

广义配对求逆的一种更快方法

Lael Cellier

lael.cellier@laposte.net

2026年9月15日

摘要

Satoh 最近给出了广义配对求逆问题 (GPI) 的一个算法, 它利用 Miller 函数的结构, 而非穷举搜索或固定参数预言机。在常曲线上, 其期望代价约为 $(q^k - 1)/\ell^2$ 次对次数为 $\Omega(\ell)$ 的求根子程序的调用, 即 $\tilde{O}((q^k - 1)/\ell)$ 次运算。本文对同一问题给出另一种方法, 适用于嵌入次数为偶数 $k > 2$ 且具有偶数次 $e \geq 4$ 扭曲的常曲线, 其期望代价为 $q^{k/e}/2$ 个各需数次配对的候选: 以 $\mathbb{F}_{q^k}$ 中的乘法计, 相对 Satoh 算法的改进因子为 $q^{k-k/e}/\ell$ (忽略常数与对数)。分析使用长度为 ℓ 的倍数的 Miller 循环, 如 Tate 配对; 而 Satoh 的循环长度为 $q^{k/2} \equiv -1 \pmod{\ell}$ 。目标配对仅通过一次最终的成员检验出现, 故算法直接解决 Satoh 配对的 GPI, 无需在配对之间转换, 也不在任何地方使用离散对数。约化配对值与原始 Miller 值的范数是独立的坐标——这是中国剩余定理的事实, 因为 $\gcd(\ell, q^{k/2} - 1) = 1$; 相应地, 本方法是对横坐标对的搜索加一次最终配对检验, 我不作其他声称: 技术核心——在两个参数均未知时对原始 Miller 值的多项式时间求逆——用于确定该搜索空间并表明此路线上无法将其缩小。该测试的输入是最终幂运算之前的原始 Miller 值——与 Satoh 本人的 Miller 求逆算法的输入相同, 没有任何协议会暴露它; 从约化值到它的过渡是 Galbraith、Hess 与 Vercauteren 的幂运算求逆步骤, 第 6–8 节以搜索处理之, 而命题 6.2 表明它无法经由范数抄近路——它将 Satoh 早先关于 Miller 求逆的工作中的范数关系与一个 $\mathbb{F}_q$ -线性投影相结合, 后者分离两个未知的横坐标——它们位于 $\mathbb{F}_{q^{k/2}}$ 中互补的 $\mathbb{F}_q$ -子空间内; 对这一子域结构的利用可追溯至 Akagi 与 Nogami, 但他们的归约要求其中一个参数已知。在 BN254 上期望代价从约 2^{2800} 降至 2^{518} 次 $\mathbb{F}_{q^k}$ 中的乘法, 在 BLS12-381 上从约 2^{4325} 降至 2^{772} 。所有这些数字仍远高于 $\mathbb{F}_{q^k}$ 中指数演算的代价; 此结果是结构性的, 而非密码分析性的。

1 引言

Galbraith、Hess 与 Vercauteren [3] 为双线性配对 $e: G_1 \times G_0 \rightarrow \mu_\ell$ 分离出三个求逆问题: 两个固定参数问题 FAPI-1 与 FAPI-2, 其中一个参数已给定; 以及广义问题 GPI, 其中只给定目标值 z , 任何原像对均可接受。

Satoh [7] 注意到尚无算法利用配对计算的数学结构 (而非在其中一个群中搜索), 并给出了一个: 将第 ℓ 个 Miller 函数写成因子系统, 他得到 Ate 配对的一个分解, 由此通过一个求根步骤装配出 GPI 的解。所得过程 [7, Alg. 6.1] 遍历 $\gamma \in \mu_{\nu(s-1)}$, 其中 $s = q^{k/2}$, $\nu = (s+1)/N$, 每步求一个次数为 $(N-1)/2$ 的函数 φ 的根。在常曲线上, $\nu(s-1) = (q^k - 1)/\ell$, 每步成功概率至多为 $(\ell-1)/((s-1)\nu)$ [7, Rem. 6.5], 故期望代价约为 $(q^k - 1)/\ell^2$ 次 $\ell/2$ 次求根, 即 $\tilde{O}((q^k - 1)/\ell)$ 次运算; Satoh 将此情形描述为“即便对小的 q 值做数值实验也过于低效”。

本文对同一问题给出一种期望代价更低的不同方法。它与 Satoh 的方法一样, 是带最终配对检验的盲目搜索——此处对象为横坐标对; 命题 6.2 说明了为何任何建立在 Miller 值范数之上的方法都只能如此: 约化配对值与该范数是独立的坐标。有两点框架性说明至关重要, 先行陈述。

循环长度。本方法取 $\mathbb{F}_q$ -有理参数 $A \in G_1$ 处的 Miller 函数 $h_{d,A}$, 在迹零参数 $Q \in G_0$ 处求值, 循环长度 d 为 ℓ 的倍数——即 Tate 框架。Satoh 的算法 6.1 产生的量在本文记号下为 $h_{q^{k/2}, -Q}(A)$ (他的字母 A 、 Q 与本文相反: 他的 A 属于 G_0): Miller 函数取在迹零参

数处，循环长度为 $s = q^{k/2}$ 。真正重要的区别不在于取向，而在于循环长度模 ℓ 的剩余类：本文所依赖的范数关系（命题 3.1）在 $d \equiv 0 \pmod{\ell}$ 时给出 $(\xi(Q) - \xi(A))^d$ ，而在 $d \equiv -1 \pmod{\ell}$ 时给出 $(\xi(Q) - \xi(A))^{d-1}$ ，后者在 $d = s$ 时恒等于 1（注 3.2）。因此本方法并不替换 [7, Alg. 6.1] 的内层步骤，我也不作此声称。确实成立的是：目标配对仅通过一次最终的成员检验进入本方法，故可将其取为 Satoh 配对本身（第 6 节）；配对之间的任何转换，特别是任何离散对数，均不在任何地方出现。

新意所在。本方法的核心是一个多项式时间过程：给定原始 Tate–Miller 值 $h_{d,A}(Q)$ ，在 A 与 Q 均未知的情况下恢复 A 与 Q （第 5 节）。它将 Satoh 在固定参数框架中使用的范数关系 [6] 与一个线性投影相结合，后者分离位于 $\mathbb{F}_{q^{k/2}}$ 中互补 $\mathbb{F}_q$ -子空间内的两个未知横坐标（第 4 节）。这一子域结构最早由 Akagi 与 Nogami [1] 利用，他们通过构造已知横坐标的极小多项式，将 FAPI-2 的幂求逆问题归约到指数 $q-1$ ；其构造需要 $\text{Tr}(\xi(Q)^3)$ 与 $N(\xi(Q))$ ，无法移植到 Q 未知的情形。从“一个未知量、极小多项式”到“两个未知量、线性投影”的过渡，是技术上的新意。围绕它，本文补充了配对值与范数的独立性（命题 6.2），它确定了搜索空间并表明此路线上无法缩小它；循环长度 s 与 q 的 Miller 值作为约化 Tate 配对的幂的封闭形式（引理 3.3、注 3.4），使算法可直接以 Satoh 的配对为目标；以及对相对 [7, Alg. 6.1] 改进的四因子核算，每个因子归于上述结果之一（第 10 节）。

顺带指出，GPI 并非没有密码学后果：一个 Groth16 证明 [5] 只要单一的配对乘积方程成立即被接受，而将其第三个元素置为 $\mathcal{O}$ 后，目标值仅由验证密钥与公开输入即可算出，从而任何 GPI 的解都给出对任意命题的伪造。其利害并非抽象。BLS12-381 上的 Groth16 是 Zcash 的 Sapling 屏蔽资金池所用的证明系统，而 BN254 上的 Groth16 是以太坊配对预编译合约原生验证的证明系统，被若干 rollup、跨链桥与混币器用作最终证明层；一次伪造将使攻击者铸造毫无储备支撑的屏蔽币，或从跨链桥提取从未存入的资金——在托管巨额资金的系统中直接盗取资金。第 10 节的代价使此类攻击遥不可及，本文中的任何内容都不改变这一点；但正是这些代价，使得 GPI——而不仅是 FAPI——成为这些系统值得跟踪的量。

2 设定与记号

设 q 为奇素数的幂， $E/\mathbb{F}_q$ 为常椭圆曲线，短 Weierstrass 模型为 $Y^2 = X^3 + a_4X + a_6$ 。设 ℓ 为奇素数， $\ell \parallel \#E(\mathbb{F}_q)$ ——恰好整除，即 $\ell \mid \#E(\mathbb{F}_q)$ 且 $\ell^2 \nmid \#E(\mathbb{F}_q)$ ，从而 $h := \#E(\mathbb{F}_q)/\ell$ 与 ℓ 互素，这是引理 6.1 所需要的——嵌入次数为偶数 $k > 2$ ；由于 $k = \text{ord}_\ell(q)$ 整除 $\ell-1$ ，自动有 $\ell \nmid k$ 。遵循 [7, § 5]，令

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

于是 $G_0 \cong G_1 \cong \mathbb{Z}/\ell\mathbb{Z}$ ， $G_0 \cap G_1 = \{\mathcal{O}\}$ ，且 $E[\ell] = G_1 \oplus G_0$ 。由 $\ell \mid s+1$ ，对 $P \in G_0$ 有 $\text{Fr}_q^{k/2} P = -P$ ；又由 $\ell \nmid s-1$ ， $\text{Fr}_q^{k/2}$ 仅在 G_1 上有特征值 1、在 G_0 上有特征值 -1 ，从而

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

ξ, η 记坐标函数， $\tau := -\xi/\eta$ 记 $\mathcal{O}$ 处的单值化参数， $h_{n,A}$ 记 A 处正规化的第 n 个 Miller 函数，即满足 $\text{div } h_{n,A} = n[A] - [nA] - (n-1)[\mathcal{O}]$ 且关于 τ 有 $\text{lc}_{\mathcal{O}}(h_{n,A}) = 1$ 的函数。

