Arithmetic and pairings on Kummer lines

2023/10/13 — Leuven

Damien Robert

Équipe Canari, Inria Bordeaux Sud-Ouest

université de BORDEAUX

Inria

2^m-isogenies in higher dimension

- Previously: isogenies in higher dimension for number theory
- [KNRR. 2021] used to compute modular forms in dimension 4 to study the Schotkky locus
- "Fast" isogenies: a 3-isogeny over $\mathbb{F}_{59}$ in 70s!

- Currently: used in cryptography
- "Fast" = needs to compute a 2^{128}-isogeny over a field $\mathbb{F}_{p^2}$ of 512 bits in a few ms…

Cryptographic usage of 2^m-isogenies in higher dimension:

- Dimension 2: Festa, QFesta, Scallop-HD, Is-Cube
- Dimension 2 or 4: SQISignHD, SQIFish, VRFs/VDFs, SétaHD
- Dimension 8: ISétaHD

2^m-isogenies in higher dimension

[R. 2023]: faster formula for 2^m-isogenies in the theta model

- Optimised Sage implementation of 2^m-isogenies in dimension 2 (with Dartois, Kunzweiler, Maino, Pope)
- In dimension 1, a 2^{602}-isogeny over a field of 2360 bits: decomposition in 270 ms, images in 8 ms.
- In dimension 2 (theta): decomposition in 490 ms, images in 25 ms
- Richelot: decomposition in 4850 ms, image in 470 ms

- Implementation in dimension 4 (Dartois): A 2^{128}-isogeny over a field of 500 bits in 620 ms.
  $\Rightarrow$ SQISign-HD verification in 850 ms

In FESTA, the bottleneck is now arithmetic in dimension 1 (torsion basis, pairings…)

Faster scalar multiplication on Kummer lines

- Exploit the action of the theta group $G(2(0_E))$ on $\Gamma(2(0_E)) = \langle X, Z \rangle$
- On a Montgomery model with a rational two torsion point $T = (x_T : 1) \neq (0 : 1)$: Variable base scalar multiplication ladder $P = (X_P : Z_P) \to \ell.P$ in $4M + 4S + 2m_0$ by bit.
- Montgomery ladder: $5M + 4S + 1m_0$ for a normalised point $P = (X_P : 1)$.

- On a Theta Kummer surface, fixed base scalar multiplication ladder in $7M + 4S + 3m_0$ by bit.
- Theta ladder: $10M + 9S + 6m_0$.
- Interesting for signatures (eg qDSA)

Faster pairings on Kummer lines

- Isogeny based cryptography needs generic pairings
- New pairing formula on the Montgomery model:
  given $x(P), x(Q), x(P+Q)$, ladder approach in $9M + 6S$ by bit
- Faster than any generic Miller doubling formula I found
- Special cases: $\ell = 2^m$ or $Q = P$: $6M + 4S$ by bit
  $\ell = 2^m$ and $Q = P$: $3M + 2S$ by bit

- Double and add variant (in the theta model):
  Double = $6M + 5S$, Add=$24M + 6S$.

- Timings in Sage for a 3^{363} pairing over a field of 2360 bits:

```
Sage's Tate pairing computation: 0.13450s
Biextension Tate pairing computation: 0.02748s

Sage's Weil pairing computation: 0.09782s
Biextension Weil pairing computation: 0.04764s
```

Biextensions

- Introduced by Mumford, developed by Grothendieck in [SGA7, Exposés VII, VIII]
- Grothendieck deals with biextensions $\mathbf{BiExt}(A, B; C)$ of abelian groups in an arbitrary topos
- Object $X \to A \times B$ with two partial group laws $\star_1, \star_2$ such that for all $a, b \in A, B$, $(X_b, \star_1)$ is an extension of A by C and $(X_a, \star_2)$ an extension of B by C
- Compatibility requirement:
  for $x_{a_1,b_1} \to (a_1, b_1), x_{a_2,b_1} \to (a_2, b_1), x_{a_1,b_2} \to (a_1, b_2), x_{a_2,b_2} \to (a_2, b_2)$;

$$(x_{a_1,b_1} \star_1 x_{a_2,b_1}) \star_2 (x_{a_1,b_2} \star_1 x_{a_2,b_2}) = (x_{a_1,b_1} \star_2 x_{a_1,b_2}) \star_1 (x_{a_2,b_1} \star_2 x_{a_2,b_2}).$$

- $\mathbf{BiExt}(A, B; C)$ additive fibrant left exact in A, B, and additive cofibrant left exact in C.
- $\mathbf{BiExt}^0(A, B; C) \simeq \mathbf{Hom}(A \otimes B, C)$
- $\mathbf{BiExt}^1(A, B; C) \simeq \mathbf{Ext}^1(A \overset{L}{\otimes} B, C)$

$\Rightarrow$ Pairings!

