Collisions in Supersingular Isogeny Graphs and
the SIDH-based Identification Protocol

Wissam Ghantous\(^1\), Federico Pintore\(^2\) and Mattia Veroni\(^3\)

\(^1\) Mathematical Institute, University of Oxford, UK, wissam.ghanous@maths.ox.ac.uk
\(^2\) Department of Mathematics, University of Bari, IT, federico.pintore@uniba.it
\(^3\) NTNU - Norwegian University of Science and Technology, Trondheim, NO, mattia.veroni@ntnu.no

Abstract. The digital signatures that have been proposed so far in the setting of the Supersingular Isogeny Diffie-Hellman scheme (SIDH) were obtained by applying the Fiat-Shamir transform - and a quantum-resistant analogous, the Unruh transform - to an interactive identification protocol introduced by De Feo, Jao and Plût. The security of the resulting schemes is therefore deduced from that of the base identification protocol.

In this paper, we revisit the proofs that have appeared in the literature for the special soundness property of the above mentioned SIDH-based identification protocol. All such proofs consider the same extraction algorithm, which is claimed to always extract a valid witness for a statement when given two valid transcripts, with the same commitment and different challenges, relative to itself. We show that this is not always the case, with some explicit counterexamples. The general argument fails due to some special cycles in supersingular isogeny graphs. The existence of these special cycles not only enjoys a theoretical interest, but is generally relevant for the Isogeny-based Cryptography. We provide some theoretical results on their presence in supersingular isogeny graphs, and discuss the relevance of the obtained results for some known cryptographic applications.

Keywords: Isogeny-based Cryptography · Identification Protocol · Special Soundness · Supersingular Isogeny Graph · Digital Signature

1 Introduction

While traditional Elliptic Curve Cryptography (ECC) relies on the Elliptic Curve Discrete Logarithm Problem (ECDLP), which is easily solvable on a quantum computer using Shor’s algorithm [34], Isogeny-based Cryptography is a newer field of elliptic-curve cryptosystems which rely on different assumptions - e.g., the hardness of the CSSI problem [17] - that so far have resisted quantum cryptanalysis. As a consequence, this field represents one of the options for Post-Quantum Cryptography. Nevertheless, Isogeny-based Cryptography is less studied than
traditional ECC, and has only recently received broad attention to scrutinise hardness assumptions and existing primitives, and build new ones based on them.

The first isogeny-based cryptographic primitive was a Diffie-Hellman-like key exchange, usually named CRS, based on the action of ideal class groups on isomorphism classes of ordinary elliptic curves. This was designed independently by Couveignes [14] and Rostovtsev and Stolbunov [33]. Due to the inefficiency of the CRS scheme and the subsequent subexponential attack by Childs et al. [12], supersingular elliptic curves were suggested as a potential replacement to ordinary ones. In 2006, Charles, Lauter and Goren [11] introduced a collision resistant hash function, exploiting the supersingular isogeny graph. Subsequently, Jao et al. [17] constructed the Supersingular-isogeny Diffie-Hellman scheme, named SIDH, featuring small key sizes and whose security relies on a newly introduced isogeny problem, named SSDDH problem. In [23], Galbraith et al. showed that SIDH is vulnerable to an adaptive attack when one party uses a static key, which led to the introduction of the CCA-secure Key Encapsulation Mechanism SIKE [4]. SIKE is obtained from an encryption scheme which was proposed, together with an SIDH-based identification protocol, in [17]. Both cryptosystems are deduced from the SIDH scheme.

The only existing SIDH-based digital signatures [24, 41] were obtained by transforming the above-mentioned identification protocol into a non interactive one via the Fiat-Shamir transform [21] and a quantum-resistant analogous, the Unruh transform [36]. The UnForgeability against Chosen Message Attack (UF-CMA) of such digital signature schemes is deduced from the Honest-Verifier Zero-Knowledge (HVZK) and Special Soundness (SS) properties of the base identification protocol, and the hardness of the isogeny-based SSDDH and CSSI [17] problems. Currently, the best known classical and quantum attacks on the CSSI problem are generic claw-finding attacks, and both require exponential complexity [13, 28].

Our contribution. We revisit the proofs, provided in [17, 24, 41], for the special soundness property of the SIDH-based identification protocol. All such proofs consider the same extractor - which we denote by $\text{Ex}_{\text{SIDH}}$ - that, on input two valid transcripts with the same commitment and different challenges for a statement $x$, is claimed to output a witness $w$ for $x$.

In more details, let the cyclic secret isogeny $\varphi : E_0 \to e_1$ of prime-power degree $\ell_1^{e_1}$ be a witness $w$ for the statement $x = (e_1, \varphi(P_2), \varphi(Q_2))$, where $\{P_2, Q_2\}$ is a basis of the torsion subgroup $E_0[\ell_2^{e_2}]$, with $\ell_2$ a prime different from $\ell_1$. The isogeny $\varphi$ is uniquely identified by its kernel $\text{Ker}(\varphi)$. Then, two valid transcripts with the same pair of curves $(E_2, E_3)$ as commitment and different challenges for $x$ give knowledge of three cyclic isogenies $\phi, \psi, \phi'$ satisfying the following conditions:

- $\phi : E_0 \to E_2$ and $\phi' : e_1 \to E_3$ have degree $\ell_2^{e_2}$;
- $\psi : E_2 \to E_3$ has same degree $\ell_1^{e_1}$ of $\varphi$.

Hence, the isogeny $\hat{\phi}' \circ \psi \circ \phi$ goes from $E_0$ to $e_1$, where $\hat{\phi}'$ denotes the dual isogeny of $\phi'$. The extractor $\text{Ex}_{\text{SIDH}}$ is designed to output $\text{Ker}(\hat{\phi}' \circ \psi \circ \phi) \cap E_0[\ell_1^{e_1}]$ as a witness $w$ of $x$. 
We depict two scenarios, detailed below, where the produced $w$ is not a witness for $x$, i.e. where $\text{ExSIDH}$ fails in outputting the kernel defining $\varphi$. By providing some explicit examples, we demonstrate the concrete existence of such scenarios, even for some of the parameters sets considered for SIKE. Therefore, this invalidates the special-soundness proofs given in the literature, which incorrectly assumed the kernel of $\psi$ to be always of the form $\phi(\text{Ker}(\varphi))$.

In the first of the two exception scenarios, the cyclic isogeny $\psi$ is completely unrelated to $\varphi$, i.e. $\text{Ker}(\psi) \neq \phi(\text{Ker}(\varphi))$, despite being an $\ell_1$-degree isogeny from $E_0$ to $e_1$. In this case $\text{Ker}(\hat{\varphi}' \circ \psi \circ \phi) \cap E_0[\ell_1^{1}]$ determines an isogeny of degree $\ell_1$ going from $E_0$ to an elliptic curve $E'$ different from $e_1$. In the second scenario, the cyclic isogeny $\psi$ corresponds to an isogeny $\varphi'$ rather than to $\varphi$, i.e. $\text{Ker}(\psi) = \phi(\text{Ker}(\varphi'))$ instead of being equal to $\phi(\text{Ker}(\varphi))$. The isogeny $\varphi'$ is twinned with $\varphi$, meaning that, despite being different from $\varphi$, it goes from $E_0$ to $e_1$, has degree $\ell_1$ and there exists a point $R \in E_0$ of order $\ell_2$ such that the isogenies having kernels $\langle \varphi(R) \rangle$ and $\langle \varphi'(R) \rangle$ both go into the curve $E_3$. In this case $\text{Ker}(\hat{\varphi}' \circ \psi \circ \phi) \cap E_0[\ell_1^{1}]$ determines the isogeny $\varphi'$ instead of the isogeny $\varphi$.

We note that both scenarios exploit collisions in supersingular isogeny graphs, i.e. different cyclic isogenies with the same degree, domain and codomain. In particular, in the first scenario the isogeny $\psi$ forms a collision with the isogeny having $\phi(\text{Ker}(\varphi))$ as kernel, while in the second scenario both the isogenies $\varphi, \varphi'$ and those with kernels $\langle \varphi(R) \rangle, \langle \varphi'(R) \rangle$ form a collision. In the second case, the two collisions are tightly related, and for this reason we call them double collisions. The relevance of collisions in supersingular isogeny graphs has emerged also in other cryptographic contexts, as for example the adaptive attacks against SIDH [23] and the analysis of the claw-finding attack against the CSSI problem [13]. However, such collisions are usually overlooked, as they are deemed as unlikely to exist.

In this work, we study the collisions formed by cyclic isogenies of degree $\ell^e$ that occur in the supersingular isogeny graph $\mathcal{G}_{p^2}(\ell)$ for primes $p$ and $\ell$, whose vertices are isomorphism classes of supersingular elliptic curves over $\mathbb{F}_{p^2}$ and whose edges are isogenies of degree $\ell$. By relating the total number of such collisions to traces of Brandt matrices, we express it as a sum of modified Hurwitz class numbers. We then obtain upper bounds for the total number of collisions that we can have in $\mathcal{G}_{p^2}(\ell)$. This method, however, cannot yield any meaningful lower bounds, as it would involve getting a strong handle on the behaviour of certain incomplete character sums. In fact, bounding incomplete character sums is a very difficult problem in analytic number theory, and the best known bounds are not tight enough for our purposes. Instead, we introduce a statistical model to mimic the splitting behaviour of Legendre symbols and estimate the modified Hurwitz class numbers. We then obtain heuristic lower bounds for the number of collisions, under our statistical model.

Building on the above results, we then give estimates for the number of double collisions for fixed primes $p, \ell$ and $\ell'$. Our model suggests that the number of such double collisions is non-negligible. Moreover, our results are analysed in the context of the adaptive attacks against SIDH and the claw-finding algorithm for
the CSSI problem, as they show that certain collisions are extremely rare, a fact that is implicitly assumed in [23] and [13]. We provide a rigorous proof of this fact by computing an upper bound for the corresponding collisions.

Finally, we discuss possible alternatives, from recent results on quaternion algebras, to the extractor $\text{ExSIDH}$. Furthermore, we highlight that a modification of $\text{ExSIDH}$ which returns $\hat{\phi'} \circ \psi \circ \phi$ when $\text{Ker}(\hat{\phi'} \circ \psi \circ \phi) \cap E_0[\ell]$ is not a witness of $x$ provides the SIDH-based sigma protocol with a weaker property, called gap (or relaxed) special soundness. This property allows the extraction of a witness $w$ which is different from the proper witness being proven within the protocol but contained in a relaxed binary relation having the proper binary relation as a subset. We stress that the digital signature schemes deduced in [24, 41] by applying the Fiat Shamir and Unruh transforms are still secure under the relaxed special soundness, since the relaxed binary relation is hard.

