Quantum Algorithms for Supersingular Isogeny Problems

Against Post-Quantum Crypto Protocol

Zhengyi Han

Peking University -> Rice University

Jan 23rd, 2024

Table of Contents

1. Pre-quantum era
2. Mathematical Background
3. Ordinary cases
4. Supersingular isogeny graphs
5. Approximate quantum walk on the graph
6. Can we make improvement?
7. Future work

Table of Contents

1. Pre-quantum era
2. Mathematical Background
3. Ordinary cases
4. Supersingular isogeny graphs
5. Approximate quantum walk on the graph
6. Can we make improvement?
7. Future work

Elliptic curves

Definition

An elliptic curve over a field k is a smooth projective curve of genus 1 with a point at infinity.

Elliptic curves

Definition

An elliptic curve over a field k is a smooth projective curve of genus 1 with a point at infinity.

If $char(k) \neq 2, 3$, every elliptic curve in affine space $\mathbb{A}^2$can be written in the form:

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

with$a, b \in k$
It can also be written in projective coordinates in projective space $\mathbb{P}^2$:

$$y^2z = x^3 + axz^2 + bz^3$$

$(0 : 1 : 0)$ denotes the infinite point.

Group Law

Theorem

For $P, Q \in E(k)$, the line $\overline{PQ}$ intersects E in a rational point, because E is a cubic curve, $\#(\overline{PQ} \cap E(k)) = 3$.

We define a group operation $+$, for $P, Q, R \in E(k)$, $R \in \overline{PQ},\ s.t. P + Q + R = O$

Group Law

Theorem

For $P, Q \in E(k)$, the line $\overline{PQ}$ intersects E in a rational point, because E is a cubic curve, $\#(\overline{PQ} \cap E(k)) = 3$.

We define a group operation $+$, for $P, Q, R \in E(k)$,
$R \in \overline{PQ},\ s.t. P + Q + R = O$
The inverse of a point R is the reflection of the point about the x-axis.
The identity of the group is the point at infinity.

Group Law

Theorem

For $P, Q \in E(k)$, the line $\overline{PQ}$ intersects E in a rational point, because E is a cubic curve, $\#(\overline{PQ} \cap E(k)) = 3$.

We define a group operation $+$, for $P, Q, R \in E(k)$,
$R \in \overline{PQ},\ s.t. P + Q + R = O$
The inverse of a point R is the reflection of the point about the x-axis.
The identity of the group is the point at infinity.

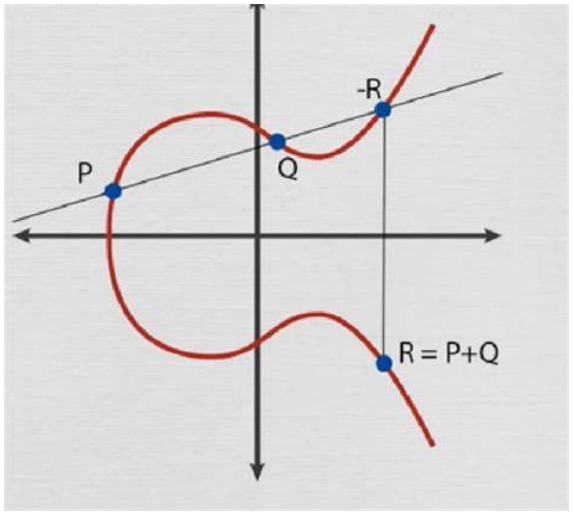


Figure 1: Group Law

Group Law

Any elliptic curve over $\mathbb{C}$ can be obtained from a torus by $\wp$-function, so the additive structure is natural.

$$\wp : \ \mathbb{C}/L \ \longrightarrow \mathbb{CP}^2$$

Diffie-Hellman

- It is very similar to the RSA protocol which is based on factoring. Its intractability is based on the difficulty of solving discrete logarithm problems.

Diffie-Hellman

- It is very similar to the RSA protocol which is based on factoring. Its intractability is based on the difficulty of solving discrete logarithm problems.
- Diffie-Hellman performs better than RSA. 256-bit Diffie-Hellman's security is better than 2048-bit RSA. (Its construction is more complicated than RSA)

Diffie-Hellman

- It is very similar to the RSA protocol which is based on factoring. Its intractability is based on the difficulty of solving discrete logarithm problems.
- Diffie-Hellman performs better than RSA. 256-bit Diffie-Hellman's security is better than 2048-bit RSA. (Its construction is more complicated than RSA)

Diffie-Hellman Key Exchange Protocol

1. **Choose Public Elliptic Curve and Base Point G:**
   - Select an elliptic curve E over a finite field $\mathbb{F}_p$ or $\mathbb{F}_{2^m}$.
   - Choose a base point G on E with a large order.

Diffie-Hellman Key Exchange Protocol

1. **Choose Public Elliptic Curve and Base Point G:**
   - Select an elliptic curve E over a finite field $\mathbb{F}_p$ or $\mathbb{F}_{2^m}$.
   - Choose a base point G on E with a large order.
2. **Private Key Selection**:
   - Alice randomly selects a private key a, a large integer.
   - Bob independently selects a private key b, another large integer.

Diffie-Hellman Key Exchange Protocol

1. **Choose Public Elliptic Curve and Base Point G:**
   - Select an elliptic curve E over a finite field $\mathbb{F}_p$ or $\mathbb{F}_{2^m}$.
   - Choose a base point G on E with a large order.
2. **Private Key Selection:**
   - Alice randomly selects a private key a, a large integer.
   - Bob independently selects a private key b, another large integer.
3. **Compute and Exchange Public Keys:**
   - Alice computes her public key: $A = aG$ (multiplying the base point G by her private key a).
   - Bob computes his public key: $B = bG$ (similarly, using his private key b).
   - Alice and Bob exchange their public keys A and B over the public channel.

