

Une méthode plus rapide pour l'inversion généralisée de couplage

Lael Cellier

lael.cellier@laposte.net

5 octobre 2026

Résumé

Satoh a récemment proposé un algorithme pour le problème d'inversion généralisée de couplage (GPI) qui exploite la structure de la fonction de Miller plutôt que la recherche exhaustive ou un oracle à argument fixé. Sur une courbe ordinaire, son coût espéré est de l'ordre de $(q^k - 1)/\ell^2$ appels à une recherche de racines de degré $\Omega(\ell)$, soit $\tilde{O}((q^k - 1)/\ell)$ opérations. Je donne une méthode différente pour le même problème, valable pour les courbes ordinaires de degré de plongement pair $k > 2$ admettant une tordue de degré pair $e \geq 4$, dont le coût espéré est de $q^{k/e}/2$ candidats coûtant chacun quelques couplages : mesuré en multiplications dans $\mathbb{F}_{q^k}$, le gain sur l'algorithme de Satoh est un facteur $q^{k-k/e}/\ell$ aux constantes et logarithmes près. L'analyse utilise une boucle de Miller de longueur multiple de ℓ , comme le couplage de Tate, tandis que la boucle de Satoh a pour longueur $q^{k/2} \equiv -1 \pmod{\ell}$; le couplage cible n'intervient qu'à travers un test final d'appartenance, de sorte que l'algorithme résout GPI pour le couplage de Satoh directement, sans conversion entre couplages ni logarithme discret nulle part. La valeur de couplage réduite et la norme de la valeur de Miller brute sont des coordonnées indépendantes, fait de restes chinois puisque $\gcd(\ell, q^{k/2} - 1) = 1$; la méthode est en conséquence une recherche sur les paires d'abscisses avec un test de couplage final, et je ne prétends pas autre chose : le cœur technique — une inversion en temps polynomial de la valeur de Miller brute à deux arguments inconnus — sert à fixer cet espace de recherche et à montrer que rien sur cette voie ne peut le réduire. Le test prend en entrée la valeur de Miller brute avant l'exponentiation finale — la même entrée que l'algorithme d'inversion de Miller de Satoh lui-même, qu'aucun protocole n'expose ; passer de la valeur réduite à celle-ci est l'étape d'inversion de l'exponentiation de Galbraith, Hess et Vercauteren, que les sections 6–8 traitent par recherche et que la proposition 6.2 montre impossible à raccourcir par la norme — et combine la relation de norme du travail antérieur de Satoh sur l'inversion de Miller avec une projection $\mathbb{F}_q$ -linéaire séparant les deux abscisses inconnues, qui vivent dans des sous-espaces $\mathbb{F}_q$ -complémentaires de $\mathbb{F}_{q^{k/2}}$; l'exploitation de cette structure de sous-corps remonte à Akagi et Nogami, dont la réduction exige toutefois qu'un argument soit connu. Sur BN254 le coût espéré passe d'environ 2^{2800} à 2^{518} multiplications dans $\mathbb{F}_{q^k}$, sur BLS12-381 d'environ 2^{4325} à 2^{772} . Tous ces chiffres restent très au-dessus du coût du calcul d'indice dans $\mathbb{F}_{q^k}$; le résultat est structurel, non cryptanalytique.

1 Introduction

Galbraith, Hess et Vercauteren [3] ont isolé trois problèmes d'inversion pour un couplage bilinéaire $e: G_1 \times G_0 \rightarrow \mu_\ell$: les deux problèmes à argument fixé FAPI-1 et FAPI-2, où l'un des arguments est donné, et le problème généralisé GPI, où seule la cible z est donnée et où toute paire de préimages est admissible.

Satoh [7] a observé qu'aucun algorithme n'était connu qui exploite la structure mathématique du calcul du couplage, par opposition à une recherche dans l'un des groupes, et en a donné un : en écrivant la ℓ -ième fonction de Miller comme un système de facteurs, il obtient une décomposition du couplage Ate à partir de laquelle une solution de GPI s'assemble par une étape de recherche de racines. La procédure obtenue [7, Alg. 6.1] parcourt $\gamma \in \mu_{\nu(s-1)}$, où $s = q^{k/2}$ et $\nu = (s + 1)/N$, et cherche à chaque pas les

racines d’une fonction φ de degré $(N - 1)/2$. Sur une courbe ordinaire, $\nu(s - 1) = (q^k - 1)/\ell$ et la probabilité de succès par pas est au plus $(\ell - 1)/((s - 1)\nu)$ [7, Rem. 6.5], de sorte que le coût espéré est de l’ordre de $(q^k - 1)/\ell^2$ recherches de racines de degré $\ell/2$, soit $\tilde{O}((q^k - 1)/\ell)$ opérations ; Satoh décrit ce cas comme « trop inefficace même pour des expériences numériques à petites valeurs de q ».

Cette note donne une méthode différente pour le même problème, de coût espéré plus petit. C’est, comme celle de Satoh, une recherche aveugle avec un test de couplage final — ici sur les paires d’abscisses — et la proposition 6.2 montre pourquoi rien de bâti sur la norme de la valeur de Miller ne peut être autre chose : la valeur de couplage réduite et cette norme sont des coordonnées indépendantes. Deux points de cadrage sont essentiels et sont énoncés d’emblée.

Longueur de boucle. La méthode prend la fonction de Miller $h_{d,A}$ en l’argument $\mathbb{F}_q$ -rationnel $A \in G_1$, évaluée en l’argument de trace nulle $Q \in G_0$, avec une longueur de boucle d multiple de ℓ — le cadre de Tate. L’algorithme 6.1 de Satoh produit $h_{q^{k/2}, -A}(Q)$, fonction de Miller en l’argument de trace nulle et boucle de longueur $s = q^{k/2}$. La distinction qui compte n’est pas l’orientation mais le résidu de la longueur de boucle modulo ℓ : la relation de norme sur laquelle repose cette note (proposition 3.1) donne $(\xi(Q) - \xi(A))^d$ lorsque $d \equiv 0 \pmod{\ell}$, et $(\xi(Q) - \xi(A))^{d-1}$ lorsque $d \equiv -1 \pmod{\ell}$, ce qui pour $d = s$ vaut identiquement 1 (remarque 3.2). La présente méthode ne remplace donc *pas* l’étape interne de [7, Alg. 6.1], et je ne prétends pas qu’elle le fasse. Ce qui est vrai, c’est que le couplage cible n’intervient dans la méthode qu’à travers un test final d’appartenance, de sorte qu’on peut le prendre égal au couplage de Satoh lui-même (section 6) ; aucune conversion entre couplages, et en particulier aucun logarithme discret, n’intervient nulle part.

Ce qui est nouveau. Le cœur de la méthode est une procédure en temps polynomial qui, à partir d’une valeur de Tate–Miller brute $h_{d,A}(Q)$ avec A et Q inconnus, récupère A et Q (section 5). Elle combine la relation de norme utilisée par Satoh dans le cadre à argument fixé [6] avec une projection linéaire séparant les deux abscisses inconnues, qui vivent dans des sous-espaces $\mathbb{F}_q$ -complémentaires de $\mathbb{F}_{q^{k/2}}$ (section 4). Cette structure de sous-corps fut exploitée en premier par Akagi et Nogami [1], qui ramènent le problème d’inversion d’exponentiation à l’exposant $q - 1$ pour FAPI-2 en formant le polynôme minimal de l’abscisse *donnée* ; leur construction requiert $\text{Tr}(\xi(Q)^3)$ et $N(\xi(Q))$ et ne se transporte pas au cas où Q est inconnu. Le passage de « une inconnue, polynôme minimal » à « deux inconnues, projection linéaire » est la nouveauté technique. Autour d’elle, la note ajoute l’indépendance de la valeur de couplage et de la norme (proposition 6.2), qui fixe l’espace de recherche et montre qu’il ne peut être réduit sur cette voie ; les formes closes des valeurs de Miller de longueurs de boucle s et q comme puissances du couplage de Tate réduit (lemme 3.3, remarque 3.4), qui permettent à l’algorithme de viser directement les couplages de Satoh ; et un décompte de l’amélioration sur [7, Alg. 6.1] en quatre facteurs, chacun attribué à l’un de ces résultats (section 10).

Je note en passant que GPI n’est pas sans conséquence cryptographique : une preuve Groth16 [5] est acceptée dès qu’une unique équation produit de couplages est vérifiée, et poser son troisième élément égal à $\mathcal{O}$ laisse une valeur cible calculable à partir de la seule clé de vérification et de l’entrée publique, si bien que toute solution de GPI fournit une forge pour un énoncé arbitraire.

2 Cadre et notations

Soit q une puissance d’un premier impair et $E/\mathbb{F}_q$ une courbe elliptique ordinaire de modèle de Weierstrass court $Y^2 = X^3 + a_4X + a_6$. Soit ℓ un premier impair avec $\ell \parallel \#E(\mathbb{F}_q)$ — divisibilité exacte, $\ell \mid \#E(\mathbb{F}_q)$ et $\ell^2 \nmid \#E(\mathbb{F}_q)$, de sorte que $h := \#E(\mathbb{F}_q)/\ell$ est premier à ℓ , ce dont le lemme 6.1 a besoin — de degré de plongement pair $k > 2$; comme $k = \text{ord}_\ell(q)$ divise $\ell - 1$, on a automatiquement $\ell \nmid k$. Suivant [7, §5] je pose

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

de sorte que $G_0 \cong G_1 \cong \mathbb{Z}/\ell\mathbb{Z}$, $G_0 \cap G_1 = \{\mathcal{O}\}$ et $E[\ell] = G_1 \oplus G_0$. Comme $\ell \mid s + 1$, on a $\text{Fr}_q^{k/2} P = -P$ pour $P \in G_0$; et comme $\ell \nmid s - 1$, $\text{Fr}_q^{k/2}$ n’a pour valeurs propres que 1 sur G_1 et -1 sur

G_0 , d'où

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

ξ, η désignent les fonctions coordonnées, $\tau := -\xi/\eta$ l'uniformisante en $\mathcal{O}$, et $h_{n,A}$ la n -ième fonction de Miller normalisée en A , c'est-à-dire la fonction telle que $\mathrm{div} h_{n,A} = n[A] - [nA] - (n-1)[\mathcal{O}]$ et $\mathrm{lc}_{\mathcal{O}}(h_{n,A}) = 1$ relativement à τ .

