

Adding Level Structure to Supersingular Elliptic Curve Isogeny Graphs

Sarah Arpin, University of Colorado Boulder

`sarah.arpin@colorado.edu`

The Ohio State University Number Theory Seminar

November 22nd, 2021

Table of Contents

- 1** Background
 - Elliptic Curves
 - Quaternion Algebras
 - Cryptographic Motivation

- 2** Isogeny Graph With Level Structure
 - Eichler Orders
 - Equivalence of Categories

- 3** Counting Isogenous Conjugates

- 4** Conclusion
 - Summary

Supersingular Elliptic Curves

Definition (Chapter V[Sil09])

Let E be an elliptic curve defined over a field K of characteristic $p \neq 1$. E is **supersingular** iff one of the following equivalent conditions hold:

- $[p] : E \rightarrow E$ is purely inseparable and $j(E) \notin \mathbb{F}_{p^2}$,
- $\text{End}(E)$ is a maximal order in a quaternion algebra.

For a given p , there are finitely many isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$.

Convention

- p : a fixed **large** prime (cryptographic size)
- $p \equiv 3 \pmod{4}$ (minor adjustments for other p)

Frobenius Isogeny

ρ -power Frobenius map $\pi_\rho : E \rightarrow E^{(\rho)}$
 $\pi_\rho(x, y) = (x^\rho, y^\rho)$

- Induced by the field automorphism
- $a \in \mathbb{F}_p$, then $a^\rho = a$.
- If $E : y^2 = x^3 + ax + b$, then
 $E^{(\rho)} : y^2 = x^3 + a^\rho x + b^\rho$
- $j(E)^\rho = j(E^{(\rho)})$



Figure: [https://commons.wikimedia.org/wiki/File:GeorgFrobenius_\(cropped\).jpg](https://commons.wikimedia.org/wiki/File:GeorgFrobenius_(cropped).jpg)

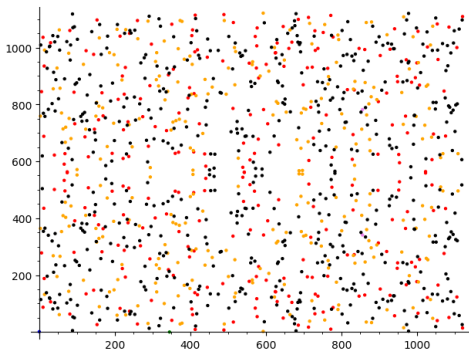
Torsion Subgroups

The points of an elliptic curve form a group under addition [Sil09].

Torsion points are points for which some multiple gives O_E .

$$E[N] = (\mathbb{Z}/N\mathbb{Z})^2$$

Below, a supersingular elliptic curve over F_{1123} , points colored by order in the group:



Blue = 1, green = 2, violet = 4, red = 281, orange = 562, black = 1124.

Isogenies

Definition

An **isogeny** $\phi : E_1 \rightarrow E_2$ is a morphism between elliptic curves such that $\phi(O_{E_1}) = O_{E_2}$. It has a dual $\hat{\phi} : E_2 \rightarrow E_1$.

Theorem (Corollary III.4.9 and Proposition III.4.12 [Sil09])

The kernel of a nonzero isogeny is a finite group. A given finite subgroup of points uniquely determines a separable isogeny.

Theorem (Theorem III.4.10(c) [Sil09])

The degree of a separable isogeny is equal to the size of the kernel.

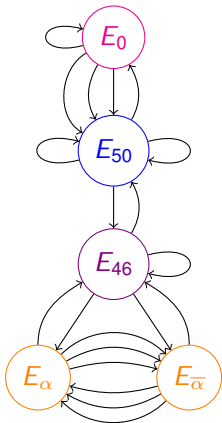
Convention

Isogenies will be degree ℓ or ℓ^r , with ℓ a small prime.

Supersingular elliptic curves over $\overline{\mathbb{F}}_p$ are all ℓ -power isogenous.