Diffie-Hellman Key Exchange Protocol

1. **Choose Public Elliptic Curve and Base Point G:**
   - Select an elliptic curve E over a finite field $\mathbb{F}_p$ or $\mathbb{F}_{2^m}$.
   - Choose a base point G on E with a large order.
2. **Private Key Selection:**
   - Alice randomly selects a private key a, a large integer.
   - Bob independently selects a private key b, another large integer.
3. **Compute and Exchange Public Keys:**
   - Alice computes her public key: $A = aG$ (multiplying the base point G by her private key a).
   - Bob computes his public key: $B = bG$ (similarly, using his private key b).
   - Alice and Bob exchange their public keys A and B over the public channel.
4. **Compute the Shared Secret:**
   - Alice computes the shared secret: $S = aB = a(bG)$.
   - Bob computes the same shared secret: $S = bA = b(aG)$.
   - The shared secret S is now a point on the elliptic curve, and its coordinates are used to derive the encryption key.

Remarks on Diffie Hellman

- The computation of shared secret relies on the commutability of the group action (scalar multiplication)

Remarks on Diffie Hellman

- The computation of shared secret relies on the commutability of the group action (scalar multiplication)
- To recover the private secret, i.e. a and b, implies solving the discrete logarithm problem.

Remarks on Diffie Hellman

- The computation of shared secret relies on the commutability of the group action (scalar multiplication)
- To recover the private secret, i.e. a and b, implies solving the discrete logarithm problem.
- Shor's algorithms can break Diffie-Hellman in polynomial time.

Supersingular Isogeny Diffie-Hellman

Supersingular Isogeny Diffie-Hellman (SIDH), also known as SIKE when referring to its key encapsulation mechanism, was indeed one of the candidates considered in the NIST Post-Quantum Cryptography Standardization process.

Supersingular Isogeny Diffie-Hellman

Supersingular Isogeny Diffie-Hellman (SIDH), also known as SIKE when referring to its key encapsulation mechanism, was indeed one of the candidates considered in the NIST Post-Quantum Cryptography Standardization process.
SIDH/SIKE is based on the hardness of problems in supersingular isogeny graphs and was designed to resist attacks from adversaries equipped with quantum computers. **Before vulnerabilities were discovered**, SIDH was notable for its relatively small key sizes compared to other post-quantum key exchange mechanisms, and it provided features like perfect forward secrecy.

Supersingular Isogeny Diffie-Hellman

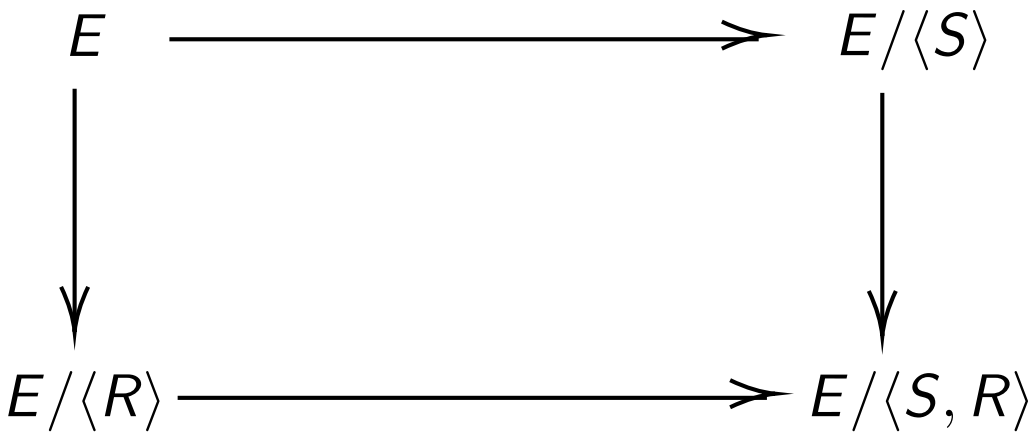
1. Created in 2011 by De Feo, Jao, and Plut.

Supersingular Isogeny Diffie-Hellman

1. Created in 2011 by De Feo, Jao, and Plut.
2. In 2017, Petit first demonstrated a technique that exploited auxiliary elliptic-curve points present in SIDH public keys to attack some specific SIDH variants. However, the "standard" SIDH employed in the NIST submission remained initially unbroken.
3. However, SIDH is vulnerable to a devastating key-recovery attack published in July 2022 and is therefore insecure. The attack does not require a quantum computer.
4. I have personally experienced this shocking event. But the attack crucially relies on the auxiliary points given in SIDH, and there is no known way to apply similar techniques to the general isogeny problem. (So our investigation is not so meaningless:), even if I gave up.)

