Outline

- Background on Isogenies
- Rostovstev and Stolbunov's cryposystem
- "Constructing elliptic curve isogenies in quantum subexponential time," (Childs, Jao, Soukharev) 2011
- "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies," (Jao, de Feo) 2011

Elliptic Curve

Let K be a field.

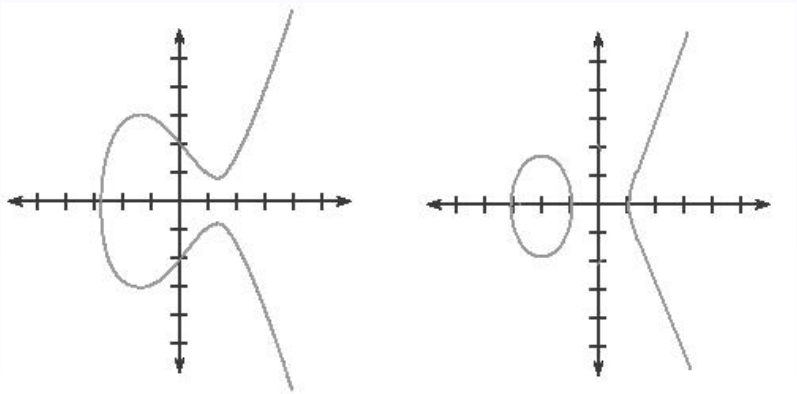
An elliptic curve E is a nonsingular curve of genus 1 with at least one K-rational point.

- Weierstrass form

$$E : y^2 + a_1xy + a_3xy = x^3 + a_2x^2 + a_4x + a_6.$$

- Short Weierstrass form (char$(K) \neq 2, 3$):

$$E : y^2 = x^3 + ax + b.$$



Isogenies

- An isogeny ϕ is a non-constant homomorphism between elliptic curves given by rational maps.
- Examples:
  - Let $\phi : E \to E$ be defined by $\phi(P) = P + P + ... + P = [n]P$, for some integer n.
  - Let E be defined over $\mathbb{F}_p$. Let $\pi : E \to E$ where $\pi(x, y) = (x^p, y^p)$. The isogeny π is known as the *Frobenius*.
- Given a finite subgroup F of $E(K)$, there is an isogeny $\phi : E \to E/F$ such that $\ker(\phi) = F$.
- If $|F| = \ell$, then the degree of ϕ is ℓ, and ϕ is an ℓ-isogeny.

Vélu's formula

- Let E be an elliptic curve with finite subgroup F. Then there is an isogeny ϕ from E with kernel F.
- For $P = (x_P, y_P) \notin F$, let

$$\phi(P) = \left(x_P + \sum_{\substack{Q \in F, \\ Q \neq \infty}} (x_{P+Q} - x_Q), y_P + \sum_{\substack{Q \in F, \\ Q \neq \infty}} (y_{P+Q} - y_Q) \right).$$

- If $|F| = \ell$, then ϕ is known as an ℓ-isogeny.

Vélu's formula - alternate version

- Let ϕ be an ℓ-isogeny, with ℓ odd.
- Let

$$\begin{aligned} D(x) &= \prod_{\infty \neq Q \in F,} (x - x_Q) \\ &= x^{\ell-1} - \sigma x^{\ell-2} + \ldots \\ &= g(x)^2. \end{aligned}$$

- Then $\phi(x, y) = (R(x), yR'(x))$, with

$$R(x) = \ell x - \sigma - (3x^2 + a)\frac{D'(x)}{D(x)} - 2(x^3 + ax + b)\left(\frac{D'(x)}{D(x)}\right)'.$$

- So ϕ is completely determined by $D(x) = g(x)^2$.
- $g(x)$ is known as the *kernel polynomial*