Related Work. In an independent work [16] recently published on eprint, De Feo et al. also dispute the existing proofs for the special soundness property of the SIDH-based identification protocol. In particular, they show that two valid transcripts can be easily produced for a statement $x$ for which does not exist a corresponding witness. Consequently, not just $\text{ExSIDH}$, but every extractor would fail in extracting a witness for $x$ given such transcripts. Therefore, they propose a modified version of the SIDH-based identification protocol, for which they prove special soundness. Compared to the original protocol, the modified version is less efficient both in terms of computation and bandwidth.

We note that in the literature two slightly different notions of special soundness can be found. In the first one, the extraction algorithm is required to extract a witness given two valid transcripts for a statement $x$ in the language, i.e. there must exist a witness $w$ for $x$ [20, 31]. In the second one, the statement $x$ is not required to be in the language [3,37]. We note that the latter definition includes the former as a special case. The main reason for considering one notion instead of the other appears to be the cryptographic application for which the identification protocol which satisfies the special soundness property is considered. For some applications, the first definition is enough, and then there is no reason for considering the more general definition. For example, if the considered identification protocol is turned into a digital signature by applying the Fiat-Shamir transform, the first definition is sufficient to prove the UF-CMA security of the scheme.

Therefore, despite the counterexamples provided in [16], the original SIDH-based identification protocol appears to be still exploitable to construct Fiat-Shamir digital signatures. In fact, [16] shows that $\text{ExSIDH}$ does not provide special soundness to the protocol only when considering the second definition. Moreover, the original protocol would be the preferable choice in terms of efficiency.

It is only in this work that we show that $\text{ExSIDH}$ does not provide special soundness to the protocol even when considering the first definition, and therefore that the original protocol cannot be safely used for Fiat-Shamir digital signatures as it stands. In the light of this, we deem [16] and this paper to be two
complementary results, both helpful in assessing the security of the SIDH-based identification protocol proposed in [17].

Roadmap. The rest of the paper is organised as follows. In Section 2, we provide some preliminaries on identification schemes, isogenies, quaternion algebras and algebraic number theory. In Section 3 we show two scenarios where the extractor $\text{Ex}_{\text{SIDH}}$ fails to extract a witness for a statement $x$ (for which a witness exists) given two valid transcripts for $x$. In particular, some concrete counterexamples are provided, even for some of the SIKE parameters sets. Section 4 discusses the implications of the presented counterexamples and possible countermeasures. In Section 5, we provide a deterministic upper bound on the number of collisions in an isogeny graph. We also determine heuristic lower bounds for the same quantity. Section 6 analyses the provided results on collisions in the context of the adaptive attacks against SIDH and the claw-finding algorithm for the CSSI problem. Finally, in Section 7 we draw some conclusions.

2 Preliminaries

2.1 Identification Protocols

Let $X$ and $Y$ be two sets whose size depends on a security parameter $\lambda$. Then $\mathcal{R} \subseteq X \times Y$ is a polynomially-computable binary relation on $X \times Y$ if, for any $(x, w) \in X \times Y$, whether $(x, w)$ belongs to $\mathcal{R}$ can be checked in time $\text{poly}(|x|)$. If $(x, w) \in \mathcal{R}$, we call $w$ a witness for the statement $x$. The language corresponding to $\mathcal{R}$ is $L_\mathcal{R} = \{x \in X \mid \exists w \in Y : (x, w) \in \mathcal{R}\}$. Hereafter, we omit $\mathcal{R}$ from the subscript when the relation is clear from context.

An identification protocol $\mathcal{ID}$ for a polynomially-computable binary relation $\mathcal{R}$ is a special type of public-coin three-move interactive protocol between a prover and a verifier. Informally, a prover holding a pair $(x, w) \in \mathcal{R}$ can prove to a verifier that they possess a valid witness $w$ for $x$, without revealing any information about $w$.

Definition 1 (Identification protocols). An identification protocol $\mathcal{ID}$ for a binary relation $\mathcal{R}$ consists of three algorithms $(P = (P_1, P_2), V)$, where $V$ is deterministic and we assume that $P_1$ and $P_2$ are probabilistic polynomial-time (PPT) algorithms sharing states. We denote by $\text{ComSet}$, $\text{ChSet}$, and $\text{ResSet}$ the commitment space, challenge space, and response space, respectively. Then $\mathcal{ID}$ has the following three-move flow:

- On input $(x, w) \in \mathcal{R}$, the prover runs $\text{com} \leftarrow P_1(x, w)$ and sends the commitment $\text{com}$ to the verifier.
- The verifier chooses a random challenge $\text{ch} \leftarrow \text{ChSet}$, and sends $\text{ch}$ to the prover.
- Given $\text{ch}$, the prover runs $\text{resp} \leftarrow P_2(x, w, \text{ch})$ and returns the response $\text{resp}$ to the verifier.
- The verifier runs $V(x, \text{com}, \text{ch}, \text{resp})$ and outputs 1 if they accept, 0 otherwise.
A transcript \((x, \text{com}, \text{ch}, \text{resp}) \in X \times \text{ComSet} \times \text{ChSet} \times \text{ResSet}\) of the protocol is said to be valid (relative to \(x\)) in case \(V(x, \text{com}, \text{ch}, \text{resp})\) outputs 1.

We require the following three properties from an identification protocol \(ID\):

1. **Correctness.** All transcripts that are honestly generated must be valid. More precisely, for all \((x, w) \in \mathcal{R}\),
   
   \[
   \Pr \left[ V(x, \text{com}, \text{ch}, \text{resp}) = 1 \middle| \begin{array}{l}
   \text{com} \leftarrow P_1(x, w), \\
   \text{ch} \leftarrow \text{ChSet}, \\
   \text{resp} \leftarrow P_2(x, w, \text{ch})
   \end{array} \right] = 1.
   \]

2. **Honest-Verifier Zero-Knowledge (HVZK).** The view of an honest verifier on a protocol run can be simulated, and thus an honest verifier learns nothing on the secret witness. More formally, there exists a PPT simulator algorithm \(Sim\) that, on input a statement \(x \in \mathcal{L}_R\) and challenge \(\text{ch} \in \text{ChSet}\), outputs a commitment \(\text{com}\) and response \(\text{resp}\) such that \((x, \text{com}, \text{ch}, \text{resp})\) is a valid transcript. Moreover, the output distribution of \(Sim\) on input \((x, \text{ch})\) is computationally indistinguishable from the distribution of those outputs generated via an honest execution of \(ID\) conditioned on the verifier sampling \(\text{ch}\) as the challenge.

The third property which is required is special soundness. Two slightly different definitions of special soundness can be considered, which can be both found in the literature. The only difference between the two is in the set where the statement \(x\) lives.

3a. **Special Soundness.** There exists a polynomial-time extraction algorithm \(Ex\) such that, given any two valid transcripts \((x, \text{com}, \text{ch}, \text{resp})\) and \((x, \text{com}, \text{ch}', \text{resp}')\) relative to the same statement \(x \in \mathcal{L}_R\), with the same commitment \(\text{com}\) and two distinct challenges \(\text{ch} \neq \text{ch}'\), outputs \(w\) such that \((x, w) \in \mathcal{R}\).

3b. **Special Soundness (general).** There exists a polynomial-time extraction algorithm \(Ex\) such that, given any two valid transcripts \((x, \text{com}, \text{ch}, \text{resp})\) and \((x, \text{com}, \text{ch}', \text{resp}')\) relative to the same statement \(x\), with the same commitment \(\text{com}\) and two distinct challenges \(\text{ch} \neq \text{ch}'\), outputs \(w\) such that \((x, w) \in \mathcal{R}\).

We note that, in order for definition 3b to be verified, one can produce no more than one valid transcript relative to a statement not in the language. On the contrary, this limitation is not imposed by definition 3a. As definition 3a is contained into definition 3b, one could ask why preferring using the former over the latter. Depending on the targeted application, however, the first definition might be enough. For example, it is very common to use the Fiat-Shamir transform \([21]\) to turn an identification protocol (with an exponentially-large challenge set) \(ID\) into a digital signature. When signing a message \(m\), the prover (which is now the signer) first produces a commitment \(\text{com}\) by running \(P_1\) on a pair \((x, w) \in \mathcal{R}\), with \(w\) acting as the secret key corresponding to the verification key \(x\). Instead of waiting for a challenge from the verifier, the prover produces it by computing the image of a random function on the message \(m\) and the commitment...
com. This allows the verifier to later replicate the computation and check that the challenge has been honestly generated. Finally, the signature consists of the commitment and the response to the commitment. The HVZK property and the special soundness defined by definition 3a of ID are sufficient to prove the UF-CMA security of the resulting digital signature scheme. In fact, the general reduction [1] to prove the digital signature secure retrieves a witness for a statement \( x \) by running an adversary against the UF-CMA game as a sub-routine, and in particular by making it output two valid transcripts relative to \( x \). The reduction algorithm then executes the extractor \( \text{Ex} \) on the two valid transcripts. If it extracts correctly, then it knows that \( x \in \mathcal{L}_R \); if it does not, then it knows that \( x / \notin \mathcal{L}_R \). Therefore, in this case, it is not necessary to use the more general definition of special soundness, and one can use definition 3a instead, as the possibility of producing more than one valid transcripts for a statement not in the language does not affect the reduction algorithm.

For identification protocols for binary relations defined over post-quantum algebraic structures, it is standard to consider a relaxation of the soundness notion. To be more precise, for ID it is only required the existence of an extraction algorithm which recovers a (weaker) witness in a larger binary relation \( \mathcal{R}' \) - with \( \mathcal{R} \subset \mathcal{R}' \) - rather than in \( \mathcal{R} \). Such property, that can be given in two different flavours like the notion of special soundness, is formalised as follows.

**Relaxed Special Soundness.** There exists a polynomial-time (relaxed) extraction algorithm \( r\text{Ex} \) such that, given a statement \( x \in \mathcal{L}_R \) (alternatively, a statement \( x \in X \)) and any two valid transcripts relative to \( x \), \((x, \text{com}, \text{ch}, \text{resp})\) and \((x, \text{com}, \text{ch}', \text{resp}')\) with the same commitment \( \text{com} \) and \( \text{ch} \neq \text{ch}' \), outputs \( w \) satisfying \((x, w) \in \mathcal{R}' \), where \( \mathcal{R}' \) is a polynomially-computable binary relation on \( X \times Y \) which contains \( \mathcal{R} \).

