

Более быстрый метод обобщённого обращения спаривания

Лаэль Селье

lael.cellier@laposte.net

5 октября 2026 г.

Аннотация

Сато недавно предложил алгоритм для задачи обобщённого обращения спаривания (GPI), использующий структуру функции Миллера, а не полный перебор или оракул с фиксированным аргументом. На обыкновенной кривой его ожидаемая стоимость имеет порядок $(q^k - 1)/\ell^2$ вызовов процедуры поиска корней степени $\Omega(\ell)$, т.е. $\tilde{O}((q^k - 1)/\ell)$ операций. Я предлагаю иной метод для той же задачи, применимый к обыкновенным кривым чётной степени вложения $k > 2$, допускающим скручивание чётной степени $e \geq 4$, с ожидаемой стоимостью $q^{k/e}/2$ кандидатов ценой нескольких спариваний каждый: в умножениях в $\mathbb{F}_{q^k}$ выигрыш по сравнению с алгоритмом Сато составляет множитель $q^{k-k/e}/\ell$ с точностью до констант и логарифмов. Анализ использует цикл Миллера длины, кратной ℓ , как в спаривании Тейта, тогда как у Сато длина цикла равна $q^{k/2} \equiv -1 \pmod{\ell}$; целевое спаривание участвует лишь через финальную проверку принадлежности, так что алгоритм решает GPI для спаривания Сато непосредственно, без преобразования между спариваниями и без дискретного логарифма где бы то ни было. Приведённое значение спаривания и норма сырого значения Миллера — независимые координаты, факт китайской теоремы об остатках, ибо $\gcd(\ell, q^{k/2} - 1) = 1$; метод, соответственно, есть поиск по парам абсцисс с финальной проверкой спаривания, и ничего иного я не утверждаю: техническое ядро — полиномиальное обращение сырого значения Миллера при обоих неизвестных аргументах — служит тому, чтобы зафиксировать это пространство поиска и показать, что ничто на этом пути не может его сжать. Тест принимает на вход сырое значение Миллера до финального возведения в степень — тот же вход, что и у собственного алгоритма обращения Миллера Сато, которого ни один протокол не раскрывает; переход от приведённого значения к нему есть шаг обращения возведения в степень Гэлбрейта, Хесса и Веркотерена, который разделы 6–8 выполняют поиском и который, как показывает предложение 6.2, нельзя сократить через норму, — и сочетает нормовое соотношение из более ранней работы Сато об обращении Миллера с $\mathbb{F}_q$ -линейной проекцией, разделяющей две неизвестные абсциссы, лежащие в дополнительных $\mathbb{F}_q$ -подпространствах поля $\mathbb{F}_{q^{k/2}}$; использование этой подполевой структуры восходит к Акаги и Ногами, однако их редукция требует знания одного из аргументов. На BN254 ожидаемая стоимость падает примерно с 2^{2800} до 2^{518} умножений в $\mathbb{F}_{q^k}$, на BLS12-381 примерно с 2^{4325} до 2^{772} . Все эти величины остаются много выше стоимости метода исчисления индексов в $\mathbb{F}_{q^k}$; результат структурный, а не криптоаналитический.

1. Введение

Гэлбрейт, Хесс и Веркотерен [3] выделили три задачи обращения для билинейного спаривания $e: G_1 \times G_0 \rightarrow \mu_\ell$: две задачи с фиксированным аргументом FAPI-1 и FAPI-2, в которых один из аргументов задан, и обобщённую задачу GPI, в которой задана лишь цель z и допустима любая пара прообразов.

Сато [7] заметил, что не известен алгоритм, использующий математическую структуру вычисления спаривания, в отличие от поиска в одной из групп, и предложил такой: записав ℓ -ю функцию Миллера как систему факторов, он получает разложение спаривания Ate, из которого решение GPI собирается шагом поиска корней. Полученная процедура [7, Alg. 6.1] перебирает $\gamma \in \mu_{\nu(s-1)}$, где $s = q^{k/2}$ и $\nu = (s + 1)/N$, и на каждом шаге ищет корни функции φ степени $(N - 1)/2$.

На обыкновенной кривой $\nu(s-1) = (q^k - 1)/\ell$, а вероятность успеха на шаге не превосходит $(\ell - 1)/((s-1)\nu)$ [7, Rem. 6.5], так что ожидаемая стоимость имеет порядок $(q^k - 1)/\ell^2$ поисков корней степени $\ell/2$, то есть $\tilde{O}((q^k - 1)/\ell)$ операций; Сато характеризует этот случай как «слишком неэффективный даже для численных экспериментов при малых значениях q ».

Настоящая заметка предлагает иной метод для той же задачи с меньшей ожидаемой стоимостью. Это, как и у Сато, слепой поиск с финальной проверкой спаривания — здесь по парам абсцисс, — и предложение 6.2 показывает, почему ничто, построенное на норме значения Миллера, не может быть ничем иным: приведённое значение спаривания и эта норма — независимые координаты. Два момента постановки существенны и оговариваются сразу.

Длина цикла. Метод берёт функцию Миллера $h_{d,A}$ в $\mathbb{F}_q$ -рациональном аргументе $A \in G_1$, вычисляемую в аргументе нулевого следа $Q \in G_0$, с длиной цикла d , кратной ℓ , — постановка Тейта. Алгоритм 6.1 Сато выдаёт, в обозначениях этой заметки, $h_{q^{k/2}, -Q}(A)$ (его буквы A и Q противоположны моим: его A лежит в G_0): функция Миллера в аргументе нулевого следа и цикл длины $s = q^{k/2}$. Существенно не ориентация, а вычет длины цикла по модулю ℓ : нормовое соотношение, на котором основана заметка (предложение 3.1), даёт $(\xi(Q) - \xi(A))^d$ при $d \equiv 0 \pmod{\ell}$ и $(\xi(Q) - \xi(A))^{d-1}$ при $d \equiv -1 \pmod{\ell}$, что при $d = s$ тождественно равно 1 (замечание 3.2). Поэтому предлагаемый метод *не* заменяет внутренний шаг [7, Alg. 6.1], и я этого не утверждаю. Верно же то, что целевое спаривание участвует в методе лишь через финальную проверку принадлежности, так что его можно взять равным самому спариванию Сато (раздел 6); никакое преобразование между спариваниями и, в частности, никакой дискретный логарифм нигде не участвуют.

Что нового. Ядро метода — полиномиальная процедура, которая по сырому значению Тейта-Миллера $h_{d,A}(Q)$ при *обоих* неизвестных A и Q восстанавливает A и Q (раздел 5). Она сочетает нормовое соотношение, использованное Сато в случае фиксированного аргумента [6], с линейной проекцией, разделяющей две неизвестные абсциссы, лежащие в дополнительных $\mathbb{F}_q$ -подпространствах поля $\mathbb{F}_{q^{k/2}}$ (раздел 4). Эту подполевую структуру впервые использовали Акаги и Ногами [1], сводя задачу обращения возведения в степень к показателю $q-1$ для FAPI-2 через минимальный многочлен *заданной* абсциссы; их построение требует $\text{Tr}(\xi(Q)^3)$ и $N(\xi(Q))$ и не переносится на случай неизвестного Q . Переход от «одна неизвестная, минимальный многочлен» к «две неизвестные, линейная проекция» — техническая новизна. Вокруг неё заметка добавляет независимость значения спаривания и нормы (предложение 6.2), фиксирующую пространство поиска и показывающую, что на этом пути его нельзя сжать; замкнутые формы значений Миллера при длинах цикла s и q как степеней приведённого спаривания Тейта (лемма 3.3, замечание 3.4), позволяющие алгоритму напрямую целиться в спаривания Сато; и учёт улучшения по сравнению с [7, Alg. 6.1] в четырёх множителях, каждый из которых отнесён к одному из этих результатов (раздел 10).

Отмечу попутно, что GPI не лишена криптографических следствий: доказательство Groth16 [5] принимается, как только выполнено единственное уравнение произведения спариваний, и полагание его третьего элемента равным $\mathcal{O}$ оставляет целевое значение, вычисляемое лишь по ключу проверки и открытому входу, так что любое решение GPI даёт подделку для произвольного утверждения.

2. Постановка и обозначения

Пусть q — степень нечётного простого числа, а $E/\mathbb{F}_q$ — обыкновенная эллиптическая кривая с короткой моделью Вейерштрасса $Y^2 = X^3 + a_4X + a_6$. Пусть ℓ — нечётное простое с $\ell \parallel \#E(\mathbb{F}_q)$ — точная делимость, $\ell \mid \#E(\mathbb{F}_q)$ и $\ell^2 \nmid \#E(\mathbb{F}_q)$, так что $h := \#E(\mathbb{F}_q)/\ell$ взаимно просто с ℓ , что нужно лемме 6.1, — и чётной степени вложения $k > 2$; поскольку $k = \text{ord}_\ell(q)$ делит $\ell - 1$, автоматически $\ell \nmid k$. Следуя [7, §5], я полагаю

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

так что $G_0 \cong G_1 \cong \mathbb{Z}/\ell\mathbb{Z}$, $G_0 \cap G_1 = \{\mathcal{O}\}$ и $E[\ell] = G_1 \oplus G_0$. Поскольку $\ell \mid s+1$, имеем $\text{Fr}_q^{k/2} P = -P$ для $P \in G_0$; а поскольку $\ell \nmid s-1$, у $\text{Fr}_q^{k/2}$ нет собственных значений, кроме 1 на G_1

и -1 на G_0 , откуда

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

ξ, η обозначают координатные функции, $\tau := -\xi/\eta$ — униформизирующий параметр в $\mathcal{O}$, а $h_{n,A}$ — нормированную n -ю функцию Миллера в A , т.е. функцию с $\mathrm{div} h_{n,A} = n[A] - [nA] - (n-1)[\mathcal{O}]$ и $\mathrm{lc}_{\mathcal{O}}(h_{n,A}) = 1$ относительно τ .

