Isogenies in a quantum world

David Jao

University of Waterloo

September 19, 2011

Summary of main results

A. Childs, D. Jao, and V. Soukharev, arXiv:1012.4019

- For ordinary isogenous elliptic curves of equal endomorphism ring, we show (under GRH) how to find an isogeny in subexponential time on a quantum computer.

D. Jao and L. De Feo, ePrint:2011/506

- We propose a public-key cryptosystem based on the difficulty of finding isogenies between supersingular elliptic curves (in a certain special case). The fastest known attack against the system takes exponential time, even on a quantum computer.

Isogenies

Definition

Let E and E' be elliptic curves over F.

- An *isogeny* $\phi\colon E \to E'$ is a non-constant algebraic morphism

$$\phi(x, y) = \left(\frac{f_1(x, y)}{g_1(x, y)}, \frac{f_2(x, y)}{g_2(x, y)} \right)$$

  satisfying $\phi(\infty) = \infty$ (equivalently, $\phi(P + Q) = \phi(P) + \phi(Q)$).
- The *degree* of an isogeny is its degree as an algebraic map.
- The *endomorphism ring* $\mathrm{End}(E)$ is the set of isogenies from $E(\bar{F})$ to itself, together with the constant homomorphism. This set forms a ring under pointwise addition and composition.

Ordinary and supersingular curves

Theorem

Let E be an elliptic curve defined over a finite field. As a $\mathbb{Z}$-module, $\dim_{\mathbb{Z}} \mathrm{End}(E)$ *is equal to either* 2 *or* 4*.*

Definition

An elliptic curve E over a finite field is *supersingular* if $\dim_{\mathbb{Z}} \mathrm{End}(E) = 4$, and *ordinary* otherwise.

Isogenous curves are always either both ordinary, or both supersingular.

Isogenies and kernels

Theorem

For every finite subgroup $G \subset E(\bar{F})$, there exists a unique (up to isomorphism) elliptic curve E/G and a unique (up to isomorphism) separable isogeny $E \to E/G$ of degree $\#G$. Every separable isogeny arises in this way.

Corollary

Every separable isogeny ϕ factors into a composition of prime degree isogenies.

Proof.

Let $G = \ker \phi$. Factor G using the fundamental theorem of finite abelian groups. Apply the previous theorem to each factor. $\square$

Solving the decision problem

Theorem (Tate 1966)

Two curves E and E' are isogenous over $\mathbb{F}_q$ if and only if $\#E = \#E'$.

Remark

The cardinality $\#E$ of E can be calculated in polynomial time using Schoof's algorithm [Schoof 1985], which is also based on isogenies.

First main theorem of complex multiplication

Theorem (First main theorem of complex multiplication)

- *Let* $\mathrm{Cl}(\mathcal{O}_D)$ *denote the ideal class group of* $\mathcal{O}_D \subset K$.
- *Let* $h = \#\,\mathrm{Cl}(\mathcal{O}_D)$ *denote the class number of* $\mathcal{O}_D$.
- *There exists a number field* L*, called the Hilbert class field of* K*, with* $[L : K] = h$ *and* $\mathrm{Gal}(L/K) = \mathrm{Cl}(\mathcal{O}_D)$*, such that:*
  - *Fix any prime ideal* $\mathfrak{p} \subset \mathcal{O}_L$ *of norm* p.
  - *For every fractional ideal* $\mathfrak{a} \in \mathcal{O}_D$*, the complex elliptic curve* $\mathbb{C}/\mathfrak{a}$ *corresponding to the lattice* $\mathfrak{a}$ *is defined over* L*, and has endomorphism ring* $\mathcal{O}_D$.
  - *The reduction of* $\mathbb{C}/\mathfrak{a}$ *mod* $\mathfrak{p}$ *yields an elliptic curve over* $\mathbb{F}_p$ *with endomorphism ring* $\mathcal{O}_D$.
  - *Every ordinary elliptic curve over* $\mathbb{F}_p$ *arises in this way.*
  - *Two fractional ideals yield isomorphic curves if and only if they belong to the same ideal class.*

Remarks on the first main theorem

Stated more succintly, there is an isomorphism between elements of $\mathrm{Cl}(\mathcal{O}_D)$ and isomorphism classes of elliptic curves $E/\mathbb{F}_p$ with $\mathrm{End}(E) = \mathcal{O}_D$.