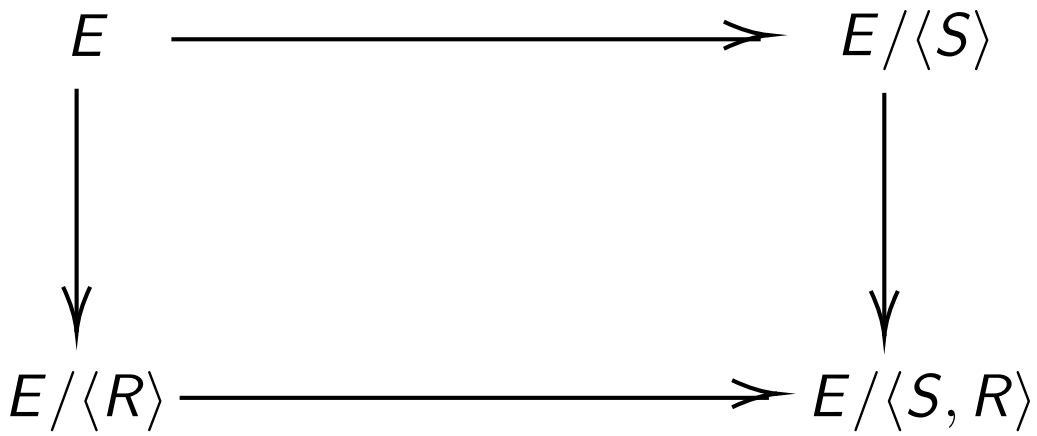
SIKE protocol

Given a secret point S of a supersingular curve E over $\mathbb{F}_{p^2}$, and a public point R, SIKE can be described by the following commutative diagram in general:



SIKE protocol

Given a secret point S of a supersingular curve E over $\mathbb{F}_{p^2}$, and a public point R, SIKE can be described by the following commutative diagram in general:



SIDH's procedure is very similar to Diffie-Hellman, but it's based on the isogeny rather than the DLog. It use the j-invariant of the resulting elliptic curves to encrypt.

Table of Contents

1. Pre-quantum era
2. Mathematical Background
3. Ordinary cases
4. Supersingular isogeny graphs
5. Approximate quantum walk on the graph
6. Can we make improvement?
7. Future work

Isogeny

- Morphism between abelian varieties is a rational map over the function field that is defined everywhere.

Isogeny

- Morphism between abelian varieties is a rational map over the function field that is defined everywhere.
- Morphism preserving the zero is said to be isogeny. Isogeny preserves the group structure of abelian varieties.

Isogeny

- Morphism between abelian varieties is a rational map over the function field that is defined everywhere.
- Morphism preserving the zero is said to be isogeny. Isogeny preserves the group structure of abelian varieties.

For curves E, E' over k, an isogeny:

$$\psi : E(\bar{k}) \longrightarrow E'(\bar{k})$$

$\deg(\psi) := |\ker(\psi)|$.
Every isogeny has its dual isogeny:

$$\hat{\psi} : E' \longrightarrow E, \ s.t.$$

$$[\deg(\psi)] = \hat{\psi} \circ \psi : E \longrightarrow E$$

Isogeny

Theorem (Informal)

We can uniquely determine the isogeny ψ by its kernel (under isomorphism equivalence).

- By Velu's formulas, to compute the isogeny ψ with $\deg(\psi) = n$ needs $O(n)$ field operations.
- If $\phi = \phi_1 \circ \cdots \circ \phi_k \circ [n]$, then $\deg(\phi) = n^2 \cdot \prod_{i=1}^{k} \deg(\phi_i)$. If we take ϕ_i all isogenies with a small prime degree, for example 2. Then the complexity of computing the isogeny ϕ is $O(k)$, instead of $O(2^k)$ by Velu's formulas.

Over finite field

(Hesse Theorem) The points of elliptic curves E over finite field $\mathbb{F}_q$, char($\mathbb{F}_q$)=p:

$$\#E(\mathbb{F}_q) = q - 1 + t, \text{ where } |t| \leq 2\sqrt{q}$$

Over finite field

(Hesse Theorem) The points of elliptic curves E over finite field $\mathbb{F}_q$, char($\mathbb{F}_q$)=p:

$$\#E(\mathbb{F}_q) = q - 1 + t, \text{ where } |t| \leq 2\sqrt{q}$$

- E is ordinary if $p \nmid t \Leftrightarrow \#E[p] = p$
- E is supersingular if $p|t \Leftrightarrow E[p] = \{\mathbf{0}_E\}$

Ordinary curves are only isogenous to ordinary curves, so do supersingular curves.

j-invariant

j-invariant can distinct isomorphism classes of elliptic curves over algebraic closure.

j-invariant

j-invariant can distinct isomorphism classes of elliptic curves over algebraic closure.

We can define isogeny graph $G_l(\mathbb{F}_q)$. Its vertices are j-invariant of curves over $\mathbb{F}_q$, there is an edge from j_1 to j_2 if an isogeny maps j_1 to j_2 with degree l.

j-invariant

j-invariant can distinct isomorphism classes of elliptic curves over algebraic closure.

We can define isogeny graph $G_l(\mathbb{F}_q)$. Its vertices are j-invariant of curves over $\mathbb{F}_q$, there is an edge from j_1 to j_2 if an isogeny maps j_1 to j_2 with degree l.