It has been shown that, as long as \( \mathcal{R}' \) is still a sufficiently hard relation, then identification protocols satisfying relaxed special soundness are as useful as standard identification protocols (see, for example, [2, 5, 6, 20]).

### 2.2 Supersingular Elliptic Curves, Isogenies, and Hardness Assumptions

In this section we briefly recall some standard properties of isogenies between elliptic curves over finite fields. We refer the interested reader to [35] for a detailed treatment of the topic.

Let \( \mathbb{F}_q \) be a finite field, where \( q \) is a power \( p^n \) of a prime \( p > 5 \). Given two elliptic curves \( E \) and \( E' \) defined over \( \mathbb{F}_q \), an isogeny \( \varphi : E \to E' \) is a non-constant regular rational map such that \( \varphi(0_E) = 0_{E'} \). Every isogeny \( \varphi \) can be written in the form \((F_1(x)/F_2(x), yG_1(x)/G_2(x))\), where \( F_1, F_2, G_1, G_2 \in \mathbb{F}_q[x] \) (\( \mathbb{F}_q \) being the algebraic closure of \( \mathbb{F}_q \)), \( F_1 \) is coprime with \( F_2 \), and \( G_1 \) is coprime with \( G_2 \). If the coefficients of the four polynomials are contained in \( \mathbb{F}_{q^k} \), then \( \varphi \) is said to be defined over \( \mathbb{F}_{q^k} \), and \( E, E' \) are isogenous over \( \mathbb{F}_{q^k} \). Tate’s theorem states that \( E, E' \) are isogenous over \( \mathbb{F}_{q^k} \) if and only if \( \#E(\mathbb{F}_{q^k}) = \#E'(\mathbb{F}_{q^k}) \).
An isomorphism is an isogeny that is invertible. An isogeny with the same domain and range is an endomorphism. The set $\text{End}(E)$ of all endomorphisms of an elliptic curve $E$ together with the zero map form a ring under pointwise addition and composition, called endomorphism ring of $E$. $E$ is said to be ordinary if $\text{End}(E)$ is commutative, supersingular otherwise. Every supersingular elliptic curve over an extension of $\mathbb{F}_p$ is isomorphic to an elliptic curve defined over $\mathbb{F}_{p^2}$.

The degree $\deg(\phi)$ of an isogeny $\phi$ is the maximum in $\{\deg(F_1), \deg(F_2)\}$. Two elliptic curves $E$ and $E_1$ are $d$-isogenous if there exists an isogeny $\phi : E \to E_1$ of degree $d$, and in this case we say $\phi$ is a $d$-isogeny. Given a natural number $d$ and a prime power $q$, we denote by $G_q(d)$ the graph whose vertices are $\mathbb{F}_q$-isomorphism classes of supersingular elliptic curves over $\mathbb{F}_q$ and whose edges are isogenies of degree $d$.

The composition of two isogenies of degrees $d_1$ and $d_2$, respectively, is an isogeny of degree $d_1d_2$. Given an isogeny $\phi : E \to E'$, the dual $\hat{\phi} : E' \to E$ of $\phi$ is an isogeny - defined on the same field and having the same degree $d$ - such that $\phi \circ \hat{\phi} = \hat{\phi} \circ \phi = [d]$. If $(d, p) = 1$ and $\text{Ker}(\phi) = \langle T \rangle$, given another point $R \in E$ such that $\{T, R\}$ is a basis for $E[d]$, we have $\text{Ker}(\hat{\phi}) = \langle \psi(R) \rangle$.

Each isogeny $\phi$ has a finite kernel and, for a separable isogeny $\phi$, it holds that $\deg(\phi) = \text{Ker}(\phi)$. In the following we restrict our attention to separable isogenies. Vice versa, if $H$ is a finite subgroup of an elliptic curve $E$, then there are unique (modulo isomorphisms) elliptic curve $E/H$ and a separable isogeny $\psi : E \to E'$ such that $\text{Ker}(\psi) = H$. Both $E/H$ and $\psi$ can be computed with complexity $O(\#H)$ using Velu’s formulas.

Given a natural number $\ell$, we denote by $E[\ell]$ the $\ell$-torsion subgroup $\{P \in E \mid [\ell]P = 0\}$ of $E$. When $\ell$ and $p$ are relatively prime, $E[\ell] \simeq \mathbb{Z}_\ell \times \mathbb{Z}_\ell$. Cryptographic schemes deduced from the SIDH [17] paradigm consider primes $p$ of the form $p = \ell_1^{e_1} \ell_2^{e_2} f \pm 1$, where $e_1, e_2, f$ are natural numbers, $\ell_1, \ell_2$ are small primes and $\ell_1^{e_1} \approx \ell_2^{e_2}$. Under these hypotheses, every supersingular elliptic curve over $\mathbb{F}_{p^2}$ is isomorphic, over $\mathbb{F}_{p^2}$, to an elliptic curve $E$ defined over $\mathbb{F}_{p^2}$ and such that $E(\mathbb{F}_{p^2}) = (\ell_1^{e_1} \ell_2^{e_2} f)^2$. As a consequence, $E[\ell_1^{e_1}], E[\ell_2^{e_2}]$ are both contained in $E(\mathbb{F}_{p^2})$. We will denote by $\{P_A, Q_A\}$ and $\{P_B, Q_B\}$ a basis for $E[\ell_1^{e_1}]$ and $E[\ell_2^{e_2}]$, respectively.

**Hardness Assumptions.** The hard problems based on isogenies which we will consider in the subsequent sections are presented here. We first introduce the (arguably) most standard problem for isogenies.

**Problem 1** (Explicit Isogeny Problem for Fixed Degree [15]). Given a natural number $d$ and two $d$-isogenous elliptic curves $E_0$ and $E_1$ the explicit isogeny problem for fixed degree $d$ (EI$_d$) asks to find an isogeny $\phi : E_0 \to E_1$ of degree $d$.

The fastest algorithm to solve the above problem is based on the classical meet-in-the-middle strategy, and has computational complexity $O(d^2)$ [17].

The following hard problems are tailored to the SIDH paradigm. In particular, the elliptic curves taken into consideration are supersingular, defined over
\( \mathbb{F}_p^2 \) for a prime \( p \) of the form \( \ell_1^e \ell_2^f \pm 1 \), and with \( \ell_1^e \ell_2^f \) rational points. As the adversary is always required to determine an isogeny between two given elliptic curves, for simplicity we denote by \( E_0 \) the starting curve, and by \{\( P_A, Q_A \), \( P_B, Q_B \)\} two bases for \( E_0[\ell_1^e] \) and \( E_0[\ell_2^f] \), respectively.

**Problem 2** (Computational Supersingular Isogeny (CSSI) Problem, \[17\]). Let \( \phi : E_0 \to E_1 \) be an isogeny whose kernel is \( \langle [m_A]P_A + [n_A]Q_A \rangle \), where \( m_A, n_A \) are uniformly sampled from \( \mathbb{Z}/\ell_1^e \mathbb{Z} \) and are not both divisible by \( \ell_1 \). Given \( e_1 \) and the values \( \phi(P_B), \phi(Q_B) \), determine a generator of the subgroup \( \langle [m_A]P_A + [n_A]Q_A \rangle \subset E_0[\mathbb{F}_p^2] \).

The fastest algorithms to solve the above problem are still based on the meet-in-the-middle strategy, both for classical and quantum attacks. The best classical attack has computational complexity \( \tilde{O}(\ell_1^{1/2}) \), and the best quantum attack has computational complexity \( \tilde{O}(\ell_1^{1/3}) \) \[17\].

The next two problems were originally formulated in \[17\] and are believed to be as hard as the computational variants. For example, the Decisional SIDH Isogeny problem reduces to its computational variant in the trivial way, and Jao and Urbanik \[38\] show that the converse holds as well.

**Problem 3** (Decisional SIDH Isogeny Problem, \[17\]). Given two supersingular elliptic curves \( E_0, E_1 \) and a basis \{\( P'_B, Q'_B \)\} of \( E_1[\ell_1^e] \), determine whether or not there exists an isogeny \( \phi : E_0 \to E_1 \) such that \( \deg(\phi) = \ell_1^e \), and \( \phi(P_B) = P'_B \) and \( \phi(Q_B) = Q'_B \).

**Problem 4** (Decisional Supersingular Product (DSSP) Problem, \[41\]). Let \( \phi : E_0 \to E_1 \) be an isogeny of degree \( \ell_1^e \). Given \( (E_2, E_3, \psi) \) sampled with probability \( 1/2 \) from one of the following distributions, determine which distribution it is from:

- choose a random point \( R \in E_0[\ell_2^f] \) of order \( \ell_2^f \). Let \( \phi' : E_0 \to E_2 \) and \( \phi' : E_1 \to E_3 \) be the isogenies with kernels \( \langle R \rangle \) and \( \langle \phi(R) \rangle \), respectively. Then let \( \psi : E_1 \to E_2 \) be the isogeny having \( \langle \phi(S) \rangle \) as kernel, where \( \deg(\psi) = \ell_1^e \).
- choose \( E_2 \) randomly among all the supersingular elliptic curves defined over \( \mathbb{F}_p^2 \) having the same number of rational points as \( E_0 \). Then, choose a random point \( U \in E_2 \) of order \( \ell_1^e \) and compute the isogeny \( \psi : E_2 \to E_3 \) having \( \langle U \rangle \) as kernel.

In the next section we will relate the security of the identification scheme to the DSSP problem. Since the public parameters of a protocol instance consist of the tuple \( pp_{\text{SIDH}} = (\ell_1, \ell_2, e_1, e_2, f, p, E_0, P_1, P_2, Q_2) \), and the hardness of the problem depends on these parameters, we denote by \( \text{DSSP}_{pp} \) the DSSP problem on a fixed parameter set \( pp \).

### 2.3 Quaternion algebras and Brandt matrices

A quaternion algebra \( B \) is a 4-dimensional central simple algebra over a field, which is \( \mathbb{Q} \) in our case of interest. Given a basis \{1, i, j, k\} of \( B \), with \( ij = -ji = k \),
a quaternion algebra can be written as

\[ B = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k \]

with \( a, b \in \mathbb{Q}^\times \) such that \( i^2 = a, j^2 = b \). A quaternion algebra is usually denoted by the Hilbert symbol as \( H_{\mathbb{Q}}(a, b) \) or \( (a, b)_{\mathbb{Q}} \). Several examples in the literature show that \( a \) and \( b \) are not enough to uniquely determine \( B \) up to isomorphisms, so we need a new characterization.

