오라클이 아니다. 이것이 이 논문이 [1]을 넘어서는 점이다. 그들의 식 (8)은 A 와 Q 의 역할을 바꾼 (3)과 정확히 같으며 그들의 이후의 환원은 알려진 $\xi(Q)$ 의 최소다항식을 리용하는데 여기서는 그것을 쓸수 없다.

6 Miller 거꿀계산으로부터 GPI에로

e 를 $G_1 \times G_0$ 또는 $G_0 \times G_1$ 우에서 정의되고 μ_ℓ 에 값을 가지는 임의의 비퇴화 쌍선형넘기기 — 어느 변수순서로든 축약 Tate 쌍선형넘기기 t , 또는 Satoh의 쌍선형넘기기 — 라고 하고 $z \in \mu_\ell \setminus \{1\}$ 을 e 에 대한 GPI의 목표값이라고 하자.

$v^{(q^k-1)/\ell} = t(A, Q)$ 인 원시 Tate-Miller 값 v 는 축약값에 의하여 $x \mapsto x^{(q^k-1)/\ell}$ 의 핵을 제외하고서만 결정되는데 이 핵은 $\nu := (s+1)/\ell$ 일 때 위수가 $(q^k-1)/\ell = (s-1)\nu$ 인 부분군이다. 이것은 모두 돌아보기에는 너무나 크며 알고리즘 5.1이 필요로 하는것도 아니다. 그것이 필요로 하는것은 ζ 이며 아래의 명제 6.2는 v 가 그 핵의 잉여류를 돌 때 ζ 가 $\mathbb{F}_{q^{k/2}}^\times$ 전체를 돈다는것을 보여준다. 즉 목표값은 ζ 를 전혀 제한하지 않는다. 그러므로 GPI 알고리즘은 x 자리표쌍 $(x_A, x_Q) \in \mathbb{F}_q \times W$ 를 직접 돌거나(제 8절), 동등하지만 더 느리게, 알고리즘 5.1의 3-4단계로 복호되는 $\zeta \in \mathbb{F}_{q^{k/2}}^\times$ 를 돈다(주의 8.1). 두 경우 모두 매 쌍은 z 에 대하여 검사되며 2단계의 d 제곱뿌리는 결코 필요하지 않다.

이하에서 본질적인 점은 어느 순환도 최종검사 전에는 쌍선형넘기기를 계산하지 않는다는것이다. e 는 최종검사에서만, 그리고 $e(A, Q) \in \{z, z^{-1}\}$ 인가 하는 물음을 통해서만 들어온다. 따라서 다음과 같다.

- 알고리즘은 최종검사에서 계산되는 쌍선형넘기기 e 가 무엇이든 그것에 대한 GPI를 풀며, 명제 7.1의 세기론증은 쌍선형성과 비퇴화성만을 쓰므로 이 명제는 그러한 모든 e 에 대하여 그대로 적용된다.
- 특히 $e(A, Q) := h_{s,-Q}(A)$ — 이것은 Satoh의 문자로 $h_{q^{k/2}, -A}(Q)$ 이며 [7, Alg. 6.1]의 출력 조건이다 — 로 잡으면 알고리즘은 Satoh의 GPI 문제를 직접 푼다. 보조정리 3.3에 의하여 이 e 는 $t(Q, A)^{1/2}$ 이고 쌍선형이며 비퇴화이므로 최종검사를 동등하게 $t(Q, A) \in \{z^2, z^{-2}\}$ 로 할수 있으며 이것은 길이 s 의 Miller 순환보다 싸다. 마찬가지로 [7, Alg. 6.6]의 순환길이 q 의 목표 $h_{q,-Q}(A)$ 는 주의 3.4에 의하여 $t(Q, A)^{1/(kq^{k/2-1})}$ 이며 $t(Q, A) \in \{z^{\pm kq^{k-1}}\}$ 로 검사된다.

- 서로 다른 두 쌍선형넘기기사이의 관계는 전혀 계산되지 않으며, 설사 계산된다 하더라도 리산로그를 필요로 하지 않을것이다. 실례로 $t(Q, A) = t(A, Q)^{\kappa'}$ 인 상수 κ' 는 명시적공식

$$\kappa' = \frac{kh}{kh - c(q-1)} \bmod \ell, \quad c := \frac{q^k - 1}{\ell}, \quad h := \frac{\#E(\mathbb{F}_q)}{\ell} \quad (13)$$

을 가지는데 이것은 Weil 쌍선형넘기기를 통한 Tate 쌍선형넘기기의 Frey–Rück 표현으로부터 나온다(보조정리 6.1). 그 값은 제 9절의 시험곡선에서 15이다. 이 방법은 그것을 쓰지 않으며 이 논문의 어디에도 리산로그는 나타나지 않는다.

보조정리 6.1. e_ℓ 을 Miller의 공식 $e_\ell(A, Q) = (-1)^\ell h_{\ell,A}(Q)/h_{\ell,Q}(A)$ 로 주어지는 Weil 쌍선형넘기기라고 하고 c, h 는 (13)에서와 같으며 $\rho := kh/(q-1) \bmod \ell$ 이라고 하자. 그러면 $A \in G_1, Q \in G_0$ 에 대하여

$$t(A, Q) = e_\ell(A, Q)^{c-\rho}, \quad t(Q, A) = e_\ell(A, Q)^{-\rho}$$

이며 이로부터 (13)이 나온다. $t(Q, A)$ 의 비퇴화성은 $\rho \neq 0$, 즉 $\ell \nmid kh$ 인것이다. 여기서 $k = \text{ord}_\ell(q)$ 가 $\ell - 1$ 을 나누므로 $\ell \nmid k$ 이며 $\ell \parallel \#E(\mathbb{F}_q)$ 이므로 $\ell \nmid h$ 이다. $t(A, Q)$ 의 비퇴화성은 $\rho \neq c$ 인것이며 이것은 바로 (13)의 분모 $kh - c(q-1) = (q-1)(\rho - c)$ 가 영이 아니라는것이다.