Definition

The set of isomorphism classes of elliptic curves $E/\mathbb{F}_p$ with $\mathrm{End}(E) = \mathcal{O}_D$ is denoted $\mathrm{Ell}_{p,n}(\mathcal{O}_D)$, where $n = \#E$.

Remark

1. This isomorphism is *not canonical!* It depends on the choice of $\mathfrak{p}$.
2. This isomorphism is very hard to compute. The fastest known algorithm operates by computing the *Hilbert class polynomial*, which takes $O(p)$ time.

Second main theorem of complex multiplication

Theorem (Second main theorem of complex multiplication)

Let $\mathfrak{a}$ be any fractional ideal, and let $\mathfrak{b}$ be an ideal. Then

- $\mathfrak{a}\mathfrak{b}^{-1} \supset \mathfrak{a}$ *(n.b. "to contain is to divide").*
- *The map $\mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{a}\mathfrak{b}^{-1}$ is an isogeny of degree $N(\mathfrak{b})$, denoted $\phi_{\mathfrak{b}}$.*
- *Every horizontal separable isogeny mod p arises from the mod $\mathfrak{p}$ reduction of such an isogeny $\phi_{\mathfrak{b}}$.*

Remarks on the second main theorem

- The isomorphism between ideal classes $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_D)$ and curves $E \in \mathrm{Ell}_{p,n}(\mathcal{O}_D)$ is not canonical.
- However, the correspondence between ideals $\mathfrak{b}$ and isogenies $\phi_{\mathfrak{b}}$ *is* canonical, up to endomorphism.

$$\begin{array}{ccc} \mathbb{C}/\mathfrak{a} & \xrightarrow{\phi_{\mathfrak{b}}} & \mathbb{C}/\mathfrak{a}\mathfrak{b}^{-1} \\ \Big\downarrow{\scriptstyle \bmod \mathfrak{p}} & & \Big\downarrow{\scriptstyle \bmod \mathfrak{p}} \\ E & \xrightarrow[\phi_{\mathfrak{b}}]{} & E' \end{array}$$

- Thus we may *represent* isogenies using ideal classes in $\mathcal{O}_D$.

The main group action

Theorem (Waterhouse 1969)

There is a group action $*\colon \mathrm{Cl}(\mathcal{O}_D) \times \mathrm{Ell}_{p,n}(\mathcal{O}_D) \to \mathrm{Ell}_{p,n}(\mathcal{O}_D)$, *defined as follows.*

- *Given* $\mathfrak{b} \in \mathrm{Cl}(\mathcal{O}_D)$, *and* $E \in \mathrm{Ell}_{p,n}(\mathcal{O}_D)$, *let* $\phi_{\mathfrak{b}}\colon E \to E'$ *be the isogeny corresponding to* $\mathfrak{b}$.
- *Set* $\mathfrak{b} * E = E'$.

$\mathrm{Ell}_{p,n}(\mathcal{O}_D)$ *is a principal homogeneous space for the group* $\mathrm{Cl}(\mathcal{O}_D)$ *under this action. In other words, the action is free and transitive.*

Computational problems

There are two main computational questions:

1. Given $\mathfrak{b}$ and E, compute $\mathfrak{b} * E$.
2. Given E and E', find $\mathfrak{b} \in \mathrm{Cl}(\mathcal{O}_D)$ such that $\mathfrak{b} * E = E'$ (the so-called *quotient* of E' and E).

These are believed to be hard problems.

1. Computing the group action:
   - Previous work: $O(N(\mathfrak{b})^3)$ (!!)
   - Our work:
     - $L_p(\frac{1}{2}, \frac{\sqrt{3}}{2})$ with heuristics (Jao and Soukharev, ANTS 2010)
     - $L_p(\frac{1}{2}, \frac{\sqrt{3}}{2})$ under GRH (Childs, Jao and Soukharev)
2. Computing quotients:
   - Previous work: $O(h^{1/2}) = O(p^{1/4})$ with heuristics [Galbraith, Hess, Smart 2002]
   - Our work: $L_p(\frac{1}{2}, \frac{\sqrt{3}}{2})$ with quantum computers (Childs, Jao, Soukharev)

[Bisson, J. Math. Cryptol. 2011] improves these times to $L_p(\frac{1}{2}, \frac{\sqrt{2}}{2})$

Isogeny-based cryptography

- Cryptosystems based on isogenies have been proposed by Couveignes (1996), Rostovtsev and Stolbunov (2006), and Stolbunov (2010).
- Given $\mathfrak{b}$ and E, computing $\mathfrak{b} * E$ is hard, but it can be easy if you choose $\mathfrak{b}$ to be of the form $\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_t^{e_t}$.
- Given E and E', computing the quotient seems hard, and (as an attacker) you may not have the ability to choose E and E'.
- This leads to the design of public key cryptosystems based on group actions.