Partout, $A \in G_1$, $Q \in G_0$, et d est un entier avec

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

lorsqu'une racine d -ième doit être extraite (lemme 3.5) je suppose de plus $d \mid s+1$, la seconde condition de [6, Alg. 4.1]. La valeur de Miller brute est $v := h_{d,A}(Q) \in \mathbb{F}_{q^k}^\times$ et le couplage de Tate réduit est $t(A, Q) := h_{\ell,A}(Q)^{(q^k-1)/\ell} \in \mu_\ell$, bilinéaire et non dégénéré sur $G_1 \times G_0$.

3 La relation de norme

Proposition 3.1. *Avec les notations ci-dessus, en n'utilisant que $\ell \mid d$,*

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

En particulier $v^{s+1} = -(\xi(Q) - \xi(A))^\ell$ pour $d = \ell$.

Démonstration. Comme $\ell \mid d$ et $A \in E[\ell]$, $[d]A = \mathcal{O}$ et $\mathrm{div} h_{d,A} = d([A] - [\mathcal{O}])$; de même $\mathrm{div} h_{d,-A} = d([-A] - [\mathcal{O}])$. Donc $h_{d,A}h_{d,-A}$ et $(\xi - \xi(A))^d$ ont le même diviseur $d([A] + [-A] - 2[\mathcal{O}])$, et toutes deux ont pour coefficient dominant 1 en $\mathcal{O}$ puisque $\xi = \tau^{-2} + O(\tau^{-1})$; ainsi

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

Ensuite, $h_{d,A} \circ [-1]$ et $h_{d,-A}$ ont le même diviseur; comme $\tau \circ [-1] = -\tau$ pour un modèle de Weierstrass court et $\mathrm{ord}_{\mathcal{O}} h_{d,A} = -d$, on a $\mathrm{lc}_{\mathcal{O}}(h_{d,A} \circ [-1]) = (-1)^d$, d'où

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

Enfin $h_{d,A}$ est définie sur $\mathbb{F}_q$ et $\mathrm{Fr}_q^{k/2} Q = -Q$, donc $v^s = h_{d,A}(\mathrm{Fr}_q^{k/2} Q) = h_{d,A}(-Q) = (-1)^d h_{d,-A}(Q)$ par (5), et $v^{s+1} = v \cdot v^s = (-1)^d (h_{d,A} h_{d,-A})(Q)$, ce qui est (3) par (4). $\square$

Le membre de droite de (3) ne contient aucune valeur de Miller. Comparer avec la factorisation $h_{s+1,A} = (\xi - \xi(A)) h_{s,A}$ qui sous-tend [6, Alg. 4.1] : là, le facteur $h_{s,A}(Q)$ est éliminé par une puissance $(s+1)$ -ième. Sa structure exacte est donnée par le lemme 3.3 : $h_{s,A}(Q) = -t(A, Q)^{-1/2}$, élément d'ordre exactement 2ℓ divisant $s+1$, dont l'opposé $-h_{s,A}(Q) = t(A, Q)^{-1/2}$ appartient à μ_ℓ ; avec la fonction de Miller en l'argument de trace nulle on obtient au contraire $h_{s,Q}(A) = t(Q, A)^{-1/2} \in \mu_\ell$, ce qui est l'énoncé de [4] dans ce cadre, avec sa forme close. C'est le phénomène que Satoh décrit par « (valeur avant exponentiation finale) = (fonction simple) $\times$ (un autre couplage) ». Deux remarques sur la constante. D'abord, c'est un signe connu, non une quantité à précalculer. Ensuite, les implémentations qui ne normalisent pas la fonction de Miller en $\mathcal{O}$ (`elltatepairing` de PARI/GP en est une) la remplacent par une autre constante; qu'elle soit à nouveau indépendante de A et Q est une observation empirique sur la normalisation des fonctions de droite de PARI, faite sur la courbe jouet de la section 9, et elle se lit alors sur une seule paire connue.

Remarque 3.2 (Longueur de boucle, non orientation). Pour une longueur de boucle n quelconque avec $[n]P \neq \mathcal{O}$, le même calcul de diviseurs donne, exactement et sans signe,

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

les deux membres ayant coefficient dominant 1 en $\mathcal{O}$; (6) vaut pour P dans l'un ou l'autre groupe. (Le signe de (5) est $(-1)^{\text{ord } h_{n,P}}$, soit $(-1)^{n-1}$ lorsque $[n]P \neq \mathcal{O}$ et $(-1)^n$ lorsque $\ell \mid n$; il n'intervient que si l'on évalue $h_{n,P}$ en $-R$ au lieu de $h_{n,-P}$ en R .) Trois résidus de n modulo ℓ importent.

Si $n \equiv 0 \pmod{\ell}$, le dénominateur vaut 1 et la relation de norme restitue $(\xi - \xi(P))^n$: c'est la proposition 3.1, et elle vaut dans les deux orientations. Dans l'orientation Ate, $\text{Fr}_q^{k/2}$ agit sur les coefficients de $h_{n,Q}$ et l'envoie sur $h_{n,-Q}$, sans évaluation en un point opposé et donc sans signe, de sorte que

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

les deux normes coïncident.

Si $n \equiv -1 \pmod{\ell}$, alors $[n]P = -P$ et (6) devient $(\xi - \xi(P))^{n-1}$. Pour $n = s$ l'exposant $s - 1$ annule $\mathbb{F}_{q^{k/2}}^\times$, donc $h_{s,P}(R)^{s+1} = 1$ identiquement et aucune information sur les abscisses ne survit; c'est la boucle utilisée par [7, Alg. 6.1] dans le cas ordinaire, et c'est pourquoi cet algorithme ne peut pas être alimenté par le présent test. Pour les autres $n \equiv -1 \pmod{\ell}$, p. ex. $n = 2\ell - 1$, la norme n'est pas triviale, mais elle ne détermine ζ qu'à $\gcd(n - 1, s - 1)$ candidats près : 48 sur la courbe jouet, et $48u \approx 2^{67,7}$ sur BN254 (calculé pour cette courbe; en général $\gcd(2\ell - 2, s - 1)$ est un multiple de $\gcd(\ell - 1, q - 1) = 6u$, les cofacteurs $6u^3 + 6u^2 + 3u + 1$ et $6u^3 + 6u^2 + 4u + 1$ étant premiers entre eux, et le facteur 8 vient des autres facteurs de $s - 1$). L'unicité de la racine est exactement ce qu'achète $\ell \mid d \mid s + 1$ via $\gcd(d, s - 1) = \gcd(d, 2)$ (lemme 3.5), et exactement ce que perd $n \equiv -1 \pmod{\ell}$.

Si $n \equiv q \pmod{\ell}$, comme pour la boucle Ate $T = t - 1$ avec $P = Q \in G_0$, alors $[n]Q = \text{Fr}_q Q$ et

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

à nouveau sans signe. Comme $\xi(A) \in \mathbb{F}_q$, le dénominateur vaut $(\xi(A) - \xi(Q))^q$, de sorte que (8) se réduit à $(\xi(A) - \xi(Q))^{T-q} = (\xi(A) - \xi(Q))^{-h\ell}$ avec $h = \#E(\mathbb{F}_q)/\ell$: c'est la puissance $(-h)$ -ième de (7) — pas de signe, une inversion — et elle porte la même information que la proposition 3.1 avec $d = h\ell$, qui n'a besoin que de $\ell \mid d$. (De façon cohérente, $h_{q,Q} = h_{T,Q} h_{\ell,Q}^h$ en tant que fonctions normalisées, et $h_{q,Q}(A)^{s+1} = 1$.) Toutes les identités de cette remarque ont été vérifiées numériquement (section 9).

Lemme 3.3. *Pour $P \in E[\ell]$, en tant que fonctions rationnelles,*

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

De plus, pour $A \in G_1$ et $Q \in G_0$ non nuls, $t(\cdot, \cdot)$ désignant le couplage de Tate réduit dans l'un ou l'autre ordre des arguments,

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

de sorte que $h_{s,A}(Q) = -t(A, Q)^{-1/2}$ et $h_{s,Q}(A) = t(Q, A)^{-1/2}$, les racines carrées étant les uniques racines dans μ_ℓ . En particulier $h_{s,Q}(A) \in \mu_\ell$ est d'ordre exactement ℓ , et $h_{s,A}(Q)$ est d'ordre exactement 2ℓ , avec $2\ell \mid s + 1$.

Démonstration. La règle de composition $h_{mn,P} = h_{m,P}^n h_{n,[m]P}$ (mêmes diviseurs, deux membres normalisés) donne, en calculant $h_{\ell s,P}$ de deux façons, $h_{s,P}^\ell h_{\ell,[s]P} = h_{\ell,P}^s h_{s,[\ell]P}$; comme $[s]P = -P$ et $h_{s,\mathcal{O}} = 1$, c'est (9). En évaluant : en orientation Ate, $h_{\ell,Q}(A)^s = \text{Fr}_q^{k/2}(h_{\ell,Q}(A)) = h_{\ell,-Q}(A)$ par conjugaison des coefficients, donc $h_{s,Q}(A)^\ell = 1$; en orientation Tate, $h_{\ell,A}(Q)^s = h_{\ell,A}(-Q) = -h_{\ell,-A}(Q)$ par (5) avec ℓ impair, donc $h_{s,A}(Q)^\ell = -1$.

Pour (10), la même règle avec $[\ell]A = [s + 1]A = \mathcal{O}$ donne $h_{\ell,A}^c = h_{\ell c,A}$ pour tout c et $h_{(s+1)(s-1),A} = h_{s+1,A}^{s-1}$, tandis que les diviseurs donnent $h_{s+1,A} = (\xi - \xi(A)) h_{s,A}$. Ainsi, avec $\zeta = \xi(Q) - \xi(A) \in \mathbb{F}_{q^{k/2}}^\times$,

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

la dernière étape parce que $h_{s,A}(Q)^{2\ell} = 1$ et $2\ell \mid s+1$. Le cas Ate est identique en échangeant A et Q . Comme ℓ est impair, l'élévation au carré est une bijection de μ_ℓ , ce qui fixe les racines carrées ; le signe de $h_{s,A}(Q)$ est imposé par $h_{s,A}(Q)^\ell = -1$. Enfin $t(A, Q) \neq 1$ par non-dégénérescence, donc $h_{s,A}(Q)^2 \neq 1$ et l'ordre est exactement 2ℓ , et non 2 ; de même $h_{s,Q}(A) \neq 1$ et son ordre est exactement ℓ . $\square$

Quatre conséquences. D'abord, la valeur de Miller de longueur de boucle s est le couplage de Tate réduit, à l'exposant $-1/2$ près et sans exponentiation finale : le « another pairing » de Satoh est littéral. Elle est bilinéaire en ses deux arguments en tant que valeur de Miller brute, ce qui a été vérifié directement (section 9). Ensuite, le signe est une fois de plus le $(-1)^\ell$ de (5), le mécanisme de (7) ; (9) donne en deux lignes l'énoncé de [4] en orientation Ate. Enfin, la proposition 3.1 pour $d = \ell$ est la même identité relue : $h_{\ell,A}(Q)^{s+1} = h_{s+1,A}(Q)^\ell = \zeta^\ell h_{s,A}(Q)^\ell = -\zeta^\ell$. Enfin, la même règle donne la valeur pour la longueur de boucle q , remarque 3.4.