An order \( \mathcal{O} \) in a \( \mathbb{Q} \)-algebra \( B \) is a subring of \( B \) that is also a lattice (a finitely generated \( \mathbb{Z} \)-module) that spans \( B \) over \( \mathbb{Q} \) (i.e. \( \mathcal{O} \otimes \mathbb{Z} \mathbb{Q} = B \)). Given a prime \( p \), we define \( B_p := B \otimes \mathbb{Q} \mathbb{Q}_p \) as the quaternion algebra obtained by extending the scalars of \( B \) from \( \mathbb{Q} \) to \( \mathbb{Q}_p \) (i.e. the \( p \)-adic completion of \( \mathbb{Q} \) with respect to the \( p \)-adic norm). We extend this notation to include \( \infty \) by setting \( B_\infty := B \otimes \mathbb{Q} \mathbb{R} \). It follows from Wedderburn’s theorem that \( B_p \) is either isomorphic to the matrix algebra \( M_2(\mathbb{Q}_p) \), and we say that \( B \) is unramified at \( p \), or it is a division ring, in which case we say that \( B \) is ramified at \( p \). A quaternion algebra is uniquely determined, up to isomorphisms, by the set of primes at which it ramifies: this set has even cardinality, and may include \( \infty \). Conversely, any such set may arise as the set of primes at which a quaternion algebra ramifies.

Given a quaternion \( \alpha = t + xi + yj + zk \in B \), the involution of \( \alpha \) is defined as \( \overline{\alpha} := t - xi - yj - zk \in B \). Via the involution we can define the reduced trace of \( \alpha \) as \( rd(\alpha) := \alpha + \overline{\alpha} = 2t \) and the reduced norm of \( \alpha \) as \( Nm(\alpha) := a\overline{a} = t^2 - ax^2 - by^2 + absz^2 \).

Let \( p \) be a prime and \( B \) be the quaternion algebra over \( \mathbb{Q} \) ramified at \( p \) and infinity. Fix a maximal order \( \mathcal{O} \) of \( B \). Since multiplication of quaternions is not commutative, we must be careful when defining the following objects which involve multiplication; their left or right analogues can be easily deduced. Two left ideals \( I \) and \( J \) of \( \mathcal{O} \) are equivalent if there exists \( \beta \in B^\times \) such that \( J = I\beta \). Let \( \{I_1, \ldots, I_n\} \) be a set of representatives of the equivalence classes of the left ideals of \( \mathcal{O} \), setting \( I_1 = \mathcal{O} \) by convention, and let \( cl(\mathcal{O}) \) denote the class group. The class number \( n \) is the same for every maximal order \( \mathcal{O} \) in \( B \). For every left ideal \( I_i \), let \( \mathcal{O}_R(I_i) := \{ \beta \in B : I_i \beta \subseteq I_i \} \) be the right order of \( I_i \), then each conjugacy class of a maximal order of \( B \) is represented in the set \( \{\mathcal{O}_R(I_1), \ldots, \mathcal{O}_R(I_n)\} \). The set \( \Gamma_i := \mathcal{O}_R(I_i)^\times / \mathbb{Z}^\times \) is finite, as it is a discrete subgroup of the compact group \( (B \otimes \mathbb{R})^\times / \mathbb{R}^\times \cong SO_3(\mathbb{R}) \). Let \( w_i \) be its cardinality.

We now introduce theta series and Brandt matrices, the main reference for this part being [25]. Let the inverse ideal of \( I_i \) be defined as \( I_i^{-1} := \{ \beta \in B : I_i \beta I_i \subseteq I_i \} \), and \( M_{ij} := I_i^{-1}I_j = \{ \sum a_kb_k : a_k \in I_i^{-1}, b_k \in I_j \} \). Let \( Nm(M_{ij}) \) and \( a \in Nm(M_{ij}) \) have no common factors; the definition of Brandt matrix \( B(m) := [B_{ij}(m)]_{1 \leq i, j \leq n} \) arises from the following definition of theta series \( \theta_{ij} \):

\[
\theta_{ij}(r) := \frac{1}{2w_j} \sum_{a \in M_{ij}} e^{2\pi i \frac{Nm(a)}{Nm(M_{ij})} r} = \sum_{m \geq 0} B_{ij}(m)q^m,
\]
where \( q := e^{2\pi i \tau} \). The integer \( m \) is called the degree of \( B(m) \); if \( m = 0 \), we have
\[
B(0) = \frac{1}{2} \begin{bmatrix}
\frac{1}{w_1} & \frac{1}{w_2} & \cdots & \frac{1}{w_n} \\
\frac{1}{w_1} & \frac{1}{w_2} & \cdots & \frac{1}{w_n} \\
\vdots & \vdots & \ddots & \vdots \\
\frac{1}{w_1} & \frac{1}{w_2} & \cdots & \frac{1}{w_n}
\end{bmatrix},
\]
while \( B(1) \) is the identity matrix. We hereby list some properties of Brandt matrices, which are proved in [25, Prop. 2.7]:

1. If \( m \geq 1 \), then each entry \( B_{ij}(m) \in \mathbb{N} \), and the sum of the entries in a row is independent of the chosen row, i.e. for all \( 1 \leq i \leq n \),
\[
\sum_{j=1}^{n} B_{ij}(m) = \sum_{\gcd(d,m)=1} d.
\]
2. If \( m \) and \( m' \) are coprime, then \( B(mm') = B(m)B(m') \).
3. If \( \ell \neq p \) is a prime, then \( B(\ell^k) = B(\ell^{k-1})B(\ell) - \ell B(\ell^{k-2}) \) for all \( k \geq 2 \).
4. \( w_j B_{ij}(m) = w_i B_{ji}(m) \) for all \( m \) and for all \( 1 \leq i, j \leq n \).

Recent advances in isogeny-based cryptography have put quaternion algebras under the spotlight, due to their intimate connection with supersingular elliptic curves via a correspondence of categories. The original result by Deuring [19] has been enriched by several later works, the last of which being [18]. In particular,

– a supersingular \( j \)-invariant over \( \mathbb{F}_{p^2} \) corresponds to a maximal orders in the quaternion algebra \( B_{p,\infty} \), and the set of supersingular \( j \)-invariants corresponds to the class group \( \text{cl}(\mathcal{O}) \);
– endomorphisms correspond to principal ideals;
– isogenies of degree \( \ell \) correspond to left ideals of norm \( \ell \) of maximal orders;
– composition of isogenies corresponds to multiplication of ideals

Given the further connection between quaternion algebras and Brandt matrices, we can exploit the latter to study elliptic curves. First and foremost, let us now introduce Hurwitz Class Numbers. Given an order \( \mathcal{O} \) of rank 2 over \( \mathbb{Z} \) of negative discriminant \( d \), let \( h(d) \) be the size of the class group \( \text{cl}(\mathcal{O}) \) and define \( u(d) := \mathcal{O}^\times / \mathbb{Z}^\times = \mathcal{O}^\times / 2 \). For \( D > 0 \), the Hurwitz Class Numbers \( H(D) \) is
\[
H(D) = \sum_{d \mid D} \frac{h(d)}{u(d)}.
\]

Let \( \mathcal{O}_{-D} \) be the order of discriminant \(-D\); we define the modified Hurwitz Class Number \( H_p(D) \) as
\[
H_p(D) := \begin{cases} 
0 & \text{if } p \text{ splits in } \mathcal{O}_{-D}; \\
H(D) & \text{if } p \text{ is inert in } \mathcal{O}_{-D} \\
\frac{1}{2} H(D) & \text{if } p \text{ ramifies in } \mathcal{O}_{-D} \\
& \text{and does not divide the conductor of } \mathcal{O}_{-D}; \\
H(\frac{D}{p^2}) & \text{if } p \text{ divides the conductor of } \mathcal{O}_{-D}; \\
\end{cases}
\]
For \( D = 0 \), we set \( H(0) = -\frac{1}{12} \) and \( H_p(0) := \frac{p-1}{24} \).

**Theorem 1.** [25, Prop. 1.9] For all \( m \geq 0 \),

\[
\text{Tr}(B(m)) = \sum_{s \in \mathbb{Z}} H_p(4m - s^2).
\]

**Theorem 2.** [26, Sec. 7] For \( m \in \mathbb{Z} \),

\[
\sum_{s \in \mathbb{Z}} H(4m - s^2) = 2 \sum_{d|m} d - \sum_{d|m} \min\{d, m/d\}.
\]

3 The SIDH-based Identification Protocol and Its Special Soundness

In their seminal work [17], Jao, De Feo, and Plût proposed an identification scheme in the SIDH setting, which we will refer to as the SIDH-based identification protocol \( \text{ID}_{\text{SIDH}} \). In this protocol, a prover persuades a verifier that, for a given pair \((E_0, E_1)\) of supersingular elliptic curves, it knows a cyclic isogeny \( \varphi : E_0 \rightarrow E_1 \) - having degree \( \ell_1^\ell_1 \), where \( \ell_1 \) is a prime - without revealing any information about the isogeny itself.

Later on, Yoo et al. [41] and Galbraith et al. [24] turned \( \text{ID}_{\text{SIDH}} \) into the first SIDH-based digital signature schemes by applying the Fiat-Shamir transform [21] and the Unruh transform [36]. The Unruh transform provides security in the quantum random oracle, while the Fiat-Shamir transform generally guarantees security only in the random oracle model. The UF-CMA security of the resulting digital signatures is deduced from both the HVZK and special soundness properties of \( \text{ID}_{\text{SIDH}} \). Proofs for the special soundness property of the protocol are given in [17, 24, 41], and all of them consider the same extractor, which we will denote by \( \text{Ex}_{\text{SIDH}} \) in the following.

In this section, we detail two scenarios where the proposed extraction algorithm \( \text{Ex}_{\text{SIDH}} \) fails to extract any meaningful witness for a statement \( x \in L_R \) when given two valid transcripts relative to \( x \). The consequence of such failure is that, when \( \text{ID}_{\text{SIDH}} \) is turned into a signature scheme via either the Fiat-Shamir or Unruh transform, unforgeability can no longer be argued. In the next sections, we will show some concrete examples of the two scenarios mentioned above, even for some of the SIKE parameters sets.