Example: Key exchange

Public parameters: p, $E \in \mathrm{Ell}_{p,n}(\mathcal{O}_K)$

Key generation: Choose an ideal $\mathfrak{b} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_t^{e_t}$.

Public key: $\mathfrak{b} * E$

Private key: $\mathfrak{b}$

To generate a shared key, take $\mathfrak{b}_1 * \mathfrak{b}_2 * E = \mathfrak{b}_2 * \mathfrak{b}_1 * E$. Breaking the system (conjecturally) requires finding the quotient $\mathfrak{b}$, given E and $\mathfrak{b} * E$.

Quoting Stolbunov (Adv. Math. Comm. **4**(2), 2010):

> *Besides being interesting from the theoretical point of view, the proposed cryptographic schemes might also have an advantage against quantum computer attacks.... In case a quantum attack is discovered later, the proposed cryptographic schemes would seemingly become of theoretical interest only.*

The abelian hidden shift problem

- Let A be a finite abelian group.
- Let S be a finite set.
- Let $f : A \to S$ and $g : A \to S$ be two injective functions that differ by a shift. That is, there exists $b \in A$ such that, for all $x \in A$,
$$f(x) = g(xb).$$
- Problem: Find b.

Isogeny construction as a hidden shift problem

Suppose we are given two isogenous curves E and E'.

- Define $f_0, f_1 \colon \mathrm{Cl}(\mathcal{O}_D) \to \mathrm{Ell}_{p,n}(\mathcal{O}_D)$ by

$$f_0(\mathfrak{a}) = \mathfrak{a} * E$$
$$f_1(\mathfrak{a}) = \mathfrak{a} * E'$$

- E and E' are isogenous, so there exists $\mathfrak{b} \in \mathrm{Cl}(\mathcal{O}_D)$ such that

$$\mathfrak{b} * E = E'.$$

- Then $f_1(\mathfrak{a}) = \mathfrak{a} * E' = \mathfrak{a} * \mathfrak{b} * E = f_0(\mathfrak{a}\mathfrak{b})$.
- f_0 and f_1 are injective since $*$ is regular.
- Solving the hidden shift problem on f_0, f_1 yields $\mathfrak{b}$.

Kuperberg's algorithm

Theorem (Kuperberg, 2003)

For a group A of size N, the hidden shift problem can be solved on a quantum computer in $\exp(O(\sqrt{\ln N})) = L_N(\frac{1}{2}, 0 + o(1))$ *time, space, and queries to f and g.*

- Note that Kuperberg's algorithm requires querying the functions f and g (potentially) a large number of times.
- $f(\mathfrak{a}) = \mathfrak{a} * E$ and $g(\mathfrak{a}) = \mathfrak{a} * E'$ are just group action operations.
- Thus, computing quotients can be reduced to computing the action.

Computing the group action: direct approach

Problem

Given $\mathfrak{b}$ and E, compute $\mathfrak{b} * E$.

The direct approach is to work with $\mathfrak{b}$ itself.

- By factoring $\mathfrak{b}$ (which takes subexponential time), we may reduce to the case where $\mathfrak{b} = \mathfrak{L}$ is prime.
- If $\mathfrak{L}$ does not have prime norm, then it is a principal ideal, and the action is trivial.
- Hence we may assume $\mathfrak{L}$ has prime norm. Write $N(\mathfrak{L}) = \ell$.

Computing the group action: direct approach

- Write $E : y^2 = x^3 + ax + b$.
- Let $j = j(E)$ be the j-invariant of E.
- Let $\Phi_\ell(x, y)$ be the classical modular polynomial of level ℓ.
- Let j' be a root of $\phi_\ell(x, j(E))$.
- Set

$$s = -\frac{18}{\ell}\frac{b}{a}\frac{\frac{\partial\Phi}{\partial x}(j(E), j')}{\frac{\partial\Phi}{\partial y}(j(E), j')}$$

$$a' = -\frac{1}{48}\frac{s^2}{j'(j' - 1728)}$$

$$b' = -\frac{1}{864}\frac{s^3}{j'^2(j' - 1728)}$$

Then $y^2 = x^3 + a'x + b'$ is the equation for E'. This computation takes $O(\ell^{3+\varepsilon})$ time (to compute $\Phi_\ell(x, y)$) which is enormous as ℓ grows.