Supersingular ℓ -isogeny graph

$$p = 53, \ell = 3$$



- With the right conditions on p , can be taken to be *undirected* by identifying isogenies with their duals
- Connected
- Out-degree $\ell + 1$
- $b_{12}^p c$ nodes

Quaternion Algebras

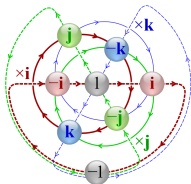


Figure: https://en.wikipedia.org/wiki/File:Cayley_08_quaternion_multiplication_graph.svg

Definition (Quaternion algebra ramified at p and ℓ)

$B_{p,\ell} : \mathbb{Q}\langle i, j \rangle$ such that $i^2 = -1$, $j^2 = -p$, and $ij = -ji$

If $E/\overline{\mathbb{F}}_p$ is supersingular, then $\text{End}(E)$ is isomorphic to a maximal order in $B_{p,\ell}$.

Quaternion Algebras: A Comparison to Number Fields

Quaternion Algebra	Number Field
Noncommutative	Commutative
$B_{p,\gamma}/\mathbb{Q}$	K/\mathbb{Q}
Maximal orders (finitely many)	\mathcal{O}_K
Eichler orders of level N	Orders of conductor N : $\mathbb{Z} + N\mathcal{O}_K$
Class set of left or right ideals Class group of two-sided ideals	Class group of ideals

Deuring Correspondence

A categorical equivalence:

Theorem (Deuring Correspondence, [Deu41])

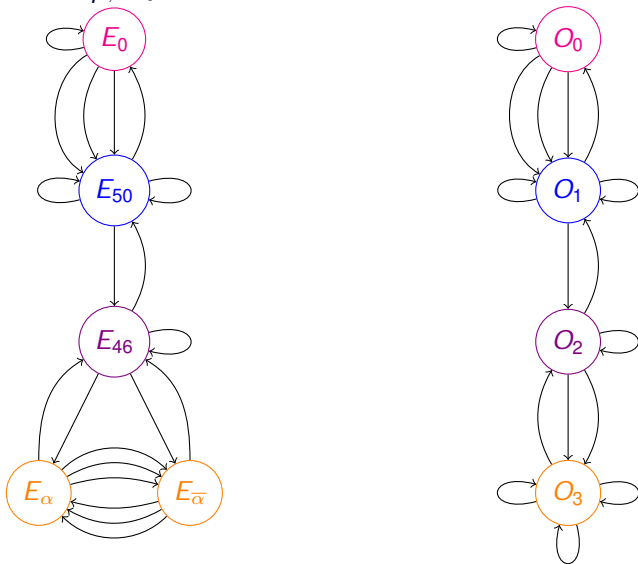
There is a bijection between isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ and left ideal classes of a fixed maximal order \mathcal{O} of $B_{p,1}$.

Theorem (Deuring Correspondence II)

If $E/\overline{\mathbb{F}}_p$ is supersingular, then there is a maximal order \mathcal{O} of $B_{p,1}$ such that $\text{End}(E) = \mathcal{O}$. This association is either 2-1 or 1-1, depending on the size of the two-sided ideal class group of \mathcal{O} .

The Deuring correspondence is **not** computationally feasible, in terms of runtime.

Quaternion $G_{p,l}$, $p = 53$, $l = 3$



Cryptographic Motivation

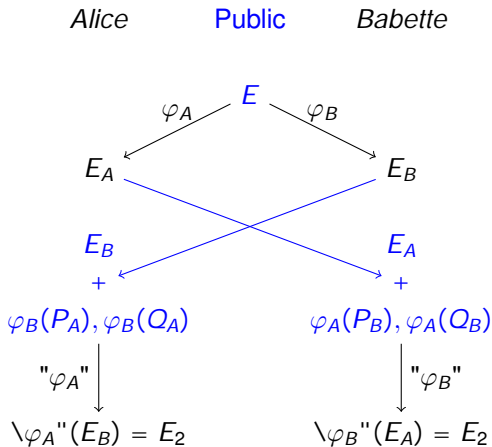
Post-Quantum Cryptography

- NIST: 2015 call for proposals of post-quantum safe cryptography protocols. Now in Round 3.
- Supersingular Isogeny Graph Cryptography: 15 years old: original hash function by Charles-Goren-Lauter [**CGL06**]; SIKE key exchange [**SIKE**]

Hard Problems

- Path-finding in supersingular ℓ -isogeny graph
- Path-finding with additional torsion point information

