PART 3
Generalisations

KU LEUVEN

Sylow

for Abelian Varieties

-Torsion Basis

l

Subgroup Membership Test in Dimension 2

Generalised Entangled Basis for Elliptic Curves

easy

,

,

,

,

medium

just need

where the

This gives

with different non-trivial profiles

Using **Theorem 5**, we can easily sample basis to generalize this to *any* elliptic curve in terms of 2-torsion

a Montgomery curve.

Easy: Solve the linear system

, with

With our knowledge of **2-profiles**, we know we denote the reduced 2-Tate pairings.

for

$$(P, Q)$$

$$E[2^n]$$

E

P, Q

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

E

$$f_1(P) = \quad f_1(Q)$$

$$f_2(P) = -f_3(Q)$$

$$f_3(P) = -f_2(Q)$$

f_i

x_P, x_Q

$E[2]$

and

between

At the heart of all these results lies the duality

-Tate profile gives us a set of coordinates

Given a basis of

,

The

Main Theorem (sketch).

,

, and make things practical.

to view both as

we can use the

and the cofactor

of

-Tate profile

sample a basis

as isomorphism to the Sylow

Exercise: Even when

is unknown!

to **efficiently**

-torsion,

and

$$A[\ell](\mathbb{F}_q)$$

$$A(\mathbb{F}_q)/[\ell]A(\mathbb{F}_q)$$

l

$$\mu_\delta$$

$$A[\ell](\mathbb{F}_q)$$

h

[h]

ℓ

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

l

$t_{[\ell]}$

$$\langle P_1, \ldots, P_r \rangle$$

$$S_{\ell,q}(A)$$

$$|A(\mathbb{F}_q)|$$

,

We can now generalise this to abelian varieties has

this profile approach is **fourteen times faster**.

Efficiency: Compared to testing

profiles to perform subgroup membership tests

Gaudry-Schost’s Kummer surface

with a **non-degenerate** cofactor. For example, Using **Theorem 6**, we can sometimes use trivial non-degenerate cofactor 2, so we find

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

$$K(\mathbb{F}_p)$$

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

$$[r]P \stackrel{?}{=} \mathbf{0}_K$$

Man at the Street (2003)

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 $\langle P_1, \ldots, P_r \rangle$. The *generalised f-Tate profile* $t_{\ker f}$ is the map

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

Man at the Street (2003)