Applications

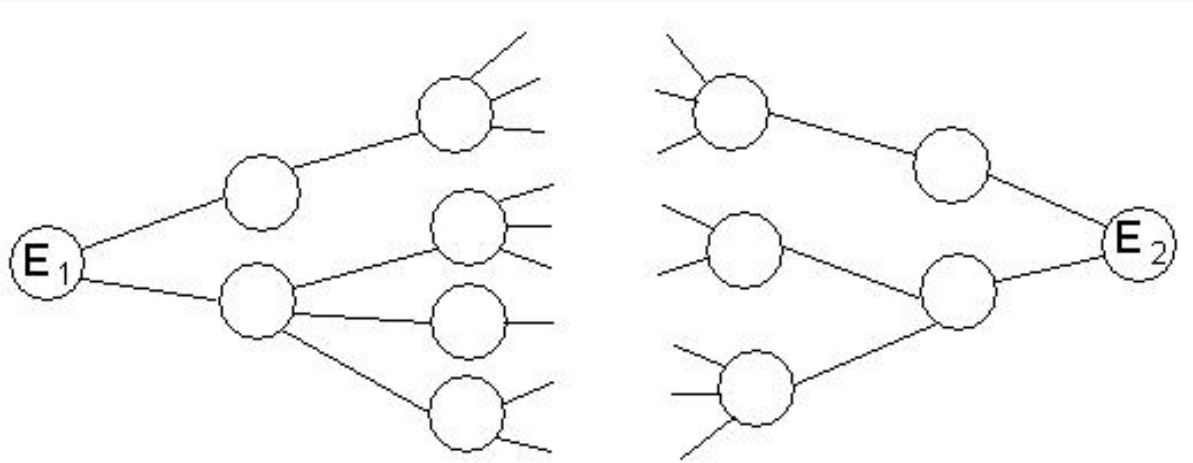
- SEA algorithm - count number of points on an elliptic curve over finite field
- Distortion maps - needed for pairing-based crypto
- Efficient point multiplication - key operation in ECC
- Avoid ZVP attack
- Random number generator
- Isogeny volcanoes
- Security - isogenies transfer Discrete Log Problem between curves
- Public key cryptosystems

Ordinary and Supersingular

- Let $K = \mathbb{F}_p$
- Then $\#(E(\mathbb{F}_p)) = p + 1 - t$, for some $t \leq 2\sqrt{p}$.
- If $p|t$, then E is *supersingular*, otherwise E is *ordinary*
- Most elliptic curves are ordinary
- Supersingular curves have more special properties

Hard Problem

- Tate's Theorem: E_1 is $\mathbb{F}_p$-isogenous to E_2 if and only if $\#(E_1(\mathbb{F}_p)) = \#(E_2(\mathbb{F}_p))$.
- Hard Problem: Given $\#(E_1(\mathbb{F}_p)) = \#(E_2(\mathbb{F}_p))$, find an isogeny from E_1 to E_2.

