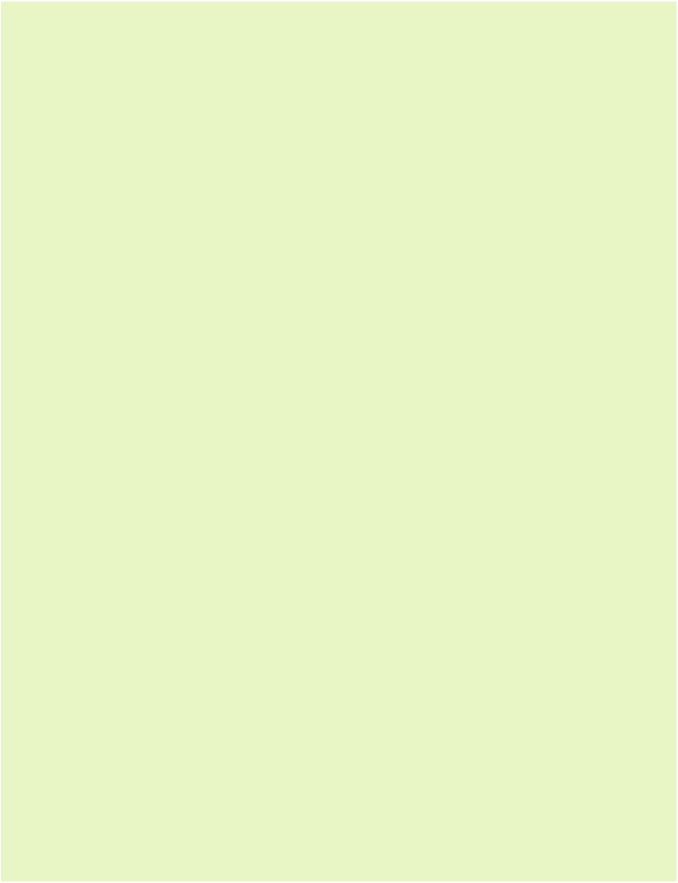
PART 3

Generalisations





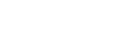
Subgroup Membership Test

in Dimension 2

Generalised Entangled Basis for Elliptic Curves







in terms of 2-torsion

With our knowledge of 2-profiles, we know we

This gives

with different non-trivial profiles

a Montgomery curve.

denote the reduced 2-Tate pairings.

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

Easy: Solve the linear system

to generalize this to any elliptic curve

just need

where the





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

 $f_1(P) =$

 $f_1(Q)$

 $f_2(P) =$

 $-f_3(Q)$

 $-f_2(Q)$

 $f_3(P) =$





profiles to perform subgroup membership tests

Gaudry-Schost's Kummer surface

Using Theorem 6, we can sometimes use trivial

non-degenerate cofactor 2, so we find

Efficiency: Compared to testing

with a **non-degenerate** cofactor. For example,

We can now generalise this to abelian varieties

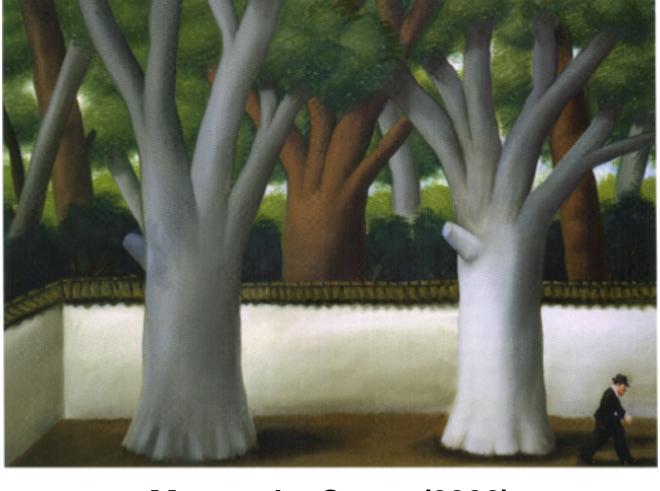
this profile approach is fourteen times faster.

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

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

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

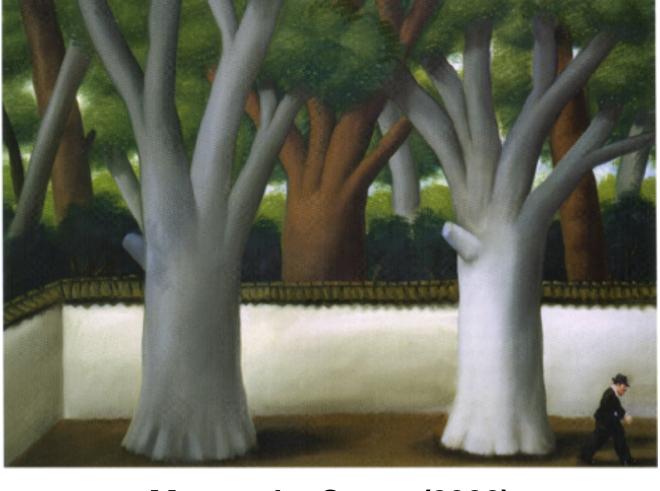
 \Leftrightarrow



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)