全文中 $A \in G_1$ ， $Q \in G_0$ ， d 为满足

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

的整数；当需要开 d 次根时（引理 3.5），我进一步假设 $d \mid s+1$ ，即 [6, Alg. 4.1] 的第二个条件。原始 Miller 值为 $v := h_{d,A}(Q) \in \mathbb{F}_{q^k}^\times$ ，约化 Tate 配对为 $t(A, Q) := h_{\ell,A}(Q)^{(q^k-1)/\ell} \in \mu_\ell$ ，它在 $G_1 \times G_0$ 上双线性且非退化。

3 范数关系

命题 3.1. 在上述记号下，且仅用到 $\ell \mid d$ ，

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

特别地, 当 $d = \ell$ 时 $v^{s+1} = -(\xi(Q) - \xi(A))^\ell$ 。

证明. 由 $\ell \mid d$ 及 $A \in E[\ell]$, $[d]A = \mathcal{O}$, 故 $\operatorname{div} h_{d,A} = d([A] - [\mathcal{O}])$; 同理 $\operatorname{div} h_{d,-A} = d([-A] - [\mathcal{O}])$ 。因此 $h_{d,A}h_{d,-A}$ 与 $(\xi - \xi(A))^d$ 有相同除子 $d([A] + [-A] - 2[\mathcal{O}])$, 且由 $\xi = \tau^{-2} + O(\tau^{-1})$, 二者在 $\mathcal{O}$ 处首项系数均为 1; 于是

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

其次, $h_{d,A} \circ [-1]$ 与 $h_{d,-A}$ 有相同除子; 对短 Weierstrass 模型有 $\tau \circ [-1] = -\tau$, 又 $\operatorname{ord}_{\mathcal{O}} h_{d,A} = -d$, 故 $\operatorname{lc}_{\mathcal{O}}(h_{d,A} \circ [-1]) = (-1)^d$, 从而

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

最后, $h_{d,A}$ 定义在 $\mathbb{F}_q$ 上且 $\operatorname{Fr}_q^{k/2} Q = -Q$, 故由 (5), $v^s = h_{d,A}(\operatorname{Fr}_q^{k/2} Q) = h_{d,A}(-Q) = (-1)^d h_{d,-A}(Q)$, 且 $v^{s+1} = v \cdot v^s = (-1)^d (h_{d,A} h_{d,-A})(Q)$, 由 (4) 此即 (3)。□

(3) 的右端不含任何 Miller 值。与 [6, Alg. 4.1] 所依赖的分解 $h_{s+1,A} = (\xi - \xi(A)) h_{s,A}$ 相比: 在那里, 因子 $h_{s,A}(Q)$ 被 $(s+1)$ 次幂消去。其精确结构由引理 3.3 给出: $h_{s,A}(Q) = -t(A, Q)^{-1/2}$, 阶恰为 2ℓ 且整除 $s+1$, 其相反数 $-h_{s,A}(Q) = t(A, Q)^{-1/2}$ 属于 μ_ℓ ; 若 Miller 函数取在迹零参数处, 则反而得到 $h_{s,Q}(A) = t(Q, A)^{-1/2} \in \mu_\ell$, 这正是 [4] 在此情形下的结论, 并带有其封闭形式。这正是 Satoh 所描述的 “(最终幂运算前的值) = (简单函数) $\times$ (另一配对)” 现象。关于常数有两点说明。其一, 它是一个已知的符号, 而非需预先计算的量。其二, 不在 $\mathcal{O}$ 处正规化 Miller 函数的实现 (PARI/GP 的 `elltatepairing` 即是一例) 会将其替换为另一常数; 该常数仍与 A, Q 无关这一点, 是在第 9 节的玩具曲线上对 PARI 直线函数正规化方式的经验观察, 届时可从任意一个已知点对读出。

注 3.2 (循环长度而非取向). 对任意循环长度 n , 若 $[n]P \neq \mathcal{O}$, 同样的除子计算精确地、无符号地给出

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

两端在 $\mathcal{O}$ 处的首项系数均为 1; (6) 对两个群中任一群内的 P 均成立。((5) 中的符号为 $(-1)^{\operatorname{ord}_{\mathcal{O}} h_{n,P}}$, 当 $[n]P \neq \mathcal{O}$ 时为 $(-1)^{n-1}$, 当 $\ell \mid n$ 时为 $(-1)^n$; 它只在用 $h_{n,P}$ 在 $-R$ 处求值、而非用 $h_{n,-P}$ 在 R 处求值时才出现。) n 模 ℓ 的三个剩余类是相关的。

若 $n \equiv 0 \pmod{\ell}$, 分母为 1, 范数关系恢复出 $(\xi - \xi(P))^n$: 此即命题 3.1, 且在两种取向下均成立。在 Ate 取向下, $\operatorname{Fr}_q^{k/2}$ 作用于 $h_{n,Q}$ 的系数并将其映为 $h_{n,-Q}$, 不涉及在相反点处求值, 因而没有符号, 故

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

两个范数相同。

若 $n \equiv -1 \pmod{\ell}$, 则 $[n]P = -P$, (6) 变为 $(\xi - \xi(P))^{n-1}$ 。当 $n = s$ 时, 指数 $s-1$ 零化 $\mathbb{F}_{q^{k/2}}^\times$, 故 $h_{s,P}(R)^{s+1} = 1$ 恒成立, 横坐标的任何信息均不保留; 这正是 [7, Alg. 6.1] 在常曲线情形所用的循环, 也正是该算法无法接入本测试的原因。对其他 $n \equiv -1 \pmod{\ell}$, 例如 $n = 2\ell - 1$, 范数并非平凡, 但它只能将 ζ 确定到 $\gcd(n-1, s-1)$ 个候选: 玩具曲线上为 48, BN254 上为 $48u \approx 2^{67.7}$ (对该曲线计算所得; 一般地 $\gcd(2\ell-2, s-1)$ 是 $\gcd(\ell-1, q-1) = 6u$ 的倍数, 因为余因子 $6u^3 + 6u^2 + 3u + 1$ 与 $6u^3 + 6u^2 + 4u + 1$ 互素, 而因子 8 来自 $s-1$ 的其余因子)。根的唯一性正是 $\ell \mid d \mid s+1$ 通过 $\gcd(d, s-1) = \gcd(d, 2)$ (引理 3.5) 所换得的, 也正是 $n \equiv -1 \pmod{\ell}$ 所失去的。

若 $n \equiv q \pmod{\ell}$, 如取 Ate 循环 $T = t - 1$ 与 $P = Q \in G_0$, 则 $[n]Q = \operatorname{Fr}_q Q$,

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

同样没有符号。由于 $\xi(A) \in \mathbb{F}_q$ ，分母为 $(\xi(A) - \xi(Q))^q$ ，故 (8) 化为 $(\xi(A) - \xi(Q))^{T-q} = (\xi(A) - \xi(Q))^{-h\ell}$ ， $h = \#E(\mathbb{F}_q)/\ell$ ：它是 (7) 的 $(-h)$ 次幂——无符号，但取了逆——所含信息与 $d = h\ell$ 时的命题 3.1 相同，后者只需 $\ell \mid d$ 。（与此一致，作为正规化函数 $h_{q,Q} = h_{T,Q} h_{\ell,Q}^h$ ，且 $h_{q,Q}(A)^{s+1} = 1$ 。）本注的全部恒等式均已数值验证（第 9 节）。

引理 3.3. 对 $P \in E[\ell]$ ，作为有理函数，

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

此外，对非零的 $A \in G_1$ 与 $Q \in G_0$ ，以 $t(\cdot, \cdot)$ 记任一参数次序下的约化 Tate 配对，有

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

故 $h_{s,A}(Q) = -t(A, Q)^{-1/2}$ 且 $h_{s,Q}(A) = t(Q, A)^{-1/2}$ ，其中平方根取 μ_ℓ 中唯一的那个。特别地， $h_{s,Q}(A) \in \mu_\ell$ 的阶恰为 ℓ ，而 $h_{s,A}(Q)$ 的阶恰为 2ℓ ，且 $2\ell \mid s+1$ 。

证明. 复合规则 $h_{mn,P} = h_{m,P}^n h_{n,[m]P}$ （除子相同，两端均正规化）给出，以两种方式计算 $h_{\ell s,P}$ ： $h_{s,P}^\ell h_{\ell,[s]P} = h_{\ell,P}^s h_{s,[\ell]P}$ ；由 $[s]P = -P$ 及 $h_{s,\mathcal{O}} = 1$ ，此即 (9)。求值：在 Ate 取向向下，由系数的共轭， $h_{\ell,Q}(A)^s = \text{Fr}_q^{k/2}(h_{\ell,Q}(A)) = h_{\ell,-Q}(A)$ ，故 $h_{s,Q}(A)^\ell = 1$ ；在 Tate 取向向下，由 (5) 及 ℓ 为奇数， $h_{\ell,A}(Q)^s = h_{\ell,A}(-Q) = -h_{\ell,-A}(Q)$ ，故 $h_{s,A}(Q)^\ell = -1$ 。

对于 (10)，同一规则在 $[\ell]A = [s+1]A = \mathcal{O}$ 下给出对每个 c 有 $h_{\ell,c,A}^c = h_{\ell,c,A}$ 及 $h_{(s+1)(s-1),A} = h_{s+1,A}^{s-1}$ ，而除子给出 $h_{s+1,A} = (\xi - \xi(A)) h_{s,A}$ 。于是，记 $\zeta = \xi(Q) - \xi(A) \in \mathbb{F}_{q^{k/2}}^\times$ ，

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

最后一步因 $h_{s,A}(Q)^{2\ell} = 1$ 及 $2\ell \mid s+1$ 。Ate 情形交换 A, Q 后完全相同。由于 ℓ 为奇数，平方是 μ_ℓ 的双射，从而平方根被唯一确定； $h_{s,A}(Q)$ 的符号由 $h_{s,A}(Q)^\ell = -1$ 强制。最后，由非退化性 $t(A, Q) \neq 1$ ，故 $h_{s,A}(Q)^2 \neq 1$ ，其阶恰为 2ℓ 而非 2；同理 $h_{s,Q}(A) \neq 1$ ，其阶恰为 ℓ 。□

