An Ode to ANTS (by William Shakespeare)

Shall I compare thee to another conference?
Thou art more lovely, and more algorithmic.
Rough winds do shake the darling bugs of Sage,
And Magma's license hath all too short a date.
Sometimes too hot the Brauer group shines,
And often are the local conditions dimmed;
And every running time eventually declines,
By new techniques, or Moore's law;
But thy elliptic curves shall not fade,
Nor lose possession of their rational points,
Nor shall the LMS brag thou wandrest in pure maths' shade,
when international reviews state that the importance of computational mathematics grow'st.
So long as men can breathe, or jobs on amazon EC2 run,
So long lives this, and this gives life to thee.

Some Questions about Supersingular Curves and Isogeny Cryptosystems

- In 2011, Jao and de Feo introduced the supersingular isogeny Diffie–Hellman key exchange protocol as a candidate for a post-quantum key exchange.
- This leads to some nice questions.

Jao and De Feo scheme

- **Set up:** $p = 2^n \cdot 3^m \cdot f \pm 1$ is prime where f is small and $2^n \approx 3^m$; E a supersingular elliptic curve over $\mathbb{F}_{p^2}$; $P_A, Q_A \in E[2^n]$ and $P_B, Q_B \in E[3^m]$ linearly independent points.
- **Key exchange:** Alice picks random integers $0 \leq a_1, a_2 < 2^n$ (not both divisible by 2) and Bob picks random integers $0 \leq b_1, b_2 < 3^m$ (not both divisible by 3).
- Alice and Bob compute

$$G_A = \langle [a_1]P_A + [a_2]Q_A \rangle, \quad G_B = \langle [b_1]P_B + [b_2]Q_B \rangle$$

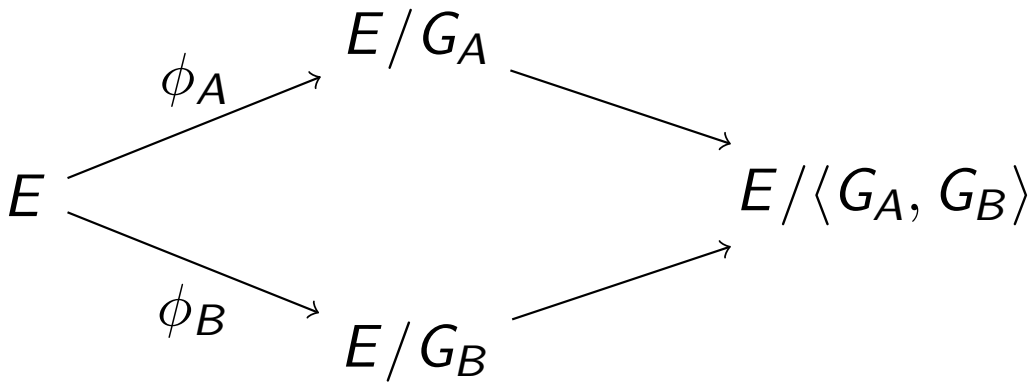
  respectively.
- Using Vélu's formula, they can compute isogenies ϕ_A and ϕ_B with respective kernels G_A and G_B.

Jao and De Feo scheme

- Let $E_A = \phi_A(E) = E/G_A$, $\phi_A(P_B)$, $\phi_A(Q_B)$ and $E_B = \phi_B(E) = E/G_B$, $\phi_B(P_A)$, $\phi_B(Q_A)$.
- Alice sends message $E_A, \phi_A(P_B), \phi_A(Q_B)$ to Bob.
- Bob sends $E_B, \phi_B(P_A), \phi_B(Q_A)$ to Alice.
- Alice can then compute $\phi_B(G_A)$, while Bob can compute $\phi_A(G_B)$.
- The shared key is $E_{AB} = E_A/\phi_A(G_B) = E_B/\phi_B(G_A)$ (up to isomorphism).

Problem 1

This can be summarised in the following diagram, where we use the notation from above.



Find a new algorithm to compute G_A given $(E, E_A, P_B, Q_B, \phi_A(P_B), \phi_A(Q_B))$.

Problem 2

- Let p be a prime and let $\alpha \in \mathbb{F}_p$ and $\mathbb{F}_{p^2} = \mathbb{F}_p(\theta)$.
- Define
$$S_{p,\alpha} = \{\text{supersingular } j = \alpha + \beta\theta : \beta \in \mathbb{F}_p\}.$$
- Determine minimal function $B(p)$ such that $\#S_{p,\alpha} \leq B(p)$ for all p, α.

Problem 3

- Find an efficiently computable injective function $\{$ supersingular $j \in \mathbb{F}_{p^2}\} \rightarrow \mathbb{F}_p$.