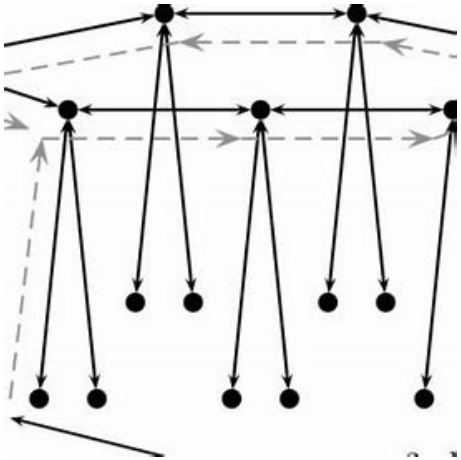
- ordinary case is called "volcano"
- supersingular case is a regular expander graph

j-invariant

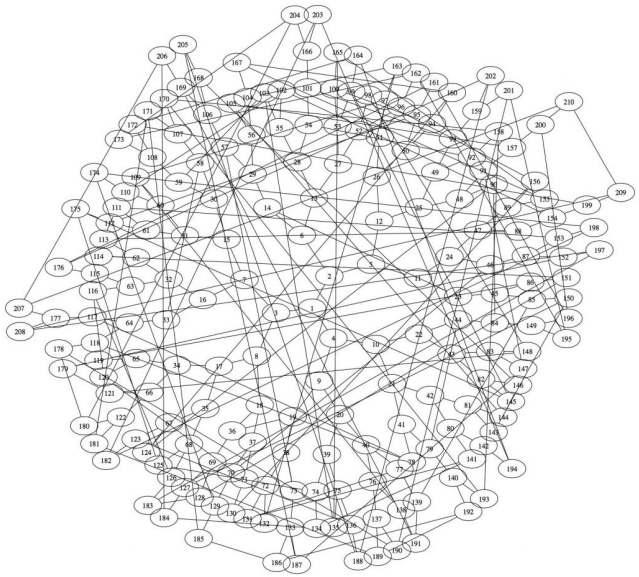
j-invariant can distinct isomorphism classes of elliptic curves over algebraic closure.

We can define isogeny graph $G_l(\mathbb{F}_q)$. Its vertices are j-invariant of curves over $\mathbb{F}_q$, there is an edge from j_1 to j_2 if an isogeny maps j_1 to j_2 with degree l.

- ordinary case is called "volcano"
- supersingular case is a regular expander graph



(a) ordinary



(b) supersingular

Table of Contents

1. Pre-quantum era
2. Mathematical Background
3. Ordinary cases
4. Supersingular isogeny graphs
5. Approximate quantum walk on the graph
6. Can we make improvement?
7. Future work

Quantum algorithms for ordinary cases

Theorem (Childs, Jao, Soukharev 10)

Given two ordinary elliptic curves over a finite field with the same endomorphism ring, there is a subexponential quantum algorithm to compute the corresponding isogeny between them.

Quantum algorithms for ordinary cases

Theorem (Childs, Jao, Soukharev 10)

Given two ordinary elliptic curves over a finite field with the same endomorphism ring, there is a subexponential quantum algorithm to compute the corresponding isogeny between them.

They reduced the problem to solving the hidden subgroup problem of dihedral groups. Kuperberg's algorithm or Regev's algorithm can solve this problem in quantum subexponential time.

Quantum algorithms for ordinary cases

Theorem (Childs, Jao, Soukharev 10)

Given two ordinary elliptic curves over a finite field with the same endomorphism ring, there is a subexponential quantum algorithm to compute the corresponding isogeny between them.

They reduced the problem to solving the hidden subgroup problem of dihedral groups. Kuperberg's algorithm or Regev's algorithm can solve this problem in quantum subexponential time.
I plan to show you their methods briefly, which can not apply to the supersingular case.

Complex multiplication

From the isogeny graph view, we know that the ordinary and supersingular case have different graph structure. From the algebraic view, they are also different.

Complex multiplication

From the isogeny graph view, we know that the ordinary and supersingular case have different graph structure. From the algebraic view, they are also different.

We consider the endomorphism ring (algebra).

$$\mathrm{End}(E) := \{\psi : E \to E |\ \psi \text{ is an isogeny}\}$$

$$\mathrm{End}^0(E) := \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$$

Complex multiplication

Theorem

Let E be an elliptic curve over $\mathbb{F}_q$. Either E is supersingular, $End^0(E_{\bar{\mathbb{F}}_q})$ is a quaternion algebra, or E is ordinary, $End^0(E_{\bar{\mathbb{F}}_q})$ is an imaginary quadratic field.

Here an imaginary quadratic field is
$\mathbb{Q}(\alpha) := \{x + y\alpha : \ x, y \in \mathbb{Q}, \ \alpha^2 < 0\}$, a quaternion algebra
$\mathbb{Q}(\alpha, \beta) := \{x + y \cdot \alpha + z \cdot \beta + t \cdot \alpha\beta : \ x, y, z, t \in \mathbb{Q}, \alpha\beta = -\beta\alpha, \ \alpha^2, \beta^2 < 0\}$.

Complex multiplication

Theorem

Let E be the endomorphism algebra of an isogeny class of elliptic curves, $\mathcal{O}$ an order in it which is a possible endomorphism ring.

- *If E is commutative, the isomorphism classes of curves with endomorphism ring $\mathcal{O}$ form a principal homogeneous space for $cl(\mathcal{O})$*
- *If E is non-commutative, the number of isomophism classes $\#Ell_{\mathcal{O}}(k) = \#cl(\mathcal{O})$. (the classes are homogeneous space for Brandt groupoid).*

Complex multiplication

Theorem

Let E be the endomorphism algebra of an isogeny class of elliptic curves, $\mathcal{O}$ an order in it which is a possible endomorphism ring.

- *If E is commutative, the isomorphism classes of curves with endomorphism ring $\mathcal{O}$ form a principal homogeneous space for $cl(\mathcal{O})$*
- *If E is non-commutative, the number of isomophism classes $\#Ell_{\mathcal{O}}(k) = \#cl(\mathcal{O})$. (the classes are homogeneous space for Brandt groupoid).*

The principal homogeneous space means that, for any $j_1, j_2 \in \mathrm{Ell}_{\mathcal{O}}(k)$, there exists a **unique** $[\mathfrak{a}] \in \mathrm{cl}(\mathcal{O})$, such that $[\mathfrak{a}]j_1 = j_2$.