四个推论。其一，循环长度为 s 的 Miller 值就是约化 Tate 配对的 $-1/2$ 次幂，且无需最终幂运算：Sato 的“another pairing”是字面意义上的。作为原始 Miller 值，它对两个参数均双线性，这已直接验证（第 9 节）。其二，该符号再次是 (5) 中的 $(-1)^\ell$ ，与 (7) 机制相同；(9) 用两行给出了 [4] 在 Ate 取向下的结论。其三， $d = \ell$ 时的命题 3.1 是同一恒等式的再一次解读： $h_{\ell,A}(Q)^{s+1} = h_{s+1,A}(Q)^\ell = \zeta^\ell h_{s,A}(Q)^\ell = -\zeta^\ell$ 。其四，同一规则给出循环长度 q 的值，见注 3.4。

注 3.4 (循环长度 q)。同一复合规则用于 $h_{q^k,Q}$ ，给出 $h_{q^k,Q} = \prod_{i=0}^{k-1} h_{q,[q^i]Q}^{q^{k-1-i}}$ ；由于 $[q^i]Q = \text{Fr}_q^i Q$ 且 A 有理， $h_{q,\text{Fr}_q^i Q}(A) = h_{q,Q}(A)^{q^i}$ ，从而 $h_{q^k,Q}(A) = h_{q,Q}(A)^{kq^{k-1}}$ 。另一方面 $\text{div } h_{q^k,Q} = (q^k-1)([Q] - [\mathcal{O}]) = \text{div } h_{\ell,Q}^{(q^k-1)/\ell}$ ，故 $h_{q^k,Q}(A) = t(Q, A)$ 。仅此只能得 $h_{q,Q}(A) \in \mu_{k\ell}$ ；其属于 μ_ℓ 由同一规则用于 $h_{q\ell,Q}$ 得出： $h_{q,Q}^\ell h_{\ell,[q]Q} = h_{\ell,Q}^q$ ，而 $h_{\ell,Q}(A)^q = h_{\ell,\text{Fr}_q Q}(A)$ 且 $[q]Q = \text{Fr}_q Q$ ，故 $h_{q,Q}(A)^\ell = 1$ 。于是，由 μ_ℓ 中根的唯一性，

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

后一形式因 $q^{k-1} = sq^{k/2-1} \equiv -q^{k/2-1} \pmod{\ell}$ （且 $\ell \nmid k$ ，第 2 节）。[7, Alg. 6.6]——其算法 6.1 的循环长度 q 包装——的目标在本文记号下为 $h_{q,-Q}(A) = t(Q, A)^{1/(kq^{k/2-1})}$ （ $h_{q,Q}(A)$ 作为 t 的固定次幂对 Q 双线性）；故第 8 节第 15 行的最终检验 $t(Q, A) = z^{-kq^{k-1}}$ 也直接解决该问题。（数值验证，第 9 节。）

引理 3.5. 设 $d \mid s+1$ 。则 $\gcd(d, s-1) = \gcd(d, 2)$ ，且对 $u \in \mathbb{F}_{q^{k/2}}^\times$ ，方程 $\zeta^d = u$ 在 $\mathbb{F}_{q^{k/2}}^\times$ 中或无解，或恰有 $\gcd(d, 2)$ 个解。当其可解时：

1. 若 d 为奇数，解唯一，等于 $u^{d^{-1} \bmod (s-1)}$ ；
2. 若 d 为偶数，解为 $\pm \zeta_0$ ，其中 ζ_0 为任一解，可如下得到：写 $d = 2^a d'$ ， d' 为奇数，令 $u_1 := u^{d'^{-1} \bmod (s-1)}$ ，再用任一标准算法在 $\mathbb{F}_{q^{k/2}}$ 中对 u_1 连续开 a 次平方根。

证明. 标准结论： s 为奇数，故 $\gcd(s+1, s-1) = 2$ 且 $\gcd(d, s-1) \mid 2$ ，其余是循环群中方程 $\zeta^d = u$ 的解数计数，如 [6, Thm. 4.2] 的证明。下文只用到情形 (i)，因为 d 始终为奇数。□

对奇数 $d = \ell$ ，适用情形 (i)。情形 (ii) 即 [6, Alg. 4.1, 步骤 3–4] 中可见的符号歧义，那里产生两个横坐标 $\xi(A) \pm u$ ；它只是使代价加倍而已。

4 分离引理

设 E 具有 $e \mid k$ 次扭曲 E' ，令 $m := k/e$ 。由于 k 为偶数， $e \geq 3$ 意味着 $e \in \{4, 6\}$ ： $e = 3$ 次扭曲迫使 $j(E) = 0$ 且 $6 \mid k$ ，从而存在六次扭曲，故 $e = 3$ 从不是最大扭曲次数，全文取 e 为偶数。该扭曲由 $\mathbb{F}_{q^m}$ 上的参数 $\theta \in \mathbb{F}_{q^m}^\times$ 定义，其类生成 $\mathbb{F}_{q^m}^\times / (\mathbb{F}_{q^m}^\times)^e$ ，在 $\varphi(e)$ 个可能的类中选取使 $\ell \mid \#E'(\mathbb{F}_{q^m})$ 者（通常术语中的 D 型或 M 型扭曲），扭曲同构 $\psi: E' \rightarrow E$ 将 (x', y') 映为 $(\omega x', \omega^{3/2} y')$ ，其中 $\omega := \theta^{2/e}$ 。由 $G_0 = \psi(E'(\mathbb{F}_{q^m})[\ell])$ ，

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

这是一个 $m = k/e$ 维的 $\mathbb{F}_q$ -子空间，因 e 为偶数而含于 $\mathbb{F}_{q^{k/2}}$ 。（与此一致， $\xi(P) \in \mathbb{F}_{q^{k/2}}$ ，因为 ξ 是偶函数而 $\text{Fr}_q^{k/2}$ 在 G_0 上作用为 $[-1]$ ，[7, Lem. 5.2]。）另一方面，对 $A \in G_1$ 有 $\xi(A) \in \mathbb{F}_q$ 。

引理 4.1 (分离). 设 $e \in \{4, 6\}$ ，令 $\lambda := \omega^{q^m-1}$ 。则 $\omega \notin \mathbb{F}_{q^m}$ ，故 $\lambda \neq 1$ 且 $\mathbb{F}_q \cap W = \{0\}$ ；此外 $\lambda \in \mathbb{F}_{q^{k/2}}$ ，因为对任意 $Q_0 \in G_0 \setminus \{\mathcal{O}\}$ 有 $\lambda = \xi(Q_0)^{q^m} / \xi(Q_0)$ 而 $\xi(Q_0) \in \mathbb{F}_{q^{k/2}}$ ，故 $\mathbb{F}_q$ -线性映射

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

良定义，满足 $\ker L = W$ 及 $L|_{\mathbb{F}_q} = (1 - \lambda) \text{id}$ ；且对 $\zeta := \xi(Q) - \xi(A)$ ($\xi(Q) \in W$, $\xi(A) \in \mathbb{F}_q$) 有

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

证明. 若 $\omega \in \mathbb{F}_{q^m}$ ，则 $\theta^2 = \omega^e \in (\mathbb{F}_{q^m}^\times)^e$ ，故 θ 的类在 e 阶循环群中的阶整除 2，而按假设其阶为 e ；于是 $e \mid 2$ ，与 $e \geq 4$ 矛盾。因此 $\omega \notin \mathbb{F}_{q^m}$ ，即 $\lambda \neq 1$ 。若 $a \in \mathbb{F}_q \cap W$ 且 $a \neq 0$ ，则 $a = \omega x'$ ， $x' \in \mathbb{F}_{q^m}^\times$ ，从而 $\omega = a/x' \in \mathbb{F}_{q^m}$ ，矛盾；故 $\mathbb{F}_q \cap W = \{0\}$ 。 L 是 $\mathbb{F}_q$ -线性的，因为 $u \mapsto u^{q^m}$ 是；对 $u = \omega x' \in W$ ， $u^{q^m} = \omega^{q^m} x' = \lambda u$ ，故 $L(u) = 0$ ，即 $W \subseteq \ker L$ 。反之， $\omega^{e/2} = \theta$ ，而 $X^{e/2} - \theta$ 在 $\mathbb{F}_{q^m}$ 上不可约：其次数 $e/2 \in \{2, 3\}$ 为素数，且 θ 不是 $(e/2)$ 次幂，否则 θ^2 将是 e 次幂而 θ 的类的阶整除 2。于是 $1, \omega, \dots, \omega^{e/2-1}$ 是 $\mathbb{F}_{q^{k/2}}$ 的一组 $\mathbb{F}_{q^m}$ -基（注意 $[\mathbb{F}_{q^{k/2}} : \mathbb{F}_{q^m}] = e/2$ ），由 $u \mapsto u^{q^m}$ 的特征向量组成，特征值 λ^j ($0 \leq j < e/2$) 两两不同，因为 $\lambda \neq 1$ 且 $\lambda^{e/2} = \theta^{q^m-1} = 1$ ， $e/2$ 为素数。故 $u \mapsto u^{q^m}$ 可对角化， $\ker L$ 是其 λ -特征空间，即 $\omega \mathbb{F}_{q^m} = W$ 。对 $a \in \mathbb{F}_q$ ， $a^{q^m} = a$ ，故 $L(a) = (1 - \lambda)a$ 。对 ζ 施加 L 得 $L(\zeta) = -(1 - \lambda)\xi(A)$ ，此即 (12)。□

注 4.2. 当 $e = 2$ 时 $m = k/2$ ， $W = \omega \mathbb{F}_{q^{k/2}} = \mathbb{F}_{q^{k/2}}$ ：投影退化 ($\lambda = 1$, $L = 0$)，但并不失败—— $\xi(A) \in \mathbb{F}_q$ 仍只有 q 个可能值，故算法 5.1 的步骤 3 变为对 $x_A \in \mathbb{F}_q$ 的循环、取 $x_Q = \zeta + x_A$ ，代价由 $O(1)$ 变为 $O(q)$ ；第 8 节的算法则遍历 $\mathbb{F}_q \times \mathbb{F}_{q^{k/2}}$ ，代价为其一般公式的 $q^{k/e}/2 = q^{k/2}/2$ 。因此 $O(1)$ 解码需要四次或六次扭曲——BN 与 BLS12 ($e = 6$)、KSS16 ($e = 4$)、[1] 的 Brezing–Weng 曲线——而不覆盖仅具二次扭曲的曲线。