Remarque 3.4 (Longueur de boucle q). La même règle de composition, appliquée à $h_{q^k,Q}$, donne $h_{q^k,Q} = \prod_{i=0}^{k-1} h_{q,[q^i]Q}^{q^{k-1-i}}$, et comme $[q^i]Q = \text{Fr}_q^i Q$ et A est rationnel, $h_{q,\text{Fr}_q^i Q}(A) = h_{q,Q}(A)^{q^i}$, d'où $h_{q^k,Q}(A) = h_{q,Q}(A)^{kq^{k-1}}$. D'autre part $\text{div } h_{q^k,Q} = (q^k - 1)([Q] - [\mathcal{O}]) = \text{div } h_{\ell,Q}^{(q^k-1)/\ell}$, donc $h_{q^k,Q}(A) = t(Q, A)$. Cela seul donne $h_{q,Q}(A) \in \mu_{k\ell}$; l'appartenance à μ_ℓ découle de la même règle appliquée à $h_{q\ell,Q}$, $h_{q,Q}^\ell h_{\ell,[q]Q} = h_{\ell,Q}^q$, puisque $h_{\ell,Q}(A)^q = h_{\ell,\text{Fr}_q Q}(A)$ et $[q]Q = \text{Fr}_q Q$, d'où $h_{q,Q}(A)^\ell = 1$. Ainsi, la racine étant unique dans μ_ℓ ,

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

la dernière forme parce que $q^{k-1} = s q^{k/2-1} \equiv -q^{k/2-1} \pmod{\ell}$ (et $\ell \nmid k$, section 2). La cible de [7, Alg. 6.6], l'enveloppe à boucle q de son algorithme 6.1, est $h_{q,-Q}(A) = t(Q, A)^{1/(kq^{k/2-1})}$ dans les notations de cette note ($h_{q,Q}(A)$ est bilinéaire en Q , étant une puissance fixe de t) ; un test final $t(Q, A) = z^{-kq^{k-1}}$ à la ligne 15 de la section 8 résout donc aussi ce problème directement. (Vérifié numériquement, section 9.)

Lemme 3.5. Soit $d \mid s+1$. Alors $\gcd(d, s-1) = \gcd(d, 2)$, et pour $u \in \mathbb{F}_{q^{k/2}}^\times$ l'équation $\zeta^d = u$ a soit aucune solution, soit exactement $\gcd(d, 2)$ solutions dans $\mathbb{F}_{q^{k/2}}^\times$. Lorsqu'elle est résoluble :

1. si d est impair, la solution est unique et vaut $u^{d^{-1} \bmod (s-1)}$;
2. si d est pair, les solutions sont $\pm \zeta_0$ pour n'importe quelle solution ζ_0 , que l'on obtient en écrivant $d = 2^a d'$ avec d' impair, en posant $u_1 := u^{d'^{-1} \bmod (s-1)}$ et en extrayant a racines carrées successives de u_1 dans $\mathbb{F}_{q^{k/2}}$ par n'importe quel algorithme standard.

Démonstration. Classique : s est impair, donc $\gcd(s+1, s-1) = 2$ et $\gcd(d, s-1) \mid 2$, et le reste est le décompte des solutions de $\zeta^d = u$ dans un groupe cyclique, comme dans la preuve de [6, Thm. 4.2]. Seul le cas (i) sert ci-dessous, d étant impair partout. $\square$

Pour $d = \ell$ impair, le cas (i) s'applique. Le cas (ii) est l'ambiguïté de signe visible dans [6, Alg. 4.1, étapes 3–4], où deux abscisses $\xi(A) \pm u$ sont produites ; il double le coût et rien de plus.

4 Le lemme de séparation

Supposons que E admette une tordue E' de degré $e \mid k$, et posons $m := k/e$. Comme k est pair, $e \geq 3$ signifie $e \in \{4, 6\}$: une tordue $e = 3$ force $j(E) = 0$ et $6 \mid k$, donc l'existence d'une tordue sextique, de sorte que $e = 3$ n'est jamais le degré de tordue maximal et je prends e pair partout. La tordue est définie sur $\mathbb{F}_{q^m}$ par un paramètre $\theta \in \mathbb{F}_{q^m}^\times$ dont la classe engendre $\mathbb{F}_{q^m}^\times / (\mathbb{F}_{q^m}^\times)^e$, choisie parmi les $\varphi(e)$ classes possibles comme celle pour laquelle $\ell \mid \#E'(\mathbb{F}_{q^m})$ (la tordue de type D ou de type M,

dans la terminologie usuelle), et l'isomorphisme de tordue $\psi: E' \rightarrow E$ envoie (x', y') sur $(\omega x', \omega^{3/2} y')$ avec $\omega := \theta^{2/e}$. Comme $G_0 = \psi(E'(\mathbb{F}_{q^m})[\ell])$,

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

un $\mathbb{F}_q$ -sous-espace de dimension $m = k/e$, contenu dans $\mathbb{F}_{q^{k/2}}$ puisque e est pair. (De façon cohérente, $\xi(P) \in \mathbb{F}_{q^{k/2}}$ car ξ est paire et $\text{Fr}_q^{k/2}$ agit comme $[-1]$ sur G_0 , [7, Lem. 5.2].) De l'autre côté, $\xi(A) \in \mathbb{F}_q$ pour $A \in G_1$.

Lemme 4.1 (Séparation). *Supposons $e \in \{4, 6\}$ et posons $\lambda := \omega^{q^m-1}$. Alors $\omega \notin \mathbb{F}_{q^m}$, donc $\lambda \neq 1$ et $\mathbb{F}_q \cap W = \{0\}$; de plus $\lambda \in \mathbb{F}_{q^{k/2}}$, puisque $\lambda = \xi(Q_0)^{q^m} / \xi(Q_0)$ pour tout $Q_0 \in G_0 \setminus \{\mathcal{O}\}$ et $\xi(Q_0) \in \mathbb{F}_{q^{k/2}}$, de sorte que l'application $\mathbb{F}_q$ -linéaire*

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

est bien définie, vérifie $\ker L = W$ et $L|_{\mathbb{F}_q} = (1 - \lambda) \text{id}$; et pour $\zeta := \xi(Q) - \xi(A)$ avec $\xi(Q) \in W$, $\xi(A) \in \mathbb{F}_q$,

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

Démonstration. Si $\omega \in \mathbb{F}_{q^m}$ alors $\theta^2 = \omega^e \in (\mathbb{F}_{q^m}^\times)^e$, donc la classe de θ est d'ordre divisant 2 dans un groupe cyclique d'ordre e où elle est d'ordre e ; donc $e \mid 2$, contre $e \geq 4$. Ainsi $\omega \notin \mathbb{F}_{q^m}$, i.e. $\lambda \neq 1$. Si $a \in \mathbb{F}_q \cap W$ avec $a \neq 0$ alors $a = \omega x'$ avec $x' \in \mathbb{F}_{q^m}^\times$ et $\omega = a/x' \in \mathbb{F}_{q^m}$, contradiction; donc $\mathbb{F}_q \cap W = \{0\}$. L est $\mathbb{F}_q$ -linéaire car $u \mapsto u^{q^m}$ l'est; pour $u = \omega x' \in W$, $u^{q^m} = \omega^{q^m} x' = \lambda u$, donc $L(u) = 0$, i.e. $W \subseteq \ker L$. Réciproquement, $\omega^{e/2} = \theta$, et $X^{e/2} - \theta$ est irréductible sur $\mathbb{F}_{q^m}$: son degré $e/2 \in \{2, 3\}$ est premier et θ n'est pas une puissance $(e/2)$ -ième, sans quoi θ^2 serait une puissance e -ième et la classe de θ serait d'ordre divisant 2. Ainsi $1, \omega, \dots, \omega^{e/2-1}$ est une $\mathbb{F}_{q^m}$ -base de $\mathbb{F}_{q^{k/2}}$ (noter $[\mathbb{F}_{q^{k/2}} : \mathbb{F}_{q^m}] = e/2$), formée de vecteurs propres de $u \mapsto u^{q^m}$ de valeurs propres λ^j , $0 \leq j < e/2$, deux à deux distinctes car $\lambda \neq 1$ et $\lambda^{e/2} = \theta^{q^m-1} = 1$ avec $e/2$ premier. Donc $u \mapsto u^{q^m}$ est diagonalisable et $\ker L$ est son espace propre pour λ , qui est $\omega \mathbb{F}_{q^m} = W$. Pour $a \in \mathbb{F}_q$, $a^{q^m} = a$, donc $L(a) = (1 - \lambda)a$. En appliquant L à ζ on obtient $L(\zeta) = -(1 - \lambda)\xi(A)$, ce qui est (12). $\square$

Remarque 4.2. Pour $e = 2$ on a $m = k/2$ et $W = \omega \mathbb{F}_{q^{k/2}} = \mathbb{F}_{q^{k/2}}$: la projection dégénère ($\lambda = 1$, $L = 0$), mais rien n'échoue — $\xi(A) \in \mathbb{F}_q$ n'a toujours que q valeurs possibles, de sorte que l'étape 3 de l'algorithme 5.1 devient une boucle sur $x_A \in \mathbb{F}_q$ avec $x_Q = \zeta + x_A$, au coût $O(q)$ au lieu de $O(1)$, et l'algorithme de la section 8 parcourt $\mathbb{F}_q \times \mathbb{F}_{q^{k/2}}$ au coût $q^{k/e}/2 = q^{k/2}/2$ de sa formule générale. Le décodage en $O(1)$ exige donc les tordues quartiques ou sextiques — BN et BLS12 ($e = 6$), KSS16 ($e = 4$), les courbes de Brezing–Weng de [1] — et non les courbes ne portant qu'une tordue quadratique.

Remarque 4.3. Pour $k = 2$, en particulier pour les courbes supersingulières de [7, §4] où $t = 0$ force $k \leq 2$, on a $s = q$ et les deux abscisses appartiennent à $\mathbb{F}_q$: aucune application $\mathbb{F}_q$ -linéaire ne les sépare. C'est, à mon sens, la raison structurelle pour laquelle [6] (FAPI, un argument connu, temps polynomial) et [7] (GPI, les deux inconnus, exponentiel) ont des domaines d'utilité disjoints.