Hidden abelian shift

Since the ideal class group $\mathrm{cl}(\mathcal{O})$ is abelian, to find the isogeny between two given elliptic curves (isomorphism classes) is similar to find the group element which implement the **abelian shift**.

Hidden abelian shift

Since the ideal class group $\mathrm{cl}(\mathcal{O})$ is abelian, to find the isogeny between two given elliptic curves (isomorphism classes) is similar to find the group element which implement the **abelian shift**.

Suppose $[\mathfrak{s}]j_0 = j_1$.
We can define two functions:

$$f_0, f_1 : \mathrm{cl}(\mathcal{O}) \to \mathrm{Ell}(\mathcal{O})$$

$$[\mathfrak{a}] \mapsto [\mathfrak{a}]j_b$$

Then $f_0([\mathfrak{a}][\mathfrak{s}]) = f_1([\mathfrak{a}])$, $[\mathfrak{s}]$ is our desired abelian hidden shift. We can define $f([\mathfrak{a}], b) = f_b([\mathfrak{a}])$, in the group $\mathrm{cl}(\mathcal{O}) \rtimes \mathbb{Z}_2$, with $f([\mathfrak{a}][\mathfrak{s}], 0) = f([\mathfrak{a}], 1)$. Find $[\mathfrak{s}]$ is equal to finding the subgroup $(\mathfrak{s}, 1)$.

Compute the isogeny

Algorithm 1: Isogeny computation between ordinary curves defined over a finite field

Input: A discriminant of $\Delta < 0$, and Weierstrass equations of horizontally isogeneous ordinary elliptic curves E_0, E_1 defined over $\mathbb{F}_q$ with characteristic p

Output: $[\mathfrak{s}] \in \mathrm{cl}(\mathcal{O}_\Delta),\ s.t.\ [\mathfrak{s}]j(E_0) = j(E_1)$

1 Decompose $\mathrm{cl}(\mathcal{O}_\Delta) = \langle[\mathfrak{a}_1]\rangle \oplus \cdots \oplus \langle[\mathfrak{a}_k]\rangle$, where $|\langle[\mathfrak{a}_i]\rangle| = n_i$

2 Solve the hidden shift problem defined by
$f_0, f_1 : \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k} \longrightarrow \mathrm{Ell}_{\mathbb{F}_q,n}(\mathcal{O}_\Delta)$ satisfying
$f_c(x_1, \cdots, x_k) = ([\mathfrak{a}_1]^{x_1} \cdots [\mathfrak{a}_k]^{x_k})j(E_c)$, with hidden shift
$(s_1, \cdots, s_k) \in \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$

3 Output $[\mathfrak{s}] = ([\mathfrak{a}_1]^{x_1} \cdots [\mathfrak{a}_k]^{x_k})$

Table of Contents

1. Pre-quantum era
2. Mathematical Background
3. Ordinary cases
4. Supersingular isogeny graphs
5. Approximate quantum walk on the graph
6. Can we make improvement?
7. Future work

Supersingular isogeny graphs

Consider all the isomorphism classes of supersingular elliptic curves over $\mathbb{F}_p$, their j-invariants over $\mathbb{F}_{p^2}$ can identify them. Two points are connected if there is an isogeny of degree l between them. We denote the graph as $G_l(\mathbb{F}_{p^2})$.

Supersingular isogeny graphs

Consider all the isomorphism classes of supersingular elliptic curves over $\mathbb{F}_p$, their j-invariants over $\mathbb{F}_{p^2}$ can identify them. Two points are connected if there is an isogeny of degree l between them. We denote the graph as $G_l(\mathbb{F}_{p^2})$.

$G_l(\mathbb{F}_{p^2})$ is $l+1$ regular, but not a simple graph. It's a directed, multi-graph with more than one distinct edge between two points. But we do not take the vertices $0, 1728$ into consideration, it can be viewed as an undirected graph.

Supersingular isogeny graphs

Consider all the isomorphism classes of supersingular elliptic curves over $\mathbb{F}_p$, their j-invariants over $\mathbb{F}_{p^2}$ can identify them. Two points are connected if there is an isogeny of degree l between them. We denote the graph as $G_l(\mathbb{F}_{p^2})$.

$G_l(\mathbb{F}_{p^2})$ is $l+1$ regular, but not a simple graph. It's a directed, multi-graph with more than one distinct edge between two points. But we do not take the vertices $0, 1728$ into consideration, it can be viewed as an undirected graph.

In addition, $G_l(\mathbb{F}_{p^2})$ is highly connected. It's an **expander graph**.

Expander graph

Expander graph can be used to construct pseudorandom sequence due to its mixing property, which means random walk on it can converge to uniform distribution rapidly in just $O(log(n))$ steps.

Expander graph

Expander graph can be used to construct pseudorandom sequence due to its mixing property, which means random walk on it can converge to uniform distribution rapidly in just $O(log(n))$ steps.

Hence, searching and finding a path in an expander is a hard problem! (Finding isogenies can be viewed as a path finding problem.)

Ramanujan graph

Supersingular isogeny graph is the optimal expander **Ramanujan Graph**.
We assume the location has no regulation.

Ramanujan graph

Supersingular isogeny graph is the optimal expander **Ramanujan Graph**. We assume the location has no regulation.