### 3.1 ID\(_{\text{SIDH}}\) and Ex\(_{\text{SIDH}}\)

The public parameters of \( \text{ID}_{\text{SIDH}} \) consists of a tuple \( \text{pp}_{\text{SIDH}} = (\ell_1, \ell_2, e_1, e_2, f, p, E_0, P_1, Q_1, P_2, Q_2) \) where:

- \( \ell_1 \) and \( \ell_2 \) are two distinct small primes;
- \( e_1, e_2 \) and \( f \) are natural numbers, and \( \ell_1^{\ell_1} \approx \ell_2^{\ell_2} \).
\(- p \) is a prime of the form \( \ell_1^e \ell_2^e f \pm 1 \);
\(- E_0 \) is a starting supersingular elliptic curve defined over the finite field \( \mathbb{F}_{p^2} \);
\(- \{ P_1, Q_1 \} \) and \( \{ P_2, Q_2 \} \) are two bases for \( E_0[\ell_1^e] \) and \( E_0[\ell_2^e] \), respectively.

\( \text{ID}_{\text{SIDH}} \) is an identification protocol for a binary relation \( \mathcal{R} \) contained in \( X \times Y \), where:

\[
X = \{(E_1, P', Q') | E_1 \text{ sup. elliptic curve over } \mathbb{F}_{p^2} \wedge E_1[\ell_2^e] = \langle P', Q' \rangle \} \quad (3)
\]

\[
Y = \{ \varphi \mid \varphi \text{ is a cyclic isogeny from } E_0 \text{ s.t. } \deg(\varphi) \in \{ \ell_1^e, \ell_2^e \ell_1^e \} \}. \quad (4)
\]

The binary relation \( \mathcal{R} \) is induced by the CSSI problem, and therefore it is defined as follows:

\[
\mathcal{R} = \{(E_1, P', Q'), \varphi \mid \varphi : E_0 \to E_1 \wedge \deg(\varphi) = \ell_1^e \wedge \varphi(P_2) = P', \varphi(Q_2) = Q' \}. \quad (5)
\]

Here we note that each statement \( x \in \mathcal{L}_{\mathcal{R}} \) admits a unique witness \( w \) (see \[38\]).

\( \text{ID}_{\text{SIDH}} \) is a binary-challenge identification protocol, i.e. \( \text{ChSet} = \{0, 1\} \), which consists of three algorithms \((P_1, P_2, V)\) defined as:

\(- \text{com} \leftarrow P_1((E_1, P', Q'), \varphi) : \text{on input } (E_1, P', Q', \varphi) \in \mathcal{R}, \text{ it generates two random integers } m_2, n_2 \in \mathbb{Z}_{\ell_2^e}, \text{ not both divisible by } \ell_2, \text{ and computes the point } R = [m_2]P_2 + [n_B]Q_2 \text{ - of order } \ell_2^e - \text{ and the elliptic curves } E_2 = E_0/\langle R \rangle \text{ and } E_3 = E_1/\langle [m_2]P' + [n_2]Q' \rangle. \text{ Then it outputs the commitment } \text{com} = (E_2, E_3).
\]

\(- \text{resp} \leftarrow P_2((E_1, P', Q'), \varphi, \text{ch}) : \text{if the challenge } \text{ch} \text{ is equal to } 0, \text{ the algorithm sets } \text{resp} \text{ to the pair } (m_B, n_B). \text{ Otherwise, given the point } S \text{ - of order } \ell_1^e - \text{ generating } \text{Ker}(\varphi) \text{ and by the isogeny } \phi : E_0 \to E_2 \text{ with } R = [m_2]P_2 + [n_B]Q_2 \text{ as kernel, it sets } \text{resp} \text{ to } \phi(S). \text{ It then returns the response } \text{resp}.
\]

\(- \{0, 1\} \ni b \leftarrow V((E_1, P', Q'), \text{com}, \text{ch}, \text{resp}) : \text{the deterministic verification algorithm checks whether}
\]

\[
\bullet (\text{ch} = 0) \text{ given } \text{resp} = (m_2, n_2), \text{ m}_2 \text{ and } n_2 \text{ are not both divisible by } \ell_2, \text{ E}_0/\langle [m_2]P_2 + [n_2]Q_2 \rangle \text{ is isomorphic to } E_2, \text{ and } E_1/\langle [m_2]P' + [n_2]Q' \rangle \text{ is isomorphic to } E_3;
\]

\[
\bullet (\text{ch} = 1) \text{ given } \text{resp} = T, T \in E_2 \text{ has order } \ell_1^e \text{ and } E_2/\langle T \rangle \text{ is isomorphic to } E_3.
\]

If the conditions are fulfilled, \( V \) outputs 1 (accept), otherwise outputs 0 (reject).

It is easy to show that \( \text{ID}_{\text{SIDH}} \) is correct. We here show that it satisfies the Honest-Verifier Zero-Knowledge property by constructing a zero-knowledge simulator \( \text{Sim} \) as follows. On input \((E_1, P', Q') \in \mathcal{L}_{\mathcal{R}}\) and \( \text{ch} = 0 \), \( \text{Sim} \) chooses two random integers \( m_2, n_2 \) in \( \mathbb{Z}_{\ell_2^e} \), not both divisible by \( \ell_2 \), computes the point \( R = [m_2]P_2 + [n_2]Q_2 \) of order \( \ell_2^e \), and outputs

\[
(\text{com} = (E_0/\langle R \rangle, E_1/\langle [m_2]P_2 + [n_2]Q_2 \rangle), \text{ch} = 0, \text{resp} = (m_2, n_2)).
\]

This simulated transcript is distributed exactly as a real one conditioned on \( \text{ch} = 0 \). In order to simulate a transcript on input \((E_1, P', Q') \in \mathcal{L}_{\mathcal{R}}\) and \( \text{ch} = 1 \),
Sim chooses a random supersingular elliptic curve $E_2$, defined over $\mathbb{F}_{p^2}$ and with the same number of rational points as $E_0$. Then it chooses a random cyclic subgroup $\langle T \rangle \subset E_2[\ell_1^1]$ having order $\ell_1^1$, and outputs

\[(\text{com} = (E_2, E_3 = E_2/ \langle T \rangle), \text{ch} = 1, \text{resp} = T).\]

This is computationally indistinguishable from a valid transcript conditioned on $\text{ch} = 1$, under the assumption that the DSSP$_{pp}$ problem (Problem 4) is hard.

In [17, 24, 41], the special soundness property of ID$_{\text{SIDH}}$ is proven by considering the same extractor $\text{Ex}_{\text{SIDH}}$, defined as follows. Given two valid transcripts $(x, \text{com}, 0, (m_2, n_2))$ and $(x, \text{com}, 1, T)$ - relative to the statement $x = (E_1, P', Q')$, and with the same commitment $\text{com} = (E_1, E_2)$ and different challenges - it outputs $\hat{\phi}(T)$, where $\phi$ is the isogeny from $E_0$ with $\langle [m_2]P_2 + [n_2]Q_2 \rangle$ as kernel. We note that, under the assumption that $(T)$ is equal to $\phi(\text{Ker}(\phi))$ - where $\phi$ is the only witness for $x$ - $\text{Ex}_{\text{SIDH}}$ extracts exactly $\text{Ker}(\phi)$ (and so, equivalently, $\phi$). Despite this assumption being made in [17, 24, 41], it does not appear necessary to make it in general. In the following section we detail two different scenarios where such assumption is not valid.

### 3.2 Scenario 1 - Single Collision

Let $x = (E_1, P', Q')$ be a statement in $L_R$. Suppose there exists a point $R = [m_2]P_2 + [n_2]Q_2 \in E_0$, of order $\ell_2^1$, which defines two isogenies, $\phi : E_0 \to E_2 = E_0/ \langle R \rangle$ and $\phi' : E_1 \to E_3 = E_1/ \langle [m_2]P' + [n_2]Q' \rangle$, such that $E_2$ admits two distinct cyclic subgroups $G$ and $G'$ of order $\ell_1^1$ that generate two isogenies $\psi, \psi'$ going from $E_2$ to $E_3$. The pair $(\psi, \psi')$ forms a collision (of length $e_1$) in the isogeny graph $G_{p^2}(E_1)$. We call single collision (of length $e_1$) a collision of this form. Here we assume $G = \phi'(\text{Ker}(\phi))$ - where $\phi$ is the only witness for $x$ - and we denote by $T$ a generator for $G$.

Given the commitment $\text{com} = (E_2, E_3)$, both $(x, \text{com}, \text{ch} = 0, (m_2, n_2))$ and $(x, \text{com}, \text{ch} = 1, T)$ are valid transcripts relative to $x$. If no extra hypotheses are made, on input such two transcripts, $\text{Ex}_{\text{SIDH}}$ extracts a cyclic subgroup of $E_0$, having order $\ell_1^1$, which defines an isogeny whose codomain $E'$ is not $\mathbb{F}_{p^2}$-isomorphic to $E_1$. Therefore, $\text{Ex}_{\text{SIDH}}$ fails in extracting a witness for $x$. In order to better explain the above scenario and to show that it can actually happen in practice, we provide a concrete occurrence of such scenario.

**Example 1.** Consider the prime $p = (2^8)(3^5) - 1$ and the irreducible polynomial $f = x^2 + 62205x + 5 \in \mathbb{F}_p[x]$. Given $\mathbb{F}_{p^2} = \mathbb{F}_p[x]/(f)$, we denote by $z$ a root of $f$, which forms a basis for $\mathbb{F}_{p^2}$ together with the identity 1. Consider as $E_0$ a supersingular elliptic curve with $j$-invariant equal to 22470. The two points $P_2 = (7077z + 32228, 17988z + 60777), Q_2 = (51235z + 37453, 42878z + 1379)$ form a basis for $E_0[5^3]$. Let $E_1$ be the image curve of the $2^8$-isogeny $\varphi$ having $\langle 33446z + 46615, 52617z + 4750 \rangle$ as kernel, for which it holds $j(E_1) = 37167z + 53117$. We consider the tuple $(E_1, P' = (6505z + 32827, 20825z + 21686), Q' = (59525z + 48254, 52332z + 7163)$ as statement $x$. Then, for the curves $E_2 =$
There exist two distinct cyclic isogenies $\psi, \psi'$: $E_2 \rightarrow E_3$ of degree $2^8$. $\psi$ is the one with kernel equal to $\phi(\text{Ker}(\varphi))$, where $\varphi$ is the isogeny with kernel $\langle [161]P_2 + [183]Q_2 \rangle$. On the other hand, $\psi'$ has kernel generated by $T = (52195z + 35063, 51186z + 33135)$, with $T \notin \varphi(\text{Ker}(\varphi))$. As a consequence, $\hat{\phi}(\langle T \rangle)$ defines an isogeny whose image has $j$-invariant equal to $55144z + 45927$, which is different from that of $E_1$.