Biextensions

2. La notion de biextension de faisceaux abéliens

2.0. Dans toute la suite du présent numéro, P,Q,G désignent des Groupes commutatifs du topos T . Nous aurons à utiliser fréquemment le diagramme cartésien

(2.0.1)
$$\begin{array}{ccc} P & \longleftarrow & P\times Q \\ \downarrow & & \downarrow \\ e & \longleftarrow & Q \end{array} ,$$

et les Groupes G_P (resp. G_Q resp. $G_{P\times Q}$) sur P (resp. Q, resp. P×Q) images inverses du Groupe G sur e. On identifiera $G_{P\times Q}$ indifféremment à l'image inverse $(G_P)_{P\times Q}$ de G_P par pr_1 ou $(G_Q)_{P\times Q}$ de G_Q par pr_2 . Dans ces notations, les structures de Groupes de P,Q,P×Q n'interviennent pas. Nous n'aurons d'ailleurs partiquement jamais à utiliser la structure de groupe produit sur P×Q. Par contre, il nous sera utile de considérer sur P×Q la structure de P-Groupe image inverse de celle de Q sur e,

(2.0.2) $$P\times Q = Q_P ,$$

et de même la structure de Q-Groupe image inverse de celle de P sur e,

(2.0.3) $$P\times Q = P_Q .$$

Ainsi, sur P on aura à considérer les deux Groupes G_P et Q_P , et sur Q les deux Groupes G_Q et P_Q . Si E est un torseur sur P×Q de Groupe $G_{P\times Q}$, il peut être envisagé indifféremment comme un torseur sur Q_P de groupe $G_{P\times Q} = (G_P)_{Q_P}$, ou comme un torseur sur P_Q de groupe $G_{P\times Q}=(G_Q)_{P_Q}$. Cela a donc un sens de considérer sur E une structure d'extension (commutative) de Q_P par G_P compatible avec sa structure de torseur, ou (symétriquement) une structure d'extension de P_Q par G_Q compatible avec sa structure de torseur. De plus, 1.6, appliqué aux topos induits $T_{/P}$ resp. $T_{/Q}$, nous fournit une façon commode d'expliciter de telles structures. Utilisant les isomorphismes canoniques $T_{/P\times Q} \xrightarrow{\sim} (T_{/P})_{/P\times Q}$ et $T_{/P\times Q} \xrightarrow{\sim} (T_{/Q})_{/P\times Q}$, on trouve les descriptions suivantes. Une structure d'extension de Q_P par G_P sur le torseur E équivaut à la donnée, pour tout objet S de T et des éléments p,p' ∈ P(S), q ∈ Q(S), d'un isomorphisme de torseurs sous G_S

(2.0.4) $$\varphi_{p,p';q} : E_{p,q}E_{p',q} \xrightarrow{\sim} E_{pp',q} ,$$

satisfaisant aux conditions qu'on va rappeler ; comme d'habitude (cf. 1.1.2.1), pour tout point (p,q) ∈ (P×Q)(S) = P(S)×Q(S), on désigne par $E_{p,q}$ le torseur sous G_S image inverse du torseur E sous $G_{P\times Q}$ par (p,q) : S ⟶ P×Q. Les conditions à imposer aux données (2.0.4) sont la fonctorialité en S (i.e. la compatibilité aux images inverses par des morphismes S' ⟶ S dans T), l'associativité qui s'exprime par la commutativité des diagrammes de la forme (1.1.4.1)

(2.0.5)
$$\begin{array}{ccccc} & & E_{pp',q}E_{p'',q} & & \\ & \overset{\varphi_{p,p;q}\wedge id}{\nearrow} & & \overset{\varphi_{pp',p'';q}}{\searrow} & \\ E_{p,q}E_{p',q}E_{p'',q} & & & & E_{pp'p'',q} \\ & \underset{id\wedge\varphi_{p',p'';q}}{\searrow} & & \underset{\varphi_{p,p'p'';q}}{\nearrow} & \\ & & E_{p,q}E_{p'p'',q} & & \end{array}$$

(où p,p',p" ∈ P(S), q ∈ Q(S)), enfin la commutativité qui s'exprime par la commutativité des diagrammes de la forme (1.2.1)

(2.0.6)
$$\begin{array}{ccc} E_{p,q}E_{p',q} & \xrightarrow{\varphi_{p,p';q}} & E_{pp',q} \\ {\scriptstyle sym}\downarrow & & \downarrow{\scriptstyle id} \\ E_{p',q}E_{p,q} & \xrightarrow{\varphi_{p',p;q}} & E_{p'p,q} \end{array}$$

(où p,p' ∈ P(S), q ∈ Q(S)). On explicite de même une structure d'extension de P_Q par G_Q sur E à l'aide d'isomorphismes de torseurs sous G_S

(2.0.7) $$\psi_{p;\,q,q'} : E_{p,q}E_{p,q'} \xrightarrow{\sim} E_{pp',q} ,$$

pour p ∈ P(S) et q,q' ∈ Q(S), les ψ étant fonctoriels en S, et satisfaisant les conditions d'associativité et de commutativité symétriques de (2.0.5) et (2.0.6), s'exprimant par la commutativité des diagrammes