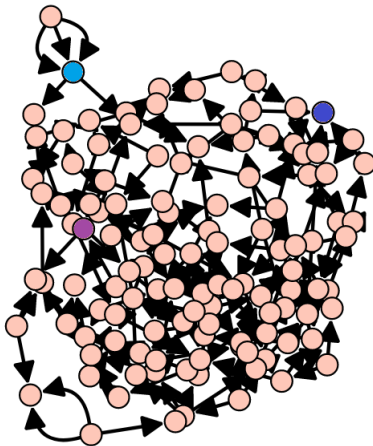
Supersingular Isogeny Diffie-Hellman (SIKE)



φ_A is degree $\ell_A^{e_A}$ and φ_B is degree $\ell_B^{e_B}$
 $E[\ell_A^{e_A}] = \langle P_A, Q_A \rangle$ and $E[\ell_B^{e_B}] = \langle P_B, Q_B \rangle$

Hard Problems

- 1 Given E_1, E_2 , find an ℓ^n -isogeny between them.
- 2 Given $E, \varphi_A(E)$, and $\varphi_B(E), \varphi_A(P_B), \varphi_A(Q_B), \varphi_B(P_A)$, and $\varphi_B(Q_A)$, find $\varphi_A(\varphi_B(E)) = \varphi_B(\varphi_A(E))$.



How to study security?

Deuring Correspondence

- Relationships between underlying hard problems [Eis+18]. The path-finding problem is equivalent to computing the Deuring correspondence.
- The path-finding problem for quaternion algebras has been solved [Koh+14].

Graph Structure

- Path-finding between F_p points of $G_{p,\ell}$ [DG16]
- The structure of the subgraph of F_p -points of $G_{p,\ell}$ is known [Arp+19]
- Public torsion point information could be a weakness [Pet17] [Que+21]. More investigation is needed.

Finding Cycles in $G_{p,\ell}$

- The WIN4 project [Ban+19] uses cycles in $G_{p,\ell}$ to generate the endomorphism ring
- [Eis+20] provides a new cycle-finding algorithm

Isogeny Graph $E_{p,\ell}^N$ With Level Structure

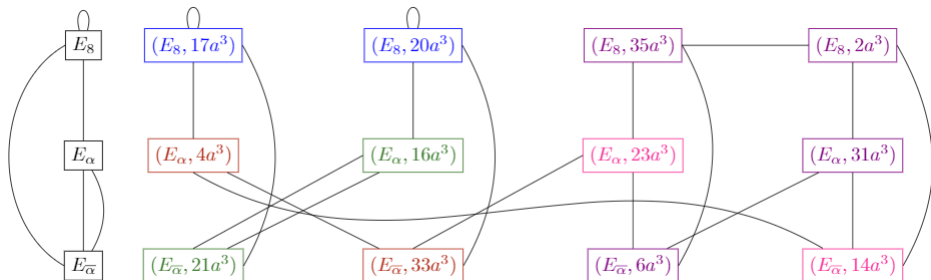
Idea: Keep track of $\varphi_A(P_B), \varphi_A(Q_B)$ in the supersingular ℓ -isogeny graph

- Nodes: (E, G)
 - E : supersingular elliptic curve
 - $G = E(\overline{\mathbb{F}}_p)$ of (small) prime order N
- Edges: $(E, G) \rightarrow (E^\theta, G^\theta)$ corresponding to an ℓ -isogeny φ :
 - $\varphi(E) = E^\theta$
 - $\varphi(G) = G^\theta$

Graph Properties

- $(N + 1)$ nodes for every node of $G_{p,\ell}$.
- $(\ell + 1)$ -regular, just like $G_{p,\ell}$
- $E_{p,\ell}^N$ is connected, just like $G_{p,\ell}$

$$p = 37, \ell = 2, N = 3$$



- Black graph on the left: $G_{p,\ell}$ Supersingular 2-isogeny graph for $p = 37$
- Colorful graph on the right: $E_{37,2}^3$ Supersingular 2-isogeny graph for $p = 37$ with added level structure for $N = 3$.
- We can see how 2-isogenies act (differently) on 3-torsion points

The Quaternion Picture

What is the endomorphism ring of a node of $E_{p,\ell}^N$?

$$\text{End}(E, G) := \{ \alpha \in \text{End}(E) : \alpha(G) = G \}$$

Theorem (Arpin)

$\text{End}(E, G)$ is isomorphic to an Eichler order of level $|G|$ of $B_{p,1}$.