증명. $[\ell]S = R, \sigma = \text{Fr}_q^k$ 일 때의 항등식 $t(P, R) = e_\ell(P, \sigma S - S)$ 는 Tate 쌍선형넘기기의 Lichtenbaum 형태 [2]이다. 이것은 고전적인것이며 여기서는 어깨수만을 계산한다. $\pi^k - 1$ 은 $E[\ell]$ 을 링으로 보내므로 $\text{End}(E)$ 에서 $\ell\phi$ 로 분해되며 따라서 $\sigma S - S = \phi(R)$ 이다. 그리고 ϕ 는 Tate 모듈 $T_\ell E$ 에서 π 의 두 고유직선에 각각 $(\alpha^k - 1)/\ell$ 과 $(\beta^k - 1)/\ell$ 로 작용한다. 여기서 $\alpha \equiv 1, \beta \equiv q \pmod{\ell}$ 은 고유값들이다. $\alpha = 1 + \ell a, \beta = q + \ell b$ 로 쓰면 $\alpha + \beta = t = q + 1 - \ell h$ 로부터 $a + b = -h$ 가, $\alpha\beta = q$ 로부터 $b \equiv -qa$ 가 나오므로 $a \equiv h/(q-1)$ 이고 $(\alpha^k - 1)/\ell \equiv ka, (\beta^k - 1)/\ell \equiv c + kq^{k-1}b \equiv c - ka \pmod{\ell}$ 이다. 따라서 $Q \in G_0$ 에 대하여 $\phi(Q) = [c - \rho]Q, A \in G_1$ 에 대하여 $\phi(A) = [\rho]A$ 이며 이로부터 $t(A, Q) = e_\ell(A, Q)^{c-\rho}$ 이고 반대칭성에 의하여 $t(Q, A) = e_\ell(Q, A)^\rho = e_\ell(A, Q)^{-\rho}$ 이다. $\square$

명제 6.2 (쌍선형넘기기값과 노름의 독립성). $\gcd(\ell, s-1) = 1$ 이므로 넘기기

$$\mathbb{F}_{q^k}^\times \longrightarrow \mu_\ell \times \mathbb{F}_{q^{k/2}}^\times, \quad v \longmapsto (v^{(q^k-1)/\ell}, v^{s+1})$$

는 핵의 위수가 $\nu = (s+1)/\ell$ 인 우로의 준동형넘기기이다. 따라서 원시 Miller 값의 축약된 쌍선형넘기기값과 노름은 서로 독립인 자리표이다. 즉 앞의것을 고정하여도 뒤의것은 $\mathbb{F}_{q^{k/2}}^\times$ 우에서 균등하게 분포되며, v 를 v^{s+1} 을 통해서만 읽는 어떤 절차도 — 특히 명제 3.1우에 세워진 어떤 절차도 — 목표값에 관한 정보를 전혀 받지 못한다.

증명. $\mathbb{F}_{q^k}^\times$ 는 위수가 $(s-1)(s+1)$ 인 순환군이다. 핵은 위수가 $\gcd((s-1)(s+1)/\ell, s+1) = \nu \gcd(s-1, \ell) = \nu$ 의 약수인 v 들로 이루어지므로 상의 위수는 $(q^k - 1)/\nu = \ell(s-1) = |\mu_\ell \times \mathbb{F}_{q^{k/2}}^\times|$ 이다. $\square$

이것이 아래 명제 7.1의 내용을 한번에 말한것이다. 노름경로는 목표값을 완전히 버리며 남는 것은 최종 쌍선형넘기기검사를 가진 x자리표쌍에 대한 탐색이다. (제 9절의 시험곡선에서 검사되었다. 상의 위수는 예측대로 $\ell(s-1)$ 이다.)

7 풀이모임의 밀도

명제 7.1. $e \in \{4, 6\}$, $k > 2$ 이고 d 는 $d \mid s+1$ 인 홀수라고 가정하며 $z \in \mu_\ell \setminus \{1\}$ 을 고정한다. v 가 $\{v : v^{(q^k-1)/\ell} = z\}$ 를 돌 때 량 $\zeta = ((-1)^{d\nu^{s+1}})^{1/d}$ 는 $\mathbb{F}_{q^{k/2}}^\times$ 전체를 돌며 매 값을 같은 회수만큼 취한다(명제 6.2와 보조정리 3.5). e 를 $G_1 \times G_0$ 또는 $G_0 \times G_1$ 위에서 μ_ℓ 에 값을 가지는 비퇴화 쌍선형넘기기라고 하자. ζ 의 $s-1$ 개의 값가운데서 정확히 $(\ell-1)/2$ 개가 알고리즘 5.1의 3-7 단계에 의하여 $e(A, Q) = z^{\pm 1}$ 인 쌍 (A, Q) 로 복호된다. 따라서 조사해야 할 후보의 기대개수는

$$\frac{1}{\pi_z} = \frac{2(s-1)}{\ell-1} \approx \frac{2q^{k/2}}{\ell} = 2\nu \quad (14)$$

이다.

증명. 첫번째 주장은 명제 6.2(z 의 원상우에서 노름은 $\mathbb{F}_{q^{k/2}}^\times$ 위에 균등하게 분포된다)와 $\mathbb{F}_{q^{k/2}}^\times$ 위에서 $\zeta \mapsto \zeta^d$ 가 일대일대응이라는것(보조정리 3.5, d 는 홀수)으로부터 나온다. 두번째 주장에 대해서는 보조정리 4.1에 의하여 넘기기 $(\xi(A), \xi(Q)) \mapsto \xi(Q) - \xi(A)$ 는 $\mathbb{F}_q \times W$ 위에서 일대일이다. $e(A, Q) \in \{z, z^{-1}\}$ 인 쌍 $(A, Q) \in (G_1 \setminus \{\mathcal{O}\}) \times (G_0 \setminus \{\mathcal{O}\})$ 의 개수는 쌍선형성과 비퇴화성에 의하여 $2(\ell-1)$ 이다(매 A 에 대하여 두 값 각각에 대응하는 Q 가 하나씩 있다). 이 쌍들은 $(A, Q) \mapsto (\pm A, \pm Q)$ 에 의하여 크기 4의 궤도들로 치환되는데 이 작용은 두 x자리표를 보존하며 각 궤도안에서 e 는 두 값을 각각 두번씩 취한다. 따라서 그것들은 ζ 의 서로 다른 값 $(\ell-1)/2$ 개를 준다. $\square$