Computing the group action: indirect approach

An indirect approach to computing $\mathfrak{b} * E$ is much faster.

- Using index calculus, find a factorization

$$[\mathfrak{b}] = [\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_t^{e_t}]$$

  valid in the ideal class group $\mathrm{Cl}(\mathcal{O}_D)$, where the primes $\mathfrak{p}_i$ are taken from a *factor base* of small primes. This process takes subexponential time.
- Evaluate $\mathfrak{p}_1^{e_1} * \cdots * \mathfrak{p}_t^{e_t} * E$ repeatedly, one (small) prime at a time.

Main results

Theorem (Jao and Soukharev, ANTS IX, 2010)

The indirect method takes $L_p(\frac{1}{2}, \frac{\sqrt{3}}{2})$ time to evaluate the group action (GRH + heuristics).

Theorem (Childs, Jao and Soukharev)

On a quantum computer, quotients can be computed in $L_p(\frac{1}{2}, \frac{\sqrt{3}}{2})$ operations (GRH).

Remark

We use a result on expansion properties of Cayley graphs of ideal class groups [Jao, Miller, Venkatesan 2009] to eliminate extra heuristics. Our results assume *only* GRH.

Polynomial space

- Kuperberg's algorithm uses space $\exp(O(\sqrt{\ln n}))$.
- [Regev 2004] presents a modified algorithm using only polynomial space for the case $A = \mathbb{Z}_{2^n}$, with running time

$$\exp(O(\sqrt{n \ln n})) = L_{2^n}(\tfrac{1}{2}, O(1)).$$

- Combining Regev's ideas with techniques used by Kuperberg for the case of a general abelian group (of order N), and performing a careful analysis, we find an algorithm with running time $L_N(\frac{1}{2}, \sqrt{2})$ using only polynomial space.
- Thus there is a quantum algorithm to construct elliptic curve isogenies using only polynomial space in time $L_p(\frac{1}{2}, \frac{\sqrt{3}}{2} + \sqrt{2})$.

Isogeny-based cryptography with supersingular curves

Motivation:

- Ordinary curves allow for a subexponential quantum attack.
- Ordinary curves are slow [Stolbunov 2010, Table 1]:

Security (bits)	$\lceil \log p \rceil$ (bits)	Time (seconds)
	224	19
80	244	21
96	304	56
112	364	90
128	428	229

- Isogenies over supersingular curves were proposed previously for use in hash functions (Charles, Goren, Lauter 2009)

Supersingular curve isogenies

Let E be a supersingular elliptic curve over $\mathbb{F}_q$.

- $j(E) \in \mathbb{F}_{p^2}$
- $\mathrm{End}(E)$ is a right order $\mathcal{O} \subset \mathbb{Q}_{p,\infty}$

For every isogeny $\phi\colon E \to E'$:

- $\ker \phi$ corresponds to a left ideal ϕ of $\mathcal{O}$ of norm $\deg \phi$
- $\mathrm{End}(E')$ is the right order of I_ϕ:

$$\mathrm{End}(E') \cong \{x \in \mathrm{End}(E) \otimes \mathbb{Q} : I_\phi x \subset I_\phi\}$$

- Suppose that $\phi_1\colon E \to E_1$ and $\phi_2\colon E \to E_2$ correspond to I_1 and I_2. Then $E_1 \cong E_2$ if and only if I_1 and I_2 are in the same left ideal class.

Unfortunately, there is no abelian group action of the set of left ideal classes on the set of supersingular j-invariants.

Kernel points

Basic idea

Represent an isogeny using (a generator of) its kernel.

- Alice chooses $R_A \in E$ and computes $\phi_A \colon E \to E/\langle R_A \rangle$
- Alice sends $E/\langle R_A \rangle$ to Bob
- Bob chooses $R_B \in E$ and computes $\phi_B \colon E \to E/\langle R_B \rangle$
- Bob sends $E/\langle R_B \rangle$ to Alice
- The quotient operation is commutative:

$$\begin{aligned}(E/\langle R_A \rangle)/\langle \phi_A(R_B) \rangle &\cong E/\langle R_A, R_B \rangle \\ &= E/\langle R_B, R_A \rangle \cong (E/\langle R_B \rangle)/\langle \phi_B(R_A) \rangle\end{aligned}$$

Given R_A (R_B etc.), one can compute ϕ_A (ϕ_B etc.) using Velu's formulas.