(2.0.8)
$$\begin{array}{ccccc} & & E_{p,qq'}E_{p,q''} & & \\ & \overset{\psi_{p;q,q'}\wedge id}{\nearrow} & & \overset{\psi_{p;qq',q''}}{\searrow} & \\ E_{p,q}E_{p,q'}E_{p,q''} & & & & E_{p,qq'q''} \\ & \underset{id\wedge\psi_{p;q',q''}}{\searrow} & & \underset{\psi_{p;q;q'q''}}{\nearrow} & \\ & & E_{p,q}E_{p,q'q''} & & \end{array}$$

(p ∈ P(S), q,q',q" ∈ Q(S)),

(2.0.9)
$$\begin{array}{ccc} E_{p,q}E_{p,q'} & \xrightarrow{\psi_{p;q,q'}} & E_{p,qq'} \\ {\scriptstyle sym}\downarrow & & \downarrow{\scriptstyle id} \\ E_{p,q'}E_{p,q} & \xrightarrow{\psi_{p;q',q}} & E_{p,q'q} \end{array}$$

(p ∈ P(S), q,q' ∈ Q(S)).

Définition 2.1. Soient P,Q,G des Groupes abéliens de T, E un torseur sous $G_{P\times Q}$, muni de plus d'une structure d'extension de Q_P par G_P défini par des isomorphismes (2.0.4) (fonctoriels en S, soumis aux conditions s'exprimant par la commutativité des diagrammes (2.0.5) et (2.0.6)), et d'une structure d'extension de P_Q par G_Q, défini par des isomorphismes (2.0.7) (fonctoriels en S, soumis aux conditions exprimées par la commutativité des diagrammes (2.0.8) et (2.0.9)). On dit que les deux structures précédentes sont compatibles si pour tout objet S de T et pour p,p' ∈ P(S), q,q' ∈ Q(S), on a commutativité dans le diagramme

(2.1.1)
$$\begin{array}{ccccc} & & E_{p,qq'}E_{p',qq'} & & \\ & \overset{\psi_{p;q,q'}\wedge\psi_{p';q,q'}}{\nearrow} & & \overset{\varphi_{p,p';qq'}}{\searrow} & \\ E_{p,q}E_{p,q'}E_{p',q}E_{p',q'} & & & & E_{pp',qq'} \\ \downarrow & & & & \\ E_{p,q}E_{p',q}E_{p,q'}E_{p',q'} & \underset{\varphi_{p,p';q}\wedge\varphi_{p,p';q'}}{\searrow} & & \underset{\psi_{pp';q,q'}}{\nearrow} & \\ & & E_{pp',q}E_{pp',q'} & & \end{array} ,$$

où la flèche verticale est déduite de l'isomorphisme de symétrie $E_{p,q'}E_{p',q} \xrightarrow{\sim} E_{p',q}E_{p,q'}$. On appelle biextension de (P,Q) par G un torseur E sous $G_{P\times Q}$, muni d'une structure d'extension de Q_P par G_P et d'une structure d'extension de G_Q par P_Q, ces deux structures étant compatibles au sens précédent.

Biextension of elliptic curves and abelian varieties

- For abelian schemes A, B, $\mathbf{BiExt}(A, B; \mathbb{G}_m) \simeq \mathbf{BiRigidifiedTorsors}(A, B; \mathbb{G}_m) \simeq \mathbf{Correspondances}(A, B) \simeq \mathbf{Hom}(A, \hat{B}) \simeq \mathbf{Hom}(B, \hat{A})$ (in the fppf topos)

- Biextensions are used in [SGA7] to study orthogonality relations on the Néron models $\mathcal{A}, \hat{\mathcal{A}}$ of an abelian variety A and its dual $\hat{A}$
- In particular Grothendieck's pairing on Néron component groups $\pi_0(\mathcal{A}_s) \times \pi_0(\hat{\mathcal{A}}_s) \to \mathbb{Q}/\mathbb{Z}$ measures the obstruction of lifting the Poincaré biextension on $A \times \hat{A}$ to $\mathcal{A} \times \hat{\mathcal{A}}$
- Key point in the proof of Grothendieck's semistable reduction theorem for abelian varieties

- Intuitive idea of a biextension: the biextension $X_f \in \mathbf{BiExt}(A, B; \mathbb{G}_m)$ associated to a morphism $f : A \to \hat{B}$ can be seen as a decurryfication of $f : A \to \hat{B} \simeq \mathbf{Ext}^1(B, \mathbb{G}_m)$
- The biextension X_f "encodes" the Weil-Cartier pairing e_f
- Biextensions have better functorial and deformation/degeneration properties than Cartier duality

- Seems like a nice theoretical tool, but too abstract to be well suited for algorithmic applications

Biextension of elliptic curves and abelian varieties

- For abelian schemes A, B, $\mathrm{BiExt}(A, B; \mathbb{G}_m) \simeq \mathrm{BiRigidifiedTorsors}(A, B; \mathbb{G}_m) \simeq \mathrm{Correspondances}(A, B) \simeq \mathrm{Hom}(A, \hat{B}) \simeq \mathrm{Hom}(B, \hat{A})$ (in the fppf topos)

