## **2.3. Isogenies**

An isogeny is a special type of function that connects two elliptic curves in a way that preserves their algebraic structure. Given two elliptic curves ​ and ​ over a finite field ​, an isogeny ​ is a non-constant map defined by rational functions (ratios of polynomials) with coefficients in ​​. This map satisfies , where represents the point at infinity on the elliptic curve. An isogeny is also a group homomorphism which means it preserves the group operation (point addition) on the elliptic curves and when two curves are connected by an isogeny, they are said to be isogenous. Interestingly, two curves over are isogenous if and only if they have the same number of rational points, denoted f #() = #().

The kernel of an isogeny, denoted as ker(), includes all points on ​ that get mapped to the point at infinity on ​: ker() = {P }. If you know a subgroup G of ​ with size N, there is a unique isogeny of degree N with the subgroup G as its kernel, ker() = G. Furthermore, For every isogeny ​ ​, there exists a dual isogeny ′:→​ of the same degree and every isogeny has a dual isogeny ′:→, which reverses the direction of the original map. The composition of the isogeny and its dual gives a scalar multiplication by N on the original curve: ′ = [N].

An elliptic curve can be represented using a specific type of equation called a WeierstraB equation and the general form look like: where x and y are the variables that represent the coordinates of points on the curve and the numbers ,,,,​ are constants (called coefficients) that come from the field and these coefficients define the specific shape and properties of the curve. ​One of the methods for computing isogenies is through Vélu’s formulas which allow us to calculate the specific map between two elliptic curves, given the kernel of the isogeny. If we are given a point Q on ​ that generate a subgroup of order N, Vélu’s formulas provide us with the rational functions that define the isogeny and can be written as ((x, y)) = (f(x), y · g(x)).

f(x) and g(x) are ratios of polynomials, and their degrees are related to the degree of the isogeny and the degree of the isogeny related to the size of the kernel. Vélu’s formulas are only practical to compute for relatively smaller values of N, so when N becomes large, especially if N is a composite number, we decompose the isogeny into smaller isogenies, each with a smaller prime degree. For example, if N has a prime factorization: N = ... where,,… are primes, we can compute the isogeny as a composition of isogenies of degree ,,… This method is feasible as long as the prime factors of N are sufficiently small.

### **2.3.1 - 2-Isogenies**

A 2-isogeny is a specific type of isogeny with degree 2 which means that it maps points between two elliptic curves in such a way that the kernel of the isogeny contains exactly two points (including the identity point). Given an elliptic curve and a point Q of order 2 on this curve, we can generate a 2-isogeny : . The point Q generates the kernel of the isogeny, which is the set of points that are mapped to the point at infinity on the target curve. Consider a point Q of order 2 on an elliptic curve ​. There are two cases: Case 1, When Q=(0,0), The isogeny and the new curves ​ are defined using specific formulas involving A and B. The formulas calculate (x,y) and update the curve coefficients to get (A′,B′). In Case 2, When Q=(,0) with ​ 0, different formulas are used to compute (x,y) and (A′,B′), involving . In both cases, the point (0,0) on lies in the kernel of the dual isogeny ​, which is needed for chaining isogenies. The dual isogeny is the inverse map of the isogeny, and its kernel consists of points that are mapped to the point at infinity.

### **2.3.2. 4-isogenie**

A 4-isogeny is a specific type of isogeny with degree 4, meaning that the kernel of the isogeny contains exactly four points, including the identity point. 4-isogenies are more complex than 2-isogenies but for efficiency purposes, some implementations may prefer to use 4-isogeny formulas more because they can be equivalent to combining two 2-isogenies formulas in a sequence.On pg 12, Case 1: Q=(1,), then 2[Q]=(0,0), in this case, Q has the x-coordinate 1, and its second multiple is (0,0). This formula computes the new x- and y-coordinates of points and defines the image curve’s parameters A′ and B′. The transformation is based on the elliptic curve’s initial parameters and accounts for the 4-isogeny structure. The formula effectively transforms points on the original curve ​ into points on the new curve , which has different parameters for A′ but the same B.On pg 12, Case 2: Q=(−1,),in this case, Q has the x-coordinate of −1, and this is similar to the first case, but the sign changes in the formulas so, we follow a similar process to derive the isogeny. This transformation also adjusts the point coordinates and the curve's parameters but in this case, the biggest difference here is that the formulas take into account the different x-coordinate of Q=(−1,).On pg 12, Case 3: Q=(,) with ±1. In this third case, the point Q has coordinates (,) and ​ is neither 1 nor -1. The new curve parameters in this case are (A′,B′)=(2−4xQ2,B)(A', B') = (A′,B′)=(2 −​,B). This formula is the most general and applies to points that are not at specific locations like 1 or −1 but it still serves the same purpose which is mapping points from one elliptic curve to another while preserving the group structure.