An exhaustive approach has been used to produce concrete examples for Scenario 1. In particular, the simple procedure we executed goes as follows:

1. produce a prime $p$ of the form $\ell_1^{e_1}\ell_2^{e_2} \pm 1$, so that $\ell_1^{e_1} \approx \ell_2^{e_2}$;
2. for each vertex $j_0$ in the isogeny graph $G_{p^2}(\ell_2)$, compute all the paths composed by $e_2$ steps (with no backtracking) and the corresponding arriving vertices;
3. for each arriving vertex $j_2$, compare all paths in the isogeny graph $G_{p^2}(\ell_1)$ which originate from $j_2$ and composed of $e_1$ steps (with no backtracking);
4. an occurrence of Scenario 1 is found whenever two paths end at the same $j$-invariant $j_3$, and they are distinct in at least one step.

### 3.3 Scenario 2 - Double Collisions

Let $x = (E_1, P', Q')$ be a statement in $\mathcal{L}_R$. Suppose $\mathcal{L}_R$ contains another statement $\bar{x}$, with $\bar{x} \neq x$, with the same first component (modulo $\mathbb{F}_{p^2}$-isomorphisms).

In other words, there exist two distinct cyclic subgroups of order $\ell_1^{e_1}$ in $E_0$, $H$ and $\bar{H}$, such that $j(E_0/H) = j(E_0/\bar{H})$. We denote by $\varphi$ and $\bar{\varphi}$ the isogenies having kernels $H$ and $\bar{H}$, respectively. We further assume there exists a point $R = [n_2]P_2 + [n_2]Q_2 \in E_0$, of order $\ell_2^{e_2}$, such that $E_1/\langle \varphi(R) \rangle$ has the same $j$-invariant of $E_1/\langle \bar{\varphi}(R) \rangle$. We denote by $\phi'$ and $\bar{\phi}'$ the isogenies having $\langle \varphi(R) \rangle$ and $\langle \bar{\varphi}(R) \rangle$ as kernels, respectively. The pairs ($\varphi, \bar{\varphi}$) and ($\phi', \bar{\phi}'$) are two collisions (of length $e_1$ and $e_2$, respectively) in the isogeny graphs $G_{p^2}(\ell_1)$ and $G_{p^2}(\ell_2)$, respectively. Since the second collision originates from the same point $R \in E_0$,
the two collisions have a tight link. For this reason we call double collision (of length $e_1 + e_2$) a pair of collisions of this form.

Given the commitment $\mathsf{com} = (E_2 = E_0/\langle R \rangle, E_3 = E_1/\langle \varphi(R) \rangle)$, the two transcripts $(x, \mathsf{com}, \mathsf{ch} = 0, (n_2, n_2))$ and $(x, \mathsf{com}, \mathsf{ch} = 1, \phi(S))$ - where $\bar{S}$ generates $\bar{H}$ - are both valid transcripts relative to $x$. However, on input such transcripts, $\mathsf{ExSIDH}$ extracts a witness $\bar{w}$ for $\bar{x}$, rather than a witness for $x$.

Also for this scenario we provide a concrete counterexample.

Example 2. Let $p = (2^8)(5^3) + 1$, and $f = x^2 + 7 \in \mathbb{F}_p[x]$ be an irreducible polynomial. We denote the primitive element $\sqrt{-7}$ by $z$. Then we consider as $E_0$ a supersingular elliptic curve over $\mathbb{F}_{p^2}$ such that $j(E_0) = 80630z + 38195$. The two distinct cyclic subgroups of order $2^8$ of $E_0$

$$H = \langle (174423z + 15317, 139167z + 27752) \rangle$$

$$\bar{H} = \langle (279804z + 121600, 104494z + 307794) \rangle,$$

are such that $j(E_0/H) = j(E_0/\bar{H}) = 255209z + 212204$. We denote by $\varphi$ and $\tilde{\varphi}$ the isogenies with kernels $H$ and $\bar{H}$, respectively. Let $E_1$ and $\bar{E}_1$ the images of these two isogenies. The point $R = (290744z + 184866, 22597z + 44859) \in E_0$ - having order $3^5$ - is such that $E_1/\langle \varphi(R) \rangle$ and $\bar{E}_1/\langle \tilde{\varphi}(R) \rangle$ have the same $j$-invariant.

Producing examples where this Scenario 2 occurs is much more difficult than it is for Scenario 1. The procedure we followed relies on two main parts. The first one consists in an exhaustive search for collisions of $\ell_1^{e_1}$-isogenies (i.e. single collisions of length $e_1$), and proceeds as follows:

1. produce a prime $p$ of the form $\ell_1^{e_1} \ell_2^{e_2} \pm 1$, so that $\ell_1^{e_1} \approx \ell_2^{e_2}$;
2. for each vertex $j_0$ in the isogeny graph $\mathcal{G}_{p^2}(\ell_1)$, compare all paths composed of $e_1$ steps (with no backtracking) and originating from the fixed vertex;
3. a single collision is found whenever two paths end at the same $j$-invariant (which we refer to as colliding $j$-invariant), and they are distinct in at least one step.

After a colliding $j$-invariant $j_1$ is found for a starting vertex $j_0$, the second part of the procedure takes the two colliding paths (which correspond to the isogenies $\varphi$ and $\tilde{\varphi}$, respectively) and continues by

- constructing a supersingular elliptic curve $E_0$, defined over $\mathbb{F}_{p^2}$ having $j_0$ as $j$-invariant;
- comparing all pair of paths of $e_2$ steps in $\mathcal{G}_{p^2}(\ell_2)$ determined by the points $\varphi(R)$ and $\tilde{\varphi}(R)$, for any $R \in E_0[\ell_2^{e_2}]$ of order $\ell_2^{e_2}$.
- a collision is found whenever the arriving $j$-invariant is the same for both paths in a pair. In this case, the two paths are said to be colliding, like the arriving $j$-invariant.

When the two colliding paths are equal in each step, we call the whole double collision a Florence flask; when the two paths differ in at least one step, we call the double collision a lemniscate.
We ran some experiments for primes of small size, always setting $\ell_1 = 2$ and $\ell_2 = 3$. The results are summarized in Section 3.3 where we list the number of vertices of $G_p^2(2)$ from which at least a single collision originates, the total number of single collisions in the graph, and the total number of double collisions (distinguishing between lemniscates and Florence Flasks). The exhaustive search conducted in both parts of the procedure becomes very expensive already with 12-bit primes and thus, from $p = 2591$ on, we restricted our analysis to some random vertices. The results show that, except for $p = 1297$, each prime we considered exhibits at least one single collision for each supersingular $j$-invariant taken as initial vertex.

<table>
<thead>
<tr>
<th>$p$</th>
<th>$e_A$</th>
<th>$e_B$</th>
<th>$+1$/$-1$</th>
<th>Initial $j$-invariants with collisions</th>
<th>Single collisions</th>
<th>Lemniscates</th>
<th>Florence flasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>431</td>
<td>4</td>
<td>3</td>
<td>-1</td>
<td>37/37</td>
<td>183</td>
<td>134</td>
<td>286</td>
</tr>
<tr>
<td>433</td>
<td>4</td>
<td>3</td>
<td>+1</td>
<td>36/36</td>
<td>213</td>
<td>229</td>
<td>152</td>
</tr>
<tr>
<td>863</td>
<td>5</td>
<td>3</td>
<td>-1</td>
<td>73/73</td>
<td>681</td>
<td>246</td>
<td>316</td>
</tr>
<tr>
<td>1297</td>
<td>4</td>
<td>4</td>
<td>+1</td>
<td>97/108</td>
<td>194</td>
<td>127</td>
<td>231</td>
</tr>
<tr>
<td>2591</td>
<td>5</td>
<td>4</td>
<td>-1</td>
<td>25/25</td>
<td>121</td>
<td>44</td>
<td>44</td>
</tr>
<tr>
<td>2593</td>
<td>5</td>
<td>4</td>
<td>+1</td>
<td>25/25</td>
<td>112</td>
<td>77</td>
<td>85</td>
</tr>
<tr>
<td>15551</td>
<td>6</td>
<td>5</td>
<td>-1</td>
<td>25/25</td>
<td>76</td>
<td>16</td>
<td>84</td>
</tr>
<tr>
<td>62207</td>
<td>8</td>
<td>3</td>
<td>-1</td>
<td>20/20</td>
<td>280</td>
<td>14</td>
<td>405</td>
</tr>
</tbody>
</table>

Table 1: A summary of the number of single and double collisions when considering small primes $p$.

3.4 Scenario 1 and SIKE parameters sets

At a first glance, one might argue that the concrete examples provided in the previous subsections exist only because of the small size of the considered graphs. In order to argue that we cannot exclude the presence of similar examples also
in supersingular isogeny graphs of cryptographic size, we focus on Scenario 1 for the largest SIKE parameters set, called SIKEp751. This name refers to the fact that the underlying prime, denoted by \( p_{751} \), has size (in bits) equal to 751.

As we detail in the Appendix, the supersingular isogeny graph \( G(p_{751})^2(3) \) admits two single collisions, of length 239, whose starting vertex is the (class of the) supersingular elliptic curve chosen as starting curve for SIKEp751. As the defining equation of this curve is \( y^2 = x^3 + 6x^2 + x \), such curve is usually denoted by \( E_6 \).

![Fig. 3: An example for Scenario 1 from a single collision originating from \( E_6 \) (the dual isogeny of \( \varphi \) is \( \phi \)).](image)

An example of Scenario 1 can then be constructed as follows. A cyclic subgroup \( K \subset E_6 \) of order \( 2^{372} \) is randomly sampled, and the image curve of the isogeny \( \varphi \) having \( K \) as kernel is denoted by \( E_0 \). Then, the obtained curve \( E_0 \) is set as the starting curve of \( \text{ID}_{\text{SIDH}} \). Let \( \varphi : E_0 \rightarrow E_1 \) be the isogeny with kernel \( \varphi(H) \). By fixing some bases \( \{P_1, Q_1\} \) and \( \{P_2, Q_2\} \) for \( E_0 \) and \( E_1 \) respectively, \( E_1 \) and \( \varphi \) can be turned into a statement-witness pair for \( \text{ID}_{\text{SIDH}} \) with public parameters

\[
\text{PP}_{\text{SIDH}} = (\ell_1 = 3, \ell_2 = 2, e_1 = 239, e_2 = 372, f = 1, p_{751}, E_0, P_1, Q_1, P_2, Q_2). 
\]

In particular, the statement \( x \) is set to \( (E_1, \varphi(P_2), \varphi(Q_2)) \), while its corresponding witness \( w \) is set to \( \varphi \). Let \( R \) be a generator of the kernel of the dual isogeny of \( \varphi \), with \( m_2, n_2 \in \mathbb{Z}/2^{372}\mathbb{Z} \) such that \( R = [m_2]P_2 + [n_2]Q_2 \), and \( T \) a generator for \( \varphi(H) \). We underline that \( T \) is the generator of the kernel of \( \psi' \). By setting \( \text{com} = (E_6, E_3) \), the two transcripts \( (x, \text{com}, \text{ch} = 0, (m_2, n_2)) \) and \( (x, \text{com}, \text{ch} = 1, T) \) are both valid relative to \( x \), and are an example of Scenario 1.