Equivalence of Categories

- S_N
 - Objects: Pairs (E, G) with E a supersingular elliptic curve over $\overline{\mathbb{F}}_p$ and an order N subgroup $G \leq E[N]$
 - Morphisms: $(E, G) \rightarrow (E^0, G^0)$ a nonzero isogeny $\psi : E \rightarrow E^0$ such that $\psi(G) = G^0$.
- LM
 - Objects: invertible left $\text{End}(E, G)$ -modules
 - Morphisms: nonzero left $\text{End}(E, G)$ -module homomorphisms.

Theorem (Arpin)

Fix $(E, G) \in S_N$. $\text{Hom}(_, (E, G)) : S_N^{op} \rightarrow LM$ is a contravariant equivalence of categories.

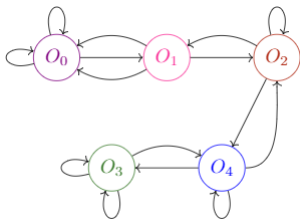
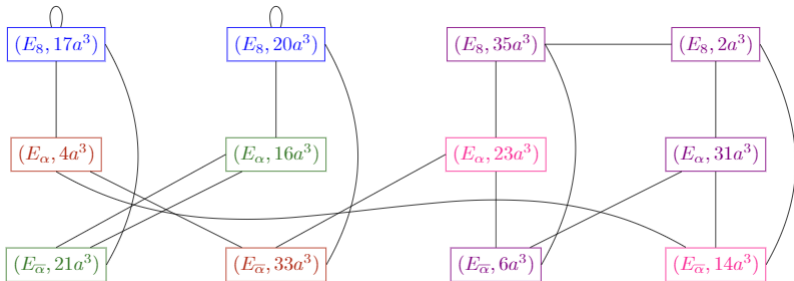
Correspondence to Eichler Orders

Theorem (Arpin)

Given a pair $(E, G) \in E_{p,\ell}^N$, there is an Eichler order \mathcal{O} of level N in $B_{p,1}$ such that $\text{End}(E, G) = \mathcal{O}$. This association is either 4-1, 2-1, or 1-1, depending on the size of the two-sided ideal class group of \mathcal{O} .*

*Curves with extra automorphisms ($j = 0, 1728$) may not conform.

$$p = 37, N = 3, \ell = 2$$



Coincidence of $\text{End}(E, G)$

What are the reasons for 4-1, 2-1, or 1-1 maps from endomorphism rings of pairs (E, G) to Eichler orders? (Arpin)

Four nodes of $E_{p,\ell}^N$ with isomorphic endomorphism rings: O :

- 1 (E, G) , where G is the kernel of an isogeny $\varphi_G : E \rightarrow E^\ell$,
- 2 $(E^{(p)}, G^{(p)})$, where $G^{(p)}$ is the image of G under π_p ,
- 3 (E^ℓ, G^ℓ) , where E^ℓ is the codomain of φ_G and $G^\ell = \ker(\widehat{\varphi})$,
- 4 $((E^\ell)^{(p)}, (G^\ell)^{(p)})$, where $(G^\ell)^{(p)}$ is the image of G^ℓ under π_p

The possibilities for coincidence of the above nodes are:

- 1 All four distinct.
- 2 $(E, G) = (E^{(p)}, G^{(p)})$ and $(E^\ell, G^\ell) = ((E^\ell)^{(p)}, (G^\ell)^{(p)})$.
- 3 $(E, G) = (E^\ell, G^\ell)$ and $(E^{(p)}, G^{(p)}) = ((E^\ell)^{(p)}, (G^\ell)^{(p)})$.
- 4 $(E, G) = ((E^\ell)^{(p)}, (G^\ell)^{(p)})$ and $(E^\ell, G^\ell) = (E^{(p)}, G^{(p)})$.
- 5 $(E, G) = ((E^\ell)^{(p)}, (G^\ell)^{(p)}) = (E^\ell, G^\ell) = (E^{(p)}, G^{(p)})$.

One instance of (4): N -isogenous conjugate pairs.

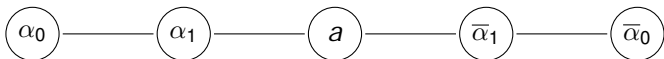
Mirror Paths

Frobenius acts on the $G_{p,\ell}$: if $\varphi : E_1 \rightarrow E_2$ is an ℓ -isogeny, then there exists an ℓ -isogeny $E_1^{(p)} \rightarrow E_2^{(p)}$.

