# Creating Quantum Resistant Cryptosystems Using Supersingular Elliptic Curves

Sherry Sarkar and Stephanie Shi, under the guidance of Euler Circle

## 1 Introduction

Many modern cryptosystems use the group structures of ordinary elliptic curves. However, these cryptosystems can be broken using quantum computers. The following paper is based on the paper referenced in (1) - it outlines a quantum resistant cryptosystem based on supersingular elliptic curves and the difficulty of finding isogenies between them.

### 1.1 Group Theory Overview

We start by defining some group theory terms.

**Definition 1.1:** A *homomorphism* is defined as a function $f : G \to H$ such that for every $u, v \in G$ the function f has the following property: $f(u \cdot v) = f(u) \cdot f(v)$.

**Definition 1.2:** A *kernel* of a homomorphism $f : G \to H$ is defined as: $\{g \in G : f(g) = e_H\}$

**Definition 1.3:** An *image* of a homomorphism is defined as $\{h \in H : h = f(g), g \in G\}$

One should note that if a homomorphism $f : G \to H$ is surjective, then the image of the homomorphism is $H$ itself. The kernel and the image are ways to measure how isomorphic a homomorphism is. In an isomorphism, the kernel consists only of the identity element of $G$ and the image is $H$ itself.

## 1.2 Elliptic Curve Overview

An elliptic curve over a field $K$ is a nonsingular cubic curve with a distinguished point (known as the infinity point). If the field characteristic is neither 2 nor 3, then the elliptic curve can be expressed in the form:

$$y^2 = x^3 + Ax + B.$$

where the discriminant is not equal to 0. The discriminant of an elliptic curve is:

$$\Delta = 16(4A^3 + 27B^2).$$

This ensures that there are no double or triple roots - we run into problems with the group structure in elliptic curves if there are repeated roots. An elliptic curve has a group law that makes it an abelian group. The identity element is the infinity point.

We can also define elliptic curves over finite fields. $E(\mathbb{F}_p)$ means all the points on $E$ with coordinates in $\mathbb{F}_p$. A nonsingular curve reduced modulo $p$ can become singular if $p|\Delta$ , since then the discriminant in $\mathbb{F}_p$ becomes 0. In this case, we say that $E$ has bad reduction modulo $p$. If $E(\mathbb{F}_p)$ is nonsingular, then we say that $E$ has good reduction modulo $p$.

We now move on to relationships between elliptic curves

**Definition 1.4:** An *isogeny* is a mapping between elliptic curves that induces a homomorphism between the groups of elliptic curves.

The distinguished points of the two elliptic curves are thus mapped to each other. If there is an isogeny between two elliptic curves, they are said to be isogenous. For example, $E \to nE$ is an isogeny.

**Definition 1.5:** An *endomorphism* is a homomorphism from a mathematical object to itself. For elliptic curves, an endomorphism is an isogeny $f : E \to E$.

*Example:* Let $E$ be an elliptic curve over a finite field $F_q$. The Frobenius endomorphism of $E$ is the map $E : (x : y : z) \to (x^q : y^q : z^q)$

The endomorphisms of an elliptic curve form a ring since they can be added and composed.

**Definition 1.6:** An *endomorphism ring* of an elliptic curve is either isomorphic to an order in an imaginary quadratic field, or an order in a quaternion algebra.

When the endomorphism ring is isomorphic to an order in a quaternion algebra, the endomorphism ring is unusually large and lacks commutativity. This dichotomy allows us to classify elliptic curves over finite fields.

# 2 Supersingular Elliptic Curves

There are five equivalent definitions of a supersingular elliptic curve given by Deuring's Theorem; however, we will only discuss two of them.

**Theorem 1.1:** An elliptic curve is supersingular if:

1. The p-torsion subgroup is trivial.

$$E[p^r] = 0 \quad \forall r \geq 1.$$

2. The endomorphism ring of the elliptic curve is an order in a quaternion algebra.

And for ordinary elliptic curves if:

1. $$E[p^r] \cong \mathbb{Z}/p^r\mathbb{Z} \quad \forall r \geq 1.$$

2. The endomorphism ring is an order in an imaginary quadratic field.

It is important to note that supersingular elliptic curves are not singular! A singular elliptic curve is an elliptic curve with repeated roots. The following are some simpler examples of a supersingular curve.

**Theorem 1.2:** Let $E/F_q$ be an elliptic curve over a field of prime order $p \geq 3$. Then $E$ is supersingular iff the trace of the Frobenius is congruent to $0 mod p$.