Всюду $A \in G_1$, $Q \in G_0$, а d — целое с

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

когда требуется извлечь корень степени d (лемма 3.5), я дополнительно предполагаю $d \mid s+1$ — второе условие из [6, Alg. 4.1]. Сырое значение Миллера есть $v := h_{d,A}(Q) \in \mathbb{F}_{q^k}^\times$, а приведённое спаривание Тейта — $t(A, Q) := h_{\ell,A}(Q)^{(q^k-1)/\ell} \in \mu_\ell$, билинейное и невырожденное на $G_1 \times G_0$.

3. Нормовое соотношение

Предложение 3.1. В указанных обозначениях, используя лишь $\ell \mid d$,

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

В частности $v^{s+1} = -(\xi(Q) - \xi(A))^\ell$ при $d = \ell$.

Доказательство. Так как $\ell \mid d$ и $A \in E[\ell]$, то $[d]A = \mathcal{O}$ и $\mathrm{div} h_{d,A} = d([A] - [\mathcal{O}])$; аналогично $\mathrm{div} h_{d,-A} = d([-A] - [\mathcal{O}])$. Значит, $h_{d,A}h_{d,-A}$ и $(\xi - \xi(A))^d$ имеют один и тот же дивизор $d([A] + [-A] - 2[\mathcal{O}])$, и обе имеют старший коэффициент 1 в $\mathcal{O}$, ибо $\xi = \tau^{-2} + O(\tau^{-1})$; итак,

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

Далее, $h_{d,A} \circ [-1]$ и $h_{d,-A}$ имеют один и тот же дивизор; поскольку $\tau \circ [-1] = -\tau$ для короткой модели Вейерштрасса и $\mathrm{ord}_{\mathcal{O}} h_{d,A} = -d$, имеем $\mathrm{lc}_{\mathcal{O}}(h_{d,A} \circ [-1]) = (-1)^d$, откуда

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

Наконец, $h_{d,A}$ определена над $\mathbb{F}_q$ и $\mathrm{Fr}_q^{k/2}Q = -Q$, поэтому $v^s = h_{d,A}(\mathrm{Fr}_q^{k/2}Q) = h_{d,A}(-Q) = (-1)^d h_{d,-A}(Q)$ по (5), и $v^{s+1} = v \cdot v^s = (-1)^d (h_{d,A}h_{d,-A})(Q)$, что и есть (3) в силу (4). $\square$

Правая часть (3) не содержит значений Миллера. Сравним с разложением $h_{s+1,A} = (\xi - \xi(A)) h_{s,A}$, лежащим в основе [6, Alg. 4.1]: там множитель $h_{s,A}(Q)$ исключается возведением в степень $s+1$. Его точная структура дана леммой 3.3: $h_{s,A}(Q) = -t(A, Q)^{-1/2}$ — элемент порядка ровно 2ℓ , делящего $s+1$, чья противоположность $-h_{s,A}(Q) = t(A, Q)^{-1/2}$ лежит в μ_ℓ ; при функции Миллера в аргументе нулевого следа получается, напротив, $h_{s,Q}(A) = t(Q, A)^{-1/2} \in \mu_\ell$, что и есть утверждение [4] в этой постановке, с его замкнутой формой. Именно это явление Сато описывает формулой «(значение до финального возведения в степень) = (простая функция) $\times$ (другое спаривание)». Два замечания о постоянной. Во-первых, это известный знак, а не величина, подлежащая предвычислению. Во-вторых, реализации, не нормирующие функцию Миллера в $\mathcal{O}$ (такова `ell Tate pairing` в PARI/GP), заменяют её другой постоянной; то, что она вновь не зависит от A и Q , — эмпирическое наблюдение о нормировке прямых в PARI, сделанное на игрушечной кривой раздела 9, и тогда её можно считать по одной известной паре.

Замечание 3.2 (Длина цикла, а не ориентация). Для произвольной длины цикла n с $[n]P \neq \mathcal{O}$ то же вычисление дивизоров даёт, точно и без знака,

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

причём обе части имеют старший коэффициент 1 в $\mathcal{O}$; (6) верно для P из любой из двух групп. (Знак в (5) равен $(-1)^{\text{ord}_{\mathcal{O}} h_{n,P}}$, то есть $(-1)^{n-1}$ при $[n]P \neq \mathcal{O}$ и $(-1)^n$ при $\ell \mid n$; он появляется лишь тогда, когда $h_{n,P}$ вычисляются в $-R$ вместо $h_{n,-P}$ в R .) Существенны три вычета n по модулю ℓ .

Если $n \equiv 0 \pmod{\ell}$, знаменатель равен 1 и нормовое соотношение восстанавливает $(\xi - \xi(P))^n$: это предложение 3.1, и оно верно в *обеих* ориентациях. В ориентации Ate $\text{Fr}_q^{k/2}$ действует на коэффициенты $h_{n,Q}$ и переводит её в $h_{n,-Q}$ — без вычисления в противоположной точке и, стало быть, без знака, — так что

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

две нормы совпадают.

Если $n \equiv -1 \pmod{\ell}$, то $[n]P = -P$ и (6) обращается в $(\xi - \xi(P))^{n-1}$. При $n = s$ показатель $s - 1$ аннулирует $\mathbb{F}_{q^{k/2}}^\times$, так что $h_{s,P}(R)^{s+1} = 1$ тождественно и никакой информации об абсциссах не остаётся; именно этот цикл использует [7, Alg. 6.1] в обыкновенном случае, и потому в тот алгоритм нельзя подставить настоящий тест. Для прочих $n \equiv -1 \pmod{\ell}$, напр. $n = 2\ell - 1$, норма нетривиальна, но определяет ζ лишь с точностью до $\gcd(n - 1, s - 1)$ кандидатов: 48 на игрушечной кривой и $48u \approx 2^{67,7}$ на BN254 (вычислено для этой кривой; в общем случае $\gcd(2\ell - 2, s - 1)$ кратен $\gcd(\ell - 1, q - 1) = 6u$, поскольку кофакторы $6u^3 + 6u^2 + 3u + 1$ и $6u^3 + 6u^2 + 4u + 1$ взаимно просты, а множитель 8 происходит от остальных множителей $s - 1$). Единственность корня — ровно то, что покупает $\ell \mid d \mid s + 1$ через $\gcd(d, s - 1) = \gcd(d, 2)$ (лемма 3.5), и ровно то, что теряется при $n \equiv -1 \pmod{\ell}$.

Если $n \equiv q \pmod{\ell}$, как для цикла Ate $T = t - 1$ с $P = Q \in G_0$, то $[n]Q = \text{Fr}_q Q$ и

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

опять-таки без знака. Поскольку $\xi(A) \in \mathbb{F}_q$, знаменатель равен $(\xi(A) - \xi(Q))^q$, и (8) сводится к $(\xi(A) - \xi(Q))^{T-q} = (\xi(A) - \xi(Q))^{-h\ell}$ при $h = \#E(\mathbb{F}_q)/\ell$: это $(-h)$ -я степень (7) — без знака, с обращением — несущая ту же информацию, что и предложение 3.1 при $d = h\ell$, которому нужно лишь $\ell \mid d$. (Согласованно, $h_{q,Q} = h_{T,Q} h_{\ell,Q}^h$ как нормированные функции, и $h_{q,Q}(A)^{s+1} = 1$.) Все тождества этого замечания проверены численно (раздел 9).

Лемма 3.3. Для $P \in E[\ell]$ как рациональные функции

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

Кроме того, для ненулевых $A \in G_1$ и $Q \in G_0$, где $t(\cdot, \cdot)$ — приведённое спаривание Тейта при любом порядке аргументов,

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

так что $h_{s,A}(Q) = -t(A, Q)^{-1/2}$ и $h_{s,Q}(A) = t(Q, A)^{-1/2}$, где квадратные корни — единственные в μ_ℓ . В частности, $h_{s,Q}(A) \in \mu_\ell$ имеет порядок ровно ℓ , а $h_{s,A}(Q)$ — порядок ровно 2ℓ , причём $2\ell \mid s + 1$.

Доказательство. Правило композиции $h_{mn,P} = h_{m,P}^n h_{n,[m]P}$ (равные дивизоры, обе части нормированы) даёт при вычислении $h_{\ell s,P}$ двумя способами $h_{\ell s,P}^\ell h_{\ell,[s]P} = h_{\ell,P}^s h_{s,[\ell]P}$; поскольку $[s]P = -P$ и $h_{s,\mathcal{O}} = 1$, это (9). Вычисляя: в ориентации Ate $h_{\ell,Q}(A)^s = \text{Fr}_q^{k/2}(h_{\ell,Q}(A)) = h_{\ell,-Q}(A)$ по сопряжению коэффициентов, так что $h_{s,Q}(A)^\ell = 1$; в ориентации Тейта $h_{\ell,A}(Q)^s = h_{\ell,A}(-Q) = -h_{\ell,-A}(Q)$ по (5) при нечётном ℓ , так что $h_{s,A}(Q)^\ell = -1$.

Для (10) то же правило при $[\ell]A = [s+1]A = \mathcal{O}$ даёт $h_{\ell,A}^c = h_{\ell c,A}$ для всякого c и $h_{(s+1)(s-1),A} = h_{s+1,A}^{s-1}$, а дивизоры дают $h_{s+1,A} = (\xi - \xi(A)) h_{s,A}$. Отсюда при $\zeta = \xi(Q) - \xi(A) \in \mathbb{F}_{q^{k/2}}^\times$

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

где последний шаг — потому что $h_{s,A}(Q)^{2\ell} = 1$ и $2\ell \mid s+1$. Случай Ate тождествен с переставленными A и Q . Так как ℓ нечётно, возведение в квадрат есть биекция μ_ℓ , что фиксирует квадратные корни; знак $h_{s,A}(Q)$ навязан равенством $h_{s,A}(Q)^\ell = -1$. Наконец, $t(A, Q) \neq 1$ по невырожденности, так что $h_{s,A}(Q)^2 \neq 1$ и порядок равен ровно 2ℓ , а не 2; аналогично $h_{s,Q}(A) \neq 1$ и его порядок равен ровно ℓ . $\square$

Четыре следствия. Во-первых, значение Миллера при длине цикла s есть приведённое спаривание Тейта в степени $-1/2$ и без финального возведения в степень: «another pairing» Сато понимается буквально. Оно билинейно по обоим аргументам как сырое значение Миллера, что проверено напрямую (раздел 9). Во-вторых, знак — вновь $(-1)^\ell$ из (5), механизм (7); (9) даёт утверждение [4] для ориентации Ate в две строки. В-третьих, предложение 3.1 при $d = \ell$ — то же тождество, прочитанное ещё раз: $h_{\ell,A}(Q)^{s+1} = h_{s+1,A}(Q)^\ell = \zeta^\ell h_{s,A}(Q)^\ell = -\zeta^\ell$. В-четвёртых, то же правило даёт значение для длины цикла q , замечание 3.4.

