Overview of elliptic curve isogenies based public-key cryptography assumptions

David Jao

Department of Combinatorics & Optimization
University of Waterloo

February 24, 2020

Elliptic curves

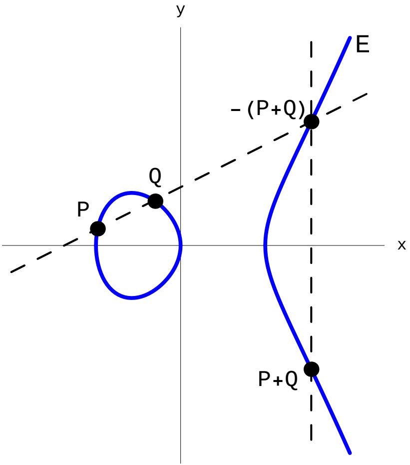
Definition

An elliptic curve over a field F is a nonsingular curve E of the form

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

for fixed constants $a, b \in F$.

The set of projective points on an elliptic curve forms a group, with identity $\infty = [0 : 1 : 0]$.



Isogenies

Definition

An isogeny is a morphism ϕ of algebraic varieties between two elliptic curves, such that ϕ is a group homomorphism.

Concretely:

$$
\begin{aligned}
\phi \colon E &\to E' \\
\phi(x, y) &= (\phi_x(x, y), \phi_y(x, y)) \\
\phi_x(x, y) &= \frac{f_1(x, y)}{f_2(x, y)} \\
\phi_y(x, y) &= \frac{g_1(x, y)}{g_2(x, y)}
\end{aligned}
$$

where f_1, f_2, g_1, and g_2 are all polynomials. The degree of an isogeny is its degree as an algebraic map.

Development of isogeny-based cryptography

Hash functions

CGL: Charles, Goren, Lauter (https://ia.cr/2006/021).

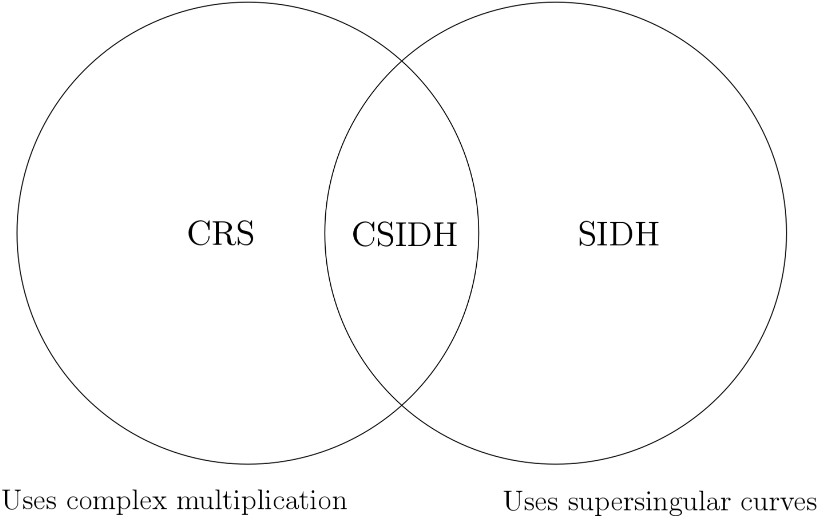
Public-key cryptosystems

CRS: Couveignes (http://ia.cr/2006/291), Rostovstev and Stolbunov (http://ia.cr/2006/145).

SIDH: Supersingular Isogeny Diffie-Hellman — Jao and De Feo (http://ia.cr/2011/506).

CSIDH: Commutative SIDH — Castryck, Lange, Martindale, Panny, Renes (http://ia.cr/2018/383).

Diagram of isogeny-based public-key cryptosystems



Constructing isogenies

Every isogeny is a group homomorphism and thus has a kernel

$$\ker \phi = \{P \in E : \phi(P) = \infty\}.$$

Given an elliptic curve E and a finite subgroup K of E, one can show that there exists a unique (up to isomorphism) separable isogeny $\phi_K : E \to E/K$ such that $\ker \phi_K = K$ and $\deg \phi_K = |K|$.

Vélu's formulas (1971) give an explicit construction of ϕ_K.