- Biextensions are used in [SGA7] to study orthogonality relations on the Néron models $\mathcal{A}, \hat{\mathcal{A}}$ of an abelian variety A and its dual $\hat{A}$
- In particular Grothendieck's pairing on Néron component groups $\pi_0(\mathcal{A}_s) \times \pi_0(\hat{\mathcal{A}}_s) \to \mathbb{Q}/\mathbb{Z}$ measures the obstruction of lifting the Poincaré biextension on $A \times \hat{A}$ to $\mathcal{A} \times \hat{\mathcal{A}}$
- Key point in the proof of Grothendieck's semistable reduction theorem for abelian varieties

- Intuitive idea of a biextension: the biextension $X_f \in \mathrm{BiExt}(A, B; \mathbb{G}_m)$ associated to a morphism $f : A \to \hat{B}$ can be seen as a decurryfication of $f : A \to \hat{B} \simeq \mathrm{Ext}^1(B, \mathbb{G}_m)$
- The biextension X_f "encodes" the Weil-Cartier pairing e_f
- Biextensions have better functorial and deformation/degeneration properties than Cartier duality

- Seems like a nice theoretical tool, but ~~too abstract to be well suited for algorithmic applications~~

Pairings via biextensions

- [SGA7]: the biextension arithmetic computes the Weil-Cartier and [Stange 2008] Tate pairings (up to a sign)
- [Stange 2008]: the arithmetic of the biextension associated to (0_E) on an elliptic curve is given by elliptic nets
- [Lubicz-R. 2010, 2015]: explicit biextension arithmetic in the theta model associated to a totally symmetric line bundle $\mathcal{L}$ of level n in any dimension
- Except we were not aware that our theta pairing algorithms were actually computing the biextension arithmetic at the time we wrote our articles…Only recently realised this thanks to an email by Katerine Stange in May 2023 pointing out the biextension interpretation of the Tate pairing as written out in her PhD!

- This talk: explicit arithmetic of the biextension associated to $2(0_E)$ on several models of Kummer lines
- Exponentiation on the biextension associated to a Montgomery model of the Kummer line is very familiar…

The Tate and Weil pairings via biextensions

- Let $X \in \mathrm{BiExt}(E, E; \mathbb{G}_m)$ be the biextension of associated to (0_E)
- Let $P \in E[\ell](\mathbb{F}_q), Q \in E(\mathbb{F}_q), \mu_\ell \subset \mathbb{F}_q$

- Let $g_{P,Q} \in X(\mathbb{F}_q)$ be any element above (P, Q)
- Since $\ell P = 0, g_{P,Q}^{\star_1,\ell}$ is a constant λ_P
- If $\mu \in \mathbb{G}_m(\mathbb{F}_q)$ and $g'_{P,Q} = \mu \cdot g_{P,Q}$, then ${g'}_{P,Q}^{\star_1,\ell} = \mu^\ell \lambda_P$
- The class of λ_P in $\mathbb{F}_q^*/\mathbb{F}_q^{*,\ell}$ is the non reduced Tate pairing
- $g_{P,Q}^{\star_1,q-1} = \lambda_P^{(q-1)/\ell}$ is the reduced Tate pairing $e_{T,\ell}(P, Q)$.
  It does not depends on the choice of $g_{P,Q}$

- If $Q \in E[\ell], g_{P,Q}^{\star_2,\ell} = \lambda_Q$; Weil pairing: $e_{W,\ell}(P, Q) = \lambda_P/\lambda_Q$.

- Pairings = exponentiations in the biextension
- Can use all usual tricks: NAF, windows, …

- We will be working with the biextension associated to the divisor of level 2, $D = 2(0_E)$, hence compute the Tate and Weil pairing associated to the polarisation ϕ_D
- This is the square of the usual Tate and Weil pairings associated to the principal polarisation.
- This is not a problem when ℓ is odd, but we lose one bit of information when ℓ is even
- But in this case, we can use the action of the theta group $G(2(0_E))$ to compute the usual Weil and Tate pairings

Biextensions in practice

- X biextension associated to (0_E)
- An element $g_{P,Q} \in X$ above $(P,Q) \in E \times E$ is a function $g_{P,Q} \in k(E)$ with divisor

$$(P) + (Q) - (P+Q) - (0_E)$$

- All such functions differ by multiplication by a constant, so X is indeed a biextension of $E \times E$ by $\mathbb{G}_m$
- $\mu_{P,Q}$: usual representative normalised at (0_E) (via the uniformiser $z = x/y$)
- Group laws:

$$(g_{P_1,Q} \star_1 g_{P_2,Q})(R) = g_{P_1,Q}(R) g_{P_2,Q}(R - P_1)$$

$$(g_{P,Q_1} \star_2 g_{P,Q_2})(R) = g_{P,Q_1}(R) g_{P,Q_2}(R) \frac{g_{Q_1,Q_2}(R-P)}{g_{Q_1,Q_2}(R)}$$

- The biextension is symmetric: $g_{P_1,Q} \star_1 g_{P_2,Q} = g_{Q,P_1} \star_2 g_{Q,P_2}$
- This implies: $\mu_{P_1,P_2}(-P_3) = \mu_{P_2,P_3}(-P_1) = \mu_{P_3,P_1}(-P_2)$.