Замечание 3.4 (Длина цикла q). То же правило композиции, применённое к $h_{q^k,Q}$, даёт $h_{q^k,Q} = \prod_{i=0}^{k-1} h_{q,[q^i]Q}^{q^{k-1-i}}$, и поскольку $[q^i]Q = \text{Fr}_Q^i Q$, а A рациональна, $h_{q,\text{Fr}_Q^i Q}(A) = h_{q,Q}(A)^{q^i}$, откуда $h_{q^k,Q}(A) = h_{q,Q}(A)^{kq^{k-1}}$. С другой стороны, $\text{div } h_{q^k,Q} = (q^k - 1)([Q] - [\mathcal{O}]) = \text{div } h_{\ell,Q}^{(q^k-1)/\ell}$, так что $h_{q^k,Q}(A) = t(Q, A)$. Одно это даёт лишь $h_{q,Q}(A) \in \mu_{k\ell}$; принадлежность μ_ℓ следует из того же правила, применённого к $h_{q\ell,Q}$: $h_{q\ell,Q}^\ell h_{\ell,[q]Q} = h_{\ell,Q}^q$, а поскольку $h_{\ell,Q}(A)^q = h_{\ell,\text{Fr}_Q Q}(A)$ и $[q]Q = \text{Fr}_Q Q$, получаем $h_{q,Q}(A)^\ell = 1$. Итак, поскольку корень в μ_ℓ единствен,

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

причём последняя форма — потому что $q^{k-1} = s q^{k/2-1} \equiv -q^{k/2-1} \pmod{\ell}$ (и $\ell \nmid k$, раздел 2). Цель [7, Alg. 6.6], обёртки с циклом q его алгоритма 6.1, есть $h_{q,-Q}(A) = t(Q, A)^{1/(kq^{k/2-1})}$ в обозначениях этой заметки ($h_{q,Q}(A)$ билинейно по Q , будучи фиксированной степенью t); финальная проверка $t(Q, A) = z^{-kq^{k-1}}$ в строке 15 раздела 8 решает, следовательно, и эту задачу напрямую. (Проверено численно, раздел 9.)

Лемма 3.5. Пусть $d \mid s+1$. Тогда $\gcd(d, s-1) = \gcd(d, 2)$, и для $u \in \mathbb{F}_{q^{k/2}}^\times$ уравнение $\zeta^d = u$ имеет либо ни одного, либо ровно $\gcd(d, 2)$ решений в $\mathbb{F}_{q^{k/2}}^\times$. Когда оно разрешимо:

1. если d нечётно, решение единственно и равно $u^{d^{-1} \bmod (s-1)}$;
2. если d чётно, решения суть $\pm \zeta_0$ для любого одного решения ζ_0 , которое получается так: записать $d = 2^a d'$ с нечётным d' , положить $u_1 := u^{d'^{-1} \bmod (s-1)}$ и извлечь из u_1 в $\mathbb{F}_{q^{k/2}}$ а последовательных квадратных корней любым стандартным алгоритмом.

Доказательство. Стандартно: s нечётно, поэтому $\gcd(s+1, s-1) = 2$ и $\gcd(d, s-1) \mid 2$, а остальное — подсчёт решений уравнения $\zeta^d = u$ в циклической группе, как в доказательстве [6, Thm. 4.2]. Ниже используется лишь случай (i), поскольку d всюду нечётно. $\square$

При нечётном $d = \ell$ применим случай (i). Случай (ii) — знаковая неоднозначность, видимая в [6, Alg. 4.1, шаги 3–4], где получаются две абсциссы $\xi(A) \pm u$; она удваивает стоимость и только.

4. Лемма о разделении

Предположим, что E допускает скручивание E' степени $e \mid k$, и положим $m := k/e$. Так как k чётно, $e \geq 3$ означает $e \in \{4, 6\}$: скручивание $e = 3$ вынуждает $j(E) = 0$ и $6 \mid k$, а значит, существование секстического скручивания, так что $e = 3$ никогда не бывает максимальной степенью скручивания, и всюду далее я беру e чётным. Скручивание определено над $\mathbb{F}_{q^m}$ параметром $\theta \in \mathbb{F}_{q^m}^\times$, класс которого порождает $\mathbb{F}_{q^m}^\times / (\mathbb{F}_{q^m}^\times)^e$ и выбран среди $\varphi(e)$ возможных классов как тот, для которого $\ell \mid \#E'(\mathbb{F}_{q^m})$ (скручивание типа D или типа M в обычной терминологии), а изоморфизм скручивания $\psi: E' \rightarrow E$ переводит (x', y') в $(\omega x', \omega^{3/2} y')$, где $\omega := \theta^{2/e}$. Поскольку $G_0 = \psi(E'(\mathbb{F}_{q^m})[\ell])$,

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

— $\mathbb{F}_q$ -подпространство размерности $m = k/e$, содержащееся в $\mathbb{F}_{q^{k/2}}$, ибо e чётно. (Согласованно с этим, $\xi(P) \in \mathbb{F}_{q^{k/2}}$, ибо ξ чётна, а $\text{Fr}_q^{k/2}$ действует на G_0 как $[-1]$, [7, Lem. 5.2].) С другой стороны, $\xi(A) \in \mathbb{F}_q$ для $A \in G_1$.

Лемма 4.1 (О разделении). *Пусть $e \in \{4, 6\}$ и $\lambda := \omega^{q^m-1}$. Тогда $\omega \notin \mathbb{F}_{q^m}$, так что $\lambda \neq 1$ и $\mathbb{F}_q \cap W = \{0\}$; $\mathbb{F}_q$ -линейное отображение*

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

корректно определено, удовлетворяет $\ker L = W$ и $L|_{\mathbb{F}_q} = (1 - \lambda) \text{id}$; и для $\zeta := \xi(Q) - \xi(A)$ с $\xi(Q) \in W$, $\xi(A) \in \mathbb{F}_q$

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

Доказательство. Если $\omega \in \mathbb{F}_{q^m}$, то $\theta^2 = \omega^e \in (\mathbb{F}_{q^m}^\times)^e$, и класс θ имеет порядок, делящий 2, в циклической группе порядка e , в которой он имеет порядок e ; значит, $e \mid 2$ вопреки $e \geq 4$. Итак, $\omega \notin \mathbb{F}_{q^m}$, т.е. $\lambda \neq 1$. Если $a \in \mathbb{F}_q \cap W$ и $a \neq 0$, то $a = \omega x'$ с $x' \in \mathbb{F}_{q^m}^\times$ и $\omega = a/x' \in \mathbb{F}_{q^m}$ — противоречие; поэтому $\mathbb{F}_q \cap W = \{0\}$. L является $\mathbb{F}_q$ -линейным, так как таково $u \mapsto u^{q^m}$; для $u = \omega x' \in W$ имеем $u^{q^m} = \omega^{q^m} x' = \lambda u$, откуда $L(u) = 0$, т.е. $W \subseteq \ker L$. Обратно, $\omega^{e/2} = \theta$, а $X^{e/2} - \theta$ неприводим над $\mathbb{F}_{q^m}$: его степень $e/2 \in \{2, 3\}$ проста, а θ не является $(e/2)$ -й степенью, иначе θ^2 было бы e -й степенью и класс θ имел бы порядок, делящий 2. Итак, $1, \omega, \dots, \omega^{e/2-1}$ — $\mathbb{F}_{q^m}$ -базис $\mathbb{F}_{q^{k/2}}$ (заметим, $[\mathbb{F}_{q^{k/2}} : \mathbb{F}_{q^m}] = e/2$), составленный из собственных векторов $u \mapsto u^{q^m}$ с собственными значениями λ^j , $0 \leq j < e/2$, попарно различными, ибо $\lambda \neq 1$ и $\lambda^{e/2} = \theta^{q^m-1} = 1$ при простом $e/2$. Следовательно, $u \mapsto u^{q^m}$ диагонализуемо, а $\ker L$ — его собственное подпространство для λ , равное $\omega \mathbb{F}_{q^m} = W$. Для $a \in \mathbb{F}_q$ имеем $a^{q^m} = a$, откуда $L(a) = (1 - \lambda)a$. Применяя L к ζ , получаем $L(\zeta) = -(1 - \lambda)\xi(A)$, что и есть (12). $\square$

Замечание 4.2. При $e = 2$ имеем $m = k/2$ и $W = \omega \mathbb{F}_{q^{k/2}} = \mathbb{F}_{q^{k/2}}$: проекция вырождается ($\lambda = 1$, $L = 0$), но ничто не ломается — у $\xi(A) \in \mathbb{F}_q$ по-прежнему лишь q возможных значений, так что шаг 3 алгоритма 5.1 становится циклом по $x_A \in \mathbb{F}_q$ с $x_Q = \zeta + x_A$ ценой $O(q)$ вместо $O(1)$, а алгоритм раздела 8 проходит по $\mathbb{F}_q \times \mathbb{F}_{q^{k/2}}$ ценой $q^{k/e}/2 = q^{k/2}/2$ своей общей формулы. Декодирование за $O(1)$ требует, таким образом, кватернического или секстического скручивания — BN и BLS12 ($e = 6$), KSS16 ($e = 4$), кривые Брезинга–Венга из [1] — и не кривые, несущие лишь квадратичное скручивание.

Замечание 4.3. При $k = 2$, в частности для суперсингулярных кривых из [7, §4], где $t = 0$ вынуждает $k \leq 2$, имеем $s = q$ и обе абсциссы лежат в $\mathbb{F}_q$: никакое $\mathbb{F}_q$ -линейное отображение их не разделяет. В этом, на мой взгляд, и состоит структурная причина того, что [6] (FAPI, один аргумент известен, полиномиальное время) и [7] (GPI, оба неизвестны, экспоненциальное) имеют непересекающиеся области полезности.