Isogenies of degree 2

- Let $E : y^2 = x^3 + ax + b$.
- Suppose $K = \{\infty, P\}$. Then $P + P = \infty$, so $P = (x_P, 0)$ with $x_P^3 + ax_P + b = 0$.
- We have

$$E/K : y^2 = x^3 + (a - 5(3x_P^2 + a))x + (b - 7x_P(3x_P^2 + a))$$

$$\phi_K(x, y) = \left(x + \frac{3x_P^2 + a}{x - x_P},\ y - \frac{y(3x_P^2 + a)}{(x - x_P)^2}\right)$$

Isogenies of degree 3

- Let $E : y^2 = x^3 + ax + b$.
- Suppose $K = \{\infty, P, -P\}$. Then $P = (x_P, y_P)$ with $3x_P^4 + 6ax_P^2 - a^2 + 12bx_P = 0$ and $y_P^2 = x_P^3 + ax_P + b$.
- We have

$$E/K : y^2 = x^3 + (a - 10(3x_P^2 + a))x + (b - 28y_P^2 - 14x_P(3x_P^2 + a))$$

$$\phi_K(x, y) = \left(x + \frac{2(3x_P^2 + a)}{x - x_P} + \frac{4y_P^2}{(x - x_P)^2}, \; y - \frac{8yy_P^2}{(x - x_P)^3} - \frac{2y(3x_P + a)}{(x - x_P)^2} \right)$$

Isogenies of degree 2^e in SIDH

- Evaluating an isogeny of degree d using Vélu's formulas directly takes $O(d)$ operations, too slow when d is large.
- Instead, we use isogenies of prime power degree, and evaluate them step by step.
- Suppose $K \cong \mathbb{Z}/2^e\mathbb{Z}$. Then the subgroup tower

$$0 \subset \mathbb{Z}/2\mathbb{Z} \subset \mathbb{Z}/4\mathbb{Z} \subset \cdots \subset \mathbb{Z}/2^e\mathbb{Z}$$

  allows us to factor $\phi_K \colon E \to E/K$ into the composition of isogenies

$$E \to E/(\mathbb{Z}/2\mathbb{Z}) \to E/(\mathbb{Z}/4\mathbb{Z}) \to \cdots \to E/(\mathbb{Z}/2^e\mathbb{Z})$$

- Each individual isogeny has degree 2 and is easy to compute.
- The composition of all the isogenies is ϕ_K, of degree 2^e.
- A similar trick works for any prime power ℓ^e where ℓ is small.

SIDH overview

1. Public parameters: Supersingular elliptic curve E over $\mathbb{F}_{p^2}$.
2. Alice chooses a kernel $A \subset E(\mathbb{F}_{p^2})$ of size 2^e and sends E/A.
3. Bob chooses a kernel $B \subset E(\mathbb{F}_{p^2})$ of size 3^f and sends E/B.
4. The shared secret is

$$E/\langle A, B\rangle = (E/A)/\phi_A(B) = (E/B)/\phi_B(A).$$

Diffie-Hellman (DH)

$$\begin{array}{ccc} g & \longrightarrow & g^x \\ \downarrow & & \downarrow \\ g^y & \longrightarrow & g^{xy} \end{array}$$

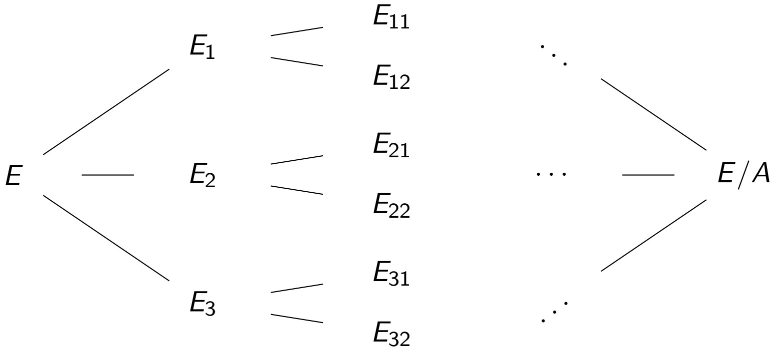
SIDH

$$\begin{array}{ccc} E & \xrightarrow{\phi_A} & E/A \\ \downarrow{\scriptstyle \phi_B} & & \downarrow \\ E/B & \longrightarrow & E/\langle A, B\rangle \end{array}$$

Attacks

Hard problem: Given E and E/A, find A.