How do can these paths connect?

- α_j : j -invariants in $F_{p^2} \cap F_p$
- a : j -invariant in F_p

Option 1: Through an F_p vertex



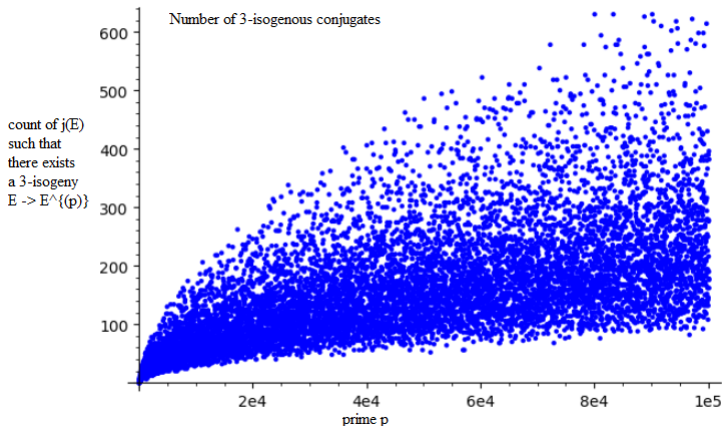
Option 2: Through an ℓ -isogenous pair of conjugate vertices



How often are paths of the second type?

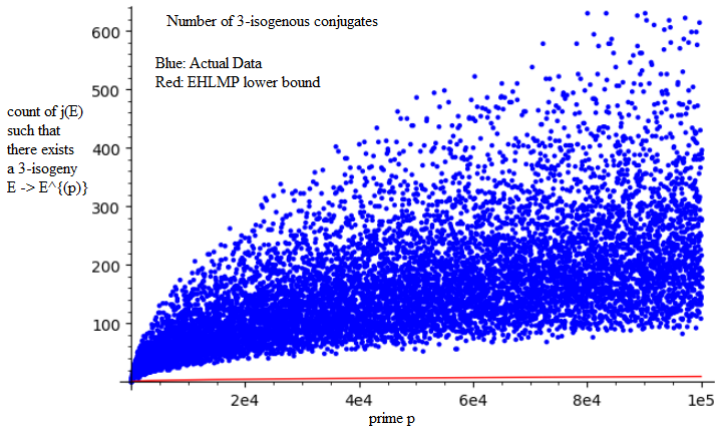
How often are conjugate j -invariants 3-isogenous?

Data: [Arp+19].



How often are conjugate j -invariants 3-isogenous?

Data: [Arp+19]. Lower bound: [Eis+20] Eisentraeger, Hallgren, Leonardi, Morrison, Park



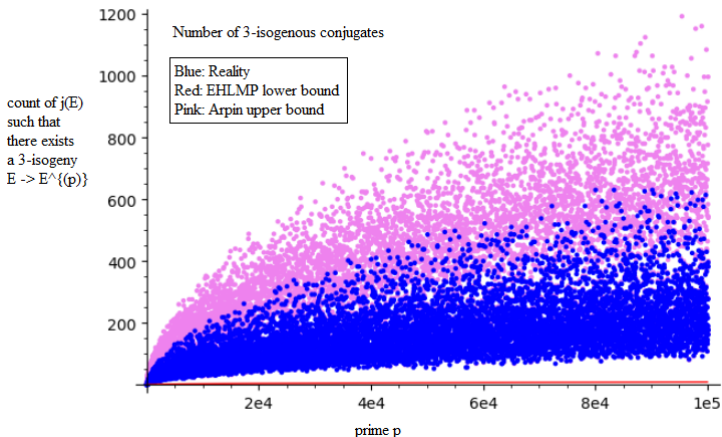
A Bound From Quaternion Algebras

N -isogenous pairs give a 2-1 association to Eichler orders, giving an upper bound:

$$4T \leq (N + 1)(\#S_p)$$

How often are conjugate j -invariants 3-isogenous?

Data: [Arp+19]. Lower bound: [Eis+20] Eisentraeger, Hallgren, Leonardi, Morrison, Park. Upper bound: Arpin



An Exact Count

Theorem (Arpin, Chenu-Smith [CS21])

$\alpha(1)$: number of pairs (E, ψ) , where E is a supersingular elliptic curve and ψ is a degree- N isogeny E to $E^{(p)}$.