Pour une courbe BN, $e = 6$, $m = 2$, $L(u) = u^{q^2} - \lambda u$ et $\lambda^3 = \theta^{q^2-1} = 1$: λ est une racine cubique primitive de l'unité. En général $\lambda^{e/2} = 1$. C'est une constante de la courbe, obtenue à partir de n'importe quel générateur connu de G_0 .

Remarque 4.4 (Test de Legendre pour G_0). Pour $x_Q \in \mathbb{F}_{q^{k/2}}$ avec $\beta := x_Q^3 + a_4 x_Q + a_6 \neq 0$, soit $Q = (x_Q, y_Q)$ avec $y_Q \in \mathbb{F}_{q^k}$, $y_Q^2 = \beta$. Alors $\text{Fr}_q^{k/2} Q = -Q$ si et seulement si β est un non-carré de $\mathbb{F}_{q^{k/2}}$: en effet $\text{Fr}_q^{k/2} Q = (x_Q, y_Q^s)$, et $y_Q^s = -y_Q$ si et seulement si $y_Q^{s-1} = \beta^{(s-1)/2} = -1$. L'appartenance de Q à $\ker(\text{Fr}_q^{k/2} + 1)$ se décide donc par un symbole de Legendre dans $\mathbb{F}_{q^{k/2}}$ avant toute extraction de racine carrée, et environ la moitié des $x_Q \in \mathbb{F}_{q^{k/2}}$ avec $\beta \neq 0$ y survivent: le nombre

de $x \in \mathbb{F}_{q^{k/2}}$ tels que $\beta(x)$ soit un non-carré vaut $(s + t_s - N_0)/2$, où t_s est la trace de Frobenius de E sur $\mathbb{F}_{q^{k/2}}$ et $N_0 = \#\{\beta = 0\}$. Sur le sous-espace $W = \omega\mathbb{F}_{q^m}$ les deux degrés de tordue se comportent différemment. Pour $e = 6$ ($a_4 = 0$), $\beta = \theta u^3 + a_6 \in \mathbb{F}_{q^m}$ pour $x_Q = \omega u$, et comme $[\mathbb{F}_{q^{k/2}} : \mathbb{F}_{q^m}] = 3$ est impair, β est un non-carré de $\mathbb{F}_{q^{k/2}}$ si et seulement s'il en est un de $\mathbb{F}_{q^m}$: environ la moitié des $x_Q \in W$ survivent, et le symbole peut se calculer directement dans $\mathbb{F}_{q^m}$. Pour $e = 4$ ($a_6 = 0$), $\beta = \omega u(\theta u^2 + a_4)$ avec $u(\theta u^2 + a_4) \in \mathbb{F}_{q^m}$, carré dans l'extension quadratique $\mathbb{F}_{q^{k/2}}$, tandis que ω est un non-carré de $\mathbb{F}_{q^{k/2}}$ ($\omega^{(s-1)/2} = \theta^{(q^m-1)/2 \cdot (q^m+1)/2} = -1$, θ étant un non-carré de $\mathbb{F}_{q^m}$ et $(q^m + 1)/2$ impair) : *tous* les $x_Q \in W$ avec $\beta \neq 0$ survivent, le test est vide, et $[\ell]Q = \mathcal{O}$ fait tout le filtrage. Le symbole ne doit pas être calculé comme une exponentiation à exposant de $\log_2 s$ bits, qui coûterait à peu près la moitié de ce qu'elle épargne ; comme $\beta^{(s-1)/2} = N_{\mathbb{F}_{q^{k/2}}/\mathbb{F}_q}(\beta)^{(q-1)/2}$, il coûte $k/2 - 1$ Frobenius et $k/2 - 1$ multiplications dans $\mathbb{F}_{q^{k/2}}$ suivis d'un symbole de Jacobi dans $\mathbb{F}_q$, dont le coût est bien inférieur à une multiplication dans $\mathbb{F}_{q^k}$. (Vérifié à la section 9.)

5 Inversion de Miller à deux inconnues

Cette section contient le résultat proprement dit : une procédure en temps polynomial prenant une valeur de Tate–Miller brute et rendant ses deux arguments. C'est [6, Alg. 4.1], qui inverse $h_{d,A}$ en un A connu, avec deux changements : l'orientation est Tate et non Ate, de sorte que la norme donne ζ^d et non ζ^2 (proposition 3.1 contre [6, éq. (4.3)]) et que la racine d -ième est unique (lemme 3.5) ; et son étape 3, $\xi(Q) = \xi(A) \pm u$, est remplacée par la projection du lemme 4.1. Les étapes 1–2 et 5–8 ci-dessous sont les siennes.

Algorithme 5.1 Inversion de Miller à deux inconnues

Entrée : $w \in \mathbb{F}_{q^k}^\times$; ici $d \mid s + 1$; les constantes λ , $(\lambda - 1)^{-1}$ et la base du lemme 4.1, précalculées une fois pour toutes par courbe

Sortie : $(A, Q) \in G_1 \times G_0$ avec $h_{d,A}(Q) = w$, ou $\perp$

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

2 : $\zeta \leftarrow$ une racine d -ième de u dans $\mathbb{F}_{q^{k/2}}^\times$ ▷ lemme 3.5 ; $\perp$ si aucune, les deux signes si deux

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

si $x_A^q \neq x_A$ **alors renvoyer** $\perp$

4 : $x_Q \leftarrow \zeta + x_A$

▷ alors $L(x_Q) = L(\zeta) + (1 - \lambda)x_A = 0$ automatiquement

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

si α n'est pas un carré dans $\mathbb{F}_q$ **alors renvoyer** $\perp$

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

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

si $N_{\mathbb{F}_{q^{k/2}}/\mathbb{F}_q}(\beta)^{(q-1)/2} \neq -1$ **alors renvoyer** $\perp$

▷ i.e. $\text{Fr}_q^{k/2} Q \neq -Q$, remarque 4.4

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

7 : **si** $[\ell]A \neq \mathcal{O}$ **ou** $[\ell]Q \neq \mathcal{O}$ **alors renvoyer** $\perp$

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

si $w = h$ **alors renvoyer** (A, Q)

si $w = -h$ **alors renvoyer** $(-A, -Q)$

si $w = h^s$ **alors renvoyer** $(A, -Q)$

si $w = -h^s$ **alors renvoyer** $(-A, Q)$

9 : **renvoyer** $\perp$

Proposition 5.1. *L'algorithme 5.1 est correct et termine en $O((k \log q)^3)$ opérations binaires.*

Démonstration. Si $w = h_{d,A_0}(Q_0)$ pour un $(A_0, Q_0) \in G_1 \times G_0$, alors par la proposition 3.1 $u = (\xi(Q_0) - \xi(A_0))^d$, donc $\zeta = \xi(Q_0) - \xi(A_0)$ (au signe du cas (ii) près, qui est essayé), et le lemme 4.1

donne $x_A = \xi(A_0)$, $x_Q = \xi(Q_0)$; les étapes 5–7 produisent alors $A = \pm A_0$, $Q = \pm Q_0$ avec des signes inconnus. Par (5) et la preuve de la proposition 3.1, les quatre valeurs brutes sont $h_{d,A_0}(Q_0) = w$, $h_{d,-A_0}(-Q_0) = -w$, $h_{d,A_0}(-Q_0) = w^s$ et $h_{d,-A_0}(Q_0) = -w^s$ (pour d impair), de sorte que l'étape 8 identifie les signes et renvoie une paire de valeur de Miller exactement w . Réciproquement, si l'algorithme renvoie une paire alors $A \in E(\mathbb{F}_q)[\ell] = G_1$ par les étapes 5 et 7, $Q \in E[\ell] \cap \ker(\text{Fr}_q^{k/2} + 1) = G_0$ par les étapes 6–7, la remarque 4.4 et (1), et sa valeur de Miller est w par l'étape 8. Sans l'étape 8, l'algorithme pourrait renvoyer une paire valide pour un w qui n'est pas du tout une valeur de Miller. Pour le coût, comptons les multiplications dans $\mathbb{F}_{q^k}$, chacune en $O((k \log q)^2)$ opérations binaires avec l'arithmétique scolaire, comme dans [6, Thm. 4.2]; une multiplication dans $\mathbb{F}_{q^{k/2}}$ ou $\mathbb{F}_q$ ne coûte pas davantage, et l'exposant $d^{-1} \bmod (s-1)$, les constantes λ , $(\lambda-1)^{-1}$ et la base du lemme 4.1 sont calculés une fois pour toutes par courbe. Étape par étape :

1. $w^{s+1} = w^s \cdot w$: une puissance de Frobenius et une multiplication, $O(k \log q)$ multiplications, ou $O(1)$ lorsque $\mathbb{F}_{q^k}$ est présenté comme extension quadratique de $\mathbb{F}_{q^{k/2}}$, où $w \mapsto w^s$ est la conjugaison.
2. Une exponentiation dans $\mathbb{F}_{q^{k/2}}$ d'exposant inférieur à s : $O(k \log q)$ multiplications.
3. ζ^{q^m} est une puissance de Frobenius ($O(k \log q)$ multiplications, ou $O(k^2)$ multiplications dans $\mathbb{F}_q$ avec une matrice précalculée), suivie d'une multiplication; le test $x_A \in \mathbb{F}_q$ est gratuit dans une $\mathbb{F}_q$ -base de $\mathbb{F}_{q^{k/2}}$ contenant 1.
4. Une addition.
5. Un symbole de Legendre et une racine carrée dans $\mathbb{F}_q$: $O(\log q)$ multiplications dans $\mathbb{F}_q$.
6. Le symbole de Legendre dans $\mathbb{F}_{q^{k/2}}$ via la norme, $k/2 - 1$ puissances de Frobenius et $k/2 - 1$ multiplications dans $\mathbb{F}_{q^{k/2}}$ puis un symbole de Jacobi dans $\mathbb{F}_q$ (remarque 4.4); une racine carrée dans $\mathbb{F}_{q^k}$, $O(k \log q)$ multiplications — en fait une racine carrée dans $\mathbb{F}_{q^{k/2}}$: dès que $\mathbb{F}_{q^k} = \mathbb{F}_{q^{k/2}}(\sqrt{\nu})$ avec ν non-carré de $\mathbb{F}_{q^{k/2}}$, l'élément β/ν est un carré de $\mathbb{F}_{q^{k/2}}$ et $\sqrt{\beta} = \sqrt{\nu} \sqrt{\beta/\nu}$.
7. $[\ell]A$ sur $E(\mathbb{F}_q)$ et $[\ell]Q$ sur $E(\mathbb{F}_{q^k})$: $O(\log \ell) = O(\log q)$ opérations de groupe chacun, chacune en un nombre borné de multiplications.
8. Une boucle de Miller de longueur $d \leq s+1$: $O(\log d) = O(k \log q)$ doublements ou additions d'un nombre borné de multiplications chacun, et quatre comparaisons coûtant une puissance de Frobenius.