Problem #1

Alice needs $\phi_B(R_A)$ in order to compute $(E/\langle R_B \rangle)/\langle \phi_B(R_A) \rangle$.

Solution

- Fix a $\mathbb{Z}$-module basis P, Q of $E(\mathbb{F}_{p^2})$.
- Alice chooses $R_A = mP + nQ$.
- Bob sends $(\phi_B(P), \phi_B(Q))$ to Alice.
- Alice computes $\phi_B(R_A) = m\phi_B(P) + n\phi_B(Q)$

Problem #2

Computing $E/\langle R_A \rangle$ from R_A from Velu's formulas requires $O(\ell^3)$ operations.

Solution

- Choose E so that $\ell^e \mid \#E(\mathbb{F}_{p^2})$, where ℓ is a small prime
- Choose R_A to have order ℓ^e
- Then $E/\langle R_A \rangle$ can be efficiently computed as a composition of e isogenies of degree ℓ

For points of smooth order, discrete log is easy. But our scheme is based on isogenies, not discrete log.

Problem #3

If $R_A = m_A P + n_A Q$, then an adversary who knows $\phi_A(P), \phi_A(Q)$ can find a generator for $\langle R_A \rangle$ by solving

$$x\phi_A(P) + y\phi_A(Q) = 0$$

for $x, y \in \mathbb{Z}$.

Solution

Use different smooth order subgroups for Alice and Bob:

- Choose E so that $\ell_A^{e_A} \ell_B^{e_B}$ divides $\#E(\mathbb{F}_{p^2})$
- Choose $\mathbb{Z}$-bases $\{P_A, Q_A\}$ of $E[\ell_A^{e_A}]$ and $\{P_B, Q_B\}$ of $E[\ell_B^{e_B}]$
- Alice chooses $R_A = m_A P_A + n_A Q_A$ of order $\ell_A^{e_A}$
- Alice computes $\phi_A \colon E \to E/\langle R_A \rangle$
- Alice sends $E/\langle R_A \rangle$ and $\phi_A(P_B), \phi_A(Q_B)$ to Bob

Now the adversary has $\phi_A(P_B), \phi_A(Q_B)$ but $R_A = m_A P_A + n_A Q_A$ is a linear combination of P_A and Q_A

Key exchange

Public parameters:

- Prime $p = \ell_A^{e_A} \ell_B^{e_B} \cdot f \pm 1$
- Supersingular elliptic curve $E/\mathbb{F}_{p^2}$ of order $(p \mp 1)^2$
- $\mathbb{Z}$-bases $\{P_A, Q_A\}$ of $E[\ell_A^{e_A}]$ and $\{P_B, Q_B\}$ of $E[\ell_B^{e_B}]$

Alice:

- Choose $R_A = m_A P_A + n_A Q_A$ of order $\ell_A^{e_A}$
- Compute $\phi_A \colon E \to E/\langle R_A \rangle$
- Send $E/\langle R_A \rangle, \phi_A(P_B), \phi_A(Q_B)$ to Bob

