PART 3

Generalisations





for Abelian Varieties

-Torsion Basis



Subgroup Membership Test in Dimension 2

Generalised Entangled Basis for Elliptic Curves









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 our knowledge of 2-profiles, we know we

denote the reduced 2-Tate pairings.





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

 $f_1(P) =$

 $f_1(Q)$

 $f_2(P) =$

 $-f_3(Q)$

 $-f_2(Q)$

 $f_3(P) =$





between

At the heart of all these results lies the duality

-Tate profile gives us a set of coordinates

Given a basis of

Main Theorem (sketch).

, and make things practical.

to view both as

we can use the

and the cofactor

-Tate profile

sample a basis

as isomorphism to the Sylow

Exercise: Even when

is unknown!

to efficiently



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









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





 $\langle P_1, ..., P_r \rangle$



We can now generalise this to abelian varieties

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

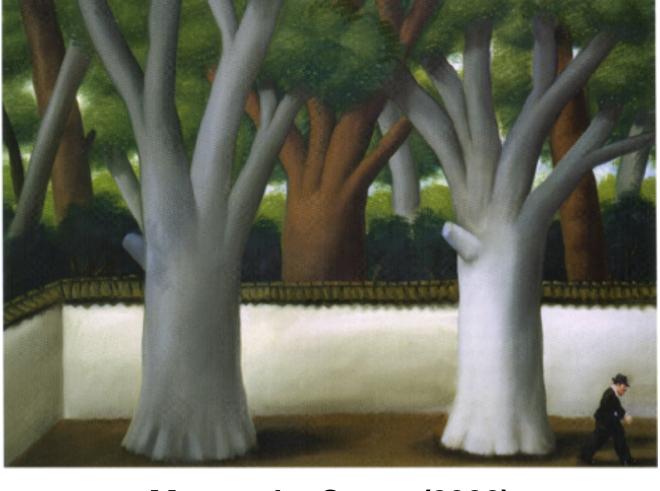
non-degenerate cofactor 2, so we find

 $E[r](\mathbb{F}_a)$

 $P \in K[r](\mathbb{F}_p)$

 $t_{[2]}(P) = 1_{\delta}$

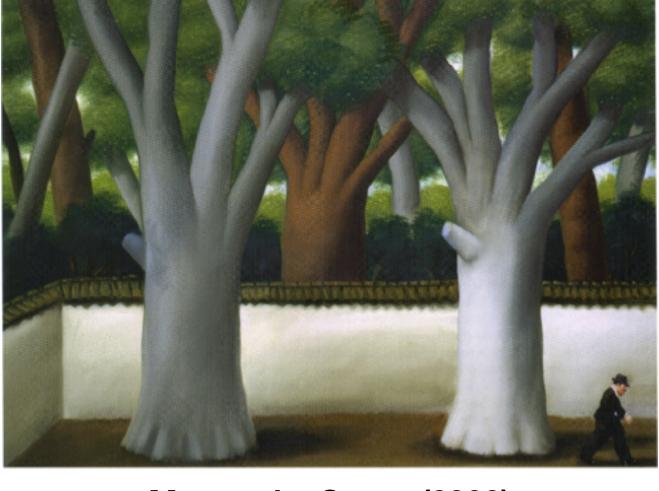
 \Leftrightarrow



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

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



Man at the Street (2003)