Chaque étape est en $O(k \log q)$ multiplications dans $\mathbb{F}_{q^k}$, soit $O((k \log q)^3)$ opérations binaires, et les étapes 1, 2, 6 et 8 atteignent cette borne. Les racines carrées sont déterministes sous le précalcul supposé dans [6], un générateur du 2-Sylow, et en temps espéré avec l'algorithme de Cipolla sinon. $\square$

Deux points méritent commentaire. D'abord, aucun test sur u seul n'est discriminant : w^{s+1} est une norme, donc dans $\mathbb{F}_{q^{k/2}}$ pour *tout* w , et tout élément de $\mathbb{F}_{q^{k/2}}$ est un carré dans $\mathbb{F}_{q^k}$; c'est pourquoi l'étape 6 teste β dans $\mathbb{F}_{q^{k/2}}$ et non dans $\mathbb{F}_{q^k}$ — la condition utile est que β soit un *non*-carré de $\mathbb{F}_{q^{k/2}}$, remarque 4.4 —, pourquoi l'étape 4 est une simple affectation (dès que $x_A \in \mathbb{F}_q$, $L(x_Q) = L(\zeta) + (1-\lambda)x_A = 0$ automatiquement), et pourquoi les tests des étapes 3, 6 et 7 portent tout le poids. Sur la courbe jouet de la section 9, 3000 racines ℓ -ièmes aléatoires d'une cible fixée ont toutes passé les conditions de norme et de carré et ont toutes été rejetées à l'étape 3. Ensuite, la procédure rend les deux arguments; ce n'est pas un oracle d'appartenance suivi d'une recherche. C'est le point où la présente note va au-delà de [1] : leur équation (8) est exactement (3) avec les rôles de A et Q échangés, et leur réduction ultérieure utilise le polynôme minimal du $\xi(Q)$ *connu*, qui n'est pas disponible ici.

6 De l'inversion de Miller à GPI

Soit e un couplage bilinéaire non dégénéré quelconque sur $G_1 \times G_0$ ou sur $G_0 \times G_1$ à valeurs dans μ_ℓ — le couplage de Tate réduit t dans l'un ou l'autre ordre des arguments, ou le couplage de Satoh —

et soit $z \in \mu_\ell \setminus \{1\}$ une cible GPI pour e .

La valeur de Tate–Miller brute v telle que $v^{(q^k-1)/\ell} = t(A, Q)$ n’est déterminée par la valeur réduite qu’à un élément près du noyau de $x \mapsto x^{(q^k-1)/\ell}$, sous-groupe d’ordre $(q^k - 1)/\ell = (s - 1)\nu$ où $\nu := (s + 1)/\ell$. C’est bien trop gros pour être énuméré, et ce n’est pas ce dont l’algorithme 5.1 a besoin : il lui faut ζ , et la proposition 6.2 ci-dessous montre que lorsque v parcourt cette classe, ζ parcourt tout $\mathbb{F}_{q^{k/2}}^\times$ — autrement dit, la cible ne contraint pas ζ du tout. L’algorithme GPI parcourt donc directement les paires d’abscisses $(x_A, x_Q) \in \mathbb{F}_q \times W$ (section 8) ou, de façon équivalente mais plus lente, $\zeta \in \mathbb{F}_{q^{k/2}}^\times$ décodé par les étapes 3–4 de l’algorithme 5.1 (remarque 8.1) ; dans les deux cas chaque paire est testée contre z , et la racine d -ième de l’étape 2 n’est jamais nécessaire.

Le point essentiel pour la suite est qu’aucune des deux boucles n’évalue de couplage avant son test final : e n’intervient que dans le test final, et seulement à travers la question de savoir si $e(A, Q) \in \{z, z^{-1}\}$. Par conséquent :

- l’algorithme résout GPI pour le couplage e , quel qu’il soit, évalué dans le test final, et la proposition 7.1 s’applique telle quelle à tout e de ce type, son argument de comptage n’utilisant que la bilinéarité et la non-dégénérescence ;
- en particulier, en prenant $e(A, Q) := h_{s,-Q}(A)$ — soit $h_{q^{k/2},-A}(Q)$ dans les lettres de Satoh, la condition de sortie de [7, Alg. 6.1] — l’algorithme résout *directement* le problème GPI de Satoh. Par le lemme 3.3 ce e vaut $t(Q, A)^{1/2}$, bilinéaire et non dégénéré, de sorte que le test final peut équivalamment être $t(Q, A) \in \{z^2, z^{-2}\}$, moins coûteux qu’une boucle de Miller de longueur s ; de même la cible à boucle q , $h_{q,-Q}(A)$, de [7, Alg. 6.6] vaut $t(Q, A)^{1/(kq^{k/2-1})}$ par la remarque 3.4, testée comme $t(Q, A) \in \{z^{\pm kq^{k-1}}\}$;
- aucune relation entre deux couplages différents n’est jamais calculée, et aucune n’exigerait de logarithme discret si elle l’était. La constante κ' avec $t(Q, A) = t(A, Q)^{\kappa'}$, par exemple, a la forme close

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

qui découle de l’expression de Frey–Rück du couplage de Tate par le couplage de Weil (lemme 6.1) ; elle vaut 15 sur la courbe jouet de la section 9. La méthode ne l’utilise pas, et aucun logarithme discret n’apparaît nulle part dans la note.

Lemme 6.1. Soit e_ℓ le couplage de Weil, donné par la formule de Miller $e_\ell(A, Q) = (-1)^\ell h_{\ell,A}(Q)/h_{\ell,Q}(A)$, et soient c, h comme dans (13), avec $\rho := kh/(q-1) \bmod \ell$. Alors pour $A \in G_1, Q \in G_0$,

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

d’où (13). La non-dégénérescence de $t(Q, A)$ est $\rho \neq 0$, c’est-à-dire $\ell \nmid kh$: ici $\ell \nmid k$ car $k = \text{ord}_\ell(q)$ divise $\ell - 1$, et $\ell \nmid h$ car $\ell \parallel \#E(\mathbb{F}_q)$. La non-dégénérescence de $t(A, Q)$ est $\rho \neq c$, qui est exactement la non-nullité du dénominateur $kh - c(q-1) = (q-1)(\rho - c)$ de (13).

Démonstration. L’identité $t(P, R) = e_\ell(P, \sigma S - S)$, où $[\ell]S = R$ et $\sigma = \text{Fr}_q^k$, est la forme de Lichtenbaum du couplage de Tate [2] ; elle est classique, et seuls les exposants sont calculés ici. Comme $\pi^k - 1$ annule $E[\ell]$, il se factorise en $\ell\phi$ dans $\text{End}(E)$, donc $\sigma S - S = \phi(R)$, et ϕ agit sur les deux droites propres de π dans le module de Tate $T_\ell E$ comme $(\alpha^k - 1)/\ell$ et $(\beta^k - 1)/\ell$, où $\alpha \equiv 1, \beta \equiv q \pmod{\ell}$ sont les valeurs propres. Écrivons $\alpha = 1 + \ell a, \beta = q + \ell b$; alors $\alpha + \beta = t = q + 1 - \ell h$ donne $a + b = -h$, et $\alpha\beta = q$ donne $b \equiv -qa$, donc $a \equiv h/(q-1)$ et $(\alpha^k - 1)/\ell \equiv ka, (\beta^k - 1)/\ell \equiv c + kq^{k-1}b \equiv c - ka \pmod{\ell}$. Ainsi $\phi(Q) = [c - \rho]Q$ pour $Q \in G_0$ et $\phi(A) = [\rho]A$ pour $A \in G_1$, ce qui donne $t(A, Q) = e_\ell(A, Q)^{c-\rho}$ et $t(Q, A) = e_\ell(Q, A)^\rho = e_\ell(A, Q)^{-\rho}$ par antisymétrie. $\square$

Proposition 6.2 (Indépendance de la valeur de couplage et de la norme). *Comme $\gcd(\ell, s-1) = 1$, l'application*

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

est un homomorphisme surjectif de noyau d'ordre $\nu = (s+1)/\ell$. La valeur de couplage réduite et la norme d'une valeur de Miller brute sont donc des coordonnées indépendantes : fixer la première laisse la seconde uniformément distribuée sur $\mathbb{F}_{q^{k/2}}^\times$, et aucune procédure qui ne lit v qu'à travers v^{s+1} — en particulier aucune bâtie sur la proposition 3.1 — ne reçoit d'information sur la cible.

Démonstration. $\mathbb{F}_{q^k}^\times$ est cyclique d'ordre $(s-1)(s+1)$. Le noyau est formé des v d'ordre divisant $\gcd((s-1)(s+1)/\ell, s+1) = \nu \gcd(s-1, \ell) = \nu$, donc l'image est d'ordre $(q^k-1)/\nu = \ell(s-1) = |\mu_\ell \times \mathbb{F}_{q^{k/2}}^\times|$. $\square$

C'est le contenu de la proposition 7.1 ci-dessous, énoncé une fois pour toutes : la voie par la norme jette la cible entièrement, et ce qui reste est une recherche sur les paires d'abscisses avec un test de couplage final. (Vérifié sur la courbe jouet de la section 9 : l'image a l'ordre prédit $\ell(s-1)$.)

