PART 3
Generalisations

KU LEUVEN

Generalised Entangled Basis

for Elliptic Curves

, with

for

just need

With our knowledge of **2-profiles**, we know we a Montgomery curve.

Using **Theorem 5**, we can easily sample basis

,

This gives

,

to generalize this to *any* elliptic curve with different non-trivial profiles

,

denote the reduced 2-Tate pairings.

,

in terms of 2-torsion

Easy: Solve the linear system

where the

$$(P, Q)$$

$$E[2^n]$$

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

$E[2]$

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)

Man at the Street (2003)