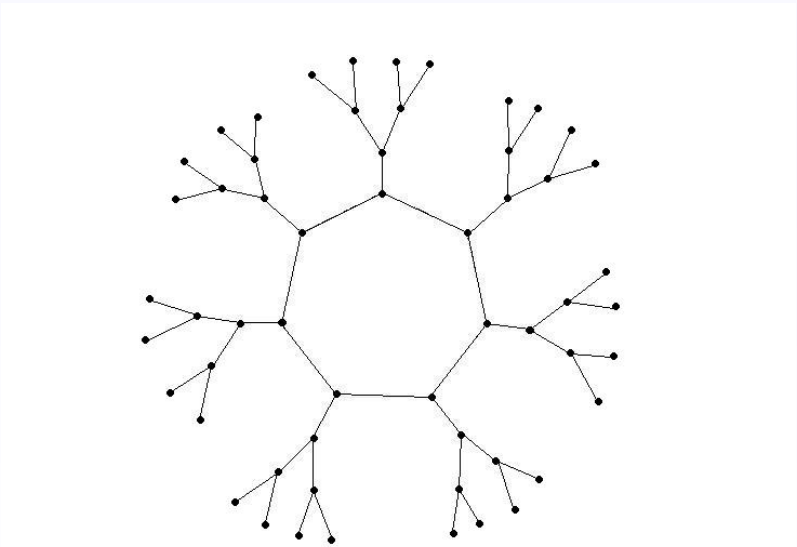


Isogeny Graphs

- Fact: E_1 and E_2 are isomorphic if and only if $j(E_1) = j(E_2)$,

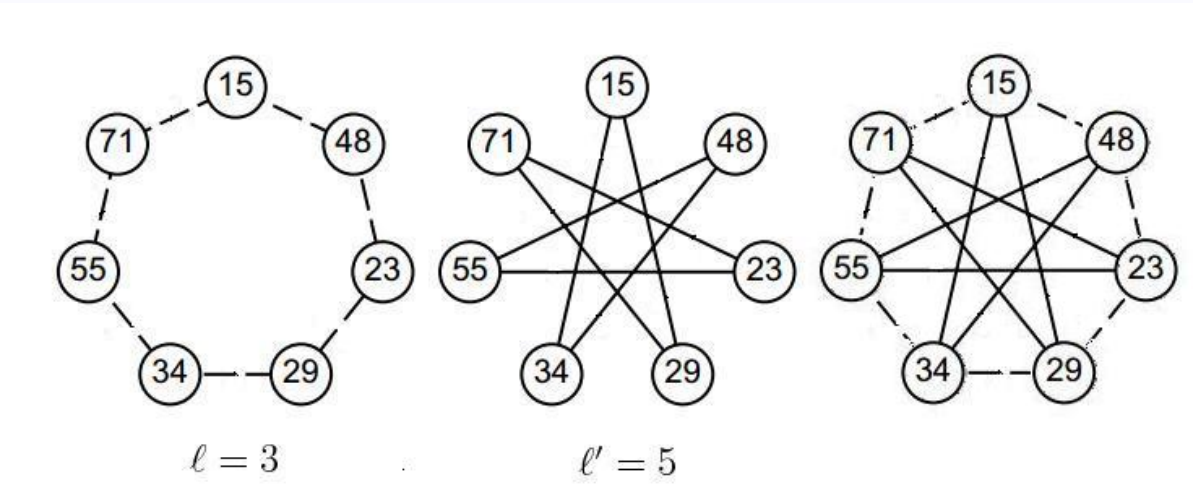
$$j(E) = \frac{4a^3}{4a^3 + 27b^2}.$$

- ℓ-Isogeny Graph
  - Vertices: j-invariants of elliptic curves
  - Edges: Connect E_1 and E_2 if they are ℓ-isogenous

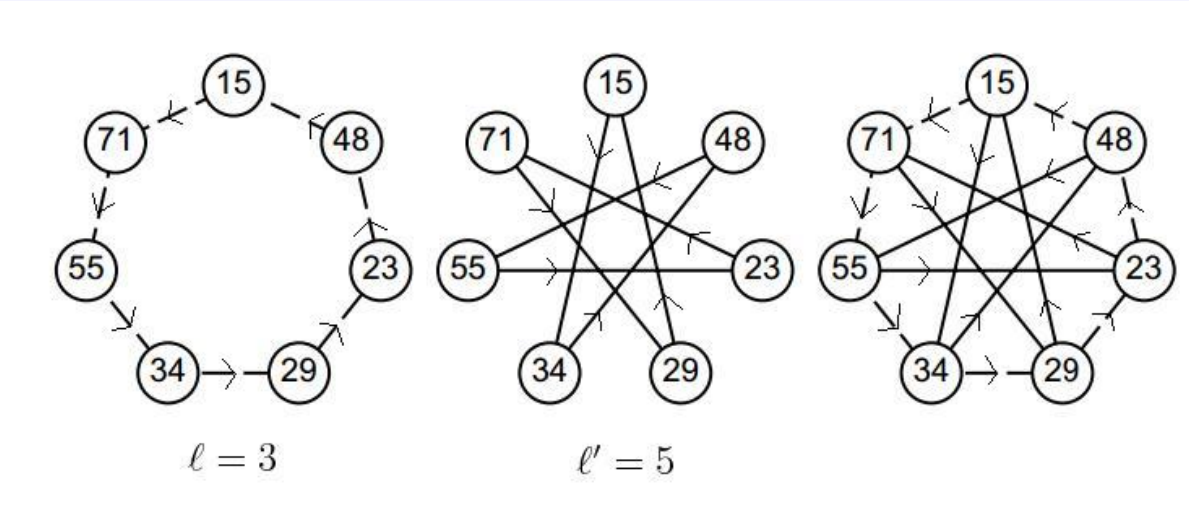


Isogeny Stars

- Let E be an ordinary elliptic curve with $\#(E(\mathbb{F}_p)) = p + 1 - t$.
- Let $D = t^2 - 4p$. Let ℓ be a prime such that D is a square mod ℓ.
- Choose parameters so that number of vertices is prime.
- Then the ℓ-isogeny graph containing E is a cycle.
- Example: Over $\mathbb{F}_{83}$, there are 7 curves with $t = 9$.



Routes



- There is a way to fix a direction on an isogeny star.
- Let R_i^ℓ denote walking i steps on ℓ-star
- Key observation: $R_i^\ell R_j^{\ell'} = R_j^{\ell'} R_i^\ell$
- Example:
  - Start at 34, with $i = 4$, $j = 3$.
- A step on a route is computing an isogeny.