7 Densité de l'ensemble des solutions

Proposition 7.1. *Supposons $e \in \{4, 6\}$, $k > 2$, d impair avec $d \mid s+1$, et fixons $z \in \mu_\ell \setminus \{1\}$. Lorsque v parcourt $\{v : v^{(q^k-1)/\ell} = z\}$, la quantité $\zeta = ((-1)^d v^{s+1})^{1/d}$ parcourt tout $\mathbb{F}_{q^{k/2}}^\times$, chaque valeur étant atteinte le même nombre de fois (proposition 6.2 et lemme 3.5). Soit e un couplage bilinéaire non dégénéré sur $G_1 \times G_0$ ou $G_0 \times G_1$ à valeurs dans μ_ℓ . Parmi les $s-1$ valeurs de ζ , exactement $(\ell-1)/2$ sont décodées par les étapes 3–7 de l'algorithme 5.1 en une paire (A, Q) avec $e(A, Q) = z^{\pm 1}$. Le nombre espéré de candidats à examiner est donc*

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

Démonstration. La première assertion est la proposition 6.2 (la norme est uniforme sur $\mathbb{F}_{q^{k/2}}^\times$ au-dessus de la fibre de z) jointe à la bijectivité de $\zeta \mapsto \zeta^d$ sur $\mathbb{F}_{q^{k/2}}^\times$ (lemme 3.5, d impair). Pour la seconde, par le lemme 4.1 l'application $(\xi(A), \xi(Q)) \mapsto \xi(Q) - \xi(A)$ est injective sur $\mathbb{F}_q \times W$. Les paires $(A, Q) \in (G_1 \setminus \{\mathcal{O}\}) \times (G_0 \setminus \{\mathcal{O}\})$ avec $e(A, Q) \in \{z, z^{-1}\}$ sont au nombre de $2(\ell-1)$ par bilinéarité et non-dégénérescence (pour chaque A , un Q pour chacune des deux valeurs) ; elles sont permutées en orbites de taille 4 par $(A, Q) \mapsto (\pm A, \pm Q)$, qui préserve les deux abscisses et à l'intérieur desquelles e prend chacune des deux valeurs deux fois, et donnent donc $(\ell-1)/2$ valeurs distinctes de ζ . $\square$

Les ζ fructueux appartiennent tous au sous-espace $\mathbb{F}_q \oplus W$, de dimension $1 + k/e$, de sorte que l'algorithme de la section 8 parcourt ce sous-espace ($q^{1+k/e}$ éléments, 2^{761} pour BN254) plutôt que $\mathbb{F}_{q^{k/2}}^\times$. Le décompte (14) vaut pour ce dernier ; pour le premier, dans l'ordre naturel par blocs (x_A à l'extérieur, x_Q à l'intérieur), le travail est de $q^{k/e}/2$ candidats dans le premier bloc valide, la moitié d'entre eux coûteux pour $e = 6$ et tous pour $e = 4$ (remarque 4.4), quel que soit ℓ (sections 8 et 9).

8 L'algorithme complet

Par le lemme 4.1, les valeurs ζ décodées par les étapes 3–4 de l'algorithme 5.1 sont exactement $\zeta = x_Q - x_A$ avec $(x_A, x_Q) \in \mathbb{F}_q \times W$, et par la proposition 6.2 la cible ne contraint pas ζ . L'algorithme GPI parcourt donc directement les paires (x_A, x_Q) ; la norme et la projection L ne sont pas évaluées du tout. L'analyse des sections 4–7 n'intervient que par ce qu'elle démontre : que c'est là l'espace de recherche, et que rien sur la voie de la norme ne peut le réduire (la section 10 énumère les réductions et ce qui justifie chacune).

Algorithme 8.1 GPI, boucle de longueur ℓ

Entrée : q ; $E : Y^2 = X^3 + a_4X + a_6$ ordinaire sur $\mathbb{F}_q$; un premier impair $\ell \parallel \#E(\mathbb{F}_q)$ de degré de plongement pair $k > 2$; un degré de tordue pair $e \geq 4$ avec $e \mid k$; un couplage bilinéaire non dégénéré e sur $G_1 \times G_0$, p. ex. $t(A, Q)$, $t(Q, A)$, ou celui de Satoh $h_{s,-Q}(A) = t(Q, A)^{1/2}$; une cible $z \in \mu_\ell \setminus \{1\}$.

Sortie : $(A, Q) \in G_1 \times G_0$ avec $e(A, Q) = z$, ou $\perp$.

```
1 : Précalcul (indépendant de  $z$ ) :
2 :  $s \leftarrow q^{k/2}$ ;  $m \leftarrow k/e$ 
3 : choisir  $Q_0 \in G_0 \setminus \{\mathcal{O}\}$ ;  $W \leftarrow \xi(Q_0) \mathbb{F}_{q^m}$ , de  $\mathbb{F}_q$ -base  $\xi(Q_0) \cdot \{1, \gamma, \dots, \gamma^{m-1}\}$  pour  $\gamma$  engendrant  $\mathbb{F}_{q^m}$  sur  $\mathbb{F}_q$ 

4 : Boucle principale :
5 : pour  $x_A \in \mathbb{F}_q$  faire
6 :    $\alpha \leftarrow x_A^3 + a_4x_A + a_6$ 
7 :   si  $\alpha$  est un carré dans  $\mathbb{F}_q$  alors
8 :      $A \leftarrow (x_A, \sqrt{\alpha})$ 
9 :     si  $[\ell]A = \mathcal{O}$  alors
10 :      pour  $x_Q \in W$  faire
11 :         $\beta \leftarrow x_Q^3 + a_4x_Q + a_6$ 
12 :        si  $N_{\mathbb{F}_{q^{k/2}}/\mathbb{F}_q}(\beta)^{(q-1)/2} = -1$  alors  $\triangleright$  i.e.  $\text{Fr}_q^{k/2}Q = -Q$ , remarque 4.4
13 :           $Q \leftarrow (x_Q, y_Q)$  avec  $y_Q \in \mathbb{F}_{q^k}$ ,  $y_Q^2 = \beta$ 
14 :          si  $[\ell]Q = \mathcal{O}$  alors
15 :             $\chi \leftarrow e(A, Q)$ 
16 :            si  $\chi = z$  alors
17 :              renvoyer  $(A, Q)$ 
18 :            si  $\chi = z^{-1}$  alors
19 :              renvoyer  $(-A, Q)$ 
20 : renvoyer  $\perp$ 
```

Le couplage e n'est évalué qu'à la ligne 15, et la cible z n'intervient qu'aux lignes 15–19. La ligne 18 utilise $e(-A, Q) = e(A, Q)^{-1}$, de sorte qu'une seule paire fructueuse donne la réponse après au plus deux choix de signe; cela est pris en compte dans le décompte $(\ell - 1)/2$ de la proposition 7.1. Toute abscisse de G_1 a exactement une abscisse partenaire dans G_0 , de sorte que la boucle s'arrête dans le bloc du premier x_A passant les lignes 7 et 9, après avoir balayé environ la moitié de W ; pour ces espérances les deux boucles sont prises en ordre uniformément aléatoire, comme à la section 9 (l'ordre fixe écrit ci-dessus rencontre toujours le même premier x_A). Le travail espéré est de $(q - n)/(n + 1) x_A$ rejetés, $n = (\ell - 1)/2$, chacun au prix d'un symbole de Legendre dans $\mathbb{F}_q$ et, lorsque $h > 1$, pour la moitié qui le passe, d'un $[\ell]A$ (pour $h = 1$ aucun x_A rejeté ne passe le symbole), suivis de $q^{k/e}/2$ candidats x_Q , la moitié d'entre eux coûteux pour $e = 6$ et tous pour $e = 4$ (remarque 4.4).

Lien avec l'algorithme 5.1. L'algorithme 5.1 n'est pas appelé par l'algorithme 8.1, et c'est délibéré. Ses étapes 1–4 (norme, racine d -ième, projection) décodent une valeur brute candidate w en une paire d'abscisses, et la proposition 6.2 montre que, lorsque w parcourt la fibre de z , elles produisent chaque paire de $\mathbb{F}_q \times W$ également souvent : les exécuter reviendrait à parcourir $\mathbb{F}_q \times W$ par un détour sur $\mathbb{F}_{q^{k/2}}^\times$, dont la remarque 8.1 donne le coût. L'algorithme 8.1 parcourt les paires directement et garde la seconde moitié de l'algorithme 5.1 ligne pour ligne : les lignes 6–8 et 11–13 sont ses étapes 5 et 6 (racines carrées et tests de Legendre), les lignes 9 et 14 son étape 7 (tests d'ordre), et les lignes 15–19 remplacent son étape 8 — la comparaison de la valeur brute $h_{d,A}(Q)$ avec w aux quatre signes près — par la comparaison de la valeur réduite $e(A, Q)$ avec $z^{\pm 1}$. Ce que l'algorithme 5.1 apporte n'est donc

pas un sous-programme mais un théorème : que $\mathbb{F}_q \times W$ est l'espace de recherche, et qu'aucun décodage fondé sur la norme ne peut le réduire.

Remarque 8.1 (La boucle sur $\mathbb{F}_{q^{k/2}}^\times$). On peut aussi parcourir $\zeta \in \mathbb{F}_{q^{k/2}}^\times$ — disons $\zeta \leftarrow g\zeta$ pour un élément g de grand ordre, qui contrairement à un générateur n'exige aucune factorisation de $s - 1$, en repartant d'un nouveau ζ_0 lorsque la classe $\zeta_0 \langle g \rangle$ est épuisée, ou simplement en tirant ζ au hasard — et décoder chaque ζ par les étapes 3–4 de l'algorithme 5.1 avant de poursuivre comme ci-dessus ; ζ^{q^m} se met à jour en une multiplication par pas et le test $x_A \in \mathbb{F}_q$ est gratuit dans une base contenant 1. Cette boucle visite $q^{k/2-1-k/e}$ éléments de $\mathbb{F}_{q^{k/2}}$ pour chaque paire (x_A, x_Q) qu'elle finit par décoder, à quelques multiplications dans $\mathbb{F}_{q^{k/2}}$ chacun ; son coût espéré est de $\frac{2(s-1)}{\ell-1}$ tels pas, environ $2^{1271}M$ sur BN254 et $2^{2032}M$ sur BLS12-381 dans l'unité de la section 10, entièrement dépensés à localiser les paires que la boucle directe ci-dessus énumère gratuitement. Elle est dominée et n'est consignée que parce que c'est la forme sous laquelle apparaît le décodage de l'algorithme 5.1.