성공하는 ζ 들은 모두 차원이 $1 + k/e$ 인 부분공간 $\mathbb{F}_q \oplus W$ 에 놓이므로 제 8절의 알고리즘은 $\mathbb{F}_{q^{k/2}}^\times$ 가 아니라 이 부분공간 ($q^{1+k/e}$ 개의 원소, BN254에서는 2^{761} 개)을 돈다. 개수 (14)는 $\mathbb{F}_{q^{k/2}}^\times$ 를 도는 경우에 대한것이다. 부분공간을 도는 경우에는 자연스러운 블록순서(x_A 가 바깥, x_Q 가 안)에서 작업량은 첫 유효블록안의 후보 $q^{k/e}/2$ 개이며 그중 절반은 $e=6$ 일 때, 전부는 $e=4$ 일 때 비싸다(주의 4.4). 이것은 ℓ 에 관계없다(제 8절과 제 9절).

8 완전한 알고리즘

보조정리 4.1에 의하여 알고리즘 5.1의 3-4단계가 복호하는 값 ζ 는 정확히 $(x_A, x_Q) \in \mathbb{F}_q \times W$ 인 $\zeta = x_Q - x_A$ 이며 명제 6.2에 의하여 목표값은 ζ 를 제한하지 않는다. 그러므로 GPI 알고리즘은 쌍 (x_A, x_Q) 를 직접 돈다. 노름과 사영 L 은 전혀 계산되지 않는다. 제 4-7절의 분석은 그것이 증명하는 내용, 즉 이것이 탐색공간이며 노름경로에서는 아무것도 그것을 줄일수 없다는것을 통해서만 들어온다(제 10절은 축소들과 그 각각의 근거를 려거한다).

쌍선형넘기기 e 는 15행에서만 계산되며 목표값 z 는 15-19행에서만 들어온다. 18행은 $e(-A, Q) = e(A, Q)^{-1}$ 을 리용하므로 성공하는 쌍 하나가 있으면 많아야 두번의 부호선택으로 답이 얻어진다. 이것은 명제 7.1의 개수 $(\ell-1)/2$ 에 반영되어있다. G_1 의 매 x자리표는 G_0 에 꼭 하나의 짝 x자리표를 가지므로 순환은 7행과 9행을 통과하는 첫 x_A 의 블록안에서 W 의 약 절반을 주사한 다음 멈춘다. 이 기대값들을 위하여 두 순환은 제 9절에서와 같이 균등우연순서로 진행한

알고리즘 8.1 길이 ℓ 의 순환에 의한 GPI

입력: $q; \mathbb{F}_q$ 위의 보통곡선 $E : Y^2 = X^3 + a_4X + a_6$; 끼워넣기차수가 짝수 $k > 2$ 인 홀씨수 $\ell \parallel \#E(\mathbb{F}_q); e \mid k$ 인 짝수 꼬임차수 $e \geq 4$; $G_1 \times G_0$ 위의 비퇴화 쌍선형넘기기 e , 실례로 $t(A, Q)$, $t(Q, A)$ 또는 Satoh의 $h_{s,-Q}(A) = t(Q, A)^{1/2}$; 목표값 $z \in \mu_\ell \setminus \{1\}$.

출력: $e(A, Q) = z$ 인 $(A, Q) \in G_1 \times G_0$ 또는 $\perp$.

- 1: **사전계산** (z 와 무관):
 - 2: $s \leftarrow q^{k/2}; \quad m \leftarrow k/e$
 - 3: $Q_0 \in G_0 \setminus \{\mathcal{O}\}$ 를 고른다; $W \leftarrow \xi(Q_0) \mathbb{F}_{q^m}$, $\mathbb{F}_q$ -기저는 $\xi(Q_0) \cdot \{1, \gamma, \dots, \gamma^{m-1}\}$, 여기서 γ 는 $\mathbb{F}_q$ 위에서 $\mathbb{F}_{q^m}$ 의 생성원
 - 4: **주순환:**
 - 5: **각 $x_A \in \mathbb{F}_q$ 에 대하여**
 - 6: $\alpha \leftarrow x_A^3 + a_4x_A + a_6$
 - 7: **만일 α 가 $\mathbb{F}_q$ 에서 두제곱 이면**
 - 8: $A \leftarrow (x_A, \sqrt{\alpha})$
 - 9: **만일 $[\ell]A = \mathcal{O}$ 이면**
 - 10: **각 $x_Q \in W$ 에 대하여**
 - 11: $\beta \leftarrow x_Q^3 + a_4x_Q + a_6$
 - 12: **만일 $N_{\mathbb{F}_{q^{k/2}}/\mathbb{F}_q}(\beta)^{(q-1)/2} = -1$ 이면** $\triangleright$ 즉 $\text{Fr}_q^{k/2}Q = -Q$, 주의 4.4
 - 13: $Q \leftarrow (x_Q, y_Q)$, 여기서 $y_Q \in \mathbb{F}_{q^k}, y_Q^2 = \beta$
 - 14: **만일 $[\ell]Q = \mathcal{O}$ 이면**
 - 15: $\chi \leftarrow e(A, Q)$
 - 16: **만일 $\chi = z$ 이면**
 - 17: **반환** (A, Q)
 - 18: **만일 $\chi = z^{-1}$ 이면**
 - 19: **반환** $(-A, Q)$
 - 20: **반환** $\perp$
-

다고 본다(우에 쓴 고정된 순서로는 언제나 같은 첫 x_A 를 만나게 된다). 기대작업량은 각각되는 $(q-n)/(n+1)$ 개의 x_A ($n = (\ell-1)/2$)로서 그 각각은 $\mathbb{F}_q$ 에서의 Legendre 기호 하나의 비용이 들고 $h > 1$ 일 때는 기호를 통과하는 절반에 대하여 $[\ell]A$ 한번이 더 든다($h = 1$ 이면 각각되는 x_A 가운데 기호를 통과하는것은 없다). 그뒤에 $q^{k/e}/2$ 개의 후보 x_Q 가 따르는데 그중 절반은 $e = 6$ 일 때, 전부는 $e = 4$ 일 때 비싸다(주의 4.4).