Для кривой BN имеем $e = 6$, $m = 2$, $L(u) = u^q - \lambda u$ и $\lambda^3 = \theta^{q^2-1} = 1$: λ — примитивный кубический корень из единицы. В общем случае $\lambda^{e/2} = 1$. Это постоянная кривой, получаемая по любому известному образующему G_0 .

Замечание 4.4 (Проверка Лежандра для G_0). Для $x_Q \in \mathbb{F}_{q^{k/2}}$ с $\beta := x_Q^3 + a_4 x_Q + a_6 \neq 0$ пусть $Q = (x_Q, y_Q)$, где $y_Q \in \mathbb{F}_{q^k}$, $y_Q^2 = \beta$. Тогда $\text{Fr}_q^{k/2} Q = -Q$ тогда и только тогда, когда β — неквадрат в $\mathbb{F}_{q^{k/2}}$: действительно, $\text{Fr}_q^{k/2} Q = (x_Q, y_Q^s)$, а $y_Q^s = -y_Q$ тогда и только тогда, когда $y_Q^{s-1} = \beta^{(s-1)/2} = -1$. Стало быть, принадлежность Q к $\ker(\text{Fr}_q^{k/2} + 1)$ решается одним символом Лежандра в $\mathbb{F}_{q^{k/2}}$ до извлечения какого-либо квадратного корня, и примерно половина $x_Q \in \mathbb{F}_{q^{k/2}}$ с $\beta \neq 0$ его проходит: число $x \in \mathbb{F}_{q^{k/2}}$, для которых $\beta(x)$ — неквадрат, равно $(s + t_s - N_0)/2$, где t_s — след Фробениуса E над $\mathbb{F}_{q^{k/2}}$, а $N_0 = \#\{\beta = 0\}$. На подпространстве $W = \omega \mathbb{F}_{q^m}$ две степени скручивания ведут себя по-разному. При $e = 6$ ($a_4 = 0$) для $x_Q = \omega u$ имеем $\beta = \theta u^3 + a_6 \in \mathbb{F}_{q^m}$, и поскольку $[\mathbb{F}_{q^{k/2}} : \mathbb{F}_{q^m}] = 3$ нечётно, β — неквадрат в $\mathbb{F}_{q^{k/2}}$ тогда и только тогда, когда неквадрат в $\mathbb{F}_{q^m}$: выживает около половины $x_Q \in W$, а символ можно вычислять прямо в $\mathbb{F}_{q^m}$. При $e = 4$ ($a_6 = 0$) $\beta = \omega u(\theta u^2 + a_4)$ с $u(\theta u^2 + a_4) \in \mathbb{F}_{q^m}$ — квадрат в квадратичном расширении $\mathbb{F}_{q^{k/2}}$, — тогда как ω есть неквадрат в $\mathbb{F}_{q^{k/2}}$ ($\omega^{(s-1)/2} = \theta^{(q^m-1)/2 \cdot (q^m+1)/2} = -1$, ибо θ — неквадрат в $\mathbb{F}_{q^m}$, а $(q^m+1)/2$ нечётно): выживает *каждое* $x_Q \in W$ с $\beta \neq 0$, проверка пуста, и всю фильтрацию выполняет $[\ell]Q = \mathcal{O}$. Символ не следует вычислять как возведение в степень с показателем из $\log_2 s$ битов — это стоило бы около половины сэкономленного; поскольку $\beta^{(s-1)/2} = N_{\mathbb{F}_{q^{k/2}}/\mathbb{F}_q}(\beta)^{(q-1)/2}$, он стоит $k/2 - 1$ Фробениусов и $k/2 - 1$ умножений в $\mathbb{F}_{q^{k/2}}$ с последующим символом Якоби в $\mathbb{F}_q$, стоимость которого много меньше одного умножения в $\mathbb{F}_{q^k}$. (Проверено в разделе 9.)

5. Обращение Миллера с двумя неизвестными

Этот раздел содержит собственно результат: полиномиальную процедуру, которая по сырому значению Тейта–Миллера возвращает оба его аргумента. Это [6, Alg. 4.1], обращающий $h_{d,A}$ при известном A , с двумя изменениями: ориентация — Тейта, а не Ате, так что норма даёт ζ^d , а не ζ^2 (предложение 3.1 против [6, ур. (4.3)]), и корень степени d единствен (лемма 3.5); а его шаг 3, $\xi(Q) = \xi(A) \pm u$, заменён проекцией леммы 4.1. Шаги 1–2 и 5–8 ниже — его.

Предложение 5.1. Алгоритм 5.1 корректен и завершается за $O((k \log q)^3)$ битовых операций.

Доказательство. Если $w = h_{d,A_0}(Q_0)$ для некоторой пары $(A_0, Q_0) \in G_1 \times G_0$, то по предложению 3.1 $u = (\xi(Q_0) - \xi(A_0))^d$, откуда $\zeta = \xi(Q_0) - \xi(A_0)$ (с точностью до знака случая (ii), который перебирается), и лемма 4.1 даёт $x_A = \xi(A_0)$, $x_Q = \xi(Q_0)$; шаги 5–7 тогда порождают $A = \pm A_0$, $Q = \pm Q_0$ с неизвестными знаками. По (5) и доказательству предложения 3.1 четыре сырых значения суть $h_{d,A_0}(Q_0) = w$, $h_{d,-A_0}(-Q_0) = -w$, $h_{d,A_0}(-Q_0) = w^s$ и $h_{d,-A_0}(Q_0) = -w^s$ (при нечётном d), так что шаг 8 распознаёт знаки и возвращает пару со значением Миллера равно w . Обратно, если алгоритм возвращает пару, то $A \in E(\mathbb{F}_q)[\ell] = G_1$ по шагам 5 и 7, $Q \in E[\ell] \cap \ker(\text{Fr}_q^{k/2} + 1) = G_0$ по шагам 6–7, замечанию 4.4 и (1), а её значение Миллера равно w по шагу 8. Без шага 8 алгоритм мог бы вернуть допустимую пару для w , вовсе не являющегося значением Миллера. Для оценки стоимости считаем умножения в $\mathbb{F}_{q^k}$, каждое по $O((k \log q)^2)$ битовых операций при школьной арифметике, как в [6, Thm. 4.2]; умножение в $\mathbb{F}_{q^{k/2}}$ или $\mathbb{F}_q$ стоит не больше, а показатель $d^{-1} \bmod (s-1)$, константы λ , $(\lambda-1)^{-1}$ и базис леммы 4.1 вычисляются один раз для кривой. По шагам:

1. $w^{s+1} = w^s \cdot w$: одна степень Фробениуса и одно умножение, $O(k \log q)$ умножений, либо $O(1)$, если $\mathbb{F}_{q^k}$ задано как квадратичное расширение $\mathbb{F}_{q^{k/2}}$, в котором $w \mapsto w^s$ — сопряжение.
2. Одно возведение в степень в $\mathbb{F}_{q^{k/2}}$ с показателем меньше s : $O(k \log q)$ умножений.
3. ζ^{q^m} — степень Фробениуса ($O(k \log q)$ умножений, либо $O(k^2)$ умножений в $\mathbb{F}_q$ с предвычисленной матрицей), затем одно умножение; проверка $x_A \in \mathbb{F}_q$ бесплатна в $\mathbb{F}_q$ -базисе поля $\mathbb{F}_{q^{k/2}}$, содержащем 1.

Алгоритм 5.1 Обращение Миллера, две неизвестные

Вход: $w \in \mathbb{F}_{q^k}^\times$; здесь $d \mid s+1$; константы $\lambda, (\lambda-1)^{-1}$ и базис леммы 4.1, предвычисленные один раз для кривой

Выход: $(A, Q) \in G_1 \times G_0$ с $h_{d,A}(Q) = w$, либо $\perp$

- 1: $u \leftarrow (-1)^d w^{s+1}$
 - 2: $\zeta \leftarrow$ корень степени d из u в $\mathbb{F}_{q^{k/2}}^\times$ ▷ лемма 3.5; $\perp$, если корня нет, оба знака, если их два
 - 3: $x_A \leftarrow L(\zeta)/(\lambda-1)$
 если $x_A^q \neq x_A$, **то вернуть** $\perp$
 - 4: $x_Q \leftarrow \zeta + x_A$ ▷ тогда $L(x_Q) = L(\zeta) + (1-\lambda)x_A = 0$ автоматически
 - 5: $\alpha \leftarrow x_A^3 + a_4 x_A + a_6$
 если α не квадрат в $\mathbb{F}_q$, **то вернуть** $\perp$
 $A \leftarrow (x_A, \sqrt{\alpha})$
 - 6: $\beta \leftarrow x_Q^3 + a_4 x_Q + a_6$
 если $N_{\mathbb{F}_{q^{k/2}}/\mathbb{F}_q}(\beta)^{(q-1)/2} \neq -1$, **то вернуть** $\perp$ ▷ т.е. $\text{Fr}_q^{k/2} Q \neq -Q$, замечание 4.4
 $Q \leftarrow (x_Q, y_Q)$, где $y_Q \in \mathbb{F}_{q^k}, y_Q^2 = \beta$
 - 7: **если** $[\ell]A \neq \mathcal{O}$ **или** $[\ell]Q \neq \mathcal{O}$, **то вернуть** $\perp$
 - 8: $h \leftarrow h_{d,A}(Q)$
 если $w = h$, **то вернуть** (A, Q)
 если $w = -h$, **то вернуть** $(-A, -Q)$
 если $w = h^s$, **то вернуть** $(A, -Q)$
 если $w = -h^s$, **то вернуть** $(-A, Q)$
 - 9: **вернуть** $\perp$
-

4. Одно сложение.
5. Символ Лежандра и квадратный корень в $\mathbb{F}_q$: $O(\log q)$ умножений в $\mathbb{F}_q$.
6. Символ Лежандра в $\mathbb{F}_{q^{k/2}}$ через норму, $k/2 - 1$ степеней Фробениуса и $k/2 - 1$ умножений в $\mathbb{F}_{q^{k/2}}$ и символ Якоби в $\mathbb{F}_q$ (замечание 4.4); один квадратный корень в $\mathbb{F}_{q^k}$, $O(k \log q)$ умножений — на деле квадратный корень в $\mathbb{F}_{q^{k/2}}$: если $\mathbb{F}_{q^k} = \mathbb{F}_{q^{k/2}}(\sqrt{\nu})$ с неквадратом ν поля $\mathbb{F}_{q^{k/2}}$, то элемент β/ν — квадрат в $\mathbb{F}_{q^{k/2}}$ и $\sqrt{\beta} = \sqrt{\nu} \sqrt{\beta/\nu}$.
7. $[\ell]A$ на $E(\mathbb{F}_q)$ и $[\ell]Q$ на $E(\mathbb{F}_{q^k})$: $O(\log \ell) = O(\log q)$ групповых операций каждое, по ограниченному числу умножений на операцию.
8. Один цикл Миллера длины $d \leq s+1$: $O(\log d) = O(k \log q)$ шагов удвоения или сложения по ограниченному числу умножений каждый, и четыре сравнения ценой одной степени Фробениуса.

