Elliptic Curve Isogeny and its Use in Post Quantum Cryptography

Carly Larsson
CS 293G Cryptographic Engineering
16 June 2017

Abstract

There are few algorithms that meet the security needs of the post-quantum computing days ahead, and already the need grows for the implementation and development of fast, efficient, and secure post-quantum crypto-systems. The popularity of lattice based post-quantum cryptography does not mean that it is the only method that is being researched and used. The use of supersingular elliptic curve isogenies in cryptosystems is also promising, and has several benefits. In this paper we will explore the background of supersingular elliptic curve isogenies, and their use in cryptogrphy.

1. The State of Cryptography

Every day, all day long, millions of people use computers. They expect there data to remain safe, there identities to remain there own, and there money to remain in there bank accounts. The majority of them don't realize the lengths to which computer scientists and math matician have gone to ensure (for the most part) the secuity of there computer. However, a time approaches when a quantum computer could readily overcome the hard problems used in ensure that security; mainly the Diffie-Hallman Probelm $y = b^x mobp$ where x is what you are solving for, the Elliptic Curve Diffie-Hallman problem, and Factoring.

Shor's algorithm for quantum computers created in 1994, breaks RSA and other factor based crypto-systems. It does this by first reducing the factoring problem to an order finding problem, and then using a quantum algorithm to solve order-finding. This order problem can again be reduced to the Abelian Hidden Subgroup Problem (AHSP), which is more general and is the reduction of all the difficult problems mentioned above that keep the majority of cryptogrphy secure. The (AHSP) can be represented as:
Input: Abelian group G, a set X, $H \leq G$, and $f : G \to X$ where $f(g_1) = f(g_2)$ iff $g_1 H = g_2 H$
Output: A generating set H

This is important because Shor's algorithm can solve the AHSP for all finite Abelian groups, but not for non-Abelian groups. Now cryptographers look toward HSPs using non-Abelian groups, like the graph isomophism problem and shortest vector problems. These two problems make up the majority of promising post-quantum cryptography papers, and in this paper we will be examining the graph isomorphism problem more closely.

The graph isomorphism problem tries to determine whether two finite graphs are isomophic. This problem does not have a general polynomial time solution yet it two problems: it is

NP-intermediate nature and contains several subclasses of the problem that can be solved in polynomial time. In the same vein, when elliptic curve isogenies were first being considered for use in cryptography all cases of elliptic curve use were thought to be secure, but when Childs, Jao, and Soukharev created an quantum algorithm for computing normal elliptic curve isogenies the general case had to be reconsidered. This began the use of supersingular elliptics curves, whose properties make finding isogenies more difficult.

2. Elliptic Curves

To understand the use a elliptic curves and supersingular elliptic curves in post-quantum cryptography, a general examination of their characteristics should be made:

Elliptic Curves

An Elliptic Curve can be defined as:
A set of solutions (x,y) over a finite field $\Bbbk$ to an equation of the form
$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$
or also commonly in the Weierstrass form
$y^2 = x^3 + ax + b$
These curves form groups $G = (x, y) \in \Bbbk : (x, y)$ is a point on E the operation over the group is elliptic curve point addition which falls into normal point addition and point doubling.
Normal Point Addition:
Addition of two points is performed by constructing the line between the two points and finding its intersection with the curve.
$R = P + Q = \binom{p_x}{p_y} + \binom{q_x}{q_y}$
$s = \frac{p_y - q_y}{p_x - q_x}$
$r_x = s^2 - p_x - q_x$
$r_y = s(p_x - r_x) - p_y$
If the line is horizontal and there is no intersection, a point at ∞ is defined, such that $A + B = \infty$
Point Doubling:

Doubling doubling produces a tangent line at the point given; the horizontal reflection of where the tangent intersects the curve is the doubled value.
$R = P + P$
$s = \frac{3p_x^2 + a}{2p_y}$
$r_x = s^2 - 2p_x$
$r_y = s(p_x - r_x) - p_y$

Supersingular Elliptic Curves

Broadly Supersingular Elliptic Curves are a class of ECs with large endomorphism rings. There are many other ways to define them:
P-torsion points of the curve E is trivial, where the characteristic of $\Bbbk = p$
$E : y^2 = x(x-1)(x-)$ is supersingular iff is a root of $f(x) = \sum_{i=0}^{\frac{p-1}{2}} (ni)^2 x^i$
If the curve E is written as a cubic homogeneous $f(x, y, z)$ in the projective plane, then E is supersingular iff the coefficient of $(xyz)^{p-1}$ in $f(x, y, z)^{p-1}$ is zero.

3. Isogenies

An isongeny is a morphism or rational map that preserves identity denoted as $\varphi : E_1 \to E_2$ (though this definition seems to vary, and be a point of contention). So a simple example would be given E_1 you could find an isogeny by multiplying by $[m]$.