- $D_Q = (Q) - (0_E)$ is algebraically equivalent to 0, hence the theta group $G(D_Q)$ is an extension of E by $\mathbb{G}_m$: $1 \to \mathbb{G}_m \to G(D_Q) \to E \to 0$
- The first biextension law $\star_1$ is the multiplication in $G(D_Q)$
- Given $g_1 \in G(D_{Q_1}), g_2 \in G(D_{Q_2}), g_1 g_2 \in G(D_{Q_1} + D_{Q_2})$
- $D_{Q_1} + D_{Q_2} = (Q_1) + (Q_2) - 2(0_E) \sim (Q_1 + Q_2) - (0_E)$, hence we have a canonical isomorphism $\phi : G(D_{Q_1} + D_{Q_2}) \simeq G(D_{Q_1+Q_2})$ induced by g_{Q_1,Q_2}
- $(g_1, g_2) \in G(D_{Q_1}) \times G(D_{Q_2}) \mapsto \phi(g_1 g_2) \in G(D_{Q_1+Q_2})$ is the second biextension law $\star_2$.

Working with biextensions: the function representation

- We represent $g_{P,Q}$ as the function $c\frac{l_{P,Q}}{v_{P+Q}} = c\frac{y+ax+b}{x-\gamma}$
- Also keep track of (P, Q)
- Compute $g_{P_1,Q} \star_1 g_{P_2,Q}$ and $g_{P,Q_1} \star_2 g_{P,Q_2}$ in $k(E)$
- Reducing modulo the equation of E, we get a representative of g_{P,Q_1+Q_2} and $g_{P_1+P_2,Q}$
- Polynomial time
- Not very efficient

Working with biextensions: the evaluation representation

- Since we keep track of (P,Q), $g_{P,Q}$ is completely determined up to a constant $c \in \mathbb{G}_m$, so we only need to keep track of c
- Fix a point $R \in E$ and represent $g_{P,Q}$ via $(P,Q,g_{P,Q}(R))$
  (Use a uniformiser if R is in the support of $g_{P,Q}$)
- Example: $R = 0_E$, represent $g_{P,Q}$ via (P,Q,c) where $g_{P,Q} = c\mu_{P,Q}$

- $(Q,P_1,c_1) \star_2 (Q,P_2,c_2) = c_1c_2\frac{g_{P_1,P_2}(R-Q)}{g_{P_1,P_2}(R)}$
- $g_{Q,P}^{\star_2,\ell} = g_{Q,P}(R)^\ell f_{\ell,P}((R-Q)-(R))$, where $\mathrm{div} f_{\ell,P} = \ell P - (\ell P) - (\ell-1)(0_E)$
- The biextension exponentiation gives Miller's algorithm

$\Rightarrow$ Geometric interpretation of Miller's group law

- We recover the Weil and Tate pairings (up to a sign)
- Can change the evaluation point R on the fly

- Variant (using the symmetry):
  $(Q,P_1,c_1) \star_2 (Q,P_2,c_2) = c_1c_2\mu_{P_1,P_2}(-Q) = c_1c_2\mu_{P_1,Q}(-P_2)$
- Miller's addition: $f_{m+1,P}(-Q) = f_{m,P}(-Q)\mu_{mP,P}(-Q) = f_{m,P}(-Q)\mu_{P,Q}(-mP)$.

Working with biextensions: isomorphisms of line bundles

- Let $\mathcal{L} = \mathcal{O}(D)$ be the line bundle associated to $D = (0_E)$, $\mathcal{L}_P := \tau_P^*\mathcal{L}$
- A function $g_{P,Q}$ is the same as an isomorphism $\Phi_{P,Q} : \mathcal{L}_{P+Q} \otimes \mathcal{L} \simeq \mathcal{L}_P \otimes \mathcal{L}_Q$
- Two isomorphisms $\Phi_{P_1,Q}, \Phi_{P_2,Q}$ give an isomorphism $\Phi_{P_1,Q} \star_1 \Phi_{P_2,Q} = \Phi_{P_1,Q} \otimes \tau_{P_1}^* \Phi_{P_2,Q} : \mathcal{L}_{P_1+P_2+Q} \otimes \mathcal{L} \simeq \mathcal{L}_{P_1+P_2} \otimes \mathcal{L}_Q$

- Algebraic Riemann relations: if $P, Q, R, S \in E, P + Q + R + S = 2T$, $P' = T - P, Q' = T - Q, R' = T - R, S' = T - S$, we have a canonical isomorphism:

$$\mathcal{L}_P \otimes \mathcal{L}_Q \otimes \mathcal{L}_R \otimes \mathcal{L}_S \simeq \mathcal{L}_{P'} \otimes \mathcal{L}_{Q'} \otimes \mathcal{L}_{R'} \otimes \mathcal{L}_{S'}$$