$2\alpha(1)$ equals the number of pairs of a supersingular elliptic curve E and an embedding $\mathbb{Z}[\sqrt{pN}]$ into $\text{End}(E)$.

$$2\alpha(1) = \begin{cases} j \text{Cl}(\mathbb{Z}[\frac{1+\sqrt{pN}}{2}]) + j \text{Cl}(\mathbb{Z}[\sqrt{pN}]) & , \quad pN \equiv 3 \pmod{4} \\ j \text{Cl}(\mathbb{Z}[\sqrt{pN}]) & , \quad pN \equiv 1 \pmod{4} \end{cases}$$

(The factor of two appears because two embeddings which differ by a factor of ± 1 on the generator \sqrt{pN} are counted as distinct, whereas the two isogenies $\psi, \psi \circ \pi$ are not considered distinct.)

Summary

- The structure of $G_{p,\ell}$ can be analyzed through properties of $E_{p,\ell}^N$.
- Supersingular isogeny graph cryptographic protocol seems very safe so far, but more research is always needed.
- Counting isogenous conjugate pairs relates to answering questions about the two-sided ideal class group of an Eichler order.

Thank You !

Reference I

- [Arp+19] Sarah Arpin et al. **Adventures in Supersingularland**. 2019. arXiv: 1909.07779 [math.NT].
- [Ban+19] Efrat Bank et al. “Cycles in the supersingular ℓ -isogeny graph and corresponding endomorphisms”. In: **Research directions in number theory—Women in Numbers IV**. Vol. 19. Assoc. Women Math. Ser. Springer, Cham, [2019] ©2019, pp. 41–66. DOI: 10 . 1007 / 978 - 3 - 030 - 19478 - 9 _ 2.
- [CS21] Mathilde Chenu and Benjamin Smith. **Higher-degree supersingular group actions**. 2021. arXiv: 2107.08832 [cs.CR].
- [Deu41] Max Deuring. “Die Typen der Multiplikatorenringe elliptischer Funktionenkörper.”. In: **Abh. Math. Sem. Hansischen Univ.** 14 (1941), pp. 197–272.

Reference II

- [DG16] Christina Delfs and Steven D. Galbraith. “Computing isogenies between supersingular elliptic curves over F_p ”. In: **Des. Codes Cryptogr.** 78.2 (2016), pp. 425–440. ISSN: 0925-1022. DOI: 10.1007/s10623-014-0010-1.
- [Eis+18] Kirsten Eisenträger et al. “Supersingular isogeny graphs and endomorphism rings: reductions and solutions”. In: **Advances in cryptology—EUROCRYPT 2018. Part III**. Vol. 10822. Lecture Notes in Comput. Sci. Springer, Cham, 2018, pp. 329–368.
- [Eis+20] Kirsten Eisenträger et al. “Computing endomorphism rings of supersingular elliptic curves and connections to path-finding in isogeny graphs”. In: **ANTS XIV—Proceedings of the Fourteenth Algorithmic Number Theory Symposium**. Vol. 4. Open Book Ser. Math. Sci. Publ., Berkeley, CA, 2020, pp. 215–235. DOI: 10.2140/obs.2020.4.215. URL: <https://doi-org.colorado.idm.oclc.org/10.2140/obs.2020.4.215>.

Reference III

- [Koh+14] David Kohel et al. “On the quaternion ℓ -isogeny path problem”. In: **LMS J. Comput. Math.** 17.suppl. A (2014), pp. 418–432. DOI: 10.1112/S1461157014000151.
- [Pet17] Christophe Petit. “Faster algorithms for isogeny problems using torsion point images”. In: **Advances in cryptography—ASIACRYPT 2017. Part II**. Vol. 10625. Lecture Notes in Comput. Sci. Springer, Cham, 2017, pp. 330–353. DOI: 10.1007/978-3-319-70697-9_12.
- [Que+21] Victoria de Quehen et al. **Improved torsion point attacks on SIDH variants**. 2021. arXiv: 2005.14681 [math.NT].
- [Sil09] Joseph H. Silverman. **The arithmetic of elliptic curves**. Second. Vol. 106. Graduate Texts in Mathematics. Springer, Dordrecht, 2009, pp. xx+513. ISBN: 978-0-387-09493-9. DOI: 10.1007/978-0-387-09494-6.