Isogeny-Based Security Assumptions
(Work in Progress)

Giacomo Pope*

August 17, 2022

Abstract A collection of the various cryptographic assumptions made in isogeny-based cryptography.

1 Introduction

The aim of this note is to collect the various problems related to isogeny-based cryptography and present them in a single document with consistent notation. This work was inspired by the website `https://issikebrokenyet.github.io`, which aims to produce "A knowledge base of most isogeny based cryptosystems and the best attacks on them". The hope is that this can be a companion to the website, offering a formal definition of the various collected security assumptions.

This note *does not* aim to give a comprehensive definition of the pieces which build these problems (e.g. what is an isogeny, what is a supersingular elliptic curve, what is an endomorphism ring...). To answer those questions we rely on a collection of references which is certainly incomplete, but hopefully a good start:

- The canonical textbooks for elliptic curves and isogenies are Silverman [Sil09], Washington [Was08] and Galbraith [Gal12].
- Voight recently published a comprehensive text on quaternion algebras [Voi21].
- Some introductory references for isogeny-based cryptography are De Feo's lectures [DF17] and Costello's introduction to SIDH [Cos19b].
- Panny's thesis is a great resource on the mathematical background to isogenies, and a brilliant resource to learn about CSIDH [Pan21].
- A fantastic resource for learning about Diffie-Hellman using group actions and isogenies is [Smi18]

Acknowledgments. TODO

*`giacomo.pope@nccgroup.com`

2 Notation and Conventions

Unless otherwise stated, we work under the conditions that:

- Isogenies are assumed to be separable and denoted by greek letters: $\phi, \psi_A, \ldots$. In all cases, isogenies which are intended to be computed will have smooth-degree.
- Elliptic curves, denoted by E, E', E_A, are assumed to be defined over the finite field $\mathbb{F}_q$. The point at infinity is denoted ∞ so as not to conflict with notation used for orders of quaternion algebras.
- The N-torsion group of an elliptic curve is denoted $E[N]$.
- Given a prime p, the unique quaternion algebra over $\mathbb{Q}$ ramified exactly at p and ∞ is denoted $B_{p,\infty}$.
- The *reduced trace* and *reduced norm* of elements of $\alpha \in B_{p,\infty}$ are denoted $\mathrm{Trd}(\alpha)$, $\mathrm{Nrd}(\alpha)$ respectively.
- An order of a number field k or a quaternion algebra B is denoted $\mathcal{O}$. It is a full-rank lattice which is also a subring. When an order is not contained inside any other, it is said to be maximal.
- As quaternion algebras are non-commutative, we must differentiate between left-orders $\mathcal{O}_L$ and right-orders $\mathcal{O}_R$ (similarly we have left- and right-ideals). For commutative rings, these are simply equivalent.
- The best-known attacks against the problems within this note are not discussed, except in the exception case of a polynomial time attack being found. In this case we consider the problem easy, and a scheme which relies on the hardness of the problem broken.

3 Supersingular isogeny problems

In this section, we list the core security assumptions of isogeny based protocols. Generally, these problems do not contain enough structure to build entire protocols from, and so should be considered as the building blocks for isogeny-based schemes.

Problem 3.1 (ℓ-Isogeny path)**.** Given a prime p and two supersingular elliptic curves E_1, E_2 defined over the field $\mathbb{F}_{p^2}$, find a path between E_1 and E_2 in the ℓ-isogeny graph. [Wes21b, Problem 1.1]

Problem 3.2 (ℓ-Isogeny path with random starting curve)**.** Take problem 3.1 and additional assume that E_1 is a random supersingular elliptic curve. In particular, its endomorphism ring $\mathrm{End}(E_1)$ is unknown.

4 Supersingular isogeny Diffie-Hellman problems

In this section, we work with supersingular elliptic curves whose field has characteristic $p = \ell_A^{e_A}\ell_B^{e_B} - 1$. The elliptic curve $E/\mathbb{F}_{p^2}$ has order $(p+1)^2$. The generators of the torsion groups are denoted $E[\ell_A^{e_A}] = \langle P_A, Q_A\rangle$ and $E[\ell_B^{e_B}] = \langle P_B, Q_B\rangle$. In more recent papers, the explicit choice of $\ell_A = 2$ and $\ell_B = 3$ is made, but we keep to allowing the chosen primes to be implicit.