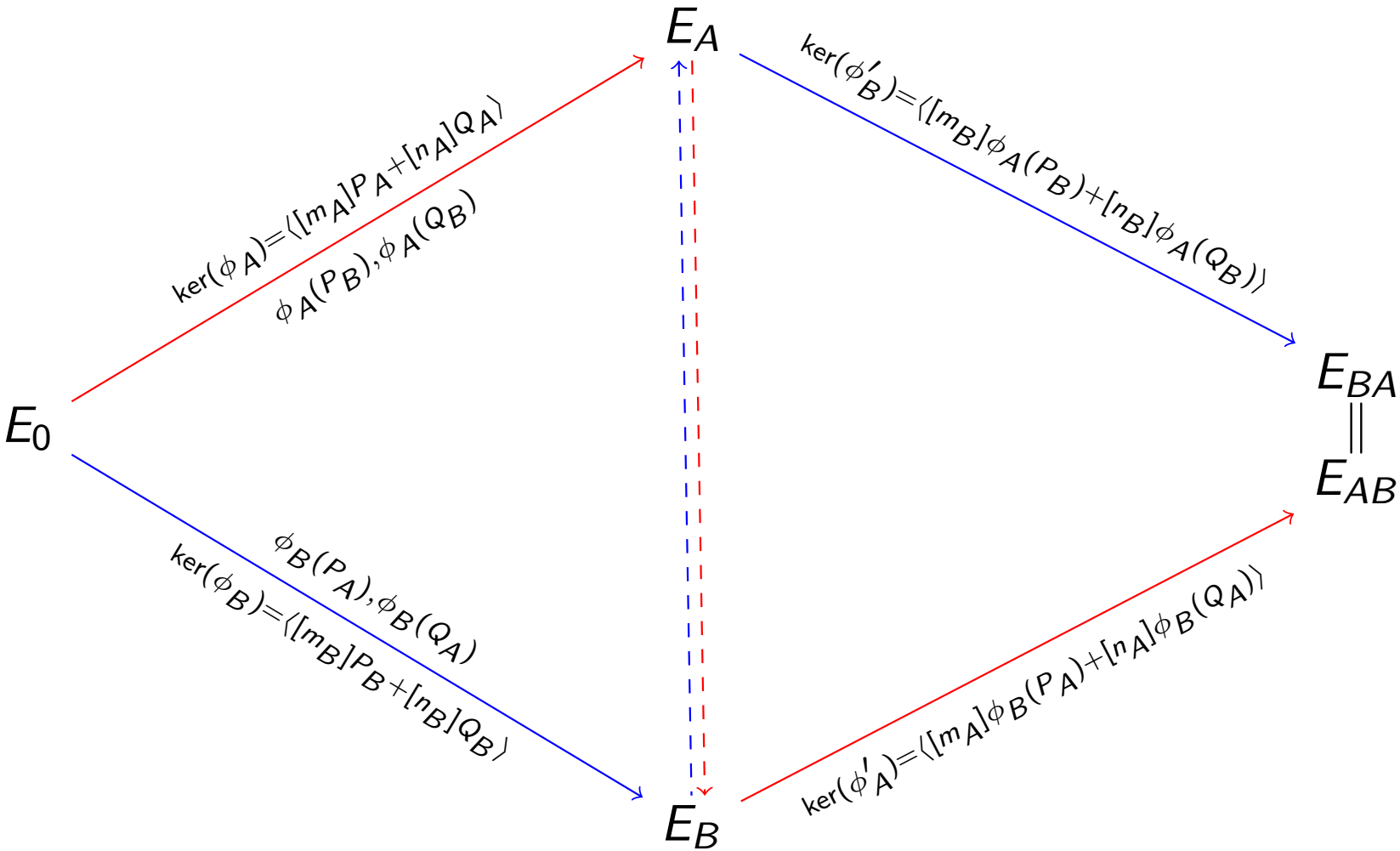
Bob:

- Choose $R_B = m_B P_B + n_B Q_B$ of order $\ell_B^{e_B}$
- Compute $\phi_B \colon E \to E/\langle R_B \rangle$
- Send $E/\langle R_B \rangle, \phi_B(P_A), \phi_B(Q_A)$ to Alice

The shared secret is

$$E/\langle R_A, R_B \rangle = (E/\langle R_A \rangle)/\langle m_A \phi_B(P_A) + n_A \phi_B(Q_A) \rangle = (E/\langle R_B \rangle)/\langle m_B \phi_A(P_B) + n_B \phi_A(Q_B) \rangle$$

Diagram


E_A
$\ker(\phi_A) = \langle [m_A]P_A + [n_A]Q_A \rangle$
$\phi_A(P_B), \phi_A(Q_B)$
$\ker(\phi'_B) = \langle [m_B]\phi_A(P_B) + [n_B]\phi_A(Q_B) \rangle$
E_0
E_{BA}
E_{AB}
$\phi_B(P_A), \phi_B(Q_A)$
$\ker(\phi_B) = \langle [m_B]P_B + [n_B]Q_B \rangle$
$\ker(\phi'_A) = \langle [m_A]\phi_B(P_A) + [n_A]\phi_B(Q_A) \rangle$
E_B

Attacks against the scheme

Fastest known attack (given E and E_A):

- Build a tree of degree ℓ_A-isogenies of depth $e_A/2$ starting from E
- Build a tree of degree ℓ_A-isogenies of depth $e_A/2$ starting from E_A
- Find a common vertex between the two trees

Using claw-finding algorithms, one can solve this problem in:

- $O(p^{1/4})$ time on a classical computer
- $O(p^{1/6})$ time on a quantum computer

Assuming that this is indeed the fastest possible attack, we need a 768-bit prime for 128-bit security against quantum computers.