9 Vérification expérimentale

Tous les énoncés ont été vérifiés en PARI/GP 2.15.4 (noyau GMP 6.3.0, 64 bits) sous Ubuntu 24.04.4 LTS, Linux 6.18, dans une machine virtuelle monocœur en nuage annonçant un Intel Xeon à 2,10 GHz avec 3,9 Gio de RAM ; $\mathbb{F}_{q^k}$ est représenté par un unique polynôme irréductible de degré 12 (ffgen de PARI), non par une tour. La courbe est la courbe BN de paramètre $u = 1$ ($u = -1$ en donne une plus petite, $q = 19$, $\ell = 13$, avec six abscisses seulement dans chaque groupe, trop peu pour que les décomptes ci-dessous signifient quelque chose) : $q = 103$, $\ell = 97$, $E : Y^2 = X^3 + 5$, $\#E(\mathbb{F}_q) = \ell$, $\mathbb{F}_{q^k} \simeq \mathbb{F}_{103^{12}}$ de 80 bits ; ici $e = 6$, $m = 2$, et λ s'est révélé d'ordre 3. Le signe $(-1)^d = -1$ de la proposition 3.1 a été confirmé avec une fonction de Miller normalisée en $\mathcal{O}$; avec `elltatepairing` de PARI, qui ne l'est pas, la constante brute est un autre élément de $\mathbb{F}_q^\times$, indépendant de (A, Q) , et le couplage réduit n'en est pas affecté puisque $(q - 1) \mid (q^k - 1)/\ell$.

vérification	résultat
$\xi(Q) \in \mathbb{F}_{q^{k/2}}$ pour $Q \in G_0$	oui
$\lambda = \xi(Q)^{q^m} / \xi(Q)$ indépendant de Q , $\text{ord}(\lambda) = 3$	oui
$L(u) = 0$ pour tout $u \in W$; $\mathbb{F}_q \cap W = \{0\}$ (tous les $a \in \mathbb{F}_q^\times$)	oui
Prop. 3.1 avec Miller normalisé : $v^{s+1} = -\zeta^\ell$	oui
Alg. 5.1 récupère $(\xi(A), \xi(Q))$ exactement, 30 paires aléatoires	30/30
3000 racines ℓ -ièmes aléatoires d'une cible acceptées	0
Prop. 7.1 : 48 ² paires d'abscisses, 96 paires avec $t = z$, 48 valeurs de ζ	oui
Rem. 3.2 : (6) exacte pour $n = 5, 11, 13$; (7); $h_{s,A}(Q)^{s+1} = 1$; $h_{2\ell-1,A}(Q)^{s+1} = \zeta^{2\ell-2}$; (8) avec $T = 6$	oui
Lem. 3.3 : (9) dans les deux orientations; (10); $-h_{s,A}(Q) = t(A, Q)^{48}$, $48 \equiv -1/2$; $\text{ord}(h_{s,A}(Q)) = 194 = 2\ell$	oui
$h_{s,Q}(A)$ bilinéaire en Q et en A sans exponentiation finale; $h_{s,-Q}(A) = t(Q, A)^{1/2}$	oui
Lem. 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) donne 15, et $t(Q, A) = t(A, Q)^{15}$	oui
$\gcd(2\ell - 2, s - 1) = 48$ sur la courbe jouet, $= 48u$ sur BN254	oui
Les quatre valeurs $w, -w, w^s, -w^s$ de la prop. 5.1	oui
Prop. 6.2 : image de $v \mapsto (v^{(q^k-1)/\ell}, v^{s+1})$ d'ordre $\ell(s-1)$	oui
Rem. 3.2 : $h_{T,Q}(A)^{s+1} = (\xi(A) - \xi(Q))^{-h\ell}$; $h_{q,Q}(A)^{s+1} = 1$; $h_{3\ell,A}(Q)^{s+1} = -\zeta^{3\ell}$ avec $3\ell \nmid s+1$	oui
Rem. 3.4 : $h_{q,Q}(A)^\ell = 1$; $h_{q,Q}(A) = t(Q, A)^{49}$, $49 \equiv -1/(kq^{k/2-1})$; $h_{q,-Q}(A) = t(Q, A)^{48}$	oui
Rem. 4.4 : β non-carré dans $\mathbb{F}_{q^{k/2}} \iff \text{Fr}_{q^{k/2}} Q = -Q$ sur 2000 $x_Q \in W$ aléatoires (1001 non-carrés, $e = 6$); β non-carré pour 30 points de G_0	oui
$1/\pi_z = (s-1)/48 = 2,49 \cdot 10^{10}$ contre $2s/\ell = 2,46 \cdot 10^{10}$ prédit	oui

Une inversion complète d'un couplage bilinéaire. L'algorithme de la section 8 a été exécuté jusqu'au bout : les candidats sont les paires $(a, x_Q) \in \mathbb{F}_q \times W$ avec $W = \xi(Q_0) \mathbb{F}_{q^2}$, c'est-à-dire $\zeta = x_Q - a$, soit $q^3 = 1\,092\,727$ candidats en tout, pour lesquels $x_A = a$ et x_Q se lisent directement et aucune projection n'est nécessaire. La cible était $z = t(A^*, Q^*)$ pour une paire uniformément aléatoire $(A^*, Q^*) \in G_1 \times G_0$, ensuite oubliée; le test final était $t(A, Q) \in \{z, z^{-1}\}$, le couplage de Tate entièrement réduit, entièrement bilinéaire. Pour que les décomptes aient un sens, a a été énuméré dans un ordre uniformément aléatoire de $\mathbb{F}_q$ et, pour chaque a , x_Q dans un ordre uniformément aléatoire de W ; le temps horloge est `getwalltime`.

Toute abscisse a de G_1 admet exactement une abscisse dans G_0 qui la complète en une solution, de sorte que l'exécution s'arrête dans le bloc du *premier* a valide rencontré : elle saute les a invalides (chacun au prix d'un symbole de Legendre, compté comme un bloc sauté de q^2), puis balaie W à la recherche des 48 abscisses de G_0 , en évaluant un couplage de Tate à chacune, jusqu'à rencontrer la bonne. En pratique l'exécution fixe A à la première abscisse valide et cherche dans W son partenaire. Dans cet ordre par blocs le travail espéré est de $(q-n)/(n+1)$ blocs sautés, $n = (\ell-1)/2$, chacun au prix d'un symbole de Legendre dans $\mathbb{F}_q$ et, lorsque $h > 1$, d'une multiplication scalaire $[\ell]A$ pour la moitié d'entre eux acceptée par ce symbole, suivis de $q^{k/e}/2$ candidats, dont la moitié coûteux, dans le premier bloc valide (1,1 bloc et 5 304 candidats sur la courbe jouet); pour un ordre uniforme sur $\mathbb{F}_q \times W$ le décompte correspondant serait $2q^{1+k/e}/\ell$ par l'argument de comptage de la proposition 7.1, qui ne coïncide avec lui qu'à une constante près, et seulement parce que $\ell \approx q$ sur une courbe BN. Sur 12 cibles indépendantes : 12 succès, la paire renvoyée étant dans $G_1 \times G_0$ avec $t(A, Q) = z$ exactement, 11 valeurs distinctes de $\xi(A)$ (jamais la paire d'origine); 0 à 4 a invalides sautés (moyenne 1,3); position du bon x_Q dans le balayage de W entre 1 022 et 10 350 sur 10 609 (moyenne 5 896), compatible avec l'uniforme; 3 à 48 couplages de Tate évalués; temps horloge entre 0,37 s et 1,92 s, dominé par les racines

carrées dans $\mathbb{F}_{q^k}$ et les multiplications scalaires par ℓ du balayage, non par les couplages. Les exécutions rapportées ici sont antérieures à la remarque 4.4 et testaient $\text{Fr}_q^{k/2} Q = -Q$ après la racine carrée ; avec le test de Legendre en premier, calculé par la norme, environ la moitié des racines carrées et des multiplications scalaires est épargnée au prix de $k/2 - 1$ multiplications. La même exécution avec le test final $t(Q, A) \in \{z_S^2, z_S^{-2}\}$, $z_S = h_{s,-Q^*}(A^*) = t(Q^*, A^*)^{1/2}$ — le couplage de Satoh lui-même — réussit de la même façon. Le problème GPI complet, pour un couplage avec exponentiation finale, est donc résolu de bout en bout, au coût que prédit la section 7.

Deux courbes supplémentaires. La courbe jouet ci-dessus a $h = 1$, de sorte que la ligne 9 de la section 8 ($[\ell]A = \mathcal{O}$) n'est jamais exercée, et $e = 6$ seulement. Les mêmes vérifications ont été faites sur deux courbes à cofacteur : $q = 53$, $E : Y^2 = X^3 + X$, $\ell = 17$, $\#E(\mathbb{F}_q) = 68$, $h = 4$, $k = 8$, $e = 4$, $m = 2$ ($j = 1728$, tordue quartique) ; et $q = 103$, $E : Y^2 = X^3 + 4$, $\ell = 37$, $\#E(\mathbb{F}_q) = 111$, $h = 3$, $k = 12$, $e = 6$, $m = 2$. Sur les deux : λ est d'ordre exactement $e/2$; $1, \omega, \dots, \omega^{e/2-1}$ sont vecteurs propres de $u \mapsto u^{q^m}$ de valeurs propres λ^j et $\ker L = W$ (lemme 4.1) ; la proposition 3.1 tient avec le signe -1 ; l'algorithme 5.1 récupère $(\xi(A), \xi(Q))$ sur 30/30 paires aléatoires ; les formes closes du lemme 3.3 et de la remarque 3.4 tiennent, avec $\text{ord}(h_{s,A}(Q)) = 2\ell$; le κ' de (13) vaut 3 et 8 respectivement et $t(Q, A) = t(A, Q)^{\kappa'}$; l'image de l'application de la proposition 6.2 est d'ordre $\ell(s-1)$; et l'algorithme de la section 8, en ordre aléatoire, a réussi sur 5/5 cibles aléatoires sur chaque courbe, la paire renvoyée étant vérifiée contre z . La ligne 9 est maintenant exercée : sur la courbe $e = 4$, parmi les x_A passant le symbole de Legendre, 4/5, 2/3, 12/13, 6/7 et 1/2 ont été rejetés par $[\ell]A \neq \mathcal{O}$ dans les cinq exécutions ($|\xi(G_1)| = 8$ parmi les 33 abscisses de $E(\mathbb{F}_q)$) ; sur la courbe $e = 6$, 0/1, 2/3, 1/2, 0/1 et 3/4 (18 parmi 55).

La courbe $e = 4$ révèle un fait structurel que les exemples $e = 6$ cachent : 400/400 des $x_Q \in W$ avec $\beta \neq 0$ avaient β non-carré dans $\mathbb{F}_{q^{k/2}}$, contre 203/399 sur la courbe $e = 6$. C'est la remarque 4.4 dans ses deux cas : pour $e = 4$ le test de Legendre est vide et $[\ell]Q = \mathcal{O}$ fait tout le filtrage ; pour $e = 6$ il rejette environ la moitié.