Problem 4.1 (Computational Supersingular Isogeny (CSSI))**.** Let $\phi_A : E_0 \to E_A$ be an isogeny whose kernel is $\langle [m_A]P_A + [n_A]Q_A\rangle$, where m_A, n_A are chosen at random from $\mathbb{Z}/\ell_A^{e_A}\mathbb{Z}$ and not both divisible by ℓ_A. Given E_A and the values $\phi_A(P_B), \phi_A(Q_B)$, find a generator R_A of $\langle [m_A]P_A + [n_A]Q_A\rangle$.

Remark. Problem 4.1 is sometimes referred to as the **Supersingular Isogeny with Torsion (SSI-T)** problem, named to emphasise the knowledge of the torsion points along with the codomain of the secret isogeny [KMP+20, Problem 1].

Problem 4.2 (Computational Supersingular Isogeny (CSSI) problem with random starting curve)**.** Take the above Problem 4.1. Additionally, assume that E_0 is a random supersingular curve. In particular, its endomorphism ring $\mathrm{End}(E_0)$ is assumed to be unknown.

Attack (Castryck-Decru)**.** In the work [CD22], Castryck and Decru described a polynomial time algorithm to solve Problem 4.1. This was then further generalised in [MM22, Rob22] to solve Problem 4.2. As such these two problems and those remaining in this section are considered easy and any protocol based on this hardness of this problem is broken. This includes SIDH [JDF11], and hence SIKE [ACC+20], the key encapsulation mechanism built from SIDH. It additionally includes B-SIDH [Cos19a], a generalisation of SIDH which includes torsion points a supersingular elliptic curve together with its quadratic twist.

Problem 4.3 (Supersingular Computational Diffie-Hellman (SSCDH))**.** Let $\phi_A : E_0 \to E_A$ be an isogeny whose kernel is equal to $\langle [m_A]P_A+[n_A]Q_A\rangle$, and let $\phi_B : E_0 \to E_B$ be an isogeny whose kernel is $\langle [m_B]P_B+[n_B]Q_B\rangle$, where m_A, n_A (respectively m_B, n_B) are chosen at random from $\mathbb{Z}/\ell_A^{e_A}\mathbb{Z}$ (respectively $\mathbb{Z}/\ell_B^{e_B}\mathbb{Z}$) and not both divisible by ℓ_A (respectively ℓ_B). Given the curves E_A, 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 the curve

$$E_0/\langle [m_A]P_A + [n_A]Q_A, [m_B]P_B + [n_B]Q_B\rangle.$$

Problem 4.4 (Supersingular Decision Diffie-Hellman (SSDDH))**.** Given data sampled with probability 1/2 from one of the following two distributions:

1. The data: E_A, E_B, $\phi_A(P_B)$, $\phi_A(Q_B)$, $\phi_B(P_A)$, $\phi_B(Q_A)$ defined as in Problem 4.3 together with the ending curve:

$$E_{AB} \cong E_0/\langle [m_A]P_A + [n_A]Q_A, [m_B]P_B + [n_B]Q_B\rangle.$$

2. The data $E_A, E_B, \phi_A(P_B), \phi_A(Q_B), \phi_B(P_A), \phi_B(Q_A)$, as defined in Problem 4.3 together with the random curve

$$E_C \cong E_0/\langle [m'_A]P_A + [n'_A]Q_A, [m'_B]P_B + [n'_B]Q_B \rangle,$$

where m'_A, n'_A (respectively m'_B, n'_B) are chosen at random from $\mathbb{Z}/\ell_A^{e_A}\mathbb{Z}$ (respectively $\mathbb{Z}/\ell_B^{e_B}\mathbb{Z}$) and not both divisible by ℓ_A (respectively ℓ_B).

determine from which distribution the data is sampled.

5 Hard homogenous spaces

We begin this section looking at the cryptographic problems associated with Couveignes *hard homogenous spaces* [Cou06]. We allow $\star : \mathfrak{G} \times X \to X$ be a transitive, finite Abelian group action for a (multiplicative) group $\mathfrak{G}$ and set X.

Problem 5.1 (Vectorisation)**.** In a principle homogenous space X under $\mathfrak{G}$, given the elements x, y of a set X, compute the unique group element $\mathfrak{g} \in \mathfrak{G}$ such that $y = \mathfrak{g} \star x$.

Problem 5.2 (Parallelisation)**.** In a principle homogenous space X under $\mathfrak{G}$, given the elements x, $\mathfrak{g} \star x$ and $\mathfrak{h} \star x$ of the set X, compute the unique element $(\mathfrak{g}\mathfrak{h}) \star x \in X$.

