Quantum Algorithm for Supersingular Isogeny Problem

Against Post-Quantum Crypto Protocol

Zhengyi Han

Students of EECS
Peking University

Learning by Research, June 2022

Table of Contents

Table of Contents

Elliptic curves

Definition

An elliptic curve over a field k is a smooth projective curve of genus 1 with a distinguished k-rational point.

Elliptic curves

Definition

An elliptic curve over a field k is a smooth projective curve of genus 1 with a distinguished k-rational point.

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

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

$(0 : 1 : 0)$ 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 $P, Q, R \in E(k)$,
$R \in \overline{PQ},\ s.t. P + Q + R = O$
Any elliptic curve over $\mathbb{C}$ is isomorphic by $\wp$-function to a torus $\mathbb{C}/L$, so the additive structure is natural.

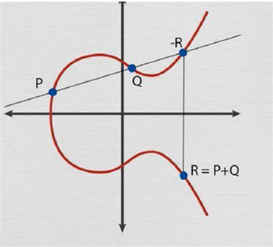


Figure 1: Group Law

Diffie-Hellman

- It is very similar to the RSA protocol which based on factoring. Its intractablity is based on the difficulty to solve discrete logarithm problem.

Diffie-Hellman

- It is very similar to the RSA protocol which based on factoring. Its intractablity is based on the difficulty to solve discrete logarithm problem.
- 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 based on factoring. Its intractablity is based on the difficulty to solve discrete logarithm problem.
- 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)

However, it can be attacked by quantum computer in $poly(log(p))$ time using Shor's algorithm.

Table of Contents

Isogeny

- Morphism between abelian varieties is a rational map over function field that defined every where.

Isogeny

- Morphism between abelian varieties is a rational map over function field that defined every where.
- 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 function field that defined every where.
- 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:

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

$$\mathrm{Id}_E = \hat{\psi} \circ \psi : E \longrightarrow E$$

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 $p \not| t \;\Leftrightarrow \#E[p] = p$
- E is supersingular if $p|t \;\Leftrightarrow E[p] = \{\mathbf{0}_E\}$

Ordinary curves only isogeneous to ordinary curves, so do supersingular curves.

$$E, E' \text{ over } \mathbb{F}_q \text{ are isogeneous } \Leftrightarrow \#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$$

Isogeny graph

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

Isogeny graph

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.

Isogeny graph

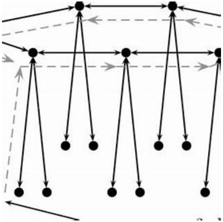
j-invariant can distinct isomorphism classes of elliptic curves over algebraic closure.We can define isogeny graph $G_l(\mathbb{F}_q)$. Its vertices are j-invariant of curves over $\mathbb{F}_q$, there is an edge from j_1 to j_2 if an isogeny maps j_1 to j_2.

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

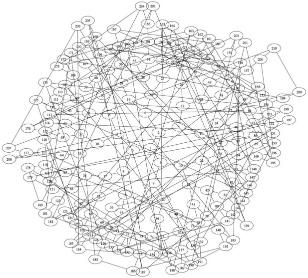
Isogeny graph

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.

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



(a) ordinary



(b) supersingular

Figure 2: Isogeny graph

Table of Contents

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 path in an expander is a hard problem!

Ramanujan graph

Supersingular isogeny graph is the optimal expander Ramanujan Graph.
We assume the location has no regulation.
Because j-invariants of supersingular curves all lie in $\mathbb{F}_{p^2}$, we can consider $G_l(\mathbb{F}_{p^2})$. The graph is completely connected, so constructing isogeny can be reduced to finding path on the graph.

Ramanujan graph

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

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

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

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

Quantum toolkits

Quantum algorithms can do better than classical cases in many problems.

Quantum toolkits

Quantum algorithms can do better than classical cases in many problems.

- It can solve isogeny problem whose endomorphism ring can be embedded to a imaginary quadratic field in subexponential time, while classical case is exponential time. e.g. ordinary isogeny problem and $\mathrm{End}_{\mathbb{F}_p}(E)$, E is defined over $\mathbb{F}_{p^2}$.

Quantum toolkits

Quantum algorithms can do better than classical cases in many problems.

- It can solve isogeny problem whose endomorphism ring can be embedded to a imaginary quadratic field in subexponential time, while classical case is exponential time. e.g. ordinary isogeny problem and $\mathrm{End}_{\mathbb{F}_p}(E)$, E is defined over $\mathbb{F}_{p^2}$.
- For general searching problem on a graph, quantum walk can provide quadratic speedup.

Existing algorithm

- One algorithm to constructing isogeny is to construct isogeny to the curves whose j-invariant in $\mathbb{F}_p$, making use of the $\mathrm{End}_{\mathbb{F}_p}(E)$. Its time complexity is $\tilde{O}(p^{1/4})$
- To construct isogeny between E_1, E_2, we can implement quantum "meet in the middle", its complexity is $\tilde{O}(p^{1/6})$.

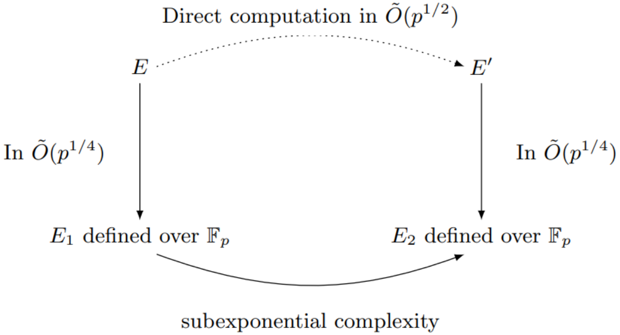


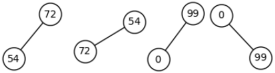
Table of Contents

Can we make improvement?

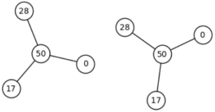
To make improvement to the existing algorithm, we need to make full use of the property of the isogeny problem instead of just taking the problem as an unordered searching problem. Then we need to exploring the detailed information.

Can we make improvement?

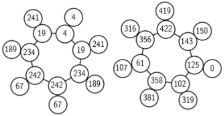
To make improvement to the existing algorithm, we need to make full use of the property of the isogeny problem instead of just taking the problem as an unordered searching problem. Then we need to exploring the detailed information.In a recent work, the set S_p be seen as probably not follows the uniform 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) $p \equiv 7 \bmod 8$

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.

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.

Bruhat-Tits tree is an infinite complete p-ary tree related to lattice in $\mathbb{Q}_p^2$. The relationship can be got from localizing the endomorphism ring and considering the isomorphism classes of lattice.

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.
Bruhat-Tits tree is an infinite complete p-ary tree related to lattice in $\mathbb{Q}_p^2$.
The relationship can be got from localizing the endomorphism ring and considering the isomorphism classes of lattice.
We begin to consider isogeny problem in this view instead of isogeny graph.
I think it will provide more information about the isogeny relationship.

Thank you!