- Proof: Fix any isomorphism $\phi : \mathcal{L}_P \otimes \mathcal{L}_Q \simeq \mathcal{L}_{R'} \otimes \mathcal{L}_{S'}$, by the symmetry of $\mathcal{L}$ this induces an isomorphism $\mathcal{L}_{P'} \otimes \mathcal{L}_{Q'} \simeq \mathcal{L}_R \otimes \mathcal{L}_S$, and the tensor product gives the required canonical isomorphism; it does not depends on ϕ.

Examples: we have canonical isomorphisms:

- $\mathcal{L}_{P+Q+R} \otimes \mathcal{L}_P \otimes \mathcal{L}_Q \otimes \mathcal{L}_R \simeq \mathcal{L} \otimes \mathcal{L}_{Q+R} \otimes \mathcal{L}_{P+R} \otimes \mathcal{L}_{P+Q}$ (cubical torsor structure)
- $\mathcal{L}_{P+Q} \otimes \mathcal{L}_{P-Q} \otimes \mathcal{L} \otimes \mathcal{L} \simeq \mathcal{L}_{-Q} \otimes \mathcal{L}_Q \otimes \mathcal{L}_P \otimes \mathcal{L}_P$ (differential additions)

Working with biextensions: cubical torsor structure

- If $\mathcal{L}$ is a line bundle algebraically equivalent to 0, it has a squared structure.
- If $\mathcal{L}$ is an arbitrary line bundle, $\tau_P^* L \otimes L^{-1}$ is algebraically equivalent to 0, hence has a squared structure.
  This is enough to define the Weil and Tate pairing.
- This squared structure is induced by a cubical structure on the Neron-Severri class $\Lambda(\mathcal{L})$ of $\mathcal{L}$.
  Biextension associated to $\mathcal{L}$ = cubical structure on $\Lambda(\mathcal{L})$.
- $\mathcal{L}$ itself has a cubical structure [Breen 1983, Moret-Bailly 1985]
- Idea: directly use this cubical torsor structure to derive efficient formulas for the biextension arithmetic
- This provides a refinement on the biextension arithmetic which gives faster self pairing formula

Working with biextensions: trivialisations of line bundles

- We want to represent a biextension element as an isomorphism $\Phi_{P,Q} : \mathcal{L}_{P+Q} \otimes \mathcal{L} \simeq \mathcal{L}_P \otimes \mathcal{L}_Q$
- Fix a local trivialisation at a point R of $\mathcal{L}_{P+Q}, \mathcal{L}_P, \mathcal{L}_Q, \mathcal{L}$
- This induces a local trivialisation of $\mathcal{L}_{P+Q} \otimes \mathcal{L} \otimes \mathcal{L}_P^{-1} \otimes \mathcal{L}_Q^{-1}$ at R, hence a global trivialisation (since it is trivial), hence an isomorphism $\Phi_{P,Q}$
- In practice take $R = 0_E$ and fix a local trivialisation of $\mathcal{L}$ at $P + Q, P, Q, 0_E$
- "Trivialisation representation"
- Redundant: changing the trivialisations by $\lambda_{PQ}, \lambda_P, \lambda_Q, \lambda_0$ does not change $\Phi_{P,Q}$ iff

$$\lambda_{PQ}\lambda_0 = \lambda_P\lambda_Q$$

- Biextension arithmetic: given trivialisations of $\mathcal{L}$ at $0, Q, P_1, P_1 + Q, P_2, P_2 + Q$ inducing the biextension elements $\Phi_{P_1,Q}, \Phi_{P_2,Q}$:
  1. we fix an arbitrary trivialisation of $\mathcal{L}$ at $P_1 + P_2$
  2. the cubical torsor structure induces a canonical trivialisation at $P_1 + P_2 + Q$
  3. we get an isomorphism $\Phi_{P_1+P_2,Q} : \mathcal{L}_{P_1+P_2+Q} \otimes \mathcal{L} \simeq \mathcal{L}_{P_1+P2} \otimes \mathcal{L}_Q$
  4. $\Phi_{P_1+P_2,Q} = \Phi_{P_1,Q} \star_2 \Phi_{P_2,Q}$