注 4.3. 当 $k = 2$ 时，特别是对 [7, § 4] 的超奇异曲线（那里 $t = 0$ 迫使 $k \leq 2$ ），有 $s = q$ ，两个横坐标均在 $\mathbb{F}_q$ 中：任何 $\mathbb{F}_q$ -线性映射都无法分离它们。在我看来，这正是 [6]（FAPI，一个参数已知，多项式时间）与 [7]（GPI，两者均未知，指数时间）适用范围不相交的结构原因。

对 BN 曲线， $e = 6$ ， $m = 2$ ， $L(u) = u^{q^2} - \lambda u$ 且 $\lambda^3 = \theta^{q^2-1} = 1$ ： λ 是本原三次单位根。一般地 $\lambda^{e/2} = 1$ 。它是曲线常数，可由任一已知的 G_0 生成元得到。

注 4.4 (G_0 的 Legendre 检验). 对 $x_Q \in \mathbb{F}_{q^{k/2}}$ ，设 $\beta := x_Q^3 + a_4 x_Q + a_6 \neq 0$ ， $Q = (x_Q, y_Q)$ ， $y_Q \in \mathbb{F}_{q^k}$ ， $y_Q^2 = \beta$ 。则 $\text{Fr}_q^{k/2} Q = -Q$ 当且仅当 β 在 $\mathbb{F}_{q^{k/2}}$ 中是非平方：事实上 $\text{Fr}_q^{k/2} Q = (x_Q, y_Q^s)$ ，而 $y_Q^s = -y_Q$ 当且仅当 $y_Q^{s-1} = \beta^{(s-1)/2} = -1$ 。因此 Q 是否属于 $\ker(\text{Fr}_q^{k/2} + 1)$ 可在开方之前由 $\mathbb{F}_{q^{k/2}}$ 中的一次 Legendre 符号判定，且满足 $\beta \neq 0$ 的 $x_Q \in \mathbb{F}_{q^{k/2}}$ 中约有一半通过：使 $\beta(x)$ 为非平方的 $x \in \mathbb{F}_{q^{k/2}}$ 的个数为 $(s + t_s - N_0)/2$ ，其中 t_s 为 E 在 $\mathbb{F}_{q^{k/2}}$ 上的 Frobenius 迹， $N_0 = \#\{\beta = 0\}$ 。在子空间 $W = \omega \mathbb{F}_{q^m}$ 上两种扭曲次数的行为不同。对 $e = 6$ ($a_4 = 0$)， $x_Q = \omega u$ 时 $\beta = \theta u^3 + a_6 \in \mathbb{F}_{q^m}$ ，因 $[\mathbb{F}_{q^{k/2}} : \mathbb{F}_{q^m}] = 3$ 为奇数， β 在 $\mathbb{F}_{q^{k/2}}$ 中非平方当且仅当在 $\mathbb{F}_{q^m}$ 中非平方：约一半 $x_Q \in W$ 通过，且符号可直接在 $\mathbb{F}_{q^m}$ 中计算。对 $e = 4$ ($a_6 = 0$)， $\beta = \omega u(\theta u^2 + a_4)$ ，其中 $u(\theta u^2 + a_4) \in \mathbb{F}_{q^m}$ 在二次扩张 $\mathbb{F}_{q^{k/2}}$ 中是平方，而 ω 在 $\mathbb{F}_{q^{k/2}}$ 中是非平方 ($\omega^{(s-1)/2} = \theta^{(q^m-1)/2 \cdot (q^m+1)/2} = -1$ ，因 θ 是 $\mathbb{F}_{q^m}$ 的非平方且 $(q^m+1)/2$ 为奇数)：满足 $\beta \neq 0$ 的每个 $x_Q \in W$ 都通过，检验为空，全部筛选由 $[\ell]Q = \mathcal{O}$ 完成。该符号不应以 $\log_2 s$ 位指数的幂运算来计算，那将耗费其所节省的约一半；由于 $\beta^{(s-1)/2} = N_{\mathbb{F}_{q^{k/2}}/\mathbb{F}_q}(\beta)^{(q-1)/2}$ ，它的代价为 $\mathbb{F}_{q^{k/2}}$ 中 $k/2 - 1$ 次 Frobenius 与 $k/2 - 1$ 次乘法，再加 $\mathbb{F}_q$ 中一次 Jacobi 符号，后者的代价远小于 $\mathbb{F}_{q^k}$ 中一次乘法。（在第 9 节验证。）

5 两个未知量的 Miller 求逆

本节包含真正的结果：一个多项式时间过程，输入原始 Tate–Miller 值，返回其两个参数。它就是 [6, Alg. 4.1]——在已知 A 处求 $h_{d,A}$ 的逆——但有两处改动：取向为 Tate 而非 Ate，故范数给出 ζ^d 而非 ζ^2 （命题 3.1 对比 [6, eq. (4.3)]），且 d 次根唯一（引理 3.5）；其步骤 3 ($\xi(Q) = \xi(A) \pm u$) 被引理 4.1 的投影取代。下面的步骤 1–2 与 5–8 是他的。

命题 5.1. 算法 5.1 正确，并在 $O((k \log q)^3)$ 次位运算内终止。

证明. 若对某 $(A_0, Q_0) \in G_1 \times G_0$ 有 $w = h_{d,A_0}(Q_0)$ ，则由命题 3.1， $u = (\xi(Q_0) - \xi(A_0))^d$ ，故 $\zeta = \xi(Q_0) - \xi(A_0)$ （相差情形 (ii) 的符号，该符号会被尝试），引理 4.1 给出 $x_A = \xi(A_0)$ ， $x_Q = \xi(Q_0)$ ；步骤 5–7 于是产生符号未知的 $A = \pm A_0$ ， $Q = \pm Q_0$ 。由 (5) 及命题 3.1 的证明，四个原始值为 $h_{d,A_0}(Q_0) = w$ ， $h_{d,-A_0}(-Q_0) = -w$ ， $h_{d,A_0}(-Q_0) = w^s$ 与 $h_{d,-A_0}(Q_0) = -w^s$ (d 为奇数)，故步骤 8 识别出符号并返回 Miller 值恰为 w 的点。反之，若算法返回一个点对，则由步骤 5 与 7， $A \in E(\mathbb{F}_q)[\ell] = G_1$ ；由步骤 6–7、注 4.4 与 (1)， $Q \in E[\ell] \cap \ker(\text{Fr}_q^{k/2} + 1) = G_0$ ；由步骤 8，其 Miller 值为 w 。若无步骤 8，算法可能对根本不是 Miller 值的 w 返回一个有效点对。至于代价，以 $\mathbb{F}_{q^k}$ 中的乘法计数，每次乘法用学校算术需 $O((k \log q)^2)$ 次位运算，如 [6, Thm. 4.2]； $\mathbb{F}_{q^{k/2}}$ 或 $\mathbb{F}_q$ 中的一次乘法代价不超过此数，而指数 $d^{-1} \bmod (s-1)$ 、常数 λ 、 $(\lambda-1)^{-1}$ 与引理 4.1 的基每条曲线只计算一次。逐步计之：

1. $w^{s+1} = w^s \cdot w$ ：一次 Frobenius 幂与一次乘法， $O(k \log q)$ 次乘法；若 $\mathbb{F}_{q^k}$ 表示为 $\mathbb{F}_{q^{k/2}}$ 的二次扩张，则 $w \mapsto w^s$ 即共轭，为 $O(1)$ 。
2. $\mathbb{F}_{q^{k/2}}$ 中一次指数小于 s 的幂运算： $O(k \log q)$ 次乘法。
3. ζ^{q^m} 是一次 Frobenius 幂 ($O(k \log q)$ 次乘法，或用预计算矩阵在 $\mathbb{F}_q$ 中 $O(k^2)$ 次乘法)，再加一次乘法；在 $\mathbb{F}_{q^{k/2}}$ 的含 1 的 $\mathbb{F}_q$ -基下，检验 $x_A \in \mathbb{F}_q$ 不需代价。

算法 5.1 Miller 求逆, 两个未知量

输入: $w \in \mathbb{F}_{q^k}^\times$; 此处 $d \mid s+1$; 常数 λ 、 $(\lambda-1)^{-1}$ 与引理 4.1 的基, 每条曲线预计算一次

输出: 满足 $h_{d,A}(Q) = w$ 的 $(A, Q) \in G_1 \times G_0$, 或 $\perp$

- 1: $u \leftarrow (-1)^d w^{s+1}$
 - 2: $\zeta \leftarrow u$ 在 $\mathbb{F}_{q^{k/2}}^\times$ 中的一个 d 次根 $\triangleright$ 引理 3.5; 若不存在则返回 $\perp$, 若有两个则两个符号均试
 - 3: $x_A \leftarrow L(\zeta)/(\lambda-1)$
 若 $x_A^q \neq x_A$ **则返回** $\perp$
 - 4: $x_Q \leftarrow \zeta + x_A$ $\triangleright$ 此时 $L(x_Q) = L(\zeta) + (1-\lambda)x_A = 0$ 自动成立
 - 5: $\alpha \leftarrow x_A^3 + a_4 x_A + a_6$
 若 α 在 $\mathbb{F}_q$ 中不是平方 **则返回** $\perp$
 $A \leftarrow (x_A, \sqrt{\alpha})$
 - 6: $\beta \leftarrow x_Q^3 + a_4 x_Q + a_6$
 若 $N_{\mathbb{F}_{q^{k/2}}/\mathbb{F}_q}(\beta)^{(q-1)/2} \neq -1$ **则返回** $\perp$ $\triangleright$ 即 $\text{Fr}_q^{k/2} Q \neq -Q$, 注 4.4
 $Q \leftarrow (x_Q, y_Q)$, $y_Q \in \mathbb{F}_{q^k}$, $y_Q^2 = \beta$
 - 7: **若** $[\ell]A \neq \mathcal{O}$ **或** $[\ell]Q \neq \mathcal{O}$ **则返回** $\perp$
 - 8: $h \leftarrow h_{d,A}(Q)$
 若 $w = h$ **则返回** (A, Q)
 若 $w = -h$ **则返回** $(-A, -Q)$
 若 $w = h^s$ **则返回** $(A, -Q)$
 若 $w = -h^s$ **则返回** $(-A, Q)$
 - 9: **返回** $\perp$
-