**Remark 1.** The constructed example could be deemed as not an example of Scenario 1 for SIKEp751, as the initial curve \( E_0 \) is not the prescribed one. However,
if we took the same parameter set and we let the initial curve vary, this example would be perfectly acceptable. Moreover, we note that constructing an example of Scenario 1 needs a single collision of length 239 in the graph $G_{(p_{751})^2}(3)$ (or of the length 372 in the graph $G_{(p_{751})^2}(3)$). It appears that the only way to compute such a collision is to exploit the knowledge of the endomorphism ring of the starting vertex (as done in the Appendix by extending the procedure, based on quaternion algebras, presented in [32]). As a consequence, it seems prohibitive to obtain a single collision starting from a random vertex $E_1$. We believe that considering a starting curve for $\text{ID}_{\text{SIDH}}$ other than $E_6$ does not diminish the relevance of the constructed example.

4 Security implications of the two exception scenarios

In [16], De Feo et al. analyse the SIDH-based identification protocol $\text{ID}_{\text{SIDH}}$ and the extractor $\text{Ex}_{\text{SIDH}}$. They show that two valid transcripts relative to a statement $x \notin L_R$ can be easily produced. When considering Definition 3b for the special soundness property, this means that $\text{ID}_{\text{SIDH}}$ cannot be proven to enjoy such property. Therefore, they propose a modified version of $\text{ID}_{\text{SIDH}}$, which they prove to achieve special soundness. In such modification, $P_1$ appends to a commitment $(E_2, E_3)$ also the images through $\psi : E_2 \to E_3$ of a basis for $E_2[\ell_{e_2}]$. Such points are then involved in the verification phase for both possible challenges. Therefore, the proposed modification is less efficient in terms of computation and bandwidth with respect to the original identification scheme $\text{ID}_{\text{SIDH}}$.

The counterexamples provided in [16] do not affect the special soundness property of $\text{ID}_{\text{SIDH}}$ when considering Definition 3a. As discussed in Section 2.1, such definition can be safely considered when exploiting an identification protocol for a Fiat-Shamir digital signature scheme. As a consequence, according to the special soundness proofs provided in [17,24,41], $\text{ID}_{\text{SIDH}}$ could still be taken as a building block to construct Fiat-Shamir SIDH-based digital signature schemes. Moreover, not only could one use $\text{ID}_{\text{SIDH}}$, but this would be the preferable choice in terms of efficiency, given the lower efficiency of the modified scheme presented in [16].

However, the two exception scenarios and concrete examples described in the previous section show, for the first time, that $\text{Ex}_{\text{SIDH}}$ does not provide special soundness to $\text{ID}_{\text{SIDH}}$, even when considering Definition 3a. Therefore, the original protocol cannot be used for secure Fiat-Shamir digital signatures as it stands. In the following subsections we analyse two possible remedies to this state of affairs.

4.1 Relaxed Special Soundness

Given the sets $X$ and $Y$ introduced in Section 3.1, a binary relation $\tilde{R}$ alternative to $R$ can be considered. Such relation is induced by Problem 1 and therefore it is defined as follows:

$$\tilde{R} = \{(E_1, P', Q') \mid \varphi : E_0 \to E_1\}.$$
It is clear that $\mathcal{R}$ is contained in $\tilde{\mathcal{R}}$. Furthermore, it can be shown that $\text{ID}_{\text{SIDH}}$ enjoys relaxed special soundness with respect to $\mathcal{R} \subset \tilde{\mathcal{R}}$.

Let $(x, \text{com}, \text{ch}, \text{resp})$, $(x, \text{com}, \text{ch}', \text{resp}')$ be two valid transcripts, relative to $x \in \mathcal{L}_\mathcal{R}$, having the same commitment and different challenges. If $x = (E_1, P', Q')$ and $\text{com} = (E_2, E_3)$, the verification phase for the two challenges guarantees the knowledge of two isogenies $\phi : E_0 \to E_2$, $\phi' : E_1 \to E_3$, and of an isogeny $\psi : E_2 \to E_3$, respectively. Therefore, $\phi' \circ \psi \circ \phi$ is an isogeny from $E_0$ to $E_1$. An extractor $r\text{Ex}_{\text{SIDH}}$ outputting $\hat{\phi}(\text{Ker}(\psi))$ or $\text{Ker}(\phi' \circ \psi \circ \phi)$ if $\hat{\phi}(\text{Ker}(\psi))$ does not define an isogeny from $E_0$ to $E_1$ makes $\text{ID}_{\text{SIDH}}$ satisfy the relaxed special soundness property.

As we already observed, all the proofs for the Fiat-Shamir and Unruh transform, which were formally given for identification protocols satisfying special soundness, naturally extend to identification protocols that enjoy relaxed special soundness. Namely, the reduction algorithms used in the security proofs of the signature schemes based on the two kinds of identification protocols are equivalent but in the extraction of the witness. The only difference between the two cases is what we can argue about the witness extracted from two valid transcripts; in the former case, a witness for the original relation $\mathcal{R}$ is extracted, while in the latter a witness for the relaxed relation $\tilde{\mathcal{R}}$ is extracted. As long as the original relation and the relaxed relation are equally hard, which is the case for our isogeny relations (see Section 2.2), then all the proofs hold.

### 4.2 Alternative extractors

The two scenarios described in Section 3, which make the extractor $\text{Ex}_{\text{SIDH}}$ fail, invalidate the proofs for the special soundness property (Definition 3.a) of $\text{ID}_{\text{SIDH}}$ based on its extractor. However, the possibility to construct an alternative special-soundness extractor for $\text{ID}_{\text{SIDH}}$ is not ruled out by the two scenarios.

Such an alternative extractor could be designed by taking into consideration the reduction proposed by Galbraith et al. in [23, Sec 4.1]. This reduction runs in polynomial time, and given an isogeny between two supersingular elliptic curves $E_0$ and $E_1$, it returns a shorter isogeny between them under the hypothesis that the endomorphism ring of $E_0$ is known. This tool could be used to retrieve an isogeny of degree $\ell^4$ from the isogeny $\phi' \circ \psi \circ \phi$ to $E_0$. However, the reduction is probabilistic, and thus it leaves open the question whether there exist examples on which the reduction fails.

In a recent work [22], Fouotsa, Kutas and Merz presented a generalisation of the above reduction. In particular, their algorithm allows to compute a secret isogeny $\varphi$ of degree $N_1$ between two supersingular elliptic curves $E_0, E_1$ given the endomorphism rings $\text{End}(E_0)$, $\text{End}(E_1)$ and the action of $\varphi$ on a basis $\{P_1, Q_1\}$ of the torsion subgroup $E_0[N_1]$. The main idea of the new reduction is the following. Since isogenies from $E_0$ to $E_1$ form a $\mathbb{Z}$-module $M$ of rank 4, the KLPT algorithm [29] can be used to compute a basis of $M$. One can then turn it in a LLL-reduced basis [30] $\{\psi_1, \psi_2, \psi_3, \psi_4\}$ and evaluate the images of $\{P_1, Q_1\}$ via these maps. Computing $\varphi$ is then reduced to solving a system of linear equations to retrieve the coefficients $x_1, \ldots, x_4$ for which $\varphi = x_1\psi_1 + x_2\psi_2 + x_3\psi_3 + x_4\psi_4$.
As argued in [22], this solution is unique when \( x_i < \frac{N_2}{2} \) and \( N_1 < \frac{4N_2}{16} \), where \( d \) is the degree of the shortest isogeny between \( E_0 \) and \( E_1 \). Note that, for balanced SIDH parameters of cryptographic interest, the ratio \( N_1/N_2 \) is approximately 1, and thus this procedure works whenever the degree of the shortest isogeny between the two curves is greater than 16. Also in this case, however, the question whether there exist examples on which the algorithm fails remains open. We defer to future work a further investigation of the two above reductions, aiming at constructing an alternative special-soundness extractor for \( \text{ID}_{\text{SIDH}} \).

5 Quantitative study of cycles in Isogeny Graphs

As detailed in Section 3.2 and Section 3.3, there are scenarios in which the existence of collisions in supersingular isogeny graphs poses a problem to the extractor \( \text{Ex}_{\text{SIDH}} \) previously considered to prove the special soundness property of the SIDH-based identification protocol \( \text{ID}_{\text{SIDH}} \). We therefore are interested in quantifying these collisions and providing bounds for them.

In the rest of the section, \( p \) will be be a large prime, \( \ell \) a small one (usually 2 or 3) and we will denote by \( G_{p^2}(\ell) \) the supersingular isogeny graph whose vertices correspond to supersingular elliptic curves over \( \mathbb{F}_{p^2} \) - modulo isomorphisms over \( \mathbb{F}_{p^2} \) - and edges correspond to isogenies of degree \( \ell \) (up to equivalence).

We are concerned with answering two main questions about supersingular isogeny graphs, which relate to the existence of single collisions and double collisions. The problem of the existence of simple collisions is addressed in Section 5.1, while in Section 5.2 we investigate the existence of double collisions.

5.1 Simple Collisions

We begin by formally stating the first problem we focus our attention on.

**Problem 5.** Fix primes \( \ell < p \), and let \( E_0 \) be a uniformly random supersingular elliptic curve \( E_0 \) (i.e. a vertex) in the graph \( G_{p^2}(\ell) \). Determine the probability that another supersingular elliptic curve \( E_1 \) in \( G_{p^2}(\ell) \) is linked to \( E_0 \) by two non-equivalent isogenies \( \varphi_A \) and \( \varphi_B \), both with cyclic kernel and of degree \( \deg(\varphi_i) = \ell^e \) for a fixed \( e \in \mathbb{N} \), with \( p = \ell^{2e} \), as in Figure 4.