Definition 5.1 (Hard homogenous spaces)**.** A *hard homogenous space* is a principle homogenous space X under $\mathfrak{G}$ in which it is efficient to compute the group action on the set, but for which the vectorisation and parallelisation problems are assumed to be computationally infeasible.

Remark. A familiar example of a hard homogenous space is when we allow the set X to be the group $\mathfrak{G}$. As a concrete example, we could take $\mathfrak{G}$ to be multiplicative group of integers modulo a prime: $\mathbb{F}_p^\times$. In this case, vectorisation and parallelisation become the discrete logarithm problem and the computational Diffie-Hellman problem respectively. See [GPSV18, Smi18] for more detailed discussion.

5.1 Class Group Action

We now focus on the specific hard homogenous space used in CSIDH [CLM+18] and related schemes.

Let $\mathbb{F}_p$ be a finite field with characteristic $p \equiv 3 \pmod 4$. Consider the imaginary quadratic number field $K = \mathbb{Q}(\sqrt{-p})$ and the corresponding order $\mathcal{O} \subseteq K = \mathbb{Z}[\sqrt{-p}]$. The ideal class group of this order $\mathrm{cl}(\mathcal{O})$ acts freely via isogenies on the set of elliptic curves with $\mathbb{F}_p$-rational endomorphism ring.

We can thus construct a principle homogenous space by picking our group action $\mathfrak{G} = \mathrm{cl}(\mathcal{O})$ and our set X as the set of supersingular elliptic curves up to $\mathbb{F}_p$-isomorphism:

$$\mathcal{E}_p(\mathcal{O}) = \{E/\mathbb{F}_p : \mathrm{End}(E) \cong \mathcal{O}\}/\{\mathbb{F}_p - \text{isomorphisms}\}$$

We denote classes in $\mathrm{cl}(\mathcal{O})$ as $[\mathfrak{a}]$ and ideals as $\mathfrak{a} \in [\mathfrak{a}]$. The action of the class group on the set of elliptic curves is denoted $E_A = [\mathfrak{a}] \star E$ via the isogeny $\phi_{\mathfrak{a}} : E \to E_A = E/\mathfrak{a}$. This can be efficiently computed assuming that the norm of $\mathfrak{a}$ is smooth.

Problem 5.3 (Key Recovery (Class Groups)). Given a supersingular elliptic curve $E/\mathbb{F}_p \in \mathcal{E}_p(\mathcal{O})$ and the element $E_A = [\mathfrak{a}] \star E \in \mathcal{E}_p(\mathcal{O})$, recover the class $[\mathfrak{a}] \in \mathrm{cl}(\mathcal{O})$. This is simply Problem 5.1 with $\mathfrak{G} = \mathrm{cl}(\mathcal{O})$ and $X = \mathcal{E}_p(\mathcal{O})$.

Problem 5.4 (Computational Diffie-Hellman (Class Groups)). Given a supersingular elliptic curve $E/\mathbb{F}_p \in \mathcal{E}_p(\mathcal{O})$ and the elements $E_A = [\mathfrak{a}] \star E \in \mathcal{E}_p(\mathcal{O})$ and $E_B = [\mathfrak{b}] \star E \in \mathcal{E}_p(\mathcal{O})$ compute the supersingular elliptic curve E_{AB} such that $E_{AB} = [\mathfrak{a}\mathfrak{b}]E$. This is simply Problem 5.2 with $\mathfrak{G} = \mathrm{cl}(\mathcal{O})$ and $X = \mathcal{E}_p(\mathcal{O})$.

Problem 5.5 (Decisional Diffie-Hellman (Class Groups)). Given data sampled with probability $1/2$ from one of the following two distributions:

1. (E, E_A, E_B) as defined in Problem 5.4 and the supersingular elliptic curve $E_{AB} = [\mathfrak{a}\mathfrak{b}]E$,
2. (E, E_A, E_B) as defined in Problem 5.4 and the supersingular elliptic curve $E_{AB} = [\mathfrak{c}]E$, where $[\mathfrak{c}]$ is class selected randomly from $\mathrm{cl}(\mathcal{O})$,

determine from which distribution the data is sampled.

Attack (Genus Theory Attack). In [CSV20] it was shown that Problem 5.5 is easy providing that the class number $h(\mathcal{O})$ is even. This is the case when $p \equiv 1 \pmod 4$. As CSIDH used $p \equiv 3 \pmod 4$, this attack does not extend to CSIDH or schemes built from CSIDH such as SeaSign and CSI-Fish.