4. 一次加法。

5. $\mathbb{F}_q$ 中一次 Legendre 符号与一次开方: $\mathbb{F}_q$ 中 $O(\log q)$ 次乘法。

6. 经由范数计算 $\mathbb{F}_{q^{k/2}}$ 中的 Legendre 符号, $k/2-1$ 次 Frobenius 幂、 $\mathbb{F}_{q^{k/2}}$ 中 $k/2-1$ 次乘法及 $\mathbb{F}_q$ 中一次 Jacobi 符号 (注 4.4); $\mathbb{F}_{q^k}$ 中一次开方, $O(k \log q)$ 次乘法——实际上是 $\mathbb{F}_{q^{k/2}}$ 中的开方: 取 $\mathbb{F}_{q^{k/2}}$ 的非平方 ν 使 $\mathbb{F}_{q^k} = \mathbb{F}_{q^{k/2}}(\sqrt{\nu})$, 则 β/ν 是 $\mathbb{F}_{q^{k/2}}$ 中的平方, 且 $\sqrt{\beta} = \sqrt{\nu} \sqrt{\beta/\nu}$ 。

7. $E(\mathbb{F}_q)$ 上的 $[\ell]A$ 与 $E(\mathbb{F}_{q^k})$ 上的 $[\ell]Q$: 各 $O(\log \ell) = O(\log q)$ 次群运算, 每次为有界次数的乘法。

8. 一次长度 $d \leq s+1$ 的 Miller 循环: $O(\log d) = O(k \log q)$ 步倍加或加法, 每步为有界次数的乘法, 外加四次比较, 代价为一次 Frobenius 幂。

每一步都是 $\mathbb{F}_{q^k}$ 中 $O(k \log q)$ 次乘法, 即 $O((k \log q)^3)$ 次位运算, 且步骤 1、2、6 与 8 达到此界。在 [6] 所假定的预计算 (2-Sylow 子群的一个生成元) 下开方是确定性的, 否则用 Cipolla 算法为期望时间。 $\square$

有两点值得评述。其一, 仅基于 u 的任何测试都不具区分力: w^{s+1} 是范数, 故对每个 w 都在 $\mathbb{F}_{q^{k/2}}$ 中, 而 $\mathbb{F}_{q^{k/2}}$ 的每个元素在 $\mathbb{F}_{q^k}$ 中都是平方; 这就是步骤 6 在 $\mathbb{F}_{q^{k/2}}$ 中而非 $\mathbb{F}_{q^k}$ 中检验 β ——有用的条件是 β 在 $\mathbb{F}_{q^{k/2}}$ 中是非平方, 注 4.4——、步骤 4 仅是一次赋值 (一旦 $x_A \in \mathbb{F}_q$, $L(x_Q) = L(\zeta) + (1-\lambda)x_A = 0$ 自动成立)、而步骤 3、6 与 7 的测试承担全部分量的原因。在第 9 节的玩具曲线上, 固定目标的 3000 个随机 ℓ 次根全部通过范数与平方条件, 又全部在步骤 3 被拒绝。其二, 该过程返回两个参数; 它不是“成员预言机加搜索”。这正是本文超出 [1] 之处: 他们的方程 (8) 恰为交换 A 、 Q 角色后的 (3), 而其后续归约使用已知 $\xi(Q)$ 的极小多项式, 这里并不可得。

6 从 Miller 求逆到 GPI

设 e 为 $G_1 \times G_0$ 或 $G_0 \times G_1$ 上任一取值于 μ_ℓ 的非退化双线性配对——任一参数次序下的约化 Tate 配对 t ，或 Satoh 的配对——并设 $z \in \mu_\ell \setminus \{1\}$ 为 e 的 GPI 目标。

满足 $v^{(q^k-1)/\ell} = t(A, Q)$ 的原始 Tate–Miller 值 v 仅由约化值确定到 $x \mapsto x^{(q^k-1)/\ell}$ 的核的一个元素——该核是 $(q^k - 1)/\ell = (s - 1)\nu$ 阶子群，其中 $\nu := (s + 1)/\ell$ 。这远大于可枚举的范围，且并非算法 5.1 所需：它所需的是 ζ ，而下面的命题 6.2 表明，当 v 遍历该陪集时， ζ 遍历整个 $\mathbb{F}_{q^{k/2}}^\times$ ——即目标对 ζ 毫无约束。因此 GPI 算法直接遍历横坐标对 $(x_A, x_Q) \in \mathbb{F}_q \times W$ （第 8 节），或等价但更慢地遍历由算法 5.1 步骤 3–4 解码的 $\zeta \in \mathbb{F}_{q^{k/2}}^\times$ （注 8.1）；两种情形下每个点对都与 z 比对，而步骤 2 的 d 次根从不需要。

对后文至关重要的一点是：两个循环在最终检验之前都不计算配对； e 仅在最终检验中出现，且仅通过“是否 $e(A, Q) \in \{z, z^{-1}\}$ ”这一问题出现。因此：

- 算法解决的是最终检验中所计算的那个配对 e 的 GPI，无论 e 为何；命题 7.1 逐字适用于每个这样的 e ，因为其计数论证只用到双线性与非退化性；
- 特别地，取 $e(A, Q) := h_{s,-Q}(A)$ ——即 Satoh 记号下的 $h_{q^{k/2}, -A}(Q)$ ，[7, Alg. 6.1] 的输出条件——算法直接解决 Satoh 的 GPI 问题。由引理 3.3，该 e 等于 $t(Q, A)^{1/2}$ ，双线性且非退化，故最终检验可等价地取为 $t(Q, A) \in \{z^2, z^{-2}\}$ ，比长度为 s 的 Miller 循环便宜；同样，[7, Alg. 6.6] 的循环长度 q 目标 $h_{q,-Q}(A)$ 由注 3.4 为 $t(Q, A)^{1/(kq^{k/2-1})}$ ，以 $t(Q, A) \in \{z^{\pm kq^{k-1}}\}$ 检验；
- 从不计算两个不同配对之间的任何关系；即便计算，也不需要离散对数。例如，满足 $t(Q, A) = t(A, Q)^{\kappa'}$ 的常数 κ' 有封闭形式

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

它由 Tate 配对通过 Weil 配对的 Frey–Rück 表达式导出（引理 6.1）；在第 9 节的玩具曲线上其值为 15。本方法不使用它，离散对数也不出现在本文的任何地方。

引理 6.1. 设 e_ℓ 为 Weil 配对，由 Miller 公式 $e_\ell(A, Q) = (-1)^\ell h_{\ell,A}(Q)/h_{\ell,Q}(A)$ 给出， c, h 如 (13) 中所定义， $\rho := kh/(q-1) \bmod \ell$ 。则对 $A \in G_1, Q \in G_0$ ，

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

由此得 (13)。 $t(Q, A)$ 的非退化性即 $\rho \neq 0$ ，亦即 $\ell \nmid kh$ ：此处 $\ell \nmid k$ 因为 $k = \text{ord}_\ell(q)$ 整除 $\ell-1$ ，而 $\ell \nmid h$ 因为 $\ell \parallel \#E(\mathbb{F}_q)$ 。 $t(A, Q)$ 的非退化性即 $\rho \neq c$ ，这恰是 (13) 中分母 $kh - c(q-1) = (q-1)(\rho - c)$ 不为零。

证明. 恒等式 $t(P, R) = e_\ell(P, \sigma S - S)$ （其中 $[\ell]S = R$ ， $\sigma = \text{Fr}_q^k$ ）是 Tate 配对的 Lichtenbaum 形式 [2]；它是经典的，这里只计算指数。由于 $\pi^k - 1$ 零化 $E[\ell]$ ，它在 $\text{End}(E)$ 中分解为 $\ell\phi$ ，故 $\sigma S - S = \phi(R)$ ，而 ϕ 在 Tate 模 $T_\ell E$ 中 π 的两条特征直线上分别作用为 $(\alpha^k - 1)/\ell$ 与 $(\beta^k - 1)/\ell$ ，其中 $\alpha \equiv 1, \beta \equiv q \pmod{\ell}$ 为特征值。写 $\alpha = 1 + \ell a, \beta = q + \ell b$ ；则 $\alpha + \beta = t = q + 1 - \ell h$ 给出 $a + b = -h$ ， $\alpha\beta = q$ 给出 $b \equiv -qa$ ，故 $a \equiv h/(q-1)$ ，且 $(\alpha^k - 1)/\ell \equiv ka$ ， $(\beta^k - 1)/\ell \equiv c + kq^{k-1}b \equiv c - ka \pmod{\ell}$ 。于是对 $Q \in G_0$ 有 $\phi(Q) = [c - \rho]Q$ ，对 $A \in G_1$ 有 $\phi(A) = [\rho]A$ ，从而 $t(A, Q) = e_\ell(A, Q)^{c-\rho}$ ，且由反对称性 $t(Q, A) = e_\ell(Q, A)^\rho = e_\ell(A, Q)^{-\rho}$ 。□

命题 6.2 (配对值与范数的独立性). 由于 $\gcd(\ell, s-1) = 1$ ，映射

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

是核的阶为 $\nu = (s+1)/\ell$ 的满同态。因此约化配对值与原始 Miller 值的范数是独立的坐标：固定前者后，后者在 $\mathbb{F}_{q^{k/2}}^\times$ 上均匀分布，而任何仅通过 v^{s+1} 读取 v 的过程——特别是任何建立在命题 3.1 之上的过程——都得不到关于目标的任何信息。

证明. $\mathbb{F}_{q^k}^\times$ 是 $(s-1)(s+1)$ 阶循环群。核由阶整除 $\gcd((s-1)(s+1)/\ell, s+1) = \nu \gcd(s-1, \ell) = \nu$ 的 v 组成, 故像的阶为 $(q^k - 1)/\nu = \ell(s-1) = |\mu_\ell \times \mathbb{F}_{q^{k/2}}^\times|_0$. $\square$