알고리즘 5.1과의 관계. 알고리즘 8.1은 알고리즘 5.1을 호출하지 않으며 이것은 의도적인것이다. 알고리즘 5.1의 1-4단계(노름, d 제곱뿌리, 사영)는 원시값의 후보 w 를 x자리표쌍으로 복호하는데 명제 6.2는 w 가 z 의 원상을 둘 때 이 단계들이 $\mathbb{F}_q \times W$ 의 매 쌍을 같은 회수만큼 만들어낸다는것을

보여준다. 따라서 그것들을 실행하는것은 $\mathbb{F}_{q^{k/2}}^\times$ 를 에돌아 $\mathbb{F}_q \times W$ 를 도는것으로 되며 그 계산량은 주의 8.1이 준다. 알고리즘 8.1은 쌍들을 직접 돌며 알고리즘 5.1의 후반부를 행마다 그대로 유지한다. 6–8행과 11–13행은 그것의 5단계와 6단계(두제곱뿌리와 Legendre 검사)이고 9행과 14행은 7단계(위수검사)이며 15–19행은 그것의 8단계 — 원시값 $h_{d,A}(Q)$ 와 w 의 네 부호를 고려한 비교 — 를 축약값 $e(A, Q)$ 와 $z^{\pm 1}$ 의 비교로 바꾼다. 따라서 알고리즘 5.1이 기여하는것은 부분프로그램이 아니라 정리이다. 즉 $\mathbb{F}_q \times W$ 가 탐색공간이며 노름우에 세워진 어떤 복호도 그것을 줄일수 없다는 것이다.

주의 8.1 ($\mathbb{F}_{q^{k/2}}^\times$ 우에서의 순환). 그대신 $\zeta \in \mathbb{F}_{q^{k/2}}^\times$ 를 돌수도 있다 — 실례로 위수가 큰 원소 g 로 $\zeta \leftarrow g\zeta$ 로 하는데(생성원과 달리 g 는 $s-1$ 의 인수분해를 요구하지 않는다), 잉여류 $\zeta_0(g)$ 가 다 소진되면 새로운 ζ_0 에서 다시 시작하거나 그저 ζ 를 우연적으로 뽑는다 — 그리고 매 ζ 를 알고리즘 5.1의 3–4단계로 복호한 다음 우에서와 같이 진행한다. ζ^{q^m} 은 매 단계 곱하기 한번으로 갱신되며 검사 $x_A \in \mathbb{F}_q$ 는 1을 포함하는 기저에서는 비용이 들지 않는다. 이 순환은 최종적으로 복호하는 매 쌍 (x_A, x_Q) 마다 $\mathbb{F}_{q^{k/2}}$ 의 원소 $q^{k/2-1-k/e}$ 개를 방문하며 매 원소에서 $\mathbb{F}_{q^{k/2}}$ 의 곱하기 몇번이 든다. 그 기대계산량은 이러한 단계 $\frac{2(s-1)}{\ell-1}$ 번, 제 10절의 단위로 BN254에서 약 $2^{1271}M$, BLS12-381에서 약 $2^{2032}M$ 이며 그 모두가 우의 직접순환이 비용없이 열거하는 쌍들을 찾아내는데 소비된다. 이 순환은 직접순환보다 못하며 알고리즘 5.1의 복호가 나타나는 형태이기때문에만 기록해둔다.

9 실험적검증

모든 주장은 Ubuntu 24.04.4 LTS, Linux 6.18에서 PARI/GP 2.15.4(GMP 6.3.0 커널, 64비트)로 검사 되었으며 계산은 Intel Xeon 2.10 GHz, 기억기 3.9 GiB로 보고되는 처리기핵심이 하나인 클라우드 가상기계에서 진행되었다. $\mathbb{F}_{q^k}$ 는 탑(tower)이 아니라 차수 12의 기약다항식 하나로 표현되었다(PARI의 `ffgen`). 곡선은 $u = 1$ 인 BN 곡선이며($u = -1$ 이면 더 작은 곡선 $q = 19$, $\ell = 13$ 이 얻어지지만 매 군에 x자리표가 여섯개밖에 없어 아래의 개수들이 의미를 가지기에는 너무 작다) $q = 103$, $\ell = 97$, $E : Y^2 = X^3 + 5$, $\#E(\mathbb{F}_q) = \ell$, $\mathbb{F}_{q^k} \simeq \mathbb{F}_{103^{12}}$ (80비트)이다. 여기서 $e = 6$, $m = 2$ 이고 λ 의 위수는 3으로 확인되었다. 명제 3.1의 부호 $(-1)^d = -1$ 은 $\mathcal{O}$ 에서 정규화된 Miller 함수로 확인되었다. 그렇게 정규화되지 않은 PARI의 `elltatepairing`에서는 원시상수가 (A, Q) 에 무관한 $\mathbb{F}_q^\times$ 의 다른 원소로 되지만 $(q-1) \mid (q^k-1)/\ell$ 이므로 축약 쌍선형넘기기는 영향을 받지 않는다.