Denote the set of all j-invariants in the graph as S_{p^2}, the j-invariants in $\mathbb{F}_p$ as S_p

$$\#S_{p^2} = \lfloor \frac{p}{12} \rfloor + \begin{cases} 0 & \text{if } p \equiv 1 \mod 12 \\ 1 & \text{if } p \equiv 5, 7 \mod 12 \\ 2 & \text{if } p \equiv 11 \mod 12 \end{cases}$$

$$\#S_p = \begin{cases} \frac{h(-4p)}{2} & \text{if } p \equiv 1 \mod 4 \\ h(-p) & \text{if } p \equiv 7 \mod 8 \\ 2h(-p) & \text{if } p \equiv 3 \mod 8 \end{cases}$$

where $h(d)$ is the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$, $h(d) \in \tilde{O}(\sqrt{d})$

Existing algorithms

- One algorithm to constructing isogeny is to construct isogeny to the curves whose j-invariant in $\mathbb{F}_p$, making use of the $\mathrm{End}_{\mathbb{F}_p}(E)$, which is commutative. We can use the quantum algorithm for the hidden abelian shift. Its time complexity is $\tilde{O}(p^{1/4})$

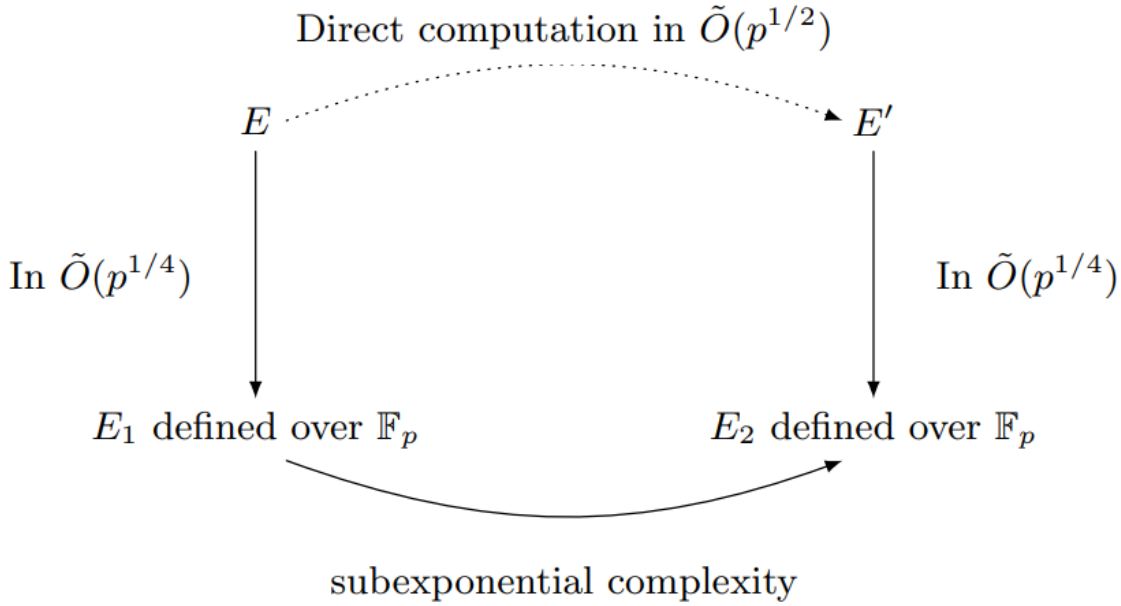


Figure 3: DJ14

Existing algorithms

To construct isogeny between E_1, E_2, we can implement quantum "meet in the middle", its complexity is $\tilde{O}(p^{1/6})$.

Existing algorithms

To construct isogeny between E_1, E_2, we can implement quantum "meet in the middle", its complexity is $\tilde{O}(p^{1/6})$.

It can be formalized as the **claw finding** problem.

Claw finding

Let $f : X \to S$ and $g : Y \to S$ be two functions. Find $x \in X$ and $y \in Y$, $s.t.$ $f(x) = g(y)$, if it exists.

Table of Contents

1. Pre-quantum era
2. Mathematical Background
3. Ordinary cases
4. Supersingular isogeny graphs
5. Approximate quantum walk on the graph
6. Can we make improvement?
7. Future work

Commutative Hecke operators

Adjacency matrices of supersingular isogeny graph $\{G_l : \ l \text{ is prime}\}$ commutes with each other, which means that they share the same eigenspace.

Commutative Hecke operators

Adjacency matrices of supersingular isogeny graph $\{G_l : \ l \text{ is prime}\}$ commutes with each other, which means that they share the same eigenspace.

The adjacency matrix of the supersingular isogeny graph is called the Hecke operator in the modular form context. How can we make use of this property?

Quantum walk

We consider the continuous-time quantum walk on an undirected graph $\Gamma = (V, E)$. The Hamiltonian of the walk is the adjacency matrix A of the graph, and the evolution operator is $W(t) = e^{iAt}$. The Hilbert space is $\mathcal{X} := \mathbb{C}^V$. Let $\{|\phi_j\rangle\}_{1 \le j \le N}$ be a set of orthonormal eigenstates of A that forms a basis of $\mathcal{X}$. The multiset $\{\lambda_j\}_{1 \le j \le N}$ is the set of eigenvalues. $\{\mathcal{X}_j\}_{1 \le j \le M}$ is the eigenspace, where $M \le N$. $I_j := \{k : |\phi_k\rangle \in \mathcal{X}_j\}$ is the indices set of eigenstates in $\mathcal{X}_j$.