这就是下面命题 7.1 的内容, 一次性陈述: 范数路线完全丢弃目标, 剩下的是对横坐标的搜索加一次最终配对检验。(在第 9 节的玩具曲线上验证: 像的阶为预测的 $\ell(s-1)$ 。)

7 解集的密度

命题 7.1. 设 $e \in \{4, 6\}$, $k > 2$, d 为奇数且 $d \mid s+1$, 固定 $z \in \mu_\ell \setminus \{1\}$ 。当 v 遍历 $\{v : v^{(q^k-1)/\ell} = z\}$ 时, 量 $\zeta = ((-1)^{d\nu s+1})^{1/d}$ 遍历整个 $\mathbb{F}_{q^{k/2}}^\times$, 每个值取到的次数相同 (命题 6.2 与引理 3.5)。设 e 为 $G_1 \times G_0$ 或 $G_0 \times G_1$ 上取值于 μ_ℓ 的非退化双线性配对。在 $s-1$ 个 ζ 值中, 恰有 $(\ell-1)/2$ 个被算法 5.1 的步骤 3-7 解码为满足 $e(A, Q) = z^{\pm 1}$ 的点 (A, Q) 。故需检验的候选的期望数为

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

证明. 第一个断言即命题 6.2 (范数在 z 的纤维上于 $\mathbb{F}_{q^{k/2}}^\times$ 均匀) 加上 $\zeta \mapsto \zeta^d$ 在 $\mathbb{F}_{q^{k/2}}^\times$ 上的双射性 (引理 3.5, d 为奇数)。对第二个, 由引理 4.1, 映射 $(\xi(A), \xi(Q)) \mapsto \xi(Q) - \xi(A)$ 在 $\mathbb{F}_q \times W$ 上单射。由双线性与非退化性, 满足 $e(A, Q) \in \{z, z^{-1}\}$ 的点 $(A, Q) \in (G_1 \setminus \{\mathcal{O}\}) \times (G_0 \setminus \{\mathcal{O}\})$ 共 $2(\ell-1)$ 个 (对每个 A , 两个值各对应一个 Q) ; 它们在保持两个横坐标的 $(A, Q) \mapsto (\pm A, \pm Q)$ 作用下分成大小为 4 的轨道, 每条轨道内 e 取两个值各两次, 故给出 $(\ell-1)/2$ 个不同的 ζ 值。 $\square$

成功的 ζ 全部位于 $1 + k/e$ 维子空间 $\mathbb{F}_q \oplus W$ 中, 故第 8 节的算法遍历该子空间 ($q^{1+k/e}$ 个元素, 对 BN254 为 2^{761}) 而非 $\mathbb{F}_{q^{k/2}}^\times$ 。计数 (14) 针对后者; 对前者, 在自然的分块顺序 (x_A 在外、 x_Q 在内) 下, 工作量为第一个有效块内的 $q^{k/e}/2$ 个候选, $e=6$ 时其中一半昂贵、 $e=4$ 时全部昂贵 (注 4.4), 与 ℓ 无关 (第 8 与 9 节)。

8 完整算法

由引理 4.1, 算法 5.1 步骤 3-4 解码出的值 ζ 恰为 $\zeta = x_Q - x_A$, $(x_A, x_Q) \in \mathbb{F}_q \times W$; 由命题 6.2, 目标不约束 ζ 。因此 GPI 算法直接遍历点 (x_A, x_Q) ; 范数与投影 L 根本不被计算。第 4-7 节的分析仅通过其所证明的内容起作用: 这就是搜索空间, 且范数路线上没有任何东西能缩小它 (第 10 节列出各项归约及其依据)。

配对 e 仅在第 15 行求值, 目标 z 仅在第 15-19 行出现。第 18 行利用 $e(-A, Q) = e(A, Q)^{-1}$, 故一个成功的点对至多经两次符号选择即得答案; 这已计入命题 7.1 的计数 $(\ell-1)/2$ 。 G_1 的每个横坐标在 G_0 中恰有一个配偶横坐标, 故循环在通过第 7 行与第 9 行的第一个 x_A 的块内停止, 此前扫描约一半的 W ; 这些期望值假定两个循环按均匀随机顺序进行, 如第 9 节 (上面写出的固定顺序总是遇到同一个第一个 x_A)。期望工作量为 $(q-n)/(n+1)$ 个被拒的 x_A ($n = (\ell-1)/2$, 每个以 $\mathbb{F}_q$ 中一次 Legendre 符号为代价, 当 $h > 1$ 时通过者中的一半再需一次 $[\ell]A$; $h=1$ 时没有被拒的 x_A 能通过该符号), 随后是 $q^{k/e}/2$ 个候选 x_Q , $e=6$ 时其中一半昂贵, $e=4$ 时全部昂贵 (注 4.4)。

与算法 5.1 的关系。 算法 8.1 并不调用算法 5.1, 这是有意为之。后者的步骤 1-4 (范数、 d 次根、投影) 把一个候选原始值 w 解码为一对横坐标, 而命题 6.2 表明, 当 w 遍历 z 的纤维时, 它们以相同频率产生 $\mathbb{F}_q \times W$ 中的每一对: 运行它们等于绕道 $\mathbb{F}_{q^{k/2}}^\times$ 来遍历 $\mathbb{F}_q \times W$, 其代价见注 8.1。算法 8.1 直接遍历这些点对, 并逐行保留算法 5.1 的后半部分: 第 6-8 行与第 11-13 行即其步骤 5 与 6 (开方与 Legendre 检验), 第 9 行与第 14 行即其步骤 7 (阶的检验), 而第 15-19 行以约化值 $e(A, Q)$ 与 $z^{\pm 1}$ 的比较取代其步骤 8——原始值 $h_{d,A}(Q)$ 与 w 在

算法 8.1 GPI, 循环长度 ℓ

输入: q ; $\mathbb{F}_q$ 上的常曲线 $E: Y^2 = X^3 + a_4X + a_6$; 奇素数 $\ell \parallel \#E(\mathbb{F}_q)$, 嵌入次数为偶数 $k > 2$; 偶数扭曲次数 $e \geq 4$, $e \mid k$; $G_1 \times G_0$ 上的非退化双线性配对 e , 例如 $t(A, Q)$ 、 $t(Q, A)$ 或 Satoh 的 $h_{s,-Q}(A) = t(Q, A)^{1/2}$; 目标 $z \in \mu_\ell \setminus \{1\}$ 。

输出: 满足 $e(A, Q) = z$ 的 $(A, Q) \in G_1 \times G_0$, 或 $\perp$ 。

- 1: **预计算** (与 z 无关):
 - 2: $s \leftarrow q^{k/2}$; $m \leftarrow k/e$
 - 3: 取 $Q_0 \in G_0 \setminus \{\mathcal{O}\}$; $W \leftarrow \xi(Q_0) \mathbb{F}_{q^m}$, 其 $\mathbb{F}_q$ -基为 $\xi(Q_0) \cdot \{1, \gamma, \dots, \gamma^{m-1}\}$, γ 为 $\mathbb{F}_{q^m}$ 在 $\mathbb{F}_q$ 上的生成元
 - 4: **主循环:**
 - 5: **对于** $x_A \in \mathbb{F}_q$ **执行**
 - 6: $\alpha \leftarrow x_A^3 + a_4x_A + a_6$
 - 7: **若** α 在 $\mathbb{F}_q$ 中是平方 **则**
 - 8: $A \leftarrow (x_A, \sqrt{\alpha})$
 - 9: **若** $[\ell]A = \mathcal{O}$ **则**
 - 10: **对于** $x_Q \in W$ **执行**
 - 11: $\beta \leftarrow x_Q^3 + a_4x_Q + a_6$
 - 12: **若** $N_{\mathbb{F}_{q^{k/2}}/\mathbb{F}_q}(\beta)^{(q-1)/2} = -1$ **则** $\triangleright$ 即 $\text{Fr}_q^{k/2}Q = -Q$, 注 4.4
 - 13: $Q \leftarrow (x_Q, y_Q)$, $y_Q \in \mathbb{F}_{q^k}$, $y_Q^2 = \beta$
 - 14: **若** $[\ell]Q = \mathcal{O}$ **则**
 - 15: $\chi \leftarrow e(A, Q)$
 - 16: **若** $\chi = z$ **则**
 - 17: **返回** (A, Q)
 - 18: **若** $\chi = z^{-1}$ **则**
 - 19: **返回** $(-A, Q)$
 - 20: **返回** $\perp$
-

四个符号意义下的比较。因此算法 5.1 所贡献的不是一个子程序，而是一条定理： $\mathbb{F}_q \times W$ 就是搜索空间，且任何建立在范数之上的解码都无法缩小它。

注 8.1 (对 $\mathbb{F}_{q^{k/2}}^\times$ 的循环). 也可改为遍历 $\zeta \in \mathbb{F}_{q^{k/2}}^\times$ ——例如取大阶元 g (与生成元不同，它不需要分解 $s-1$) 并令 $\zeta \leftarrow g\zeta$, 当陪集 $\zeta_0\langle g \rangle$ 耗尽时从新的 ζ_0 重启，或干脆随机抽取 ζ ——用算法 5.1 的步骤 3–4 解码每个 ζ , 再如上进行; ζ^{q^m} 每步一次乘法即可更新, 检验 $x_A \in \mathbb{F}_q$ 在含 1 的基下是免费的。该循环为最终解码出的每个点对 (x_A, x_Q) 要访问 $\mathbb{F}_{q^{k/2}}$ 中 $q^{k/2-1-k/e}$ 个元素, 每个耗费 $\mathbb{F}_{q^{k/2}}$ 中几次乘法; 其期望代价为 $\frac{2(s-1)}{\ell-1}$ 步, 在第 10 节的单位下 BN254 上约 $2^{1271}M$ 、BLS12-381 上约 $2^{2032}M$, 全部花在寻找上面的直接循环免费枚举出的点对上。它被占优, 之所以记录只因为它是算法 5.1 的解码所出现的形式。