검사항목	결과
$Q \in G_0$ 에 대하여 $\xi(Q) \in \mathbb{F}_{q^{k/2}}$	예
$\lambda = \xi(Q)^{q^m}/\xi(Q)$ 는 Q 에 무관, $\text{ord}(\lambda) = 3$	예
모든 $u \in W$ 에 대하여 $L(u) = 0$; $\mathbb{F}_q \cap W = \{0\}$ (모든 $a \in \mathbb{F}_q^\times$)	예
명제 3.1, 정규화된 Miller 함수: $v^{s+1} = -\zeta^\ell$	예
알고리즘 5.1이 $(\xi(A), \xi(Q))$ 를 정확히 복원, 우연적인 쌍 30개	30/30
목표값의 우연적인 ℓ 제곱뿌리 3000개중 접수된것	0
명제 7.1: x자리표쌍 48^2 개, $t = z$ 인 쌍 96개, ζ 의 값 48개	예
주의 3.2: $n = 5, 11, 13$ 에 대하여 (6)이 정확히 성립; (7); $h_{s,A}(Q)^{s+1} = 1$;	예
$h_{2\ell-1,A}(Q)^{s+1} = \zeta^{2\ell-2}$; $T = 6$ 일 때 (8)	
보조정리 3.3: 두 방향에서 (9); (10); $-h_{s,A}(Q) = t(A, Q)^{48}$, $48 \equiv -1/2$;	예
$\text{ord}(h_{s,A}(Q)) = 194 = 2\ell$	
$h_{s,Q}(A)$ 는 최종거듭제곱없이 Q 와 A 에 관하여 쌍선형; $h_{s,-Q}(A) = t(Q, A)^{1/2}$	예
보조정리 6.1: $e_\ell \in \mu_\ell$; $t(A, Q) = e_\ell^{c-\rho}$, $t(Q, A) = e_\ell^{-\rho}$ ($c \equiv 10$, $\rho \equiv 80 \pmod{\ell}$);	예
(13)은 15를 주며 $t(Q, A) = t(A, Q)^{15}$	
시험곡선에서 $\gcd(2\ell - 2, s - 1) = 48$, BN254에서 $= 48u$	예
명제 5.1의 네 부호값 $w, -w, w^s, -w^s$	예
명제 6.2: $v \mapsto (v^{(q^k-1)/\ell}, v^{s+1})$ 의 상의 위수 $\ell(s-1)$	예
주의 3.2: $h_{T,Q}(A)^{s+1} = (\xi(A) - \xi(Q))^{-h\ell}$; $h_{q,Q}(A)^{s+1} = 1$; $3\ell \nmid s+1$ 일 때	예
$h_{3\ell,A}(Q)^{s+1} = -\zeta^{3\ell}$	
주의 3.4: $h_{q,Q}(A)^\ell = 1$; $h_{q,Q}(A) = t(Q, A)^{49}$, $49 \equiv -1/(kq^{k/2-1})$; $h_{q,-Q}(A) =$	예
$t(Q, A)^{48}$	
주의 4.4: 우연적인 $x_Q \in W$ 2000개에서 β 가 $\mathbb{F}_{q^{k/2}}$ 의 두제곱이 아님 $\iff \text{Fr}_q^{k/2}Q =$	예
$-Q$ ($e = 6$, 두제곱이 아닌것 1001개); G_0 의 점 30개에서 β 는 두제곱이 아님	
$1/\pi_z = (s-1)/48 = 2.49 \cdot 10^{10}$, 예측값 $2s/\ell = 2.46 \cdot 10^{10}$	예

쌍선형넘기기의 완전한 거꿀계산. 제 8절의 알고리즘을 끝까지 실행하였다. 후보는 $W = \xi(Q_0)\mathbb{F}_{q^2}$ 일 때의 쌍 $(a, x_Q) \in \mathbb{F}_q \times W$, 즉 $\zeta = x_Q - a$ 이며 모두 $q^3 = 1092727$ 개이고 그 각각에 대하여 $x_A = a$ 와 x_Q 를 직접 읽어내므로 사영은 필요없다. 목표값은 균등우연적으로 고른 쌍 $(A^*, Q^*) \in G_1 \times G_0$ 에 대한 $z = t(A^*, Q^*)$ 이었으며 그 쌍은 곧 잊어버렸다. 최종검사는 완전히 축약되고 완전히 쌍선형인 Tate 쌍선형넘기기에 의한 $t(A, Q) \in \{z, z^{-1}\}$ 이었다. 개수들이 의미를 가지도록 a 는 $\mathbb{F}_q$ 의 균등우연순서로, 매 a 에 대하여 x_Q 는 W 의 균등우연순서로 열거하였다. 경과 시간은 getwalltime으로 잰다.

G_1 의 매 x자리표 a 에 대하여 그것을 폴이로 완성하는 G_0 의 x자리표는 꼭 하나 있으므로 실행은 처음으로 만나는 유효한 a 의 블록안에서 멈춘다. 실행은 유효하지 않은 a 들을 건너뛰고(매번 Legendre 기호 하나의 비용이 들며 크기 q^2 의 블록을 건너뛴것으로 센다) 다음 W 를 주사하면서

G_0 의 x자리표 48개를 찾아 각각에서 Tate 쌍선형넘기기를 한번씩 계산하며 옳은것을 만날 때까지 계속한다. 사실상 이 실행은 A 를 첫 유효 x자리표에 고정하고 W 에서 그 짝을 찾는것이다. 이 블록순서에서 기대작업량은 건너뛰는 블록 $(q - n)/(n + 1)$ 개($n = (\ell - 1)/2$)로서 각각 $\mathbb{F}_q$ 에서의 Legendre 기호 하나의 비용이 들고 $h > 1$ 일 때는 그 기호를 통과하는 절반에 대하여 스칼라곱하기 $[\ell]A$ 한번이 더 들며, 그뒤에 첫 유효블록안에서 후보 $q^{k/e}/2$ 개가 따르는데 그중 절반은 비싸다(시험곡선에서는 블록 1.1개와 후보 5304개). $\mathbb{F}_q \times W$ 위의 균등순서에서는 해당한 개수가 명제 7.1의 세기론증에 의하여 $2q^{1+k/e}/\ell$ 일것인데 이것은 상수배를 제외하고서만, 그것도 BN 곡선에서 $\ell \approx q$ 이기때문에 앞의 개수와 일치한다. 서로 독립인 목표값 12개에 대하여: 성공 12번, 되돌려진 쌍은 $G_1 \times G_0$ 에 속하고 정확히 $t(A, Q) = z$ 이며 $\xi(A)$ 의 서로 다른 값은 11개(원래의 쌍은 한번도 나오지 않음); 건너뛴 유효하지 않은 a 는 0개부터 4개(평균 1.3); W 의 주사에서 옳은 x_Q 의 위치는 10609개중 1022부터 10350사이(평균 5896)로서 균등분포와 맞는다; 계산된 Tate 쌍선형넘기기는 3번부터 48번; 경과시간은 0.37s부터 1.92s사이이며 쌍선형넘기기가 아니라 주사에서의 $\mathbb{F}_{q^k}$ 의 두제곱뿌리와 ℓ 배 스칼라곱하기가 대부분을 차지한다. 여기서 보고한 실행들은 주의 4.4보다 먼저 진행된것이며 두제곱뿌리를 구한 다음에 $\text{Fr}_q^{k/2}Q = -Q$ 를 검사하였다. 노름을 통하여 계산되는 Legendre 검사를 먼저 하면 곱하기 $k/2 - 1$ 번의 비용으로 두제곱뿌리와 스칼라 곱하기의 약 절반이 절약된다. 최종검사를 $t(Q, A) \in \{z_S^2, z_S^{-2}\}$, $z_S = h_{s, -Q^*}(A^*) = t(Q^*, A^*)^{1/2}$ — Satoh 자신의 쌍선형넘기기 — 로 한 같은 실행도 똑같이 성공한다. 이리하여 최종거듭제곱을 가지는 쌍선형넘기기에 대한 완전한 GPI 문제가 처음부터 끝까지, 제 7절이 예측한 계산량으로 풀린다.