Quantum walk

We consider the continuous-time quantum walk on an undirected graph $\Gamma = (V, E)$. The Hamiltonian of the walk is the adjacency matrix A of the graph, and the evolution operator is $W(t) = e^{iAt}$. The Hilbert space is $\mathcal{X} := \mathbb{C}^V$. Let $\{|\phi_j\rangle\}_{1 \le j \le N}$ be a set of orthonormal eigenstates of A that forms a basis of $\mathcal{X}$. The multiset $\{\lambda_j\}_{1 \le j \le N}$ is the set of eigenvalues. $\{\mathcal{X}_j\}_{1 \le j \le M}$ is the eigenspace, where $M \le N$. $I_j := \{k : |\phi_k\rangle \in \mathcal{X}_j\}$ is the indices set of eigenstates in $\mathcal{X}_j$.

$$P_\infty(v|\psi_0) := \lim_{T\to\infty} P_T(v|\psi_0) = \lim_{T\to\infty} \int_0^T \frac{1}{T} |\langle v|W(t)|\psi_0\rangle|^2 \, dt$$

Calculating straightforward, we get the distribution:

$$P_\infty(v|\psi_0) = \sum_{j=1}^{M} \left| \sum_{k \in I_j} \langle v|\phi_k\rangle \langle \phi_k|\psi_0\rangle \right|^2 .$$

Get the limiting distribution

If there is a quantum algorithm,

$$|\psi_0\rangle|0\rangle = \sum_{j=1}^{N} \langle\phi_j|\psi_0\rangle|0\rangle|\phi_j\rangle \mapsto \sum_{j=1}^{N} \langle\phi_j|\psi_0\rangle|t_j\rangle|\phi_j\rangle = \sum_{j=1}^{M}\sum_{k\in I_j} \langle\phi_k|\psi_0\rangle|t_j\rangle|\phi_k$$

if we measure the second register in the vertex basis, the probability corresponds with the limiting distribution.

Get the limiting distribution

If there is a quantum algorithm,

$$|\psi_0\rangle|0\rangle = \sum_{j=1}^{N} \langle\phi_j|\psi_0\rangle|0\rangle|\phi_j\rangle \mapsto \sum_{j=1}^{N} \langle\phi_j|\psi_0\rangle|t_j\rangle|\phi_j\rangle = \sum_{j=1}^{M}\sum_{k\in I_j} \langle\phi_k|\psi_0\rangle|t_j\rangle|\phi_k$$

if we measure the second register in the vertex basis, the probability corresponds with the limiting distribution.

Eigenvalues of A are natural choices, but to assure the tags are unique, the accuracy might be exponential because the minimum distance between eigenvalues can be exponentially small. $W(t)$ can be used to estimate the phases of A, but t is needed to be exponentially large.

ε-projectors

We can make use of the family of commutative operators to label distinct eigenspaces.

Definition

For an integer $r > 0$, let $\mathcal{A} = \{A_j\}_{1 \le j \le r}$ be a set of hermitian operators, acting on $\mathcal{X}$, that have the same eigenspaces. For an eigenstate $|\phi_j\rangle$, let $\lambda_{1,j}, \lambda_{2,j}, \ldots, \lambda_{r,j}$ be the eigenvalues of the operators $A_1, A_2, \ldots, A_r$ associated with $|\phi_j\rangle$, respectively. Define the vector $\boldsymbol{\lambda}_j = (\lambda_{1,j}, \lambda_{2,j}, \ldots, \lambda_{r,j})$, $j = 1, \ldots, N$. For a real number $\varepsilon > 0$, the set of operators $\mathcal{A}$ is said to be ε-separated if

$$\|\boldsymbol{\lambda}_j - \boldsymbol{\lambda}_k\|_2 \ge \varepsilon, \text{ for all } \boldsymbol{\lambda}_j \ne \boldsymbol{\lambda}_k, 1 \le j, k \le N.$$

The sampling algorithm

Theorem (Serre 00, Doliskani 22)

Let $r \geq 32 \log N$, let $l_1, l_2, \ldots, l_r$ be a set of distinct primes each bounded by poly $(\log N)$, and let $\varepsilon = 1/\sqrt{\log N}$. Then the set of operators $\mathcal{T} = \left\{ T_{l_k} / \sqrt{l_k} \right\}_{1 \leq k \leq r}$ is ε-separated with overwhelming probability.

The sampling algorithm

Algorithm 2: Sample the limiting distribution of a continuous time quantum walk via ε-projector

Input: The adjacency matrix A of a graph Γ, an ε-projector $\mathcal{A} = \{A_j\}_{1 \le j \le r}$, an initial state $|\psi_0\rangle$

Output: A sample from the limiting distribution of the walk $W(t) = e^{iAt}$ on Γ

1. Perform phase estimation on $e^{iA_1}, \ldots, e^{iA_r}$ with accuracy $\varepsilon/2\sqrt{r}$, and store the approximate phases $\tilde{\lambda_{k,j}}$ of A_k corresponding to $|\phi_j\rangle$. The resulting state is $\sum_{j=1}^{N} \langle \phi_j \mid \psi_0 \rangle |\tilde{\lambda}_{1,j}\rangle \ldots |\tilde{\lambda}_{r,j}\rangle |\phi_j\rangle$
2. Measure the last register in the vertex basis.
3. Return the measured vertex.