Rostovtsev and Stolbunov's cryptosystem

- Encryption:
  - Agree on all parameters ($\mathbb{F}_p, \ell, \ell', t$, etc...)
  - Private key: route R_{priv}
  - Public key: curve E, and curve $E_{pub} = R_{priv}(E)$
  - To send m, Bob picks random route R_{enc} and computes $E_{enc} = R_{enc}(E_{pub})$.
  - Bob sends (s, E') to Alice, where $s = m \cdot j(E_{enc})$ and $E' = R_{enc}(E)$.
  - Alice decrypts by computing $j = j(R_{priv}(E')$, and $m = s/j$.
- Diffie-Hellman-ish key exchange:
  - E is fixed. Alice sends $E_1 = R_1(E)$ to Bob. Bob sends $E_2 = R_2(E)$ to Alice.
  - They can both compute $E_{key} = R_1(E_2) = R_2(E_1)$.

Security

- To break the system, given E_1 and E_2, need to find a route $R(E_1) = E_2$.
  – That is, compute an isogeny between E_1 and E_2.
- Timings: For 128 bit security, $\approx$229 seconds to encrypt/decrypt. (normal CPU)
- The graph isn't computable
- Best attack is a meet-in-the-middle attack: Galbraith's algorithm, $O(\sqrt[4]{p})$.
- Mainly of theoretical interest.
- Possible post-quantum cryptosystem.

Hard problem	Example scheme	Recomm. public key size, bits	Operation complexity	Encryption overhead, bits	Quantum complexity
Integer factoring [1]	RSA	$\frac{0.05(s+14)^3}{\log(s+14)^2}$	$O\left(\frac{s^6}{\log(s)^3}\right)$	0	$O\left(\frac{s^9}{\log(s)^5}\right)$
DLP in $\mathbb{F}_p^*$ [2]	ElGamal	$\frac{0.05(s+14)^3}{\log(s+14)^2}$	$O\left(\frac{s^6}{\log(s)^3}\right)$	$\frac{0.05(s+14)^3}{\log(s+14)^2}$	$O\left(\frac{s^9}{\log(s)^5}\right)$
Ell. curve DLP [3]	ECIES	$2s$	$O(s^{2.6})$	$4s$	$O(s^3)$
Hash collision and preimage [4]	Merkle's sign.	$2s$	$O(s$ hash$)$	$12s^2+20s$	$O(2^{0.67s}$ hash$)$
Linear code decoding [5]	McEliece	$2.25s^2\log(s)^2$	$O(s^2\log(s)^2)$	$1.5s\log(s)$	$O(2^{0.5s})$
Lattice shortest vector problem [6]	NTRU	$3s\log(s)+1000$	$O(s\log(s)^2)$	$2.5s\log(s)+840$	$O(2^s)$
Isogeny problem [7]	$\mathcal{PE}$	$4s-8\log(s)-16$	$O(s^{5.3})$	$4s-8\log(s)-16$	$O\left(2^{6\sqrt{s\log(s)}}\right)$

Table 1.1: Comparison of hard problems used in cryptography, for the security level of s bits. Provided values are approximated. All example schemes are public-key encryption schemes, except for the Merkle's digital signature scheme. In the column "Recommended public key size" we assume that common system parameters (e.g. the DLP group order) are not included in public keys. The "Operation complexity" column shows the asymptotic number of bit operations in one encryption or signature verification operation. The "Encryption overhead" column contains the difference between the ciphertext length and the "default" message length (e.g. the RSA message length is $\log(n)$ bits, where n is the modulus), or the length of a digital signature for the Merkle's scheme. This absolute overhead size is important when sending short messages over low-bandwidth channels, for instance SMS messages. The column "Quantum complexity" contains an O-bound for the expected number of quantum gates needed to solve a random problem instance.

Childs, Jao, Soukharev

- Quantum, subexponential algorithm to compute (horizontal) isogenies.
- Algorithm is $L_p(\frac{1}{2}, \frac{\sqrt{3}}{2} + \sqrt{2})$, with polynomial space
- Assumes Generalized Riemann Hypothesis
- Key Idea: reduce to Hidden Shift Problem

Hidden Shift Problem

- Let A be a finite abelian group, and S a finite set.
- Let $f_0, f_1 : A \to S$ be injective functions.
- There is a *hidden shift* if

$$f_1(x) = f_0(xs)$$

for some $s \in A$.