*Example:* Suppose that $E$ is the elliptic curve $y^2 = x^3 + ax$, and suppose that $p$ is a prime congruent to $3 \pmod 4$. Show that $E(\mathbb{F}_p) = p + 1$.
As it turns out, $E$ is a supersingular elliptic curve!

**Definition 2.1:** The *j-invariant* of an elliptic curve $y^2 = x^3 + ax + b$ is defined as

$$j(E) = 1728\frac{4a^3}{4a^3 + 27b^2}.$$

Over an algebraically closed field, two elliptic curves are isomorphic iff they have the same j-invariant.

# 3 Key Exchange:

The key exchange is based of the Diffie-Hellman Key Exchange - rather than using the Discrete Logarithm Problem as the source of complexity, it uses the Supersingular Computational Diffie-Hellman Problem. It starts with the following public information: elliptic curve $E_0$, the four points $P_A, Q_A, P_B, Q_B$.

1. Start with a common elliptic curve $E_0$. Alice selects two points $P_A$ and $Q_A$. Bob selects two points $P_B$ and $Q_B$. These points are public.

2. Alice chooses two random coefficients $[m_a]$ and $[n_a]$. She then calculates the point $[m_a]P_A + [n_a]Q_A$. This point will be the kernel for the isogeny $\phi_A$ created using Velu's Formula. Bob does the same: 'he chooses two random coefficients $[m_b]$ and $[n_b]$ and calculates the point $[m_b]P_B + [n_b]Q_B$ to use as a kernel for his isogeny $\phi_B$.

3. Alice takes Bob's points $P_B$ and $Q_B$ and calculates the image of these points. We know the image exists since isogenies are surjective thus meaning $im(\phi_A)$ is $E_A$. Alice send the points, $\phi_A(P_B)$ and $\phi_A(Q_B)$ over to Bob. Bob does the same thing with Alice's points PA and QA and sends his calculated points $\phi_B(P_A)$ and $\phi_B(Q_A)$ to Alice.

4. Alice uses the same coefficients $[m_a]$ and $[n_a]$ to calculate the point $[m_a]\phi_B(P_A) + [n_a]\phi_B(Q_A)$. This point will be the kernel for another

isogeny $\phi'_A$ created using Velu's Formula. Bob does the same thing with his coefficients, creating a kernel and thus the isogeny $\phi'_B$ with the point $[m_b]\phi_A(P_B) + [n_b]\phi_A(Q_B)$.

5. The curve created with Alice's isogeny $\phi'_A$ and the curve created with Bob's isogeny $\phi'_B$ are isomorphic. Thus, we can calculate a common j-invariant and that will be our key.

# 4 Complexity and Security:

The security of this cryptosystem relies on the fact that the endomorphism ring of a supersingular elliptic curve is not commutative.

**Supersingular Computational Diffie-Hellman Problem:** Given the curves $E_A$ and $E_B$ and the points $\phi_A(P_B)$ , $\phi_A(Q_B)$ , $\phi_B(P_A)$, $\phi_B(Q_A)$, find the j-invariant of $E_0/\langle [m_a]P_A + [n_a]Q_A, [m_b]P_B + [n_b]Q_B \rangle$.

The fastest known algorithm for finding isogenies between supersingular curves in general takes $O(\sqrt{p} \log^2 p)$ time. However, this problem is less general since the degree of the isogeny is already known in advance and is known to be smooth.

So far, attacks on the system are theorized to be $O(p^{\frac{1}{4}})$ for ordinary computers, and $O(p^{\frac{1}{6}})$ for quantum computers. This means that the system is 128-bit secure for a prime of 768 bits.

There is a known quantum subexponential time algorithm for solving SSCDH for ordinary elliptic curves. However, this algorithm relies on the properties of abelian groups. Since the endomorphism ring of a supersingular elliptic curve is not commutative, this algorithm likely cannot be adapted for the supersingular case.

# 5 Sources:

1. Lecture #5 (n.d.): n. pag. Lecture Notes. MIT, 9 Feb. 2015. Web. 10 Mar. 2016.

2. Plt, Jrme, David Jao, and Luca De Feo, David Jao, And J Er. TOWARDS QUANTUM-RESISTANT CRYPTOSYSTEMS FROM SU-

PERSINGULAR ELLIPTIC CURVE ISOGENIES (n.d.): n. pag. International Association for Cryptologic Research. International Association for Cryptologic Research. Web. 10 Mar. 2016.

3. Rubinstein-Salzedo, Simon. Euler Circle Cryptography Notes (Week 7). Euler Circle, n.d. Web.

4. Silverman, Joseph H. The Arithmetic of Elliptic Curves. New York: Springer-Verlag, 1986. Print.