Finding an isogeny is not that difficult, but determining if two isogenies are equivalent, $f_1 : E_1 \to E_2$ versus $f_2 : E_1 \to E_2'$, complicates matters.

$$\begin{array}{ccc} E_1 & \xrightarrow{f_1} & E_2 \\ \downarrow & & \downarrow \\ E_1' & \xrightarrow{f_2} & E_2' \end{array}$$

The standard way of calculating their equivalency is by their kernals. The kernel is the set of geometric points $P \in E_1$ such that $f(P) = 0_{E_2}$
The group of separable isogenies, defined as:
Let $\varphi : E \to E'$ be an isogeny, and let $r_1(x)$ be the x-coordinate map. If the derivative of the

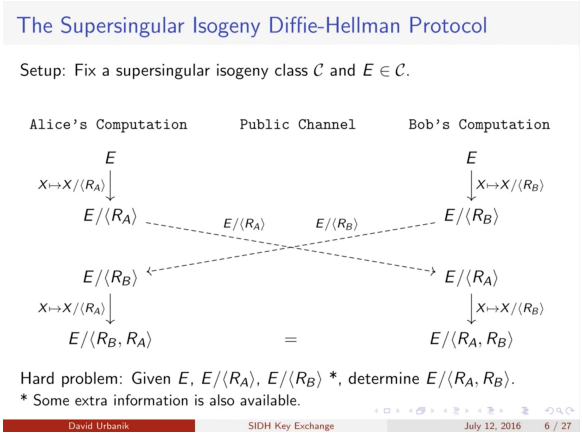
x-coordinate map $r_1'(x)$ is not 0 then φ is separable. Seperable isogenies' kernal size and degree are the same, where the degree is the degree as a rational map. Isongenies with a degree greater than 1, can factor into isogenies of a prime degree over $\mathbb{F}_q$.

You can also find isongenies that map to themselves, known as Endomorphisms: $(\varphi + \psi)(P) = \varphi(P) + \psi(P)$
Taking the endomorphism of an elliptic curve can help us categorize it. If $End(E/k) \simeq$ an order $\mathbb{O}$ in quaternion algebra over $\mathbb{Q}$, than E/k is a supersingular elliptic curve.

4. Using Elliptic Curve Isogenies

Using supersingular elliptic curves, the hard problem that is used for post-quantum cryptography is given E_1 and E_2, compute isongeny. In this case the isongeny is a surjective quotient map.

Below is an intuitive diagram of how a diffie-hallman exchange would work using elliptic curve isogenies:



However the diagram does not tell the entire story. When computing the second isogeny more information needs to be exchanged.
In order to compute $(E/R_B)/R_A = E/(R_B, R_A)$ you need to use Velu's formula which computes $E \to E/G$:
$X(P) = x(P) + \sum_{Q \in G/O_E}(x(P+Q) - x(Q))$
$Y(P) = y(P) + \sum_{Q \in G/O_E}(y(P+Q) - y(Q))$
However this requires knowledge of the subgroup of the domain curve, from the sender. This has to again be done using a DHP like exchange where a point P_A and Q_A are chosen to create, $R_A = m_A P_A + n_A Q_A$
The sender gives the receiver $\phi_B(P_A)$ and $\phi_B(Q_A)$ so the receiver can compute
$m_A \phi_B(P_A) + n_A \phi_B(Q_A) =$
$\phi_B(m_A P_A + n_A Q_A) = \phi_B(R_A)$

The fastest known implementation of this algorithm was created by Microsoft in April of 2016. As the field of Elliptic Curve Isogeny Cryptography matures, we are sure to see more efficient speed and storage. Just this past January, researchers created a hardware implementation of isogeny-based cryptography for supersingular isogeny Diffie-Hellman, and more the field is ripe for more advances.

Works Cited:

[1] Andrew M. Childs, David Jao, and Vladimir Soukharev. Constructing elliptic curve isogenies in quantum subexponential time. Cornell University, 15 July 2011.

[2] Brian Koziel, Reza Azarderakhsh, Mehran Mozaffari Kermani, and David Jao. Post-Quantum Cryptography on FPGA Based on Isogenies on Elliptic Curves. IEEE Transactions on Circuits and Systems, Vol. 64, NO. 1, January 2017.

[3] Jao D., De Feo L. (2011) Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies. In: Yang BY. (eds) Post-Quantum Cryptography. PQCrypto 2011. Lecture Notes in Computer Science, vol 7071. Springer, Berlin, Heidelberg.

[4] Robert, Damien. Isogenies and edomorphism rings of elliptic cureves. Microsoft Research, 15 September 2011.

[5] Ubanik, David. Introduction to the Post-Quantum Supersingular Isogeny Diffie-Hellman Protoco. Youtube Lecture, 11 September 16. https://youtu.be/PW5Vsu57o9I

[6] Vercauteren, Frederik. Elliptic Curve Isogeny Based Cryptosystems. KU Leuven ESAT/COSIC, 23 August 2016.