Implementation

To compute $\phi_A \colon E \to E/\langle R_A \rangle$:

- Set $R_0 := [m_A]P_A + [n_A]Q_A$.
- For $0 \leq i < e_A$, set

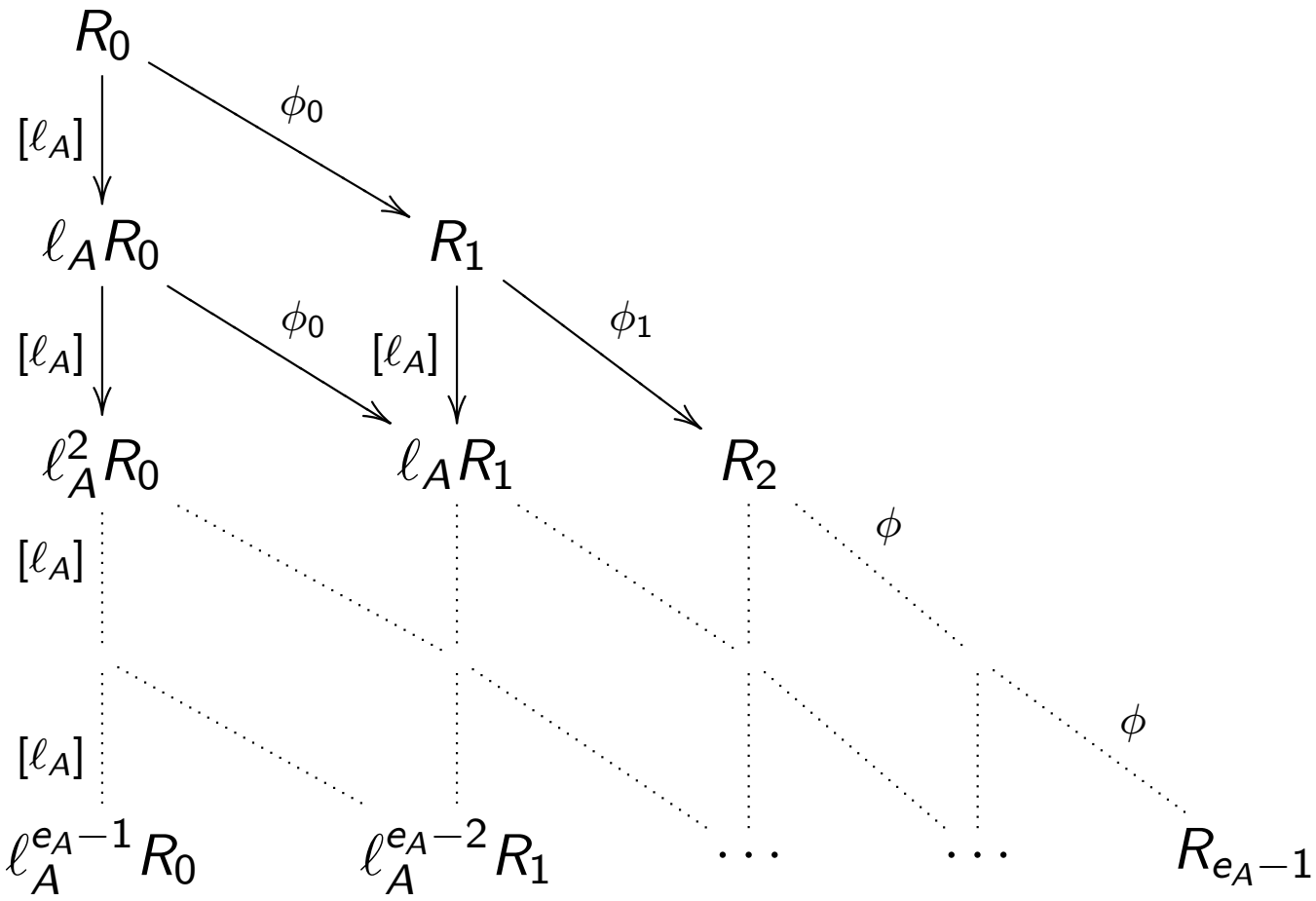
$$E_{i+1} = E_i/\langle \ell_A^{e_A - i - 1} R_i \rangle, \quad \phi_i : E_i \to E_{i+1}, \quad R_{i+1} = \phi_i(R_i)$$

- Then ϕ_i is a degree ℓ_A isogeny from E_i to E_{i+1}.
- We have

$$E_A = E_{e_A}$$
$$\phi_A = \phi_{e_A - 1} \circ \cdots \circ \phi_0$$

This algorithm is quadratic in e_A.