Fastest known (passive) attack is a meet-in-the-middle collision search or claw search on a search space of size $\deg(\phi)$.



More details: Jaques and Schanck (`https://ia.cr/2019/103`)

Complex multiplication action

For an ordinary elliptic curve $E/\mathbb{F}_p$, there is a free and transitive group action

$$*\colon \ \mathrm{Cl}(\mathrm{End}(E)) \times \mathcal{ELL}(\mathbb{F}_p) \to \mathcal{ELL}(\mathbb{F}_p)$$

where

- $\mathrm{End}(E)$ is the ring of endomorphisms of E
- $\mathrm{Cl}(\mathrm{End}(E))$ denotes the ideal class group of $\mathrm{End}(E)$
- $\mathcal{ELL}(\mathbb{F}_p)$ is the set of isomorphism classes of elliptic curves over $\mathbb{F}_p$ with endomorphism ring isomorphic to $\mathrm{End}(E)$

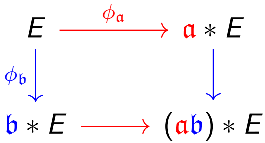
defined by

$$\begin{aligned}[\mathfrak{a}] * E = E/\ker\mathfrak{a} &= E/\{P \in E : \forall\ \phi \in \mathfrak{a},\ \phi(P) = \infty\} \\ &= E/\bigcap_{\phi\in\mathfrak{a}} \ker\phi.\end{aligned}$$

Couveignes-Rostovstev-Stolbunov (CRS)

Public parameters: Ordinary elliptic curve $E/\mathbb{F}_p$ and complex multiplication action $*$: $\mathrm{Cl}(\mathrm{End}(E)) \times \mathcal{ELL}(\mathbb{F}_p) \to \mathcal{ELL}(\mathbb{F}_p)$.

1. Alice chooses a group element $\mathfrak{a} \in G$ and sends $\mathfrak{a} * E$.
2. Bob chooses a group element $\mathfrak{b} \in G$ and sends $\mathfrak{b} * E$.
3. The shared secret is $(\mathfrak{a}\mathfrak{b}) * E = \mathfrak{a} * (\mathfrak{b} * E) = \mathfrak{b} * (\mathfrak{a} * E)$.



CSIDH uses the same group action, but over a supersingular curve.

From isogenies to hidden subgroups

- The hard problem in CRS and CSIDH is to compute group action inverses: Given $G \times X \to X$ and $x_0, x_1 \in X$, find $\gamma \in G$ such that $\gamma x_1 = x_0$.
- Let $\phi\colon \mathbb{Z}/2 \to \mathrm{Aut}(G)$ be given by $\phi(b)(g) = g^{(-1)^b}$.
- Consider the function $f\colon G \rtimes_\phi \mathbb{Z}/2 \to X$, $f(g, b) = gx_b$.
- Since the group action is free, we have

$$f(g_1, b_1) = f(g_2, b_2) \iff \begin{aligned} & b_1 = 0, b_2 = 1, \text{ and } g_1^{-1}g_2 = \gamma \\ \text{or } & b_1 = 1, b_2 = 0, \text{ and } g_2^{-1}g_1 = \gamma \\ \text{or } & b_1 = b_2 \text{ and } g_1 = g_2 \end{aligned}$$

  Hence f hides the subgroup $\{(0,0), (\gamma, 1)\} \subset G \rtimes_\phi \mathbb{Z}/2$.
- If we solve the hidden subgroup problem for f, then we will have found γ.

Dihedral hidden subgroup problem

Reference: Kuperberg, `arXiv:quant-ph/0302112`

- For simplicity, suppose $G = \mathbb{Z}/N$ and $D_N = \mathbb{Z}/N \rtimes \mathbb{Z}/2$.
- Suppose f hides the subgroup $H = \{(0,0), (\gamma, 1)\} \subset D_N$.
- Form the state
$$\frac{1}{\sqrt{|D_N|}} \sum_{d \in D_N} |d\rangle \, |f(d)\rangle$$
- Measure the second register and discard the result to obtain
$$\frac{1}{\sqrt{|(z,0)H|}} \sum_{d \in (z,0)H} |d\rangle = \frac{1}{\sqrt{2}} (|(z,0)\rangle + |(z+\gamma, 1)\rangle$$
in the first register, for some random coset $(z,0)H$. By abuse of notation, denote this "coset state" by $|(z,0)H\rangle$.
- We can generate lots of these coset states, for random cosets. (We have no control over which cosets we obtain.)

