PART 3

Generalisations

Definition 5. Let $f : A \to B$ be a separable isogeny between abelian varieties over a finite field k. Let $(\ker f)(k)$ be of type δ with associated basis $\langle P_1, \dots, P_r \rangle$. The *generalised f-Tate profile* $t_{\ker f}$ is the map

$$t_{\ker f} : (\operatorname{coker} \hat{f})(k) \to \mu_\delta, \qquad Q \mapsto (\ t_f(P_1, Q), \dots, t_f(P_r, Q)\ ).$$

easy

Generalised Entangled Basis for Elliptic Curves

Using **Theorem 5**, we can easily sample basis (P, Q) for $E[2^n]$, with E a Montgomery curve.

With our knowledge of **2-profiles**, we know we just need P, Q with different non-trivial profiles

$$t_2(P) \neq t_2(Q),$$

to generalize this to *any* elliptic curve E.

Easy: Solve the linear system

$$\begin{aligned} f_1(P) &= f_1(Q), \\ f_2(P) &= -f_3(Q), \\ f_3(P) &= -f_2(Q), \end{aligned}$$

where the f_i denote the reduced 2-Tate pairings. This gives x_P, x_Q in terms of 2-torsion $E[2]$.

medium

Subgroup Membership Test in Dimension 2

Using **Theorem 6**, we can sometimes use trivial profiles to perform subgroup membership tests

$$P \overset{?}{\in} E[r](\mathbb{F}_q).$$

We can now generalise this to abelian varieties with a **non-degenerate** cofactor. For example, Gaudry-Schost's Kummer surface $K(\mathbb{F}_p)$ has non-degenerate cofactor 2, so we find

$$P \in K[r](\mathbb{F}_p) \quad \Leftrightarrow \quad t_{[2]}(P) = 1_\delta.$$

Efficiency: Compared to testing $[r]P \overset{?}{=} \mathbf{0}_K$, this profile approach is **fourteen times faster**.

hard

Sylow ℓ-Torsion Basis for Abelian Varieties

At the heart of all these results lies the duality between $A[\ell](\mathbb{F}_q)$ and $A(\mathbb{F}_q)/[\ell]A(\mathbb{F}_q)$.

The ℓ-Tate profile gives us a set of coordinates to view both as μ_δ, and make things practical.

Main Theorem (sketch).
Given a basis of $A[\ell](\mathbb{F}_q)$ and the cofactor h, and $[h]$ as isomorphism to the Sylow ℓ-torsion,

$$A(\mathbb{F}_q)/[\ell]A(\mathbb{F}_q) \xrightarrow{[h]} S_{\ell,q}(A),$$

we can use the ℓ-Tate profile $t_{[\ell]}$ to **efficiently sample a basis** $\langle P_1, \dots, P_r \rangle$ of $S_{\ell,q}(A)$.

Exercise: Even when $|A(\mathbb{F}_q)|$ is unknown!

KU LEUVEN

The agenda for today

PART 1
The Tate Pairing

PART 2
The Tate Profile

PART 3
Generalisations