Hidden Shift Problem (HSP)

Given A, S and f_0, f_1 with a hidden shift, find s.

Representing Isogenies

- Let $\phi : E \to E'$ be an isogeny over $\mathbb{F}_p$.
- Recall $\#(E(\mathbb{F}_p)) = \#(E'(\mathbb{F}_p)) = p + 1 - t$. Let $D = t^2 - 4p < 0$.
- Fact: When E is ordinary, End(E) is an order $\mathcal{O}$ in $K = \mathbb{Q}(\sqrt{D})$.
- The isogeny ϕ is determined by E and $\ker(\phi)$ (up to isomorphism).
- $\ker(\phi)$ can be represented as an ideal $\mathfrak{b}$ in $\mathcal{O}$.

$$\phi : E \to E_{\mathfrak{b}} \longleftrightarrow \ker(\phi) \longleftrightarrow \mathfrak{b} \subseteq \mathcal{O}_K$$

Isogenies and Class Groups

$$\phi : E \to E_{\mathfrak{b}} \longleftrightarrow \ker(\phi) \longleftrightarrow \mathfrak{b} \subseteq \mathcal{O}_K$$

- Principal ideals $(\mathfrak{a})$ correspond to isomorphisms.
- Thus, the class group acts on ordinary, isogenous curves with the same endomorphism ring.
- This defines an operator $*$

$$[\mathfrak{b}] * j(E) \to j(E_{\mathfrak{b}}),$$

where $[\mathfrak{b}]$ is the ideal class of $\mathfrak{b}$.

Reducing Isogenies to HSP

- Let $\phi : E_0 \to E_1$ be an isogeny.
- Let $\mathfrak{b}$ be the ideal corresponding to ϕ.
- Let $f_i([x]) \to [x] * j(E_i)$, for $i = 0, 1$.
- Then

$$\begin{aligned} f_1([x]) &= [x] * j(E_1) \\ &= [x] * ([\mathfrak{b}] * j(E_0)) \\ &= ([x][\mathfrak{b}]) * j(E_0) \\ &= f_0([x][\mathfrak{b}]). \end{aligned}$$

- Thus the isogeny problem reduces to the Hidden Shift Problem.

Solving the HSP

- Evaluating f_0 and f_1
  - Childs, Jao, and Soukharev – compute $*$ operator in subexponential time
- Solving HSP (using quantum computer)
  - Kuperberg's algorithm – faster running time, superpolynomial space
  - Regev's algorithm – slower, but polynomial space
  - Childs, Jao, Soukharev – fill in the gaps

Conclusions

- Assuming GRH, there is a subexpontial quantum algorithm to compute isogenies.
- With classical computers, isogeny problem is ”easier” ($p^{1/4}$ to $p^{1/2}$) than discrete log, but situation is reversed with quantum computers.
- Actually, input to algorithm is End(E), or $\mathcal{O}$.
  - This is part of public parameters for all proposed isogeny based cryptosystems.
- For arbitrary, ordinary curves, there is a subexponential (quantum) algorithm to compute End(E), assuming the GRH.

Last words?

- Authors conclude: ”Since isogeny-based cryptosystems already perform poorly at moderate security levels, any improved attacks such as ours would seem to disqualify such systems from consideration in a post-quantum world.”
- Stolbunov: ”First of all, it is not clear whether the superpolynomial quantum attack of Childs, Jao and Soukharev will pose a realistic threat. The attack requires $O(2^{6\sqrt{s\log(s)}})$ quantum gates. Physicists are in doubt about the possibility of large-scale quantum computations, because of errors introduced by the quantum decoherence. If no key length adjustment will be needed to protect against the named attack, then the isogeny-based schemes will offer, in general, shorter keys and more efficient bandwidth usage, as compared to other quantum-resistant hard problems. But this will come at a cost of lower operational speeds.”