Décompte d'opérations. Aucune comparaison de temps n'est faite : à cette échelle les temps mesurent l'interpréteur GP, et les deux coûts ont des asymptotiques différentes en ℓ . Dans l'algorithme de la section 8, chaque x_A coûte un symbole de Legendre dans $\mathbb{F}_q$ et, pour la moitié qui passe, une racine carrée dans $\mathbb{F}_q$ et un $[\ell]A$; chaque x_Q coûte un symbole de Legendre dans $\mathbb{F}_{q^{k/2}}$ calculé par la norme comme à la remarque 4.4 ($k/2 - 1$ Frobenius et $k/2 - 1$ multiplications dans $\mathbb{F}_{q^{k/2}}$, puis un symbole de Jacobi dans $\mathbb{F}_q$ coûtant bien moins que $1M$), qui en rejette environ la moitié pour $e = 6$ et aucun pour $e = 4$ (remarque 4.4), et pour les survivants une racine carrée dans $\mathbb{F}_{q^k}$ et un $[\ell]Q$ sur $E(\mathbb{F}_{q^k})$ — environ 2^{12} multiplications dans $\mathbb{F}_{q^k}$ par x_Q en moyenne pour $e = 6$ aux tailles de la section 10, soit à peu près quatre couplages de Tate, et le double pour $e = 4$. Dans la boucle de la remarque 8.1, chaque ζ coûte en plus une multiplication pour mettre à jour ζ^{q^m} , trois ou quatre pour le décodage et un test d'appartenance gratuit dans une base contenant 1, le reste n'étant atteint que pour la fraction $q^{1+k/e-k/2}$ des ζ . L'étape interne de [7, Alg. 6.1] est, pour ℓ impair, la recherche des racines de $g(T) = \gamma$ sur $\mathbb{F}_{q^k}$ avec $\deg g = (\ell - 1)/2$, ici 48 ($\varphi = g(\xi)$) ; la forme $g(T)^2(T^3 + b) - \gamma^2$ de degré 99 est [7, éq. (6.1)] pour ℓ pair).

10 Comparaison avec [7]

La proposition 6.2 rend le facteur d'amélioration explicite, terme à terme. Dans [7, Alg. 6.1] la variable de boucle γ parcourt $\gamma_0 \mu_{(s-1)\nu}$, de sorte que γ^ν parcourt la classe $z^{-1} \mathbb{F}_{q^{k/2}}^\times$, chaque valeur ν fois, avec une recherche de racines de degré $(\ell - 1)/2$ à chaque pas. Cette boucle est déjà un parcours aveugle d'une coordonnée $\mathbb{F}_{q^{k/2}}^\times$: par [7, Thm. 5.3(ii)–(iii)], dans ses lettres ($A \in G_0$, P rationnel), $\varphi(A + P)^\nu h_{s,-A}(P) \in \mathbb{F}_{q^{k/2}}^\times$, de sorte que $\varphi(A + P)^\nu$ est le produit de $h_{s,-A}(P)^{-1} \in \mu_\ell$ et d'un

élément $c_{A,P} \in \mathbb{F}_{q^{k/2}}^\times$ — la scission $\mu_{\ell(s-1)} \cong \mu_\ell \times \mu_{s-1}$ de la proposition 6.2, appliquée à $\varphi(A+P)^\nu$ au lieu de v . Son c est la composante μ_{s-1} , et la boucle sur γ avec $\varphi(kR)^\nu = c/z$ fixe la composante μ_ℓ à z^{-1} et parcourt l'autre, qui ne porte aucune information sur z . La présente méthode (i) enlève la redondance ν , en prenant la coordonnée elle-même pour variable de boucle, au sein de laquelle la racine d -ième est unique (lemme 3.5); (ii) enlève la recherche de racines, puisque le décodage de la coordonnée en les deux abscisses est polynomial (algorithme 5.1); (iii) réduit la coordonnée de $\mathbb{F}_{q^{k/2}}^\times$ à $\mathbb{F}_q \oplus W$ grâce à la tordue (lemme 4.1); et (iv) teste l'appartenance de x_A à $\xi(G_1)$ par un symbole de Legendre avant de toucher à W , ce qui est l'ordre par blocs de la section 8. Les quatre facteurs sont $\nu \approx s/\ell$, $\tilde{O}(\ell)$, $q^{k/2-1-k/e}$ et environ q/ℓ ; leur produit est $q^{k-k/e}/\ell$ aux constantes et logarithmes près, le rapport des deux premières colonnes ci-dessous. Chercher dans G_0 par multiples d'un générateur au lieu de balayer W réduit la coordonnée une fois encore, à ℓ points, et c'est la dernière colonne. Rien dans cette chaîne n'utilise z avant le test final, et par la proposition 6.2 rien sur cette voie ne le pourrait.

Ce que fait la voie par la norme peut donc s'énoncer précisément. Dans l'orientation Tate avec $\ell \mid d$, l'ambiguïté de la valeur de Miller brute — une classe de taille $(s-1)\nu$ — est réduite du facteur ν en passant à la norme; le décodage de ζ en les deux abscisses devient polynomial même à deux inconnues (lemme 4.1); et la coordonnée résiduelle est indépendante de la cible (proposition 6.2), de sorte que la boucle de la section 8, ou celle, dominée, de la remarque 8.1, la parcourt sans guide.

La comparaison avec [7, Alg. 6.1] doit se faire à convention égale, espérance contre espérance. Pour [7, Alg. 6.1] sur une courbe ordinaire, la probabilité de succès par itération est au plus $(\ell-1)/((s-1)\nu)$ [7, Rem. 6.5], et chaque itération est une recherche de racines de degré $(\ell-1)/2$ sur $\mathbb{F}_{q^k}$; le coût espéré est donc au moins $\frac{(s-1)\nu}{\ell-1} \cdot \tilde{O}(\ell) \approx \tilde{O}((q^k-1)/\ell)$. Pour l'algorithme de la section 8 le nombre espéré de candidats est $q^{k/e}/2$, chacun coûtant à peu près quatre couplages en moyenne pour $e=6$ — la moitié chère environ huit — et environ huit pour $e=4$ (section 9); pour la boucle sur $\mathbb{F}_{q^{k/2}}^\times$ de la remarque 8.1 il est de $\frac{2(s-1)}{\ell-1}$ pas de quelques multiplications dans $\mathbb{F}_{q^{k/2}}$. Pour comparer ce qui est comparable, le tableau ci-dessous est dans une unité unique, M : une multiplication dans $\mathbb{F}_{q^k}$. Les conversions utilisées sont: une racine carrée dans $\mathbb{F}_{q^k}$ et une multiplication scalaire par ℓ sur $E(\mathbb{F}_{q^k})$ valent chacune $\approx 2^{12}M$ à ces tailles; un couplage de Tate de longueur de boucle ℓ avec $A \in E(\mathbb{F}_q)$, à droites creuses et exponentiation finale cyclotomique, $\approx 2^{10}M$; une multiplication dans $\mathbb{F}_{q^{k/2}} \approx 1M$; le symbole de Legendre de la remarque 4.4 $\approx k/2 M$, le symbole de Jacobi dans $\mathbb{F}_q$ étant négligeable; une recherche de racines de degré d sur $\mathbb{F}_{q^k} \approx d \log_2(q^k) M$. Toutes les entrées sont des espérances, et elles sont indicatives plutôt que des mesures: chaque conversion ci-dessus n'est exacte qu'à un petit facteur près, et les exposants héritent de ce jeu. Ce qui est robuste est le rapport entre les colonnes, $q^{k-k/e}/\ell$ aux constantes et logarithmes près, non les valeurs absolues.

courbe	[7, Alg. 6.1]	cette note (section 8)	remarque 8.1	recherche exhaustive
BN254 (alt_bn128)	$2^{2800} M$	$2^{518} M$	$2^{1271} M$	$2^{263} M$
BLS12-381	$2^{4325} M$	$2^{772} M$	$2^{2032} M$	$2^{264} M$

Deux réserves. La borne sur la probabilité de Satoh est une borne supérieure, donc son coût espéré réel peut être plus grand, ce qui ne fait qu'élargir l'écart. Et la comparaison est légitime parce que, avec $e := h_{s,-Q}(A)$ à la ligne 15, l'algorithme résout le problème même de [7, Alg. 6.1] — comme la section 9 le démontre sur la courbe jouet — non parce qu'une routine en remplace une autre.

11 Limitations

1. La méthode exige un degré de tordue pair $e \geq 4$ (remarque 4.2) et $k > 2$ (remarque 4.3). Elle ne s'applique donc pas aux courbes supersingulières sur lesquelles [7] obtient un nombre d'itérations constant; elle s'applique précisément au régime que [7] identifie comme sans espoir.

2. Chercher directement dans G_0 pour un A fixé coûte $\ell/2$ évaluations de couplage en espérance, environ $2^{263}M$ et $2^{264}M$ sur les deux courbes : moins que l'algorithme de la section 8 d'environ $4q^{k/e}/\ell$, soit 2^{256} et 2^{509} ; un logarithme discret dans μ_ℓ ($\approx 2^{100}$ et $\approx 2^{126}$ par TNFS spécial) coûte encore moins. Satoh fait la même observation à propos de son propre algorithme. L'amélioration réduit un écart sans le combler.
3. L'exploitation de $\xi(G_0) \subset \mathbb{F}_{q^{k/2}}$ par la trace et la norme est due à [1], dont la réduction à l'exposant $q - 1$ est plus forte que tout ce qui est obtenu ici dans le cadre à argument fixé. La nouveauté revendiquée sur ce point est que le mécanisme survit au passage à deux arguments inconnus ; les autres contributions sont énumérées dans l'introduction.
4. La boucle n'utilise z que dans son test final, et la proposition 6.2 dit pourquoi : rien de bâti sur la norme ne peut faire autrement. La relation (8) pour la vraie boucle Ate $T = t - 1$ n'est pas non plus une issue, puisqu'elle se réduit à la proposition 3.1 avec $d = h\ell$ (remarque 3.2). La décomposition de Satoh lui-même ne fait pas exception : la constante $c \in \mathbb{F}_{q^{k/2}}^\times$ de [7, Thm. 5.5] est la composante μ_{s-1} de $\varphi(A+P)^\nu$ dans la même scission de restes chinois (section 10) — non de v , dont la norme vaut 1 pour sa longueur de boucle (remarque 3.2) ; accessoirement $(\varphi(A+P)^\nu)^{s+1} = c_{A,P}^2$. Elle est indépendante de z pour la même raison, dont $\mu_\ell \cap \mathbb{F}_{q^{k/2}}^\times = \{1\}$, le fait qu'invoque sa preuve du théorème 5.5(iii), est le corollaire ; sa boucle sur c ne reçoit donc rien de z non plus. Je ne connais aucune décomposition de la valeur brute qui évite la coordonnée ; savoir s'il en existe une est la question laissée ouverte.

Références

- [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.