Elliptic curve isogenies based public-key cryptography assumptions

Sachin Kumar
University of Waterloo, Faculty of Mathematics

Elliptic Curves and Isogenies

Definition 0.1. *An elliptic curve over a field $\mathbb{F}$ is a non-singular curve E of the form,*

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

for fixed constants $a, b \in \mathbb{F}$.

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

Definition 0.2. *An isogeny is a morphism ϕ of algebraic varieties between two elliptic curves, such that ϕ is a group homomorphism.*

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

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

Public-Key Cryptosystems

- CRS: Couveignes, Restovstev and Stolbunov
- SIDH: Supersingular Isogeny Diffie-Hellman (Jao and De Feo)
- CSIDH: Commutative SIDH (Castryck, Lange, Martindale, Panny and Renes)

CRS uses complex multiplication, SIDH uses supersingular algebraic curves and CSIDH uses both the complex multiplication and supersingular algebraic curves.

Constructing isogenies

Every isogeny is a group homomorphism and thus has a kernel,

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

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

Vélu's formulas (1971) give an explicit construction of ϕ_K.
Let H be any finite subgroup of E. Then the map given by $P \mapsto (X, Y)$ where,

$$X = x(P) + \sum_{Q\in H\setminus\{\infty\}} (x(P+Q) - x(Q))$$
$$Y = y(P) + \sum_{Q\in H\setminus\{\infty\}} (y(P+Q) - y(Q))$$

is an isogeny ϕ with domain E and kernel H. E/G denote the co-domain of ϕ. This co-domain is unique upto isomorphism. The computational cost of evaluating Vélu's formula is $O(\sqrt{|H|}) = O(\sqrt{\deg\phi}) \leq 3$.

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 $x_P^4 + 6ax_P^2 - a^2 + 12bx_P = 0$ 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 $O(d^3)$ 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,

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

allow us to factor $\phi_K : E \to E/K$ 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

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

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

Commutative diagram of Diffie-Hellman (DH) and Supersingular Isogeny DH (SIDH),

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

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

Here ϕ_A (respectively ϕ_B) denotes the isogeny with kernel A (respectively B)

Detailed description of SIDH

Public parameters:

- Prime $p = \ell_A^{e_A}\ell_B^{e_B} - 1$.
- E is a supersingular over $\mathbb{F}_{p^2}$, $\#E(\mathbb{F}_{p^2}) = (p+1)^2 = (\ell_A^{e_A}\ell_B^{e_B})^2$
- $\mathbb{Z}$-basis $\{P_A, Q_A\}$ of $E[\ell_A^{e_A}]$ and $\{P_B, Q_B\}$ of $E[\ell_B^{e_B}]$,

Alice:

- Choose $\mathrm{sk}_A \in \mathbb{Z}$ and compute $A = \langle P_A + \mathrm{sk}_A Q_A\rangle$ of order $\ell_A^{e_A}$.
- Compute $\phi_A : E \to E_A$.
- Send $\mathrm{pk}_A = (E_A, \phi_A(P_B), \phi_A(Q_B))$ to Bob.

Bob:

- Same as Alice, replacing A with B and vice-versa.

The shared secret is derived from,

$$\begin{aligned} E/\langle A, B\rangle &= (E_A)/\langle \phi_A(P_B) + \mathrm{sk}_B\phi_A(Q_B)\rangle \\ &= (E_B)/\langle \phi_B(P_A) + \mathrm{sk}_A\phi_B(Q_A)\rangle \end{aligned}$$

Attacks

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

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

- Classical: $\sqrt{\deg \phi}$
- Quantum: $\sqrt[3]{\deg \phi}$

Complex Multiplication action

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

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

where,

- $\mathrm{End}(E)$ is the ring of endomorphisms of E.
- $\mathrm{CI}(\mathrm{End}(E))$ 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 endomorphisms 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, Restovstev and Stolbunov (CRS)

Public parameters: Ordinary elliptic curve $E/\mathbb{F}_p$ and complex multiplication action $* : \mathrm{CI}(\mathrm{End}(E)) \times \mathcal{ELL}(\mathbb{F}_p) \to \mathcal{ELL}(\mathbb{F}_p)$. Alice chooses a group element $\mathfrak{a} \in G$ and send $\mathfrak{a} * E$. Bob chooses a group element $\mathfrak{b} \in G$ and sends $\mathfrak{b} * E$. 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 algebraic curve.

$$\begin{array}{ccc} E & \xrightarrow{\phi_{\mathfrak{a}}} & \mathfrak{a} * E \\ {\scriptstyle \phi_{\mathfrak{b}}}\downarrow & & \downarrow \\ \mathfrak{b} * E & \longrightarrow & (\mathfrak{a}\mathfrak{b}) * E \end{array}$$

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 $\phi : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(G)$ be given by $\phi(b)(g) = g^{(-1)^b}$. Consider the function $f : G \rtimes_\phi \mathbb{Z}/2\mathbb{Z} \to X,\ f(g, b) = g x_b$. Since the group action is free, we have

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

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

Dihedral hidden subgroup problem

For simplicity, suppose $G = \mathbb{Z}/N$ and $D_N = \mathbb{Z}/N \rtimes \mathbb{Z}/2\mathbb{Z}$. 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).

Here is a table with some commonly used cryptosystem and their hard problems (reason, why they are used in cryptography).

Cryptosystem	**Hard Problems**
Diffie-Hellman (DH) Elliptic Curve Cryptography (ECC) Pairing-based Cryptography	Discrete Logarithm Problem (DLP)
Rivest-Shamir-Adleman (RSA) Rabin Composite Residues	Factoring integers
Code-based Cryptography	Decoding Linear Codes
Lattice-based/NTRU Isogeny-based/CRS	Finding Short Lattice vectors
SIDH/SIKE	Computing Isogenies