Computational strategies



The outer edges are always needed. For the inner nodes, one can:

- Compute *vertical* arrows (multiplication-based strategy)
- Compute *diagonal* arrows (isogeny-based strategy)

Timings

	Alice		Bob	
	round 1	round 2	round 1	round 2
$2^{253}3^{161}7-1$	365 ms	363 ms	318 ms	314 ms
$5^{110}7^{91}284-1$	419 ms	374 ms	369 ms	326 ms
$11^{74}13^{69}384-1$	332 ms	283 ms	321 ms	272 ms
$17^{62}19^{60}210+1$	330 ms	274 ms	331 ms	276 ms
$23^{56}29^{52}286+1$	339 ms	274 ms	347 ms	277 ms
$31^{51}41^{47}564-1$	355 ms	279 ms	381 ms	294 ms
$2^{384}3^{242}8-1$	1160 ms	1160 ms	986 ms	973 ms
$5^{165}7^{137}2968-1$	1050 ms	972 ms	916 ms	843 ms
$11^{111}13^{104}78+1$	790 ms	710 ms	771 ms	688 ms
$17^{94}19^{90}116-1$	761 ms	673 ms	750 ms	661 ms
$23^{85}29^{79}132-1$	755 ms	652 ms	758 ms	647 ms
$31^{77}41^{72}166+1$	772 ms	643 ms	824 ms	682 ms
$2^{512}3^{323}799-1$	2570 ms	2550 ms	2170 ms	2150 ms
$5^{220}7^{182}538+1$	2270 ms	2140 ms	1930 ms	1810 ms
$11^{148}13^{138}942+1$	1650 ms	1520 ms	1570 ms	1440 ms
$17^{125}19^{120}712-1$	1550 ms	1430 ms	1520 ms	1380 ms
$23^{113}29^{105}1004-1$	1480 ms	1330 ms	1470 ms	1300 ms

Current record

Source code: `www.prism.uvsq.fr/~dfl/`

- We represent curves in Montgomery form:

$$By^2 = x^3 + Ax^2 + x$$

- Our formulas for 2-isogenies and 4-isogenies are faster than anything else in the literature.
- Current record (2011-09-19): 500ms for 1024-bit primes
- This performance is achieved using a mixed approach:
  - "ℓ_A" $= 4^5$
  - Isogeny-based method for $4 \longrightarrow 4^5$
  - Multiplication-based method for $\ell_A \longrightarrow \ell_A^{e_A}$

References

- D. Charles, E. Goren, and K. Lauter. Cryptographic hash functions from expander graphs. J. Cryptol. 2009, pp. 93–113.
- J. Couveignes, Hard Homogeneous Spaces, eprint:2006/291.
- S. D. Galbraith, F. Hess, and N. P. Smart. Extending the GHS Weil descent attack. Eurocrypt 2002, Springer LNCS 2332, pp. 29–44.
- D. Jao, S. D. Miller, and R. Venkatesan. Expander graphs based on GRH with an application to elliptic curve cryptography. J. Num. Thy. 129 (6), 2009, pp. 1491-1504.
- D. Jao and V. Soukharev, A subexponential algorithm for evaluating large degree isogenies, ANTS IX, Springer LNCS 6197, pp. 219–233.
- G. Kuperberg, A subexponential-time quantum algorithm for the dihedral hidden subgroup problem, Siam J. Comput. 35 (1) (2005), pp. 170–188.
- O. Regev, A Subexponential Time Algorithm for the Dihedral Hidden Subgroup Problem with Polynomial Space, arxiv:quant-ph/0406151
- A. Rostovtsev and A. Stolbunov, Public-key cryptosystem based on isogenies, eprint:2006/145.
- A. Stolbunov, Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves, Adv. Math. Comm. 4 (2) (2010), pp. 215–235.

This work: arXiv:1012.4019 and ePrint:2011/506