Working with biextensions: affine lifts

- We now work with $D = 2(0_E)$, $\mathcal{L} = \mathcal{O}(D)$, $\Gamma(D) = \langle X, Z \rangle$
- Given $P = (X_P : Z_P)$, a local trivialisation of $\mathcal{L}$ at P is the same as an affine lift $\widetilde{P} = (X_P, Z_P)$ of P
- A biextension element $g_{P,Q}$ is then determined by affine lifts $\tilde{0}, \widetilde{P}, \widetilde{Q}, \widetilde{P+Q}$
- Biextension group law: from $\tilde{0}, \widetilde{Q}, \widetilde{P_1}, \widetilde{P_2}, \widetilde{P_1+Q}, \widetilde{P_2+Q}$, compute $P_1 + P_2$[1], take an arbitrary lift $\widetilde{P_1+P_2}$ and compute the canonical lift $P_1 + \widetilde{P_2} + Q$ induced by the cubical torsor structure
- $g_{P_1,Q} \star_1 g_{P_2,Q}$ is determined by $\tilde{0}, \widetilde{Q}, \widetilde{P_1+P_2}, P_1 + \widetilde{P_2} + Q$.
- Double and add algorithm for the exponentiation: from $\tilde{0}, \widetilde{P}, \widetilde{Q}, \widetilde{P+Q}$, compute $\widetilde{\ell P}, \widetilde{\ell P + Q}$.

- If $D = (0_E)$, $\Gamma(D) = \langle Z_0 \rangle$, a trivialisation of $\mathcal{L} = \mathcal{O}(D)$ at P is the same as fixing a value $Z_0(P)$
  (Slight annoyance: $Z_0(0_E) = 0$…)
- Keeping track of these values through the cubical torsor structure we recover elliptic nets
- Our representation can thus be seen as a generalisation of elliptic nets from level 1 to level 2

[1] On a Kummer line, knowing $P_1, P_2, P_1 + Q, P_2 + Q$ is enough to recover $P_1 + P_2$.

Doubling and differential additions with affine lifts

- Doubling on the biextension: from $\tilde{0}, \widetilde{P}, \widetilde{Q}, \widetilde{P+Q}$, compute $\widetilde{2P}, \widetilde{2P+Q}$.
- On a Kummer line, $2P$ is computed by a doubling and $2P+Q$ by a differential addition $\mathrm{DiffAdd}(P+Q, P, Q)$
- We just need an affine version of doublings and differential additions: $\widetilde{2P} = \mathrm{Double}(\widetilde{P}), \widetilde{2P+Q} = \mathrm{DiffAdd}(\widetilde{P+Q}, \widetilde{P}, \widetilde{Q})$.
- This extends to differential addition on the biextension: given $g_{P_1,Q}, g_{P_2,Q}, g_{P_1,Q} g_{P_2,Q}^{\star_1,-1}$ represented by $\tilde{0}, \widetilde{Q}, \widetilde{P_1}, \widetilde{P_2}, \widetilde{P_1-P_2}, \widetilde{P_1+Q}, \widetilde{P_2+Q}, P_1 - \widetilde{P_2} + Q$, we can compute $\widetilde{P_1+P_2}, P_1 + \widetilde{P_2} + Q$ representing $g_{P_1+P_2,Q} = g_{P_1,Q} \star_1 g_{P_2,Q}$ via two affine differential additions:

$$\widetilde{P_1+P_2} = \mathrm{DiffAdd}(\widetilde{P_1}, \widetilde{P_2}, \widetilde{P_1-P_2}),$$
$$P_1 + \widetilde{P_2} + Q = \mathrm{DiffAdd}(\widetilde{P_1+Q}, \widetilde{P_2}, P_1 - \widetilde{P_2} + Q).$$

- Affine doublings and differential additions allow to compute an affine ladder: $(\widetilde{P}, \widetilde{Q}, \widetilde{P+Q}) \mapsto (\widetilde{\ell P}, \widetilde{\ell P+Q})$
- This computes the biextension exponentiation $g_{P,Q}^{\star_1,\ell}$.
- Projectively, this is just the `ladder3` Montgomery algorithm $(P, Q, P+Q) \mapsto (\ell P, \ell P+Q)$

Affine doublings and differential additions in the Montgomery model

- $E : By^2 = x(x^2 + Ax + 1)$ a Montgomery curve
- Amazing fact[2]: the usual doubling and differential addition formulae in the Montgomery model already compute the biextension law:
- $\mathrm{Double}((X_P, Z_P)) = (R \cdot S, T \cdot (S + \frac{A+2}{4} T)$ with
  $R = (X_P + Z_P)^2, S = (X_P - Z_P)^2, T = R - S = 4X_P Z_P$
- $\mathrm{DiffAdd}((X_P, Z_P), (X_Q, Z_Q), (X_{P-Q}, Z_{P-Q})) = ((U+V)^2/X_{P-Q}, (U-V)^2/Z_{P-Q})$,
  with $U = (X_P - Z_P)(X_Q - Z_Q), V = (X_P - Z_P)(X_Q - Z_Q)$

$\Rightarrow$ The usual Montgomery ladder `ladder3` already computes exponentiations in the biextension

Ladder approach to the Tate and Weil pairing:

1. Start with $\widetilde{0} = (1,0), \widetilde{P} = (X_P, Z_P), \widetilde{Q} = (X_Q, Z_Q), \widetilde{P+Q} = (X_{P+Q}, Z_{P+Q})$
2. Compute $\widetilde{\ell P} = (\lambda_1, 0), \widetilde{\ell P + Q} = (\lambda_2 X_Q, \lambda_2 Z_Q)$
3. The non reduced Tate pairing is $e_{T,\ell}(P,Q) = \lambda_2/\lambda_1$