The Second Paper (Jao, de Feo)

- Flaws of previous system:
  - Not very efficient (229s for 128 bit security)
  - Subexponential attack
- New supersingular isogeny-based cryptosytem
  - Way more efficient (60ms for 128 bit security)
  - No subexponential attack known

Supersingular Curves

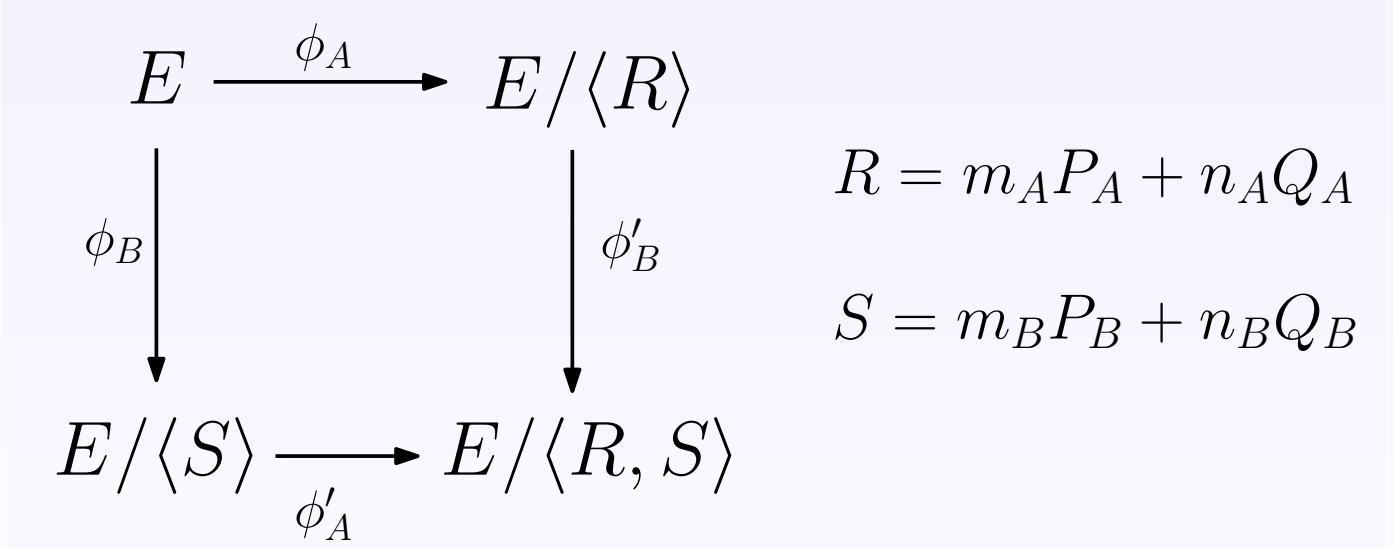
- Recall E is supersingular if $\#(E(\mathbb{F}_p)) = p + 1 - t$, and $p|t$.
- Supersingular curves are rare.
- Endomorphism ring of E is an order in quaternion algebra.
- In particular, End(E) is not commutative.
- All supersingular curves can be defined over $\mathbb{F}_{p^2}$.
- Can represent ker(ϕ) efficiently over $\mathbb{F}_{p^2}$. This is not possible for ordinary curves.
  - This fact leads to increase in speed.

Supersingular Graphs

- ℓ-isogeny graph is $\ell + 1$-regular (assuming $\ell \not| p$).
- The graph is an expander graph, or Ramanujan graph.
- Supersingular isogeny graph used for Charles, Goren, Lauter's hash function.

- Let $p = \ell_A^{e_A} \ell_B^{e_B} f \pm 1$ be prime, for small primes ℓ_A, ℓ_B.
- Usually this is bad, but we don't need discrete log to be hard.

Key Exchange



- Let P_A, Q_A be generators of $E[\ell_A^{e_a}]$, and analogously for P_B, Q_B.
- Alice chooses random m_A, n_A and computes $\phi_A : E \to E_A$ with kernel $m_A P_A + n_A Q_A$.
- Alice sends E_A,$\phi_A(P_B)$ and $\phi_A(Q_B)$ to Bob. Bob does similarly.
- Alice computes $\phi'_A : E_B \to E_{AB}$ with kernel $m_A \phi_B(P_A) + n_A \phi_B(Q_A)$. Bob does similarly.
- The key is $j(E_{AB})$.

Speed and Security

- (We skip description of encryption system)
- Best general algorithm to compute isogenies between supersingular curves is $O\left(\sqrt{p}\log^2 p\right)$.
- There is a classical "claw" attack with $O(\sqrt[4]{p})$, and a quantum "claw" attack with $O(\sqrt[6]{p})$
- Benchmarks (on desktop):

Security	85 bits	128 bits	170 bits
Time (ms)	28	66	122

Summary

- Isogeny-based cryptosystems.
- Subexponential attack on isogenies between elliptic curves.
- Jao, de Feo propose new supersingular cryptosytem
  - No quantum attacks known (yet)
  - Efficient
- Conclusion: wait and see.