Quantum Fourier transform

- Apply the quantum Fourier transform to the first coordinate:

$$\begin{aligned} |(z,0)H\rangle &= \frac{1}{\sqrt{2}}(|(z,0)\rangle + |(z+\gamma,1)\rangle) \\ &\overset{\text{QFT}}{\mapsto} \frac{1}{\sqrt{2N}} \sum_{k \in \mathbb{Z}_N} (\zeta_N^{kz} |(k,0)\rangle + \zeta_N^{k(z+\gamma)} |(k,1)\rangle) \\ &= \frac{1}{\sqrt{N}} \sum_{k \in \mathbb{Z}_N} \zeta_N^{kz} |k\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + \zeta_N^{k\gamma} |1\rangle) \end{aligned}$$

- Measure the first register to obtain $|k\rangle$ for some random k. The second register is

$$\frac{1}{\sqrt{2}}(|0\rangle + \zeta_N^{k\gamma} |1\rangle)$$

Denote this quantum state by $|\psi_k\rangle$. We can generate lots of these states for random k, with no control over k (but we do know the value of k for each such quantum state).

Overall strategy

We now assume for (further!) simplicity that N is a power of 2. The strategy is as follows:

- If we could construct

$$|\psi_k\rangle = \frac{1}{\sqrt{2}}(|0\rangle + \zeta_N^{k\gamma}|1\rangle)$$

  for k of our choice, then (for example) we could find $|\psi_{N/2}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{\gamma}|1\rangle)$.
- Measure $|\psi_{N/2}\rangle$ w.r.t. $\left\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right\}$ to obtain the least significant bit of γ.
- Reduce to $D_{N/2}$ and use induction to find γ.

Combining states

We can exert limited control over $|\psi_k\rangle$ by *combining states*:

$$\begin{aligned} |\psi_p, \psi_q\rangle &= \frac{1}{2}(|0,0\rangle + \zeta_N^{p\gamma}|1,0\rangle + \zeta_N^{q\gamma}|0,1\rangle + \zeta_N^{(p+q)\gamma}|1,1\rangle \\ &\overset{\text{CNOT}}{\mapsto} \frac{1}{2}(|0,0\rangle + \zeta_N^{p\gamma}|1,1\rangle + \zeta_N^{q\gamma}|0,1\rangle + \zeta_N^{(p+q)\gamma}|1,0\rangle \\ &= \frac{1}{\sqrt{2}}(|\psi_{p+q}, 0\rangle + \zeta_N^{q\gamma}|\psi_{p-q}, 1\rangle) \end{aligned}$$

We now measure the second register.

- If we get $|0\rangle$, then the first register is $|\psi_{p+q}\rangle$.
- If we get $|1\rangle$, then the first register is $\zeta_N^{q\gamma}|\psi_{p-q}\rangle = |\psi_{p-q}\rangle$.

We can't control which of $|\psi_{p\pm q}\rangle$ we get, but we know which one we got.

Kuperberg sieve

1. Create $A \approx 4^{\sqrt{\log N}}$ quantum states ψ_k, for random $k \in \mathbb{Z}_N$.
2. Group the quantum states into buckets according to their last $\sqrt{\log N}$ bits (least significant bits). On average each bucket has $A/2^{\sqrt{\log N}}$ quantum states and there are $2^{\sqrt{\log N}}$ buckets.
3. Combine pairs of states in each bucket, with the goal of zeroing out the last $\sqrt{\log N}$ bits.
   - On average, combining states succeeds half the time.
   - If successful, we destroy two states and create one new state.
   - If unsuccessful, we lose two states and create nothing.
   - On average, we have $1/4$ as many states as we had before.
4. We get $A/4$ quantum states, whose last $\sqrt{\log N}$ bits are zero.
5. Repeat this bucket sorting process on the next $\sqrt{\log N}$ bits, to obtain $A/4^2$ quantum states, whose last $2\sqrt{\log N}$ bits are zero.
6. ... Eventually we obtain $A/4^{\sqrt{\log N}} \approx 1$ quantum states, with all but the most significant bit zero.