9 实验验证

所有断言均在 PARI/GP 2.15.4 (GMP 6.3.0 内核, 64 位) 下验证, 操作系统为 Ubuntu 24.04.4 LTS、Linux 6.18, 运行于一台单核云虚拟机, 其报告的处理器为 Intel Xeon 2.10 GHz、内存 3.9 GiB; $\mathbb{F}_{q^k}$ 用单个 12 次不可约多项式表示 (PARI 的 `ffgen`), 而非塔式扩张。所用曲线为参数 $u=1$ 的 BN 曲线 ($u=-1$ 给出一条更小的, $q=19$, $\ell=13$, 每个群只有六个横坐标, 太小而使下面的计数失去意义): $q=103$, $\ell=97$, $E: Y^2 = X^3 + 5$, $\#E(\mathbb{F}_q) = \ell$, $\mathbb{F}_{q^k} \simeq \mathbb{F}_{103^{12}}$ 为 80 位; 此处 $e=6$, $m=2$, λ 经验证为 3 阶。命题 3.1 的符号 $(-1)^d = -1$ 用在 $\mathcal{O}$ 处正规化的 Miller 函数确认; 使用未如此正规化的 PARI

elltatepairing 时, 原始常数为 $\mathbb{F}_q^\times$ 的另一元素, 与 (A, Q) 无关, 而约化配对不受影响, 因为 $(q-1) \mid (q^k-1)/\ell$ 。

检验	结果
对 $Q \in G_0$, $\xi(Q) \in \mathbb{F}_{q^{k/2}}$	是
$\lambda = \xi(Q)^{q^m}/\xi(Q)$ 与 Q 无关, $\text{ord}(\lambda) = 3$	是
对所有 $u \in W$, $L(u) = 0$; $\mathbb{F}_q \cap W = \{0\}$ (遍历所有 $a \in \mathbb{F}_q^\times$)	是
命题 3.1, 正规化 Miller: $v^{s+1} = -\zeta^\ell$	是
算法 5.1 精确恢复 $(\xi(A), \xi(Q))$, 30 个随机点对	30/30
目标的 3000 个随机 ℓ 次根被接受的个数	0
命题 7.1: 48 ² 个横坐标对, 96 个 $t = z$ 的点对, 48 个 ζ 值	是
注 3.2: (6) 对 $n = 5, 11, 13$ 精确成立; (7); $h_{s,A}(Q)^{s+1} = 1$;	是
$h_{2\ell-1,A}(Q)^{s+1} = \zeta^{2\ell-2}$; (8), $T = 6$	
引理 3.3: (9) 在两种取向成立; (10); $-h_{s,A}(Q) = t(A, Q)^{48}$, $48 \equiv -1/2$; $\text{ord}(h_{s,A}(Q)) = 194 = 2\ell$	是
$h_{s,Q}(A)$ 对 Q 和 A 均双线性且无需最终幂运算; $h_{s,-Q}(A) = t(Q, A)^{1/2}$	是
引理 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) 给出 15, 且 $t(Q, A) = t(A, Q)^{15}$	是
玩具曲线上 $\gcd(2\ell-2, s-1) = 48$, BN254 上 $= 48u$	是
命题 5.1 的四个值 $w, -w, w^s, -w^s$	是
命题 6.2: $v \mapsto (v^{(q^k-1)/\ell}, v^{s+1})$ 的像的阶为 $\ell(s-1)$	是
注 3.2: $h_{T,Q}(A)^{s+1} = (\xi(A) - \xi(Q))^{-h\ell}$; $h_{q,Q}(A)^{s+1} = 1$; $h_{3\ell,A}(Q)^{s+1} = -\zeta^{3\ell}$, 其中 $3\ell \nmid s+1$	是
注 3.4: $h_{q,Q}(A)^\ell = 1$; $h_{q,Q}(A) = t(Q, A)^{49}$, $49 \equiv -1/(kq^{k/2-1})$;	是
$h_{q,-Q}(A) = t(Q, A)^{48}$	
注 4.4: β 在 $\mathbb{F}_{q^{k/2}}$ 中非平方 $\iff \text{Fr}_q^{k/2} Q = -Q$, 2000 个随机 $x_Q \in W$ (1001 个非平方, $e = 6$); G_0 的 30 个点上 β 均为非平方	是
$1/\pi_z = (s-1)/48 = 2.49 \cdot 10^{10}$, 预测 $2s/\ell = 2.46 \cdot 10^{10}$	是

一次双线性配对的完整求逆。 第 8 节的算法完整运行: 候选为 $(a, x_Q) \in \mathbb{F}_q \times W$, $W = \xi(Q_0)\mathbb{F}_{q^2}$, 即 $\zeta = x_Q - a$, 共 $q^3 = 1\,092\,727$ 个候选, 其中 $x_A = a$ 与 x_Q 直接读出, 无需任何投影。目标为一个均匀随机点对 $(A^*, Q^*) \in G_1 \times G_0$ 的 $z = t(A^*, Q^*)$, 随后将该点对遗忘; 最终检验为 $t(A, Q) \in \{z, z^{-1}\}$, 即完全约化、完全双线性的 Tate 配对。为使计数有意义, a 按 $\mathbb{F}_q$ 的一个均匀随机顺序枚举, 且对每个 a , x_Q 按 W 的一个均匀随机顺序枚举; 挂钟时间为 getwalltime。

G_1 的每个横坐标 a 恰有 G_0 中一个横坐标将其补全为解, 故运行在遇到的第一个有效 a 的块内停止: 它跳过无效的 a (每个以一次 Legendre 符号为代价, 计为跳过一个 q^2 的块), 然后扫描 W 寻找 G_0 的 48 个横坐标, 在每一个处求一次 Tate 配对, 直到遇到正确的那个。实际上, 运行将 A 固定于第一个有效横坐标, 并在 W 中搜索其配偶。在此分块顺序下, 期望工作量为跳过 $(q-n)/(n+1)$ 个块 ($n = (\ell-1)/2$, 每个块以 $\mathbb{F}_q$ 中一次 Legendre 符号为代价, 当 $h > 1$ 时对通过该符号的一半还需一次标量乘法 $[\ell]A$), 随后在第一个有效块内处理 $q^{k/e}/2$ 个候选 (其中一半昂贵) (玩具曲线上为 1.1 个块与 5304 个候选); 对 $\mathbb{F}_q \times W$ 上的均匀顺序, 由命题 7.1 的计数论证相应的计数应为 $2q^{1+k/e}/\ell$, 它仅在相差一个常数的意义下与之吻合, 且仅因 BN 曲线上 $\ell \approx q$ 。在 12 个独立目标上: 12 次成功, 返回的点对位于 $G_1 \times G_0$ 且精确满足 $t(A, Q) = z$, $\xi(A)$ 有 11 个不同值 (从未是原始点对); 跳过 0 到 4 个无效 a (均值 1.3); 正确的 x_Q 在 W 扫描中的位置介于 1022 与 10350 之间 (共 10609, 均值 5896), 与均匀分布相符; 求值的 Tate 配对为 3 到 48 次; 挂钟时间介于 0.37 s 与 1.92 s 之间, 主要耗费于扫描中 $\mathbb{F}_{q^k}$ 内的开方与乘以 ℓ 的标量乘法, 而非配对。这里报告的运行早于注 4.4,

在开方之后才检验 $\text{Fr}_q^{k/2}Q = -Q$ ；若先做经范数计算的 Legendre 检验，可以 $k/2$ 次乘法为代价省去约一半的开方与标量乘法。以 $z_S = h_{s,-Q^*}(A^*) = t(Q^*, A^*)^{1/2}$ ——Sato 本人的配对——为目标、以 $t(Q, A) \in \{z_S^2, z_S^{-2}\}$ 为最终检验的同一运行，同样成功。因此，对带最终幂运算的配对，完整的 GPI 问题被从头到尾解决，计数与第 7 节的预测相符。

另外两条曲线。 上面的玩具曲线 $h = 1$ ，故第 8 节的第 9 行 ($[\ell]A = \mathcal{O}$) 从未被执行，且只有 $e = 6$ 。同样的检验在两条带余因子的曲线上重做： $q = 53$, $E: Y^2 = X^3 + X$, $\ell = 17$, $\#E(\mathbb{F}_q) = 68$, $h = 4$, $k = 8$, $e = 4$, $m = 2$ ($j = 1728$, 四次扭曲)；以及 $q = 103$, $E: Y^2 = X^3 + 4$, $\ell = 37$, $\#E(\mathbb{F}_q) = 111$, $h = 3$, $k = 12$, $e = 6$, $m = 2$ 。在两条曲线上： λ 的阶恰为 $e/2$ ； $1, \omega, \dots, \omega^{e/2-1}$ 是 $u \mapsto u^{q^m}$ 的特征向量，特征值为 λ^j ，且 $\ker L = W$ (引理 4.1)；命题 3.1 以符号 -1 成立；算法 5.1 在 30/30 个随机点对上恢复 $(\xi(A), \xi(Q))$ ；引理 3.3 与注 3.4 的封闭形式成立， $\text{ord}(h_{s,A}(Q)) = 2\ell$ ；(13) 的 κ' 分别为 3 与 8，且 $t(Q, A) = t(A, Q)^{\kappa'}$ ；命题 6.2 中映射的像的阶为 $\ell(s-1)$ ；第 8 节的算法以随机顺序在每条曲线的 5/5 个随机目标上成功，返回的点对均与 z 核验。第 9 行现已执行：在 $e = 4$ 曲线上，通过 Legendre 符号的 x_A 中，五次运行分别有 4/5、2/3、12/13、6/7 与 1/2 被 $[\ell]A \neq \mathcal{O}$ 拒绝 ($E(\mathbb{F}_q)$ 的 33 个横坐标中 $|\xi(G_1)| = 8$)；在 $e = 6$ 曲线上为 0/1、2/3、1/2、0/1 与 3/4 (55 个中 18 个)。

$e = 4$ 曲线揭示了 $e = 6$ 例子所掩盖的一个结构性事实：满足 $\beta \neq 0$ 的 $x_Q \in W$ 中，400/400 的 β 在 $\mathbb{F}_{q^{k/2}}$ 中为非平方，而 $e = 6$ 曲线上为 203/399。这正是注 4.4 的两种情形： $e = 4$ 时 Legendre 检验为空，全部筛选由 $[\ell]Q = \mathcal{O}$ 完成； $e = 6$ 时它淘汰约一半。