두개의 추가곡선. 위의 시험곡선은 $h = 1$ 이므로 제 8절의 9행($[\ell]A = \mathcal{O}$)은 한번도 실행되지 않으며 $e = 6$ 뿐이다. 같은 검사를 보조인수를 가지는 두 곡선에서 진행하였다: $q = 53$, $E: Y^2 = X^3 + X$, $\ell = 17$, $\#E(\mathbb{F}_q) = 68$, $h = 4$, $k = 8$, $e = 4$, $m = 2$ ($j = 1728$, 4차꼬임); 그리고 $q = 103$, $E: Y^2 = X^3 + 4$, $\ell = 37$, $\#E(\mathbb{F}_q) = 111$, $h = 3$, $k = 12$, $e = 6$, $m = 2$. 두 곡선 모두에서: λ 의 위수는 정확히 $e/2$ 이다; $1, \omega, \dots, \omega^{e/2-1}$ 은 고유값이 λ^j 인 $u \mapsto u^{q^m}$ 의 고유벡토르들이며 $\ker L = W$ 이다 (보조정리 4.1); 명제 3.1은 부호 -1 로 성립한다; 알고리즘 5.1은 우연적인 쌍 30/30에서 $(\xi(A), \xi(Q))$ 를 복원한다; 보조정리 3.3과 주의 3.4의 명시적공식이 $\text{ord}(h_{s,A}(Q)) = 2\ell$ 과 함께 성립한다; (13)의 κ' 는 각각 3과 8이며 $t(Q, A) = t(A, Q)^{\kappa'}$ 이다; 명제 6.2의 넘기기의 상의 위수는 $\ell(s - 1)$ 이다; 그리고 제 8절의 알고리즘은 우연순서로 매 곡선에서 우연적인 목표값 5/5에 대하여 성공하였으며 되돌려진 쌍은 z 에 대하여 검증되었다. 이번에는 9행이 실행된다. $e = 4$ 인 곡선에서는 다섯번의 실행에서 Legendre 기호를 통과한 x_A 가운데 4/5, 2/3, 12/13, 6/7, 1/2의 비율이 $[\ell]A \neq \mathcal{O}$ 에 의하여 기각되었다($E(\mathbb{F}_q)$ 의 x자리표 33개 가운데 $|\xi(G_1)| = 8$). $e = 6$ 인 곡선에서는 그 비율이 0/1, 2/3, 1/2, 0/1, 3/4이었다(55개 가운데 18개).

$e = 4$ 인 곡선은 $e = 6$ 의 실례들이 감추는 구조적사실을 드러낸다. $\beta \neq 0$ 인 $x_Q \in W$ 가운데 400/400에서 β 가 $\mathbb{F}_{q^{k/2}}$ 의 두제곱이 아니었는데 $e = 6$ 인 곡선에서는 그 비율이 203/399이었다. 이것이 주의 4.4의 두 경우이다. $e = 4$ 일 때 Legendre 검사는 아무런 역할도 하지 못하며 $[\ell]Q = \mathcal{O}$ 가 모든 걸러내기를 맡고 $e = 6$ 일 때는 약 절반을 기각한다.

연산회수. 시간비교는 하지 않는다. 이 규모에서 시간은 GP 해석기를 재는것이며 두 계산량은 ℓ 에 관하여 서로 다른 점근적거동을 가진다. 제 8절의 알고리즘에서 매 x_A 는 $\mathbb{F}_q$ 에서의 Legendre 기호 하나의 비용이 들고 통과하는 절반에 대해서는 $\mathbb{F}_q$ 에서의 두제곱뿌리 하나와 $[\ell]A$ 한번이 더 든다. 매 x_Q 는 주의 4.4에서와 같이 노름을 통하여 계산되는 $\mathbb{F}_{q^{k/2}}$ 에서의 Legendre 기호 하나($\mathbb{F}_{q^{k/2}}$ 에서 Frobenius $k/2 - 1$ 번과 곱하기 $k/2 - 1$ 번, 그다음 $1M$ 보다 훨씬 작은 비용의 $\mathbb{F}_q$ 에서의 Jacobi 기호)의 비용이 드는데 이 기호는 $e = 6$ 일 때 약 절반을 기각하고 $e = 4$ 일 때는 아무것도 기각하지 않으며(주의 4.4) 살아남은것들에 대해서는 $\mathbb{F}_{q^k}$ 에서의 두제곱뿌리 하나와 $E(\mathbb{F}_{q^k})$ 우에서의 $[\ell]Q$ 한번이 더 든다 — 제 10절의 크기에서 $e = 6$ 일 때 x_Q 하나당 평균 약 2^{12} 번의 $\mathbb{F}_{q^k}$ 에서의 곱하기, 즉 대략 Tate 쌍선형넘기기 네번이며 $e = 4$ 일 때는 그 두배이다. 주의 8.1의 순환에서는 매 ζ 마다 ζ^{q^m} 을 갱신하는 곱하기 한번, 복호를 위한 곱하기 서너번, 그리고 1을 포함하는 기저에서 비용이 들지 않는 소속검사가 더 들며 우의 비용은 ζ 가운데 $q^{1+k/e-k/2}$ 의 비율에서만 생긴다. [7, Alg. 6.1]의 내부단계는 ℓ 이 홀수일 때 $\deg g = (\ell - 1)/2$ (여기서는 48)인 $g(T) = \gamma$ 의 $\mathbb{F}_{q^k}$ 우에서의 뿌리찾기이다($\varphi = g(\xi)$; 차수 99의 형태 $g(T)^2(T^3 + b) - \gamma^2$ 는 ℓ 이 짝수일 때의 [7, eq. (6.1)]이다).

10 [7]과의 비교

명제 6.2는 개선인자를 인자별로 명시적으로 만든다. [7, Alg. 6.1]에서 순환변수 γ 는 $\gamma_0\mu_{(s-1)\nu}$ 를 돌므로 γ^ν 는 잉여류 $z^{-1}\mathbb{F}_{q^{k/2}}^\times$ 를 매 값마다 ν 번씩 돌며 매 단계마다 차수 $(\ell - 1)/2$ 의 뿌리찾기를 한다. 그 순환은 이미 $\mathbb{F}_{q^{k/2}}^\times$ -자리표의 맹목적인 순회이다. 그의 문자로($A \in G_0$, P 는 유리점) [7, Thm. 5.3(ii)-(iii)]에 의하여 $\varphi(A + P)^\nu h_{s,-A}(P) \in \mathbb{F}_{q^{k/2}}^\times$ 이므로 $\varphi(A + P)^\nu$ 는 $h_{s,-A}(P)^{-1} \in \mu_\ell$ 과 원소 $c_{A,P} \in \mathbb{F}_{q^{k/2}}^\times$ 의 곱이다 — 이것은 명제 6.2의 분해 $\mu_{\ell(s-1)} \cong \mu_\ell \times \mu_{s-1}$ 을 v 대신 $\varphi(A + P)^\nu$ 에 적용한것이다. 그의 c 는 μ_{s-1} -성분이며 $\varphi(kR)^\nu = c/z$ 로 하는 γ 에 대한 순환은 μ_ℓ -성분을 z^{-1} 에 고정하고 다른 성분을 도는데 이 성분은 z 에 관한 정보를 전혀 담고있지 않다. 이 논문의 방법은 (i) 자리표 그자체를 순환변수로 함으로써 ν 겹의 중복을 없애며 그 안에서 d 제곱뿌리는 유일하다(보조정리 3.5). (ii) 자리표를 두 x자리표로 복호하는것이 다항식시간이므로 뿌리찾기를 없앤다(알고리즘 5.1). (iii) 꼬임을 통하여 자리표를 $\mathbb{F}_{q^{k/2}}^\times$ 로부터 $\mathbb{F}_q \oplus W$ 로 축소한다(보조정리 4.1). (iv) W 에 손대기 전에 Legendre 기호로 x_A 가 $\xi(G_1)$ 에 속하는가를 검사하며 이것이 제 8절의 블록 순서이다. 네 인자는 $\nu \approx s/\ell$, $\tilde{O}(\ell)$, $q^{k/2-1-k/e}$, 그리고 약 q/ℓ 이며 그 곱은 상수와 로그인자를 무시하면 $q^{k-k/e}/\ell$ 로서 아래 표의 첫 두 열의 비이다. W 를 주사하는 대신 생성원의 배수들로 G_0 을 탐색하면 자리표가 한번 더 ℓ 개의 점으로 축소되며 이것이 마지막 열이다. 이련쇄의 어느것도 최종검사 전에는 z 를 쓰지 않으며 명제 6.2에 의하여 이 경로의 어느것도 그렇게 할수 없다.

이리하여 노름경로가 하는 일을 정확히 말할수 있다. $\ell \mid d$ 인 Tate 방향에서 원시 Miller 값의 모호성 — 크기 $(s-1)\nu$ 의 잉여류 — 은 노름으로 넘어갈 때 인자 ν 만큼 줄어든다. ζ 를 두 x자리표로 복호하는것은 두 변수를 모두 모르는 경우에도 다항식시간으로 된다(보조정리 4.1). 그리고 남은 자리표는 목표값과 독립이므로(명제 6.2) 제 8절의 순환이나 그보다 못한 주의 8.1의 순환은 아무런 안내도 없이 그것을 돈다.

[7, Alg. 6.1]과의 비교는 같은 약속밑에서, 기대값대 기대값으로 하여야 한다. 보통곡선에서 [7,

Alg. 6.1]의 반복당 성공확률은 많아야 $(\ell - 1)/((s - 1)\nu)$ 이며 [7, Rem. 6.5] 때 반복은 $\mathbb{F}_{q^k}$ 위에서 차수 $(\ell - 1)/2$ 의 뿌리찾기이다. 따라서 기대계산량은 적어도 $\frac{(s-1)\nu}{\ell-1} \cdot \tilde{O}(\ell) \approx \tilde{O}((q^k - 1)/\ell)$ 이다. 제 8절의 알고리즘에서 후보의 기대개수는 $q^{k/e}/2$ 이며 각각 $e = 6$ 일 때 평균 약 쌍선형넘기기 네번 (비싼 절반은 약 여덟번), $e = 4$ 일 때는 약 여덟번의 비용이 든다(제 9절). 주의 8.1의 $\mathbb{F}_{q^{k/2}}^\times$ 에서의 순환에서는 $\mathbb{F}_{q^{k/2}}$ 의 곱하기 몇번으로 된 단계가 $\frac{2(s-1)}{\ell-1}$ 번이다. 같은것끼리 비교하기 위하여 아래 표는 단일한 단위 M , 즉 $\mathbb{F}_{q^k}$ 에서의 곱하기 한번으로 나타낸다. 리용한 환산은 다음과 같다: 이 크기에서 $\mathbb{F}_{q^k}$ 에서의 두제곱뿌리와 $E(\mathbb{F}_{q^k})$ 에서의 ℓ 배 스칼라곱하기는 각각 $\approx 2^{12}M$; 성긴 직선 함수와 원분최종거듭제곱을 쓰는 $A \in E(\mathbb{F}_q)$, 순환길이 ℓ 의 Tate 쌍선형넘기기는 $\approx 2^{10}M$; $\mathbb{F}_{q^{k/2}}$ 에서의 곱하기는 $\approx 1M$; 주의 4.4의 Legendre 기호는 $\approx k/2 M$ 이고 $\mathbb{F}_q$ 에서의 Jacobi 기호는 무시할 수 있다; $\mathbb{F}_{q^k}$ 위에서 차수 d 의 뿌리찾기는 $\approx d \log_2(q^k) M$. 모든 항목은 기대값이며 실측기준값이 아니라 레시적인것이다. 주의 때 환산은 작은 인자범위안에서만 정확하며 어깨수들은 그 오차를 물려받는다. 확고한것은 절대값이 아니라 열들사이의 비, 즉 상수와 로그인자를 무시한 $q^{k-k/e}/\ell$ 이다.

곡선	[7, Alg. 6.1]	이 논문(제 8절)	주의 8.1	전수탐색
BN254 (alt_bn128)	$2^{2800}M$	$2^{518}M$	$2^{1271}M$	$2^{263}M$
BLS12-381	$2^{4325}M$	$2^{772}M$	$2^{2032}M$	$2^{264}M$

두가지 단서를 붙인다. Satoh의 확률에 대한 한계는 상한이므로 그의 실제기대계산량은 더 클수 있으며 이것은 차이를 더 넓힐뿐이다. 그리고 이 비교가 정당한것은 15행에서 $e := h_{s,-Q}(A)$ 로 하면 알고리즘이 [7, Alg. 6.1]의 바로 그 문제를 풀기때문이며 — 제 9절이 시험곡선에서 이것을 실증한다 — 한 부분프로그램이 다른것을 대신하기때문이 아니다.

11 제한성

1. 이 방법은 짝수 꼬임차수 $e \geq 4$ (주의 4.2)와 $k > 2$ (주의 4.3)를 요구한다. 따라서 [7]이 상수번의 반복회수를 얻는 초특이곡선들에는 적용되지 않으며 바로 [7]이 가망없다고 보는 영역에 적용된다.
2. 고정된 A 에 대하여 G_0 을 직접 탐색하는데는 기대값으로 쌍선형넘기기계산 $\ell/2$ 번, 두 곡선에서 약 $2^{263}M$ 과 $2^{264}M$ 이 든다. 이것은 제 8절의 알고리즘보다 약 $4q^{k/e}/\ell$ 배, 즉 2^{256} 배와 2^{509} 배 적으며 μ_ℓ 에서의 리산로그(특수 TNFS로 $\approx 2^{100}$ 과 $\approx 2^{126}$)는 그보다도 더 싸다. Satoh도 자기의 알고리즘에 대하여 같은 관찰을 하고있다. 이 개선은 차이를 좁히지만 없애지는 못한다.
3. $\xi(G_0) \subset \mathbb{F}_{q^{k/2}}$ 의 자취/노름에 의한 리용은 [1]에 의한것이며 그들의 어깨수 $q - 1$ 에로의 환원은 고정변수설정에서는 이 논문의 어느것보다도 강하다. 이 점에서 주장하는 새로움은 그 기구가 두 변수를 모르는 경우에도 넘어가서도 살아남는다는것이다. 다른 기여들은 머리말에 려겨되어있다.

4. 순환은 z 를 최종검사에서만 리용하며 명제 6.2가 그 리유를 말해준다. 즉 노름우에 세워진 어떤것도 달리 할수 없다. 진짜 Ate 순환 $T = t - 1$ 에 대한 관계식 (8)도 출구로 되지 못하는 데 그것은 $d = h\ell$ 인 명제 3.1으로 줄어들기때문이다(주의 3.2). Satoh 자신의 분해도 제외가 아니다. [7, Thm. 5.5]의 상수 $c \in \mathbb{F}_{q^{k/2}}^\times$ 는 같은 중국나머지분해(제 10절)에서 $\varphi(A + P)^\nu$ 의 μ_{s-1} -성분이다 — v 의것이 아닌데 그의 순환길이에서는 v 의 노름이 1이기때문이다(주의 3.2). 덧붙여 말하면 $(\varphi(A + P)^\nu)^{s+1} = c_{A,P}^2$ 이다. 그것은 같은 리유로 z 와 독립이며 그의 정리 5.5(iii)의 증명이 인용하는 사실 $\mu_\ell \cap \mathbb{F}_{q^{k/2}}^\times = \{1\}$ 은 그 리유로부터 나오는 귀결이다. 따라서 c 에 대한 그의 순환도 z 로부터 아무것도 받지 못한다. 필자는 이 자리표를 피하는 원시값의 분해를 알지 못한다. 그러한 분해가 존재하는가 하는것이 남겨진 미해결문제이다.

참고문헌

- [1] S. Akagi and Y. Nogami. *Exponentiation inversion problem reduced from fixed argument pairing inversion on twistable Ate pairing and its difficulty*. IWSEC 2014, LNCS 8639, pp. 240–249, Springer, 2014.
- [2] G. Frey and H.-G. Rück. *A remark concerning m -divisibility and the discrete logarithm in the divisor class group of curves*. Math. Comp. 62(206), pp. 865–874, 1994.
- [3] S. Galbraith, F. Hess and F. Vercauteren. *Aspects of pairing inversion*. IEEE Trans. Inform. Theory 54(12), pp. 5719–5728, 2008.
- [4] R. Granger, F. Hess, R. Oyono, N. Thériault and F. Vercauteren. *Ate pairing on hyperelliptic curves*. EUROCRYPT 2007, LNCS 4515, pp. 430–447, Springer, 2007.
- [5] J. Groth. *On the size of pairing-based non-interactive arguments*. EUROCRYPT 2016, LNCS 9666, pp. 305–326, Springer, 2016.
- [6] T. Satoh. *Miller inversion is easy for the reduced Tate pairing of embedding degree greater than one*. IACR Cryptology ePrint Archive, Report 2019/385, revised 2025.
- [7] T. Satoh. *Decomposition of the Ate pairing and its relation to generalized pairing inversion*. IACR Cryptology ePrint Archive, Report 2026/1049.