The answer to this problem depends on the primes \( \ell \) and \( p \). It is impossible to find an accurate estimate that only depends on \( \ell \) and works for all elliptic curves. However, we will see that we can find an upper bound for the average number of collisions that only depends on \( p \). Finding a good lower bound is much more difficult. It is beyond the reach of current analytic number theory, as it involves bounds on [27, Chap. 12] that are tighter than what we expect to be provable.

---

4 A lot of our work does not use this assumption. However, we do need it at the end, when giving final bounds in terms of \( p \). Also, in Section 5.1.2 we need \( p > 2\ell^e \).
Fig. 4: Isogenies of the same degree sending $E_0$ in another curve $E_1 \in G_{p^2}(\ell)$.

In order to tackle Problem 5, we start by computing the expected number of pairs of same-degree isogenies mapping $E_0$ to some $E_1$, where the expectation is taken over the parameters $p$ and $E_0$.

Let $f$ and $g$ be two isogenies with the same domain $E_0 \in G_{p^2}(\ell)$. We say that $f \sim g$ if they generate the same path in $G_{p^2}(\ell)$, i.e. $f = \alpha \circ g$ for some automorphism $\alpha$. Given two points in $E_0[\ell^e]$, we will consider them equivalent if they generate the same torsion subgroup, i.e. if they generate the same isogeny (modulo equivalence). Let $E_0[\ell^e]_{\text{max}}$ denote the set of points of maximal order in $E_0[\ell^e]/\sim$. We can rephrase the above statement as follows: compute the probability of finding two non-equivalent points $P_A, P_B \in E_0[\ell^e]$ of order $\ell^e$ such that $E_0/\langle P_A \rangle \sim E_0/\langle P_B \rangle$.

For primes $p, \ell$ and some $m \in \mathbb{N}$, let $\mathcal{C}_E(\ell^m)$ denote the number of endomorphisms with no backtracking (i.e. with cyclic kernel) of degree $\ell^m$ of a vertex $E$ in $G_{p^2}(\ell)$. Let also $\text{Coll}_{\ell^e}(E_0)$ be the set of collisions $(f, g)$ of degree $\ell^e$ starting at $E_0$, such that $f \not\sim g$. Following the above discussion, we can rephrase the set $\text{Coll}_{\ell^e}(E_0)$ as

$$\{(P_A, P_B) \in (E_0[\ell^e]_{\text{max}})^2 : \frac{E_0}{\langle P_A \rangle} \cong \frac{E_0}{\langle P_B \rangle}, P_A \not\sim P_B \}/\{(P_A, P_B) \sim (P_B, P_A)\}.$$

(7)

Remark 1. In Equation (7), we mod out by the relation $(P_A, P_B) \sim (P_B, P_A)$ because we regard the two pairs of isogenies $(f, g)$ and $(g, f)$ as the same, since they clearly generate the same collisions. Note that $k$ isogenies between $E$ and $E'$ would be counted as $k^2$ pairs.

Let $n$ be the number of vertices in the graph $G_{p^2}(\ell)$. By definition, to obtain $\mathcal{C}_{E_i}(\ell^{2e})$, we need to subtract from $B_{ii}(\ell^{2e})$ the number of endomorphisms of $E_i$ of degree $\ell^{2e}$ with scalar factors. However, this number is simply given by $B_{ii}(\ell^{2e-2})$. Indeed, an endomorphism of $E_i$ of degree $\ell^{2e}$ with backtracking can be written as $[\ell] \circ f$ for an endomorphism $f$ of $E_i$ of degree $\ell^{2e-2}$. Thus, we can
write
\[\sum_{i=1}^{n} CE_i(\ell^2e) = \frac{1}{2} \sum_{i=1}^{n} (B_{ii}(\ell^2e) - B_{ii}(\ell^2e^{-2}))\]
\[= \frac{1}{2} \text{Tr}(B(\ell^2e)) - \frac{1}{2} \text{Tr}(B(\ell^2e^{-2}))\]
\[= \frac{1}{2} \sum_{s^2 \leq 4\ell^2e} H_p(4\ell^2e - s^2) - \frac{1}{2} \sum_{s^2 \leq 4\ell^2e^{-2}} H_p(4\ell^2e^{-2} - s^2).\]

Note that we divided by 2 because every endomorphism on the graph \(G_{p^2}(\ell)\) corresponds to a path that can be taken in both directions, since the graph is undirected. In more precise terms, each endomorphism corresponds to two pairs of equivalent (as described in Remark 1) isogenies \((f, g) \sim (g, f)\) that both give us the same collision: the endomorphisms \(\hat{f} \circ g\) and \(\hat{g} \circ f\) that they form are dual to each other.

In addition, \(H_p(0)\) appears in both sums, so we can cancel it out. Moreover, since \(4\ell^2e\) is a square in \(\mathbb{Z}\), \(p\) will always split in \(O_{-4\ell^2e}\), and \(H_p(4\ell^2e) = 0\). Likewise, \(H_p(4\ell^2e^{-2}) = 0\). Hence,
\[\sum_{i=1}^{n} CE_i(\ell^2e) = \frac{1}{2} \sum_{0 < s^2 < 4\ell^2e} H_p(4\ell^2e - s^2) - \frac{1}{2} \sum_{0 < s^2 < 4\ell^2e^{-2}} H_p(4\ell^2e^{-2} - s^2).\]

Remark 2. As an aside, note that the above number \(\sum_{i=1}^{n} CE_i(\ell^2e)\) is not exactly the total number of cycles (endomorphisms with no backtracking) of degree \(\ell^2e\) in \(G_{p^2}(\ell)\), as we are over-counting each cycle in the above sum. If we wanted to count the exact total number of cycles of length \(2e\) in \(G_{p^2}(\ell)\) we would have to divide by \(2e\) to get \(\frac{1}{2e} \sum_{i=1}^{n} CE_i\).

We have now related the number of endomorphisms with no backtracking \(CE(\ell^m)\) to the desired number of collisions \(\text{Coll}_{\ell^r}(E_0)\). This allows us to turn our attention to estimating \(CE(\ell^m)\).

**Lemma 1.** It is possible to bound the number \(CE(\ell^r)\) using \(\text{Coll}_{\ell^r}(E_0)\) as follows
\[CE_{E_0}(\ell^r) \leq \#\text{Coll}_{\ell^r}(E_0) \leq CE_{E_0}(\ell^r) + \sum_{i=1}^{r-1} CE_{E_0}(\ell^i)(\ell - 1)^{\ell - 1 - i}.\]

**Proof.** The first inequality is clear since, by definition, every collision also constitutes an endomorphism with no backtracking. However, there are some endomorphisms with backtracking that still constitute collisions, as in Figure 6. The collisions that form endomorphisms with backtracking can be broken into two parts: a first part that is an endomorphism without backtracking and second part at the end that constitutes the backtracking. In Figure 6, the first part is the part drawn in black between \(E\) and \(E_0\) that gives an endomorphism without backtracking ("abcdeffelhga") and the second part, drawn in blue, is the part that constitutes the backtracking.
Fig. 5: Two paths ("abcdef" and "aghief") that constitute an endomorphism ("abcdeffeihga") with backtracking and also a collision.

Therefore, to take the endomorphisms with backtracking into account when counting collisions, we simply need to count all endomorphisms without backtracking of different possible degrees \( C_{E_0}(\ell^r) \), for some \( r \in \{1, ..., e-1\} \), and add an extra factor of \( (\ell - 1)\ell^{r-1} \), which is an upper bound on the number of ways we can draw a path of length \( r + 1 \) from an elliptic curve \( E_0 \) to another one \( E' \) without backtracking, as in Figure 5. Note that this takes into account the fact that the curve \( E_0 \) already has two edges coming into it: this is why we have \( (\ell - 1)\ell^{e-1} \) instead of simply \( \ell^{e-1} \).

If we were to expand the definition of \( H_p \) appearing in (9), we would see that in order to precisely compute \( \sum_{i=1}^{n} C_{E_i}(\ell^{2r}) \), one would need to get a handle on the average splitting behaviour of \( 4\ell^{2e} - s^2 \) in \( \mathbb{F}_p \), which is beyond what is currently known. We will try to get around this issue as follows. One option is to find upper bounds (as in Section 5.1.1) for the number of collisions using the fact that \( 0 \leq H_p(D) \leq H(D) \). Unfortunately, using this same fact to find lower bounds would only give us a meaningless lower bound: zero. Another option (used in Section 5.1.2) is to replace the deterministic splitting of \( 4\ell^{2e} - s^2 \) in \( \mathbb{F}_p \) by a random Bernoulli process. We would essentially be modelling the Legendre symbols \( \left( \frac{4\ell^{2e} - s^2}{p} \right) \) by a Bernoulli random variable. This would not give us an actual value for \( \sum_{i=1}^{n} C_{E_i}(\ell^{2r}) \), but rather an estimate for it.

5.1.1 Upper bounds We hereby prove an upper bound for the number of endomorphisms without backtracking, which will allow us to bound the number collisions. The expected number of endomorphisms without backtracking in \( \mathcal{G}_{\ell^2}(\ell) \) is expressed as \( \mathbb{E}_E \left[ \mathcal{C}_E(\ell^{2r}) \right] := \frac{1}{n} \sum_{i=1}^{n} \mathcal{C}_{E_i}(\ell^{2r}) \).

Lemma 2. The upper bound

\[
\mathbb{E}_E \left[ \mathcal{C}_E(\ell^{2r}) \right] \leq \frac{\ell^{2r+1}}{n(\ell - 1)}
\]

holds for all \( r \geq 1 \).
Proof. From equation (9), we have

$$\sum_{i=1}^{n} C_{E_i}(\ell^2 r) = \frac{1}{2} \sum_{0<s^2 \leq 4\ell^2 r} H_p(4\ell^2 r - s^2) - \frac{1}{2} \sum_{0<s^2 \leq 4\ell^2 r-2} H_p(4\ell^2 r-2 - s^2)$$

$$\leq \frac{1}{2} \sum_{0<s^2 \leq 4\ell^2 r} H(4\ell^2 r - s^2)$$

$$= \frac{1}{2} \sum_{s^2 \leq 4\ell^2 r} H(4\ell^2 r - s^2) - H(0)$$

$$= \frac{1}{2} \left( 2 \sum_{d | \ell^2 r} d - \sum_{d | \ell^2 r} \min \left( d, \frac{\ell^2 r}{d} \right) \right) + \frac