Problem 5.6 ($\mathcal{O}$-Uber Isogeny). Let $p > 3$ be a prime and $\mathcal{O}$ be a quadratic order of discriminant Δ. Given $E, E_A \in \mathcal{E}_{\mathcal{O}}$[1] and an explicit embedding of $\mathcal{O}$ into $\mathrm{End}(E)$, find a powersmooth ideal $\mathfrak{a}$ of norm coprime to Δ such that $[\mathfrak{a}] \in \mathrm{cl}(\mathcal{O})$ and $[\mathfrak{a}] \star E = E_A$. [DdSGKPS19, Problem 5.1]

Remark. When $p \equiv 3 \pmod 4$ and $\Delta = -4p$, then the $\mathcal{O}$-Uber Isogeny Problem is equivalent to the key recovery problem for CSIDH. The proof is given in [DdSGKPS19, Section 5.2] along with similar reductions for OSIDH [CK20], SIDH [DFJP14] and Séta [DdSGKPS19].

6 Endomorphism ring problems

In this section, we summarise various problems in performing computations with the endomorphism ring of supersingular elliptic curves. In [Wes21b, Wes21a] it has been shown that these problems are equivalent to certain isogeny problems.

[1] $\mathcal{E}_{\mathcal{O}}$ is the set of supersingular elliptic curves admitting a primitive embedding of $\mathcal{O}$ up to isomorphism.

Problem 6.1 (Endomorphism Ring)**.** Given a prime p and a supersingular elliptic curve $E/\mathbb{F}_{p^2}$ find four endomorphisms of E (in an efficient representation) that generate $\mathrm{End}(E)$ as a lattice. [Wes21b, Problem 1.2]

Problem 6.2 (Maximal Order)**.** Given a prime p and a supersingular elliptic curve $E/\mathbb{F}_{p^2}$ find four quaternions in $B_{p,\infty}$ that generate a maximal order $\mathcal{O} \cong \mathrm{End}(E)$. [Wes21b, Problem 1.3]

Problem 6.3 (Quaternion Path)**.** Given two maximal orders $\mathcal{O}_1$, $\mathcal{O}_2$ in $B_{p,\infty}$, and a set $\mathcal{N}$ of positive integers, find a left $\mathcal{O}_1$-ideal I such that $\mathrm{Nrd}(I) \in \mathcal{N}$ and $\mathcal{O}_R \cong \mathcal{O}_2$. [Wes21b, Problem 1.4]

Problem 6.4 (B-Powersmooth Quaternion Path)**.** Consider Problem 6.3. We make the additional restriction that $\mathcal{N}$ is the set of B-powersmooth integers for a given $B > 0$. [Wes21b, Problem 1.4]

TODO!! Write about how these problems are related to the problems in other sections!!

6.1 Oriented endomorphism ring problems

Restricting our attention to oriented endomorphism ring problems is particularly useful when considering the security of CSIDH [CLM⁺18]. In [Wes21a], work was done to show the equivalence of these problems with inverting the action of class groups on oriented supersingular elliptic curves.

We let $\mathcal{O}$ be an order of a quadratic number field k. An orientation is the embedding:

$$\iota : \mathcal{O} \hookrightarrow \mathrm{End}(E)$$

and the tuple (E, ι) is an oriented elliptic curve. In [Wes21a] three variants of Problem 6.1 are given:

Problem 6.5 ($\mathcal{O}$-Endomorphism Ring)**.** Given an $\mathcal{O}$-oriented elliptic curve (E, ι), solve Problem 6.1. This is assumed to be easier due to the additional knowledge of the embedding ι.

Problem 6.6 (Endomorphism Ring$|_{\mathcal{O}}$)**.** Given an $\mathcal{O}$-oriented elliptic curve E, solve Problem 6.1. This is the same problem, with the restriction to only $\mathcal{O}$-orientable inputs.

Problem 6.7 ($\mathcal{O}$-Endomorphism Ring*)**.** Given an $\mathcal{O}$-oriented elliptic curve E, solve Problem 6.1. Additionally, recover an $\mathcal{O}$-orientation expressed in this basis.

TODO!! Write about how these problems are related to the problems in other sections!!

References

[ACC+20] Reza Azarderakhsh, Matthew Campagna, Craig Costello, Luca De Feo, Basil Hess, Aaron Hutchinson, Amir Jalali, David Jao, Koray Karabina, Brian Koziel, Brian LaMacchia, Patrick Longa, Michael Naehrig, Geovandro Pereira, Joost Renes, Vladimir Soukharev, and David Urbanik. Supersingular isogeny key encapsulation, 2020.