### **2.3.3. Other odd-degree isogenies using Vélu’s formulas**

Odd-degree isogenies are those with a kernel of odd size. Let ℓ be an odd prime, and let Q be a point on the elliptic curve ​​ of order ℓ. This point Q generates the kernel of the isogeny φ:​→, where is the codomain curve. The main idea here is that the isogeny is determined by its kernel, and knowing the point Q allows us to compute the isogeny more clearly and to compute this isogeny, we define the polynomial (x), which encodes the structure of the kernel. The polynomial is defined as the product, (x) = s∈S ​(x − ), where S={1,2,…,(ℓ−1)/2}, and ​ is the x-coordinate of the point , which is the scalar multiple of Q and this polynomial collects all the important points in the kernel of the isogeny.The parameter A′ defines the new curve given by A′=2⋅1+d​/1−d, where d, a value computed from the original elliptic curve parameter A is computed as d= (A-2/A+2 ((1)/(-1). The parameter B remains unchanged so = and it allow us to compute the new elliptic curve ​ that is isogenous to the original curve .

##### **2.3.4. Odd-degree isogenies using √ élu**

The square-root Vélu algorithm, also called the √élu algorithm, computes isogenies of elliptic curves in time O~(ℓ) rather than O(ℓ), where ℓ is the degree. The main idea is to reindex the points in the kernel subgroup in a baby-step-giant-step manner, the baby-step giant-step algorithm computes discrete logarithms in a group of order q using O( √q) group operations and this algorithm breaks down the computation into smaller steps, making a faster evaluation of the kernel polynomial (x). Instead of S={1,2,…,(ℓ−1)/2}, we use S={1,3,5,…,ℓ−2} redefining the index Sets I,J,K then continue by defining an index system (I,J) for S, where, I = {2m(2i+1) ∣ 0 ≤ i ≤ m′} and J = {2j+1 ∣ 0 ≤ j < m}. m is defined as m = √(ℓ−1/2) and m′ = 0 if m = 0 , if not then m′ = (ℓ+1)/4m and K = S∖(I±J) , where I ± J = {i+j, i-j ∣ i ∈ I, }. The sizes of these sets are all in O(√ℓ), which makes the algorithm more better.

Biquadratic polynomials are polynomials of degree 4 that can be written in the general form,P(x)=a+b+c . The term a represents the highest degree (degree 4), and there are no or terms, which differs the biquadratic polynomials from general quartic polynomials. To evaluating () in Steps First, defining Biquadratic Polynomials ,,​: (,)=(− , (,) = 2((+1)(+) + 2a), (,) = (-1). On pg 13, for polynomial ​(x), this polynomial contains roots at the x-coordinates of multiples of Q in set I. For ​(x), squares the differences, focusing roots at x = . For the Resultant Δ I,J​ , it measures the common factors between (x) and (x) and results in an element of ​. For (x), this incorporates the input and the polynomials ,,. For Resultant R, ΔI,J is an element of ​ and contains information about . For and output (), this gives the value of () needed for the isogeny

Computation.

When using efficient polynomial arithmetic, computing polynomials using product trees for efficient polynomial multiplication and remainder trees for multi-point evaluation speeds up polynomial and resultant computations. Product trees are used to multiply a series of polynomials efficiently and the polynomials are grouped in pairs and multiplied in parallel, reducing the number of steps. Remainder trees are used for multi-point evaluation which is a method that allows us to evaluate a polynomial at multiple points at once by breaking the evaluation into smaller steps which speeds up the calculation.

In SQIsign, isogenies and methods like Vélu's and √élu's algorithms help create secure and practical post-quantum signatures. They rely on the difficulty of solving isogeny problems on supersingular elliptic curves, providing strong protection against quantum attacks.

**Bibliography**

“Isogeny.” Wikipedia, Wikimedia Foundation, 24 June 2024, en.wikipedia.org/wiki/Isogeny.

Jonathan Katz and Yehuda Lindell, Introduction to Modern Cryptography (3rd edition), (Chapman & Hall/CRC Cryptography and Network Security Series)(2020)

“Degree of a Polynomial.” Wikipedia, 3 June 2024, [en.wikipedia.org/wiki/Degree\_of\_a\_polynomial#:~:text=Degree%204%20%E2%80%93%20quartic%20](http://en.wikipedia.org/wiki/Degree_of_a_polynomial#:~:text=Degree%204%20%E2%80%93%20quartic%20)(or%2C.

Santos, Maria. “Maria Santos.” PhD Student at UCL, Interested Particularly in Post-Quantum Cryptography and Applications., 7 Nov. 2020, www.mariascrs.com/2020/11/07/velus-formulas.html.