- No special cases (no intermediates zeros or poles)
- Requires x_P, x_Q, x_{P+Q}. If we only have x_P, x_Q, work over $\mathbb{F}_q[t]/((t - x_{P+Q})(t - x_{P-Q}))$ to compute the symmetrised pairings
- Self pairings: simply do a standard ladder $\widetilde{P} \mapsto \widetilde{\ell P}$

[2] The unicity of the biextension implies that any "natural" arithmetic laws on the Kummer line is already the biextension law

Application to pairing based cryptography

- $E/\mathbb{F}_q$ pairing friendly curve, embedding degree k
- $P \in G_1 = E[\ell](\mathbb{F}_q), Q \in G_2 = E[\ell][\pi_q - q]$
- Operations in $\mathbb{F}_{q^k}$: **M**=multiplication, **S**=square, M=$\mathbb{F}_q \times \mathbb{F}_{q^k}$ multiplication
  - Miller double: 2**M**+2**S**+5M
  - Miller addition: 2**M**+2**S**+5M
  - Variant [BMLL 2010]: double: 1**M**+2**S**+3M, addition: 1**M**+2.5M
  - Biextension ladder: 1**M**+2**S**+2M
- Operations in $\mathbb{F}_{q^k}$ with denominator elimination (k even):
  - Miller double: 1**M**+1**S**+1M
  - Miller addition: 1**M**+1M

$\Rightarrow$ The biextension approach is probably faster for odd embedding degree, or when $P \in G_2$ like for the ate and optimal ate pairings

Ate and optimal ate

- Tate pairing: $P \in E[\ell](\mathbb{F}_{q^k}), Q \in E(\mathbb{F}_{q^k}), \ell \mid q^k - 1$.
- Take any $g_{P,Q}$ in the biextension, since $q^k P = \pi_{q^k}(P) = P$,

$$\pi_{q^k}(g_{P,Q}) = \lambda_P \cdot g_{P,Q}^{\star_1, q^k}$$

- This is the reduced Tate pairing: $e_{T,\ell}(P,Q) = \lambda_P$

- Ate pairing: $P \in G_2 = E[\ell][\pi_q - q], Q \in G_1 = E[\ell](\mathbb{F}_q)$
- Take any $g_{P,Q}$ in the biextension, since $\pi_q(P) = qP$,

$$\pi_q(g_{P,Q}) = \lambda_P \cdot g_{P,Q}^{\star_1, q}$$

- This is the Ate pairing: $\mathrm{ate}_\ell(P,Q) = \lambda_P$
- Similar formulas for the optimal Ate pairing

- The reduced Tate pairing is the Weil-Cartier pairing $e_{\pi_{q^k}}$.
- From the biextension point of view, the Ate pairing is better understood via the Weil-Cartier pairing $e_{\hat{\pi}_q} : G_2 \times G_1 \to \mathbb{G}_m$

Other applications of biextensions

- The biextension arithmetic allow to recover the action of the theta group of level ℓn while working in level n
- An explicit version of the theorem of the square on a given model of an abelian variety gives the biextension arithmetic
- From this we can compute the addition law, pairings, but also isogenies and basis of theta functions [R.'s HDR 2021]

- [BGS 2022]'s modification of Doliskani's supersingularity testing is actually a self Tate pairing computation $e_{T,p\pm 1}(P,P) \stackrel{?}{=} 1$
- If $P \in E(\mathbb{F}_q)$ is of order ℓ with $q \equiv 1 \pmod{\ell}$, $E/\langle P\rangle[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z})^2 \Leftrightarrow e_{T,\ell}(P,P) = 1$

- The biextension arithmetic is a mix of arithmetic on E and arithmetic on $\mathbb{F}_q$
- When computing $P \mapsto \ell P$, leaking a biextension exponentiation $g_{P,Q} \mapsto g_{P,Q}^{\star 1,\ell}$ allows to solve the DLP in subexponential time (by reducing to DLPs in $\mathbb{F}_q^*$)
- One projective coordinate leak in the Montgomery ladder is enough to fully recover ℓ!
- Previously: could only recover a few bits of ℓ
- Projective coordinate leak: from $P = (x_P, 1)$, compute $\ell.P = (X,Z)$ via the Montgomery ladder, and leak (X,Z) rather than just X/Z.

Open questions

- Still a work in progress, with many open questions!

- Extend to other Kummer models?
- Other representations of the biextension elements?
- Exploit further the cubical torsor structure and the algebraic Riemann relations?
- How to do denominator elimination?
- Compute the Weil-Cartier pairing associated to any endomorphism or isogeny?
- To an isogeny $f : A \to B$ corresponds a unique biextension X_f.
  How to compute in X_f? Can we use X_f to find yet another representation of f?
- New insights on pairing inversion?
  Inverting pairings = finding a ℓ-th root in the biextension
- New insights on the DLP?