[CD22] Wouter Castryck and Thomas Decru. An efficient key recovery attack on SIDH (preliminary version). Cryptology ePrint Archive, Paper 2022/975, 2022. `https://eprint.iacr.org/2022/975`.

[CK20] Leonardo Colo and David Kohel. Orienting supersingular isogeny graphs. *Journal of Mathematical Cryptology*, 14(1):414–437, 2020.

[CLM+18] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: An efficient post-quantum commutative group action. Cryptology ePrint Archive, Report 2018/383, 2018.

[Cos19a] Craig Costello. B-SIDH: supersingular isogeny Diffie-Hellman using twisted torsion. Cryptology ePrint Archive, Report 2019/1145, 2019.

[Cos19b] Craig Costello. Supersingular isogeny key exchange for beginners. Cryptology ePrint Archive, Report 2019/1321, 2019.

[Cou06] Jean-Marc Couveignes. Hard homogeneous spaces. Cryptology ePrint Archive, Report 2006/291, 2006.

[CSV20] Wouter Castryck, Jana Sotakova, and Frederik Vercauteren. Breaking the decisional Diffie-Hellman problem for class group actions using genus theory. Cryptology ePrint Archive, Report 2020/151, 2020.

[DdSGKPS19] Cyprien Delpech de Saint Guilhem, Peter Kutas, Christophe Petit, and Javier Silva. SETA: supersingular encryption from torsion attacks. Cryptology ePrint Archive, Report 2019/1291, 2019.

[DF17] Luca De Feo. Mathematics of isogeny based cryptography, 2017.

[DFJP14] Luca De Feo, David Jao, and Jérôme Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *Journal of Mathematical Cryptology*, 8(3):209–247, 2014.

[Gal12] Steven D. Galbraith. *Mathematics of Public Key Cryptography*. Cambridge University Press, 1st edition, 2012.

[GPSV18] Steven Galbraith, Lorenz Panny, Benjamin Smith, and Frederik Vercauteren. Quantum equivalence of the DLP and CDHP for group actions. Cryptology ePrint Archive, Report 2018/1199, 2018.

[JDF11] David Jao and Luca De Feo. Towards Quantum-Resistant cryptosystems from supersingular elliptic curve isogenies. In Bo-Yin Yang, editor, *Post-Quantum Cryptography*, volume 7071 of *Lecture Notes in Computer Science*, pages 19–34, Berlin, Heidelberg, 2011. Springer Berlin / Heidelberg.

[KMP+20] Peter Kutas, Chloe Martindale, Lorenz Panny, Christophe Petit, and Katherine E. Stange. Weak instances of SIDH variants under improved torsion-point attacks. Cryptology ePrint Archive, Report 2020/633, 2020.

[MM22] Luciano Maino and Chloe Martindale. An attack on SIDH with arbitrary starting curve. Cryptology ePrint Archive, Paper 2022/1026, 2022. https://eprint.iacr.org/2022/1026.

[Pan21] Lorenz Panny. *Cryptography on Isogeny Graphs*. PhD thesis, Mathematics and Computer Science, February 2021. Proefschrift.

[Rob22] Damien Robert. Breaking sidh in polynomial time. Cryptology ePrint Archive, Paper 2022/1038, 2022. https://eprint.iacr.org/2022/1038.

[Sil09] Joseph H Silverman. *The Arithmetic of Elliptic Curves*. Graduate texts in mathematics. Springer, Dordrecht, 2009.

[Smi18] Benjamin Smith. Pre- and post-quantum diffie-hellman from groups, actions, and isogenies. Cryptology ePrint Archive, Report 2018/882, 2018.

[Voi21] John Voight. *Quaternion Algebras*. Springer Cham, 1st edition, 2021. Open Access: https://link.springer.com/book/10.1007/978-3-030-56694-4.

[Was08] Lawrence C. Washington. *Elliptic Curves: Number Theory and Cryptography, Second Edition*. Chapman & Hall/CRC, 2 edition, 2008.

[Wes21a] Benjamin Wesolowski. Orientations and the supersingular endomorphism ring problem. Cryptology ePrint Archive, Report 2021/1583, 2021.

[Wes21b] Benjamin Wesolowski. The supersingular isogeny path and endomorphism ring problems are equivalent. Cryptology ePrint Archive, Report 2021/919, 2021.