运算计数。 不作任何计时比较：在此规模下时间测量的是 GP 解释器，且两种代价关于 ℓ 的渐近性不同。在第 8 节的算法中，每个 x_A 耗费 $\mathbb{F}_q$ 中一次 Legendre 符号，通过者中的一半再耗费 $\mathbb{F}_q$ 中一次开方与一次 $[\ell]A$ ；每个 x_Q 耗费 $\mathbb{F}_{q^{k/2}}$ 中一次按注 4.4 经范数计算的 Legendre 符号 ($\mathbb{F}_{q^{k/2}}$ 中 $k/2 - 1$ 次 Frobenius 与 $k/2 - 1$ 次乘法，再加 $\mathbb{F}_q$ 中一次代价远小于 $1M$ 的 Jacobi 符号)， $e = 6$ 时淘汰约一半、 $e = 4$ 时不淘汰 (注 4.4)，幸存者再耗费 $\mathbb{F}_{q^k}$ 中一次开方与 $E(\mathbb{F}_{q^k})$ 上一次 $[\ell]Q$ ——在第 10 节的规模下 $e = 6$ 时每个 x_Q 平均约 2^{12} 次 $\mathbb{F}_{q^k}$ 中的乘法，即大致四次 Tate 配对， $e = 4$ 时为其两倍。在注 8.1 的循环中，每个 ζ 另需一次更新 ζ^{q^m} 的乘法、三到四次解码乘法以及含 1 的基下一次免费成员检验，上述开销仅对 $q^{1+k/e-k/2}$ 比例的 ζ 才会发生。[7, Alg. 6.1] 的内层步骤在 ℓ 为奇数时是在 $\mathbb{F}_{q^k}$ 上求 $g(T) = \gamma$ 的根， $\deg g = (\ell-1)/2$ ，此处为 48 ($\varphi = g(\xi)$)；99 次形式 $g(T)^2(T^3 + b) - \gamma^2$ 是 [7, eq. (6.1)] 在 ℓ 为偶数时的形式)。

10 与 [7] 的比较

命题 6.2 使改进因子逐项显式化。在 [7, Alg. 6.1] 中循环变量 γ 遍历 $\gamma_0 \mu_{(s-1)\nu}$ ，故 γ^ν 遍历陪集 $z^{-1} \mathbb{F}_{q^{k/2}}^\times$ ，每个值 ν 次，每步做一次 $(\ell-1)/2$ 次求根。该循环已经是对某个 $\mathbb{F}_{q^{k/2}}^\times$ 坐标的盲目遍历：由 [7, Thm. 5.3(ii)-(iii)]，在他的记号下 ($A \in G_0$, P 有理)， $\varphi(A+P)^\nu h_{s,-A}(P) \in \mathbb{F}_{q^{k/2}}^\times$ ，故 $\varphi(A+P)^\nu$ 是 $h_{s,-A}(P)^{-1} \in \mu_\ell$ 与某元素 $c_{A,P} \in \mathbb{F}_{q^{k/2}}^\times$ 之积——即命题 6.2 的分裂 $\mu_{\ell(s-1)} \cong \mu_\ell \times \mu_{s-1}$ ，只是用于 $\varphi(A+P)^\nu$ 而非 v_0 。他的 c 是 μ_{s-1} 分量，而以 $\varphi(kR)^\nu = c/z$ 对 γ 的循环将 μ_ℓ 分量固定为 z^{-1} 并遍历另一分量，后者不携带关于 z 的任何信息。本方法 (i) 消除了 ν 重冗余——以坐标本身为循环变量，其中 d 次根唯一 (引理 3.5)；(ii) 消除了求根——坐标到两个横坐标的解码是多项式时间的 (算法 5.1)；(iii) 借助扭曲将坐标从 $\mathbb{F}_{q^{k/2}}^\times$ 缩小到 $\mathbb{F}_q \oplus W$ (引理 4.1)；(iv) 在触及 W 之前先用 Legendre 符号检验 x_A 是否属于 $\xi(G_1)$ ，即第 8 节的分块顺序。四个因子为 $\nu \approx s/\ell$ 、 $\tilde{O}(\ell)$ 、 $q^{k/2-1-k/e}$ 与约 q/ℓ ；其乘积为 $q^{k-k/e}/\ell$ (忽略常数与对数)，即下表前两列之比。用生成元的倍点搜索 G_0 而非扫描 W ，则将坐标再缩小至 ℓ 个点，即最后一列。这条链中没有任何环节在最终检验之前使用 z ，而由命题 6.2，此路线上的任何环节都不可能使用。

由此，范数路线所做的工作可以精确陈述。在 $\ell \mid d$ 的 Tate 取向，原始 Miller 值的歧义——一个大小为 $(s-1)\nu$ 的陪集——在取范数后缩小 ν 倍；将 ζ 解码为两个横坐标即使在二者均未知时也成为多项式时间（引理 4.1）；而剩余坐标与目标无关（命题 6.2），故第 8 节的循环，或注 8.1 中被占优的循环，对其无引导地遍历。

与 [7, Alg. 6.1] 的比较必须在同一约定下进行——期望对期望。对常曲线上的 [7, Alg. 6.1]，每次迭代的成功概率至多为 $(\ell-1)/((s-1)\nu)$ [7, Rem. 6.5]，每次迭代是在 $\mathbb{F}_{q^k}$ 上一次 $(\ell-1)/2$ 次的求根；故期望代价至少为 $\frac{(s-1)\nu}{\ell-1} \cdot \tilde{O}(\ell) \approx \tilde{O}((q^k-1)/\ell)$ 。对第 8 节的算法，期望候选数为 $q^{k/e}/2$ ， $e=6$ 时每个平均耗费约四次配对（昂贵的一半约八次）， $e=4$ 时约八次；对注 8.1 中对 $\mathbb{F}_{q^{k/2}}^\times$ 的循环，则为 $\frac{2(s-1)}{\ell-1}$ 步，每步 $\mathbb{F}_{q^{k/2}}$ 中几次乘法（第 9 节）。为便于同类比较，下表采用单一单位 M ： $\mathbb{F}_{q^k}$ 中一次乘法。所用换算为：在此规模下， $\mathbb{F}_{q^k}$ 中一次开方与 $E(\mathbb{F}_{q^k})$ 上一次乘以 ℓ 的标量乘法各约 $2^{12}M$ ；循环长度 ℓ 、 $A \in E(\mathbb{F}_q)$ 、使用稀疏直线函数与分圆最终幂运算的 Tate 配对约 $2^{10}M$ ； $\mathbb{F}_{q^{k/2}}$ 中一次乘法约 $1M$ ；注 4.4 的 Legendre 符号约 $k/2 M$ ； $\mathbb{F}_{q^k}$ 上 d 次求根约 $d \log_2(q^k) M$ 。所有条目均为期望值，且它们是示意性的而非基准测量：上述每项换算仅在一个小因子内准确，指数继承了这一误差。稳健的是各列之间的比值 $q^{k-k/e}/\ell$ （忽略常数与对数），而非绝对数值。

曲线	[7, Alg. 6.1]	本文（第 8 节）	注 8.1	穷举搜索
BN254 (alt_bn128)	$2^{2800} M$	$2^{518} M$	$2^{1271} M$	$2^{263} M$
BLS12-381	$2^{4325} M$	$2^{772} M$	$2^{2032} M$	$2^{264} M$

两点保留。SatoH 的概率界是上界，故其真实期望代价可能更大，这只会扩大差距。且比较之所以合法，是因为在第 15 行取 $e := h_{s,-Q}(A)$ 时，算法解决的正是 [7, Alg. 6.1] 的那个问题——第 9 节在玩具曲线上已予演示——而非一个子程序替换了另一个。

11 局限

1. 本方法要求偶数扭曲次数 $e \geq 4$ （注 4.2）与 $k > 2$ （注 4.3）。因此它不适用于 [7] 得到常数迭代次数的超奇异曲线；它恰恰适用于 [7] 认定为无望的那个区域。
2. 对固定的 A 直接在 G_0 中搜索，期望代价为 $\ell/2$ 次配对求值，在两条曲线上约 $2^{263}M$ 与 $2^{264}M$ ：比第 8 节的算法低约 $4q^{k/e}/\ell$ 即 2^{256} 与 2^{509} 倍； μ_ℓ 中的离散对数（特殊 TNFS 下约 2^{100} 与 2^{126} ）更为便宜。SatoH 对其自身算法也作了同样的观察。本改进缩小了差距但未将其消除。
3. 通过迹与范数利用 $\xi(G_0) \subset \mathbb{F}_{q^{k/2}}$ 归功于 [1]，其到指数 $q-1$ 的归约在固定参数框架下强于此处所得的一切。本文在这一点上声称的新意是该机制在过渡到两个未知参数时得以保留；其他贡献已在引言中列出。
4. 循环仅在最终检验中使用 z ，命题 6.2 说明了原因：任何建立在范数之上的东西都无法不如此。真正的 Ate 循环 $T = t - 1$ 的关系 (8) 也不是出路，因为它化为 $d = h\ell$ 时的命题 3.1（注 3.2）。SatoH 本人的分解也不例外：[7, Thm. 5.5] 中的常数 $c \in \mathbb{F}_{q^{k/2}}^\times$ 是同一中国剩余分裂（第 10 节）下 $\varphi(A+P)^\nu$ 的 μ_{s-1} 分量——而非 v 的， v 在其循环长度下范数为 1（注 3.2）；附带地， $(\varphi(A+P)^\nu)^{s+1} = c_{A,P}^2$ 。它出于同一原因与 z 无关，而他对定理 5.5(iii) 的证明所援引的事实 $\mu_\ell \cap \mathbb{F}_{q^{k/2}}^\times = \{1\}$ 正是该原因的推论；故他对 c 的循环同样从 z 得不到任何信息。我不知道任何避开该坐标的原始值分解；是否存在这样的分解，是留下的开放问题。

参考文献

- [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.