Table of Contents

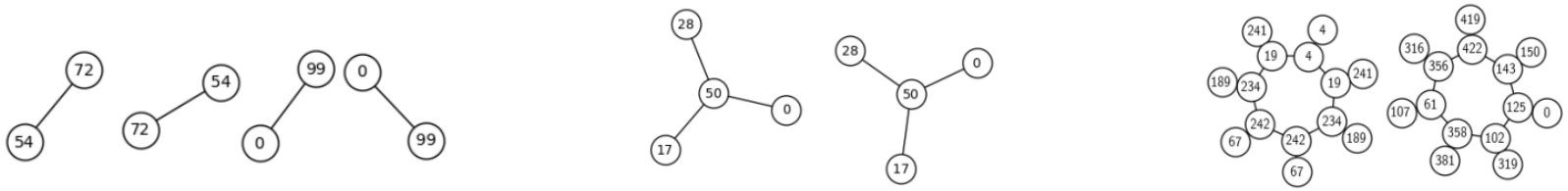
1. Pre-quantum era
2. Mathematical Background
3. Ordinary cases
4. Supersingular isogeny graphs
5. Approximate quantum walk on the graph
6. Can we make improvement?
7. Future work

Can we make improvement?

To make improvement to the existing algorithm, we need to make full use of the property of the isogeny problem instead of just taking the problem as an unordered searching problem. Then we need to exploring the detailed information.

Can we make improvement?

To make improvement to the existing algorithm, we need to make full use of the property of the isogeny problem instead of just taking the problem as an unordered searching problem. Then we need to exploring the detailed information.In a recent work, the set S_p be seen as probably not follows the uniform distribution, they have local property.
Considering the 2-isogeny graph, the distribution of S_p depends on p.



(a) $p \equiv 1 \bmod 4$ (b) $p \equiv 3 \bmod 8$ (c) $p \equiv 7 \bmod 8$

Figure 4: Isogeny graph

Can we make improvement?

Handling the problem on the isogeny graph may lose some information, which can't provide the explicit form of endomorphism ring. A recent work constructs an explicit connection between the supersingular isogeny graph and Bruhat-Tits Tree.(But it's not canonical! That's why I failed.)

Can we make improvement?

Handling the problem on the isogeny graph may lose some information, which can't provide the explicit form of endomorphism ring. A recent work constructs an explicit connection between the supersingular isogeny graph and Bruhat-Tits Tree.(But it's not canonical! That's why I failed.)

Bruhat-Tits tree is an infinite complete p-ary tree related to the lattice in $\mathbb{Q}_p^2$. The relationship can be obtained by localizing the endomorphism ring and considering the isomorphism classes of lattices. I think it will provide more information about the isogeny relationship.

Can we make improvement?

Handling the problem on the isogeny graph may lose some information, which can't provide the explicit form of endomorphism ring. A recent work constructs an explicit connection between the supersingular isogeny graph and Bruhat-Tits Tree.(But it's not canonical! That's why I failed.)

Bruhat-Tits tree is an infinite complete p-ary tree related to the lattice in $\mathbb{Q}_p^2$. The relationship can be obtained by localizing the endomorphism ring and considering the isomorphism classes of lattices. I think it will provide more information about the isogeny relationship.

Can we make improvement?

- The core of the isogeny theory is Complex-Multiplication (CM) methods, the most important objects we care about are the modular curve $X_0(N)$ and the action of the ideal class on isomorphism classes. Up to now, we still know little detailed information about the isogeny graph. Maybe we cannot improve existing algorithms using quantum computers.

Can we make improvement?

- The core of the isogeny theory is Complex-Multiplication (CM) methods, the most important objects we care about are the modular curve $X_0(N)$ and the action of the ideal class on isomorphism classes. Up to now, we still know little detailed information about the isogeny graph. Maybe we cannot improve existing algorithms using quantum computers.
- Recently there is a quasi-polynomial classical algorithm can solve the SIKE setting, with a particular elliptic curve and $l = 2, 3$. Could SIKE still be safe? How about the other cases?

Table of Contents

1. Pre-quantum era
2. Mathematical Background
3. Ordinary cases
4. Supersingular isogeny graphs
5. Approximate quantum walk on the graph
6. Can we make improvement?
7. Future work

Future work

- Quantum money from ordinary elliptic curves class group (Abelian group) action.[Zha23]

Future work

- Quantum money from ordinary elliptic curves class group (Abelian group) action.[Zha23]
- Quantum money from the supersingular isogeny (Quaternion algebra) action.[KSS21]

Future work

- Quantum money from ordinary elliptic curves class group (Abelian group) action.[Zha23]
- Quantum money from the supersingular isogeny (Quaternion algebra) action.[KSS21]
- Apply the expansion property to code design (Maybe qLDPC, quantum Tanner code) and other expander graph construction.

Future work

- Quantum money from ordinary elliptic curves class group (Abelian group) action.[Zha23]
- Quantum money from the supersingular isogeny (Quaternion algebra) action.[KSS21]
- Apply the expansion property to code design (Maybe qLDPC, quantum Tanner code) and other expander graph construction.
- Generalize [CD22]'s attack on other settings[Mam23].

Future work

- Quantum money from ordinary elliptic curves class group (Abelian group) action.[Zha23]
- Quantum money from the supersingular isogeny (Quaternion algebra) action.[KSS21]
- Apply the expansion property to code design (Maybe qLDPC, quantum Tanner code) and other expander graph construction.
- Generalize [CD22]'s attack on other settings[Mam23].
- Design reliable SIKE settings.[BCCF+23].

Thank you!