Каждый шаг — $O(k \log q)$ умножений в $\mathbb{F}_{q^k}$, т.е. $O((k \log q)^3)$ битовых операций, и шаги 1, 2, 6 и 8 достигают этой границы. Квадратные корни детерминированы при предвычислении, предполагаемом в [6], — образующей 2-силовой подгруппы, — и выполняются за ожидаемое время алгоритмом Чиполлы в противном случае. $\square$

Два обстоятельства заслуживают комментария. Во-первых, никакой тест по одному лишь u не является различающим: w^{s+1} есть норма и потому лежит в $\mathbb{F}_{q^{k/2}}$ для *любого* w , а всякий элемент $\mathbb{F}_{q^{k/2}}$ — квадрат в $\mathbb{F}_{q^k}$; поэтому шаг 6 проверяет β в $\mathbb{F}_{q^{k/2}}$, а не в $\mathbb{F}_{q^k}$ — полезное условие в том, что β есть неквадрат в $\mathbb{F}_{q^{k/2}}$, замечание 4.4, — шаг 4 — простое присваивание (как только $x_A \in \mathbb{F}_q$, $L(x_Q) = L(\zeta) + (1-\lambda)x_A = 0$ автоматически), и весь вес несут проверки шагов 3, 6 и 7. На игрушечной кривой из раздела 9 3000 случайных корней степени ℓ из фиксированной цели прошли условия нормы и квадратичности и все были отвергнуты на шаге 3. Во-вторых, процедура возвращает оба аргумента; это не оракул принадлежности, за которым следует поиск. Именно в этом настоящая заметка выходит за пределы [1]: их уравнение (8) есть в точности (3) с переставленными

ролями A и Q , а последующая редукция использует минимальный многочлен известного $\xi(Q)$, которого здесь нет.

6. От обращения Миллера к GPI

Пусть e — произвольное невырожденное билинейное спаривание на $G_1 \times G_0$ или на $G_0 \times G_1$ со значениями в μ_ℓ — приведённое спаривание Тейта t при любом порядке аргументов либо спаривание Сато, — и пусть $z \in \mu_\ell \setminus \{1\}$ — цель GPI для e .

Сырое значение Тейта–Миллера v с $v^{(q^k-1)/\ell} = t(A, Q)$ определяется приведённым значением лишь с точностью до элемента ядра отображения $x \mapsto x^{(q^k-1)/\ell}$ — подгруппы порядка $(q^k-1)/\ell = (s-1)\nu$, где $\nu := (s+1)/\ell$. Это слишком много для перебора, и не это нужно алгоритму 5.1: ему нужно ζ , а предложение 6.2 ниже показывает, что когда v пробегает этот смежный класс, ζ пробегает всё $\mathbb{F}_{q^{k/2}}^\times$, т.е. цель никак не ограничивает ζ . Алгоритм GPI, стало быть, проходит непосредственно по парам абсцисс $(x_A, x_Q) \in \mathbb{F}_q \times W$ (раздел 8) или, эквивалентно, но медленнее, по $\zeta \in \mathbb{F}_{q^{k/2}}^\times$, декодируемым шагами 3–4 алгоритма 5.1 (замечание 8.1); в обоих случаях каждая пара проверяется на совпадение с z , а корень степени d из шага 2 не нужен никогда.

Существенно для дальнейшего то, что ни один из двух циклов не вычисляет спаривания до своей финальной проверки: e участвует лишь в финальной проверке и лишь через вопрос, верно ли $e(A, Q) \in \{z, z^{-1}\}$. Следовательно:

- алгоритм решает GPI для того спаривания e , какое вычисляется в финальной проверке, и предложение 7.1 дословно применимо ко всякому такому e , ибо его подсчёт использует лишь билинейность и невырожденность;
- в частности, при $e(A, Q) := h_{s,-Q}(A)$ — это $h_{q^{k/2},-A}(Q)$ в буквах Сато, условие на выходе [7, Alg. 6.1] — алгоритм решает задачу GPI Сато *непосредственно*. По лемме 3.3 это равно $t(Q, A)^{1/2}$, билинейно и невырожденно, так что финальная проверка может быть эквивалентно записана как $t(Q, A) \in \{z^2, z^{-2}\}$, что дешевле цикла Миллера длины s ; равным образом цель с циклом q , $h_{q,-Q}(A)$, из [7, Alg. 6.6] равна $t(Q, A)^{1/(kq^{k/2-1})}$ по замечанию 3.4 и проверяется как $t(Q, A) \in \{z^{\pm kq^{k-1}}\}$;
- никакое соотношение между двумя разными спариваниями никогда не вычисляется, и ни одно из них не потребовало бы дискретного логарифма, если бы вычислялось. Например, постоянная κ' с $t(Q, A) = t(A, Q)^{\kappa'}$ имеет замкнутую формулу

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

вытекающую из выражения Фрея–Рюка спаривания Тейта через спаривание Вейля (лемма 6.1); на игрушечной кривой раздела 9 она равна 15. Метод её не использует, и никакой дискретный логарифм нигде в заметке не появляется.

Лемма 6.1. Пусть e_ℓ — спаривание Вейля, заданное формулой Миллера $e_\ell(A, Q) = (-1)^\ell h_{\ell,A}(Q)/h_{\ell,Q}(A)$, а c, h — как в (13), $c \rho := kh/(q-1) \bmod \ell$. Тогда для $A \in G_1$, $Q \in G_0$

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

откуда (13). Невырожденность $t(Q, A)$ есть $\rho \neq 0$, т.е. $\ell \nmid kh$: здесь $\ell \nmid k$, ибо $k = \text{ord}_\ell(q)$ делит $\ell-1$, и $\ell \nmid h$, ибо $\ell \parallel \#E(\mathbb{F}_q)$. Невырожденность $t(A, Q)$ есть $\rho \neq c$ — в точности отличие от нуля знаменателя $kh - c(q-1) = (q-1)(\rho - c)$ в (13).

Доказательство. Тождество $t(P, R) = e_\ell(P, \sigma S - S)$, где $[\ell]S = R$ и $\sigma = \text{Fr}_q^k$, есть форма Лихтенбаума спаривания Тейта [2]; оно классично, и здесь вычисляются лишь показатели. Поскольку $\pi^k - 1$ аннулирует $E[\ell]$, оно раскладывается как $\ell\phi$ в $\text{End}(E)$, так что $\sigma S - S = \phi(R)$,

а ϕ действует на двух собственных прямых π в модуле Тейта $T_\ell E$ как $(\alpha^k - 1)/\ell$ и $(\beta^k - 1)/\ell$, где $\alpha \equiv 1, \beta \equiv q \pmod{\ell}$ — собственные значения. Запишем $\alpha = 1 + \ell a, \beta = q + \ell b$; тогда $\alpha + \beta = t = q + 1 - \ell h$ даёт $a + b = -h$, а $\alpha\beta = q$ даёт $b \equiv -qa$, так что $a \equiv h/(q - 1)$ и $(\alpha^k - 1)/\ell \equiv ka, (\beta^k - 1)/\ell \equiv c + kq^{k-1}b \equiv c - ka \pmod{\ell}$. Итак, $\phi(Q) = [c - \rho]Q$ при $Q \in G_0$ и $\phi(A) = [\rho]A$ при $A \in G_1$, что даёт $t(A, Q) = e_\ell(A, Q)^{c-\rho}$ и $t(Q, A) = e_\ell(Q, A)^\rho = e_\ell(A, Q)^{-\rho}$ по антисимметрии. $\square$

Предложение 6.2 (Независимость значения спаривания и нормы). *Поскольку $\gcd(\ell, s - 1) = 1$, отображение*

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

есть сюръективный гомоморфизм с ядром порядка $\nu = (s + 1)/\ell$. Стало быть, приведённое значение спаривания и норма сырого значения Миллера — независимые координаты: фиксация первой оставляет вторую равномерно распределённой на $\mathbb{F}_{q^{k/2}}^\times$, и никакая процедура, читающая v лишь через v^{s+1} , — в частности, никакая, построенная на предложении 3.1, — не получает никакой информации о цели.

Доказательство. $\mathbb{F}_{q^k}^\times$ циклическа порядка $(s - 1)(s + 1)$. Ядро состоит из ν порядка, делящего $\gcd((s - 1)(s + 1)/\ell, s + 1) = \nu \gcd(s - 1, \ell) = \nu$, так что образ имеет порядок $(q^k - 1)/\nu = \ell(s - 1) = |\mu_\ell \times \mathbb{F}_{q^{k/2}}^\times|$. $\square$

Это содержание предложения 7.1 ниже, сформулированное раз и навсегда: нормовый путь отбрасывает цель целиком, а остаётся поиск по парам абсцисс с финальной проверкой спаривания. (Проверено на игрушечной кривой раздела 9: образ имеет предсказанный порядок $\ell(s - 1)$.)

7. Плотность множества решений

Предложение 7.1. *Пусть $e \in \{4, 6\}$, $k > 2$, d нечётно и $d \mid s + 1$, и зафиксировано $z \in \mu_\ell \setminus \{1\}$. Когда v пробегает $\{v : v^{(q^k-1)/\ell} = z\}$, величина $\zeta = ((-1)^d v^{s+1})^{1/d}$ пробегает всё $\mathbb{F}_{q^{k/2}}^\times$, каждое значение одинаковое число раз (предложение 6.2 и лемма 3.5). Пусть e — невырожденное билинейное спаривание на $G_1 \times G_0$ или $G_0 \times G_1$ со значениями в μ_ℓ . Среди $s - 1$ значений ζ ровно $(\ell - 1)/2$ декодируются шагами 3–7 алгоритма 5.1 в пару (A, Q) с $e(A, Q) = z^{\pm 1}$. Следовательно, ожидаемое число кандидатов, подлежащих рассмотрению, равно*

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

Доказательство. Первое утверждение — это предложение 6.2 (норма равномерна на $\mathbb{F}_{q^{k/2}}^\times$ над слоем z) вместе с биективностью $\zeta \mapsto \zeta^d$ на $\mathbb{F}_{q^{k/2}}^\times$ (лемма 3.5, d нечётно). Для второго: по лемме 4.1 отображение $(\xi(A), \xi(Q)) \mapsto \xi(Q) - \xi(A)$ инъективно на $\mathbb{F}_q \times W$. Пар $(A, Q) \in (G_1 \setminus \{\mathcal{O}\}) \times (G_0 \setminus \{\mathcal{O}\})$ с $e(A, Q) \in \{z, z^{-1}\}$ ровно $2(\ell - 1)$ по билинейности и невырожденности (для каждого A по одному Q на каждое из двух значений); они переставляются орбитами размера 4 отображением $(A, Q) \mapsto (\pm A, \pm Q)$, сохраняющим обе абсциссы, внутри которых e принимает каждое из двух значений дважды, и потому дают $(\ell - 1)/2$ различных значений ζ . $\square$

Все успешные ζ лежат в подпространстве $\mathbb{F}_q \oplus W$ размерности $1 + k/e$, так что алгоритм раздела 8 проходит по этому подпространству ($q^{1+k/e}$ элементов, 2^{761} для BN254), а не по $\mathbb{F}_{q^{k/2}}^\times$. Число (14) относится ко второму; для первого в естественном блочном порядке (x_A снаружи, x_Q внутри) работа составляет $q^{k/e}/2$ кандидатов в первом допустимом блоке, половина из них дорогих при $e = 6$ и все при $e = 4$ (замечание 4.4), каково бы ни было ℓ (разделы 8 и 9).

8. Полный алгоритм

По лемме 4.1 значения ζ , декодируемые шагами 3–4 алгоритма 5.1, суть в точности $\zeta = x_Q - x_A$ с $(x_A, x_Q) \in \mathbb{F}_q \times W$, а по предложению 6.2 цель не ограничивает ζ . Поэтому алгоритм GPI проходит по парам (x_A, x_Q) непосредственно; норма и проекция L не вычисляются вовсе. Анализ разделов 4–7 участвует лишь тем, что он доказывает: что это и есть пространство поиска и что ничто на нормовом пути не может его сжать (раздел 10 перечисляет редукции и то, что обосновывает каждую).

Алгоритм 8.1 GPI, цикл длины ℓ

Вход: q ; обыкновенная $E : Y^2 = X^3 + a_4X + a_6$ над $\mathbb{F}_q$; нечётное простое $\ell \parallel \#E(\mathbb{F}_q)$ с чётной степенью вложения $k > 2$; чётная степень скручивания $e \geq 4$ с $e \mid k$; невырожденное билинейное спаривание e на $G_1 \times G_0$, напр. $t(A, Q)$, $t(Q, A)$ или спаривание Сато $h_{s,-Q}(A) = t(Q, A)^{1/2}$; цель $z \in \mu_\ell \setminus \{1\}$.

Выход: $(A, Q) \in G_1 \times G_0$ с $e(A, Q) = z$, либо $\perp$.

1: **Предвычисление** (не зависит от z):

2: $s \leftarrow q^{k/2}$; $m \leftarrow k/e$

3: выбрать $Q_0 \in G_0 \setminus \{\mathcal{O}\}$; $W \leftarrow \xi(Q_0) \mathbb{F}_{q^m}$ с $\mathbb{F}_q$ -базисом $\xi(Q_0) \cdot \{1, \gamma, \dots, \gamma^{m-1}\}$, где γ порождает $\mathbb{F}_{q^m}$ над $\mathbb{F}_q$

4: **Основной цикл:**

5: **для** $x_A \in \mathbb{F}_q$ **выполнять**

6: $\alpha \leftarrow x_A^3 + a_4x_A + a_6$

7: **если** α — квадрат в $\mathbb{F}_q$ **то**

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

9: **если** $[\ell]A = \mathcal{O}$ **то**

10: **для** $x_Q \in W$ **выполнять**

11: $\beta \leftarrow x_Q^3 + a_4x_Q + a_6$

12: **если** $N_{\mathbb{F}_{q^{k/2}}/\mathbb{F}_q}(\beta)^{(q-1)/2} = -1$ **то** ▷ т.е. $\text{Fr}_q^{k/2}Q = -Q$, замечание 4.4

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

14: **если** $[\ell]Q = \mathcal{O}$ **то**

15: $\chi \leftarrow e(A, Q)$

16: **если** $\chi = z$ **то**

17: **вернуть** (A, Q)

18: **если** $\chi = z^{-1}$ **то**

19: **вернуть** $(-A, Q)$

20: **вернуть** $\perp$

Спаривание e вычисляется только в строке 15, а цель z участвует лишь в строках 15–19. Строка 18 использует $e(-A, Q) = e(A, Q)^{-1}$, так что одна удачная пара даёт ответ не более чем после двух выборов знака; это учтено в подсчёте $(\ell - 1)/2$ предложения 7.1. У каждой абсциссы из G_1 ровно одна абсцисса-партнёр в G_0 , так что цикл останавливается внутри блока первого x_A , прошедшего строки 7 и 9, просмотрев около половины W ; для этих ожиданий оба цикла берутся в равномерно случайном порядке, как в разделе 9 (записанный выше фиксированный порядок всегда встречает один и тот же первый x_A). Ожидаемая работа — $(q - n)/(n + 1)$ отброшенных x_A , $n = (\ell - 1)/2$, каждое ценой символа Лежандра в $\mathbb{F}_q$ и, при $h > 1$, для прошедшей его половины, одного $[\ell]A$ (при $h = 1$ ни одно отброшенное x_A не проходит символа), а затем $q^{k/e}/2$ кандидатов x_Q , половина из них дорогих при $e = 6$ и все при $e = 4$ (замечание 4.4).

Связь с алгоритмом 5.1. Алгоритм 5.1 не вызывается алгоритмом 8.1, и это намеренно. Его шаги 1–4 (норма, корень степени d , проекция) декодируют кандидат сырого значения w в пару абсцисс, а предложение 6.2 показывает, что, когда w пробегает слой над z , они выдают каждую пару из $\mathbb{F}_q \times W$ одинаково часто: выполнять их значило бы проходить $\mathbb{F}_q \times W$ в обход через $\mathbb{F}_{q^{k/2}}^\times$, стоимость чего даёт замечание 8.1. Алгоритм 8.1 проходит пары непосредственно и сохраняет вторую половину алгоритма 5.1 строка в строку: строки 6–8 и 11–13 — его шаги 5 и 6 (квадратные корни и проверки Лежандра), строки 9 и 14 — его шаг 7 (проверки порядка), а строки 15–19 заменяют его шаг 8 — сравнение сырого значения $h_{d,A}(Q)$ с w с точностью до четырёх знаков — сравнением приведённого значения $e(A, Q)$ с $z^{\pm 1}$. Вклад алгоритма 5.1, таким образом, — не подпрограмма, а теорема: что $\mathbb{F}_q \times W$ есть пространство поиска и что никакое декодирование, построенное на норме, не может его сжать.

Замечание 8.1 (Цикл по $\mathbb{F}_{q^{k/2}}^\times$). Можно вместо этого проходить по $\zeta \in \mathbb{F}_{q^{k/2}}^\times$ — скажем, $\zeta \leftarrow g\zeta$ для элемента g большого порядка, который, в отличие от образующей, не требует факторизации $s - 1$, с перезапуском с нового ζ_0 по исчерпанию смежного класса $\zeta_0 \langle g \rangle$, либо просто выбирая ζ наугад, — и декодировать каждое ζ шагами 3–4 алгоритма 5.1, а затем действовать как выше; ζ^{q^m} обновляется одним умножением за шаг, а проверка $x_A \in \mathbb{F}_q$ бесплатна в базисе, содержащем 1. Этот цикл посещает $q^{k/2-1-k/e}$ элементов $\mathbb{F}_{q^{k/2}}$ на каждую пару (x_A, x_Q) , которую в итоге декодирует, ценой нескольких умножений в $\mathbb{F}_{q^{k/2}}$ каждый; его ожидаемая стоимость — $\frac{2(s-1)}{\ell-1}$ таких шагов, около $2^{1271}M$ на BN254 и $2^{2032}M$ на BLS12-381 в единице раздела 10, целиком потраченных на поиск пар, которые прямой цикл выше перечисляет даром. Он доминирует и приводится лишь потому, что в этой форме появляется декодирование алгоритма 5.1.

9. Экспериментальная проверка

Все утверждения проверены в PARI/GP 2.15.4 (ядро GMP 6.3.0, 64 бита) под Ubuntu 24.04.4 LTS, Linux 6.18, на одноядерной облачной виртуальной машине, сообщаемой об Intel Xeon с частотой 2,10 ГГц и 3,9 ГиБ ОЗУ; поле $\mathbb{F}_{q^k}$ представлено одним неприводимым многочленом степени 12 (`ffgen` в PARI), а не башней. Кривая — кривая BN с параметром $u = 1$ ($u = -1$ даёт меньшую, $q = 19, \ell = 13$, всего с шестью абсциссами в каждой группе — слишком мало, чтобы подсчёты ниже что-либо значили): $q = 103, \ell = 97, E : Y^2 = X^3 + 5, \#E(\mathbb{F}_q) = \ell, \mathbb{F}_{q^k} \simeq \mathbb{F}_{103^{12}}$ размером 80 бит; здесь $e = 6, m = 2$, а λ оказалось порядка 3. Знак $(-1)^d = -1$ предложения 3.1 подтверждён с функцией Миллера, нормированной в $\mathcal{O}$; `elltatepairing` из PARI, не нормированной таким образом, сырая постоянная есть другой элемент $\mathbb{F}_q^\times$, не зависящий от (A, Q) , а приведённое спаривание не затрагивается, ибо $(q - 1) \mid (q^k - 1)/\ell$.

проверка	результат
$\xi(Q) \in \mathbb{F}_{q^{k/2}}$ для $Q \in G_0$	да
$\lambda = \xi(Q)^{q^m} / \xi(Q)$ не зависит от Q , $\text{ord}(\lambda) = 3$	да
$L(u) = 0$ для всех $u \in W$; $\mathbb{F}_q \cap W = \{0\}$ (все $a \in \mathbb{F}_q^\times$)	да
Предл. 3.1 с нормированным Миллером: $v^{s+1} = -\zeta^\ell$	да
Алг. 5.1 восстанавливает $(\xi(A), \xi(Q))$ точно, 30 случайных пар	30/30
3000 случайных корней степени ℓ из цели приняты	0
Предл. 7.1: 48 ² пар абсцисс, 96 пар с $t = z$, 48 значений ζ	да
Зам. 3.2: (6) точно при $n = 5, 11, 13$; (7); $h_{s,A}(Q)^{s+1} = 1$; $h_{2\ell-1,A}(Q)^{s+1} = \zeta^{2\ell-2}$;	да
(8) при $T = 6$	
Лемма 3.3: (9) в обеих ориентациях; (10); $-h_{s,A}(Q) = t(A, Q)^{48}$, $48 \equiv -1/2$;	да
$\text{ord}(h_{s,A}(Q)) = 194 = 2\ell$	
$h_{s,Q}(A)$ билинейно по Q и по A без финального возведения в степень; $h_{s,-Q}(A) = t(Q, A)^{1/2}$	да
Лемма 6.1: $e_\ell \in \mu_\ell$; $t(A, Q) = e_\ell^{c-\rho}$, $t(Q, A) = e_\ell^{-\rho}$ ($c \equiv 10$, $\rho \equiv 80 \pmod{\ell}$); (13)	да
даёт 15, и $t(Q, A) = t(A, Q)^{15}$	
$\gcd(2\ell - 2, s - 1) = 48$ на игрушечной кривой, $= 48u$ на BN254	да
Четыре значения $w, -w, w^s, -w^s$ из предл. 5.1	да
Предл. 6.2: образ $v \mapsto (v^{(q^k-1)/\ell}, v^{s+1})$ порядка $\ell(s-1)$	да
Зам. 3.2: $h_{T,Q}(A)^{s+1} = (\xi(A) - \xi(Q))^{-h\ell}$; $h_{q,Q}(A)^{s+1} = 1$; $h_{3\ell,A}(Q)^{s+1} = -\zeta^{3\ell}$	да
при $3\ell \nmid s+1$	
Зам. 3.4: $h_{q,Q}(A)^\ell = 1$; $h_{q,Q}(A) = t(Q, A)^{49}$, $49 \equiv -1/(kq^{k/2-1})$; $h_{q,-Q}(A) = t(Q, A)^{48}$	да
Зам. 4.4: β — неквадрат в $\mathbb{F}_{q^{k/2}} \iff \text{Fr}_q^{k/2}Q = -Q$ на 2000 случайных $x_Q \in W$	да
(1001 неквадрат, $e = 6$); β — неквадрат для 30 точек G_0	
$1/\pi_z = (s-1)/48 = 2,49 \cdot 10^{10}$ против предсказанного $2s/\ell = 2,46 \cdot 10^{10}$	да

Полное обращение билинейного спаривания. Алгоритм раздела 8 был выполнен до конца: кандидаты — пары $(a, x_Q) \in \mathbb{F}_q \times W$ с $W = \xi(Q_0)\mathbb{F}_{q^2}$, т.е. $\zeta = x_Q - a$, всего $q^3 = 1\,092\,727$ кандидатов, для которых $x_A = a$ и x_Q читаются непосредственно и никакой проекции не требуется. Целью было $z = t(A^*, Q^*)$ для равномерно случайной пары $(A^*, Q^*) \in G_1 \times G_0$, затем забытой; финальной проверкой было $t(A, Q) \in \{z, z^{-1}\}$ — полностью приведённое, полностью билинейное спаривание Тейта. Чтобы подсчёты имели смысл, a перебиралось в равномерно случайном порядке на $\mathbb{F}_q$ и для каждого a — x_Q в равномерно случайном порядке на W ; время по настенным часам — `getwalltime`.

Всякая абсцисса a из G_1 допускает ровно одну абсциссу в G_0 , дополняющую её до решения, так что прогон останавливается внутри блока *первого* встреченного допустимого a : он пропускает недопустимые a (каждое ценой одного символа Лежандра, считаемое как пропущенный блок из q^2), затем просматривает W в поисках 48 абсцисс G_0 , вычисляя по одному спариванию Тейта на каждой, пока не встретит нужную. Фактически прогон фиксирует A на первой допустимой абсциссе и ищет в W его партнёра. В этом блочном порядке ожидаемая работа — это $(q - n)/(n + 1)$ пропущенных блоков, $n = (\ell - 1)/2$, каждый ценой одного символа Лежандра в $\mathbb{F}_q$ и, при $h > 1$, для той половины из них, что его проходит, одного скалярного умножения $[\ell]A$, а затем $q^{k/e}/2$ кандидатов, половина из них дорогих, в первом допустимом блоке (1,1 блока и 5 304 кандидата на игрушечной кривой); для равномерного порядка на $\mathbb{F}_q \times W$ соответствующее число было бы $2q^{1+k/e}/\ell$ по подсчёту предложения 7.1, совпадающее с ним лишь с точностью до константы, и лишь потому, что $\ell \approx q$ на кривой BN. На 12 независимых целях: 12 успехов, возвращённая пара лежит в $G_1 \times G_0$ с $t(A, Q) = z$ в точности, 11 различных значений $\xi(A)$ (ни разу не исходная пара); пропущено от 0 до 4 недопустимых a (в среднем 1,3); позиция нужного x_Q при просмотре W

между 1 022 и 10 350 из 10 609 (в среднем 5 896), что согласуется с равномерностью; вычислено от 3 до 48 спариваний Тейта; время по настенным часам от 0,37 с до 1,92 с, определяемое в основном квадратными корнями в $\mathbb{F}_{q^k}$ и скалярными умножениями на ℓ при просмотре, а не спариваниями. Приведённые здесь прогоны предшествуют замечанию 4.4 и проверяли $\text{Fr}_q^{k/2}Q = -Q$ после извлечения корня; с проверкой Лежандра в начале, вычисляемой через норму, примерно половина квадратных корней и скалярных умножений экономится ценой $k/2$ умножений. Тот же прогон с финальной проверкой $t(Q, A) \in \{z_S^2, z_S^{-2}\}$, $z_S = h_{s, -Q^*}(A^*) = t(Q^*, A^*)^{1/2}$ — собственно спариванием Сато — преуспевает точно так же. Итак, полная задача GPI для спаривания с финальным возведением в степень решена от начала до конца, с теми числами, которые предсказывает раздел 7.

Ещё две кривые. У игрушечной кривой выше $h = 1$, так что строка 9 раздела 8 ($[\ell]A = \mathcal{O}$) никогда не задействуется, и только $e = 6$. Те же проверки проведены на двух кривых с кофактором: $q = 53$, $E : Y^2 = X^3 + X$, $\ell = 17$, $\#E(\mathbb{F}_q) = 68$, $h = 4$, $k = 8$, $e = 4$, $m = 2$ ($j = 1728$, кватрическое скручивание); и $q = 103$, $E : Y^2 = X^3 + 4$, $\ell = 37$, $\#E(\mathbb{F}_q) = 111$, $h = 3$, $k = 12$, $e = 6$, $m = 2$. На обеих: λ имеет порядок ровно $e/2$; $1, \omega, \dots, \omega^{e/2-1}$ — собственные векторы $u \mapsto u^{q^m}$ с собственными значениями λ^j , и $\ker L = W$ (лемма 4.1); предложение 3.1 выполняется со знаком -1 ; алгоритм 5.1 восстанавливает $(\xi(A), \xi(Q))$ на 30/30 случайных парах; замкнутые формы леммы 3.3 и замечания 3.4 верны, с $\text{ord}(h_{s,A}(Q)) = 2\ell$; κ' из (13) равно 3 и 8 соответственно, и $t(Q, A) = t(A, Q)^{\kappa'}$; образ отображения из предложения 6.2 имеет порядок $\ell(s-1)$; и алгоритм раздела 8 в случайном порядке преуспел на 5/5 случайных целях на каждой кривой, причём возвращённая пара проверена по z . Строка 9 теперь задействована: на кривой $e = 4$ из x_A , прошедших символ Лежандра, 4/5, 2/3, 12/13, 6/7 и 1/2 отброшены по $[\ell]A \neq \mathcal{O}$ в пяти прогонах ($|\xi(G_1)| = 8$ среди 33 абсцисс $E(\mathbb{F}_q)$); на кривой $e = 6$ — 0/1, 2/3, 1/2, 0/1 и 3/4 (18 среди 55).

Кривая $e = 4$ обнаруживает структурный факт, скрытый примерами $e = 6$: у 400/400 значений $x_Q \in W$ с $\beta \neq 0$ элемент β оказался неквадратом в $\mathbb{F}_{q^{k/2}}$, против 203/399 на кривой $e = 6$. Это замечание 4.4 в двух его случаях: при $e = 4$ проверка Лежандра пуста и всю фильтрацию выполняет $[\ell]Q = \mathcal{O}$; при $e = 6$ она отбрасывает около половины.

Подсчёт операций. Сравнение по времени не проводится: в этом масштабе время измеряет интерпретатор GP, а две стоимости имеют разные асимптотики по ℓ . В алгоритме раздела 8 каждое x_A стоит одного символа Лежандра в $\mathbb{F}_q$ и, для прошедшей половины, одного квадратного корня в $\mathbb{F}_q$ и одного $[\ell]A$; каждое x_Q стоит одного символа Лежандра в $\mathbb{F}_{q^{k/2}}$, вычисляемого через норму, как в замечании 4.4 ($k/2 - 1$ Фробениусов и $k/2 - 1$ умножений в $\mathbb{F}_{q^{k/2}}$, затем символ Якоби в $\mathbb{F}_q$ стоимостью много меньше $1M$), отбрасывающего примерно половину при $e = 6$ и ничего при $e = 4$ (замечание 4.4), и для уцелевших одного квадратного корня в $\mathbb{F}_{q^k}$ и одного $[\ell]Q$ на $E(\mathbb{F}_{q^k})$ — около 2^{12} умножений в $\mathbb{F}_{q^k}$ на одно x_Q в среднем при $e = 6$ и размерах раздела 10, т.е. примерно четырёх спариваний Тейта, и вдвое больше при $e = 4$. В цикле замечания 8.1 каждое ζ стоит дополнительно одного умножения для обновления ζ^{q^m} , трёх-четырёх для декодирования и бесплатной проверки принадлежности в базисе, содержащем 1, причём вышеперечисленное достигается лишь для доли $q^{1+k/e-k/2}$ значений ζ . Внутренний шаг [7, Alg. 6.1] при нечётном ℓ — поиск корней $g(T) = \gamma$ над $\mathbb{F}_{q^k}$ с $\deg g = (\ell-1)/2$, здесь 48 ($\varphi = g(\xi)$; форма $g(T)^2(T^3 + b) - \gamma^2$ степени 99 есть [7, ур. (6.1)] для чётного ℓ).

10. Сравнение с [7]

Предложение 6.2 делает множитель улучшения явным, слагаемое за слагаемым. В [7, Alg. 6.1] переменная цикла γ пробегает $\gamma_0 \mu_{(s-1)\nu}$, так что γ^ν пробегает смежный класс $z^{-1} \mathbb{F}_{q^{k/2}}^\times$, каждое значение ν раз, с поиском корней степени $(\ell-1)/2$ на каждом шаге. Этот цикл уже есть слепой обход некоторой координаты $\mathbb{F}_{q^{k/2}}^\times$: по [7, Thm. 5.3(ii)–(iii)], в его буквах ($A \in G_0$, P рациональна),

$\varphi(A + P)^\nu h_{s,-A}(P) \in \mathbb{F}_{q^{k/2}}^\times$, так что $\varphi(A + P)^\nu$ есть произведение $h_{s,-A}(P)^{-1} \in \mu_\ell$ и элемента $c_{A,P} \in \mathbb{F}_{q^{k/2}}^\times$ — расщепление $\mu_{\ell(s-1)} \cong \mu_\ell \times \mu_{s-1}$ из предложения 6.2, применённое к $\varphi(A + P)^\nu$ вместо v . Его c — это μ_{s-1} -компонента, а цикл по γ с $\varphi(kR)^\nu = c/z$ фиксирует μ_ℓ -компоненту равной z^{-1} и пробегает другую, не несущую никакой информации о z . Настоящий метод (i) убирает ν -кратную избыточность, делая переменной цикла саму координату, внутри которой корень степени d единствен (лемма 3.5); (ii) убирает поиск корней, ибо декодирование координаты в две абсциссы полиномиально (алгоритм 5.1); (iii) сжимает координату с $\mathbb{F}_{q^{k/2}}^\times$ до $\mathbb{F}_q \oplus W$ благодаря скручиванию (лемма 4.1); и (iv) проверяет принадлежность x_A к $\xi(G_1)$ символом Лежандра, не трогая W , что и есть блочный порядок раздела 8. Четыре множителя суть $\nu \approx s/\ell$, $\tilde{O}(\ell)$, $q^{k/2-1-k/e}$ и около q/ℓ ; их произведение равно $q^{k-k/e}/\ell$ с точностью до констант и логарифмов — отношение первых двух столбцов ниже. Поиск в G_0 по кратным образующей вместо просмотра W сжимает координату ещё раз, до ℓ точек, и это последний столбец. Ничто в этой цепочке не использует z до финальной проверки, и по предложению 6.2 ничто на этом пути и не могло бы.

Что делает нормовый путь, можно, стало быть, сформулировать точно. В ориентации Тейта при $\ell \mid d$ неоднозначность сырого значения Миллера — смежный класс размера $(s-1)\nu$ — уменьшается в ν раз при переходе к норме; декодирование ζ в две абсциссы становится полиномиальным даже при обеих неизвестных (лемма 4.1); а остаточная координата не зависит от цели (предложение 6.2), так что цикл раздела 8 — или доминируемый цикл замечания 8.1 — проходит по ней вслепую.

Сравнивать с [7, Alg. 6.1] следует в одинаковой конвенции, ожидание против ожидания. Для [7, Alg. 6.1] на обыкновенной кривой вероятность успеха на итерацию не превосходит $(\ell-1)/((s-1)\nu)$ [7, Rem. 6.5], а каждая итерация есть поиск корней степени $(\ell-1)/2$ над $\mathbb{F}_{q^k}$; ожидаемая стоимость поэтому не меньше $\frac{(s-1)\nu}{\ell-1} \cdot \tilde{O}(\ell) \approx \tilde{O}((q^k-1)/\ell)$. Для алгоритма раздела 8 ожидаемое число кандидатов равно $q^{k/e}/2$, и каждый стоит в среднем примерно четырёх спариваний при $e = 6$ — дорогая половина около восьми — и примерно восьми при $e = 4$ (раздел 9); для цикла по $\mathbb{F}_{q^{k/2}}^\times$ из замечания 8.1 оно равно $\frac{2(s-1)}{\ell-1}$ шагов по несколько умножений в $\mathbb{F}_{q^{k/2}}$. Чтобы сравнивать сопоставимое, таблица ниже дана в единой единице M : одно умножение в $\mathbb{F}_{q^k}$. И использованные переводы: квадратный корень в $\mathbb{F}_{q^k}$ и скалярное умножение на ℓ на $E(\mathbb{F}_{q^k})$ — каждое $\approx 2^{12}M$ при этих размерах; спаривание Тейта с циклом длины ℓ и $A \in E(\mathbb{F}_q)$, с разреженными прямыми и циклотомическим финальным возведением в степень, $\approx 2^{10}M$; умножение в $\mathbb{F}_{q^{k/2}} \approx 1M$; символ Лежандра из замечания 4.4 $\approx k/2 M$; поиск корней степени d над $\mathbb{F}_{q^k} \approx d \log_2(q^k) M$. Все элементы — ожидания, и они иллюстративны, а не измерены: каждый из приведённых переводов точен лишь с точностью до небольшого множителя, и показатели наследуют этот люфт. Устойчиво отношение между столбцами, $q^{k-k/e}/\ell$ с точностью до констант и логарифмов, а не абсолютные значения.

кривая	[7, Alg. 6.1]	эта заметка (раздел 8)	замечание 8.1	полный перебор
BN254 (alt_bn128)	$2^{2800} M$	$2^{518} M$	$2^{1271} M$	$2^{263} M$
BLS12-381	$2^{4325} M$	$2^{772} M$	$2^{2032} M$	$2^{264} M$

Две оговорки. Оценка вероятности у Сато — верхняя, так что его истинная ожидаемая стоимость может быть больше, что лишь увеличивает разрыв. И сравнение законно потому, что при $e := h_{s,-Q}(A)$ в строке 15 алгоритм решает ту самую задачу из [7, Alg. 6.1] — как раздел 9 демонстрирует на игрушечной кривой, — а не потому, что одна процедура заменяет другую.

11. Ограничения

1. Метод требует чётной степени скручивания $e \geq 4$ (замечание 4.2) и $k > 2$ (замечание 4.3). Поэтому он неприменим к суперсингулярным кривым, на которых [7] получает постоянное число итераций; он применим в точности к тому режиму, который [7] определяет как безнадёжный.

2. Прямой поиск в G_0 при фиксированном A стоит $\ell/2$ вычислений спаривания в ожидании, около $2^{263}M$ и $2^{264}M$ на двух кривых: меньше, чем алгоритм раздела 8, примерно в $4q^{k/e}/\ell$, т.е. в 2^{256} и 2^{509} раз; дискретный логарифм в μ_ℓ ($\approx 2^{100}$ и $\approx 2^{126}$ по специальному TNFS) ещё дешевле. Сато делает то же наблюдение о собственном алгоритме. Улучшение сокращает разрыв, не закрывая его.
3. Использование $\xi(G_0) \subset \mathbb{F}_{q^{k/2}}$ через след и норму принадлежит [1], чья редукция к показателю $q - 1$ сильнее всего здесь полученного в случае фиксированного аргумента. Заявляемая в этом пункте новизна — то, что механизм переживает переход к двум неизвестным аргументам; остальные вклады перечислены во введении.
4. Цикл использует z лишь в финальной проверке, и предложение 6.2 объясняет почему: ничто, построенное на норме, не может поступать иначе. Соотношение (8) для настоящего цикла Ate $T = t - 1$ тоже не выход, ибо оно сводится к предложению 3.1 с $d = h\ell$ (замечание 3.2). Собственное разложение Сато не исключение: постоянная $c \in \mathbb{F}_{q^{k/2}}^\times$ из [7, Thm. 5.5] есть μ_{s-1} -компонента $\varphi(A + P)^\nu$ в том же расщеплении по китайской теореме об остатках (раздел 10) — не v , норма которого при его длине цикла равна 1 (замечание 3.2); попутно $(\varphi(A + P)^\nu)^{s+1} = c_{A,P}^2$. Она не зависит от z по той же причине, следствием которой является $\mu_\ell \cap \mathbb{F}_{q^{k/2}}^\times = \{1\}$ — факт, на который ссылается его доказательство теоремы 5.5(iii); так что его цикл по c тоже ничего не получает от z . Мне не известно разложения сырого значения, обходящего эту координату; существует ли оно — вопрос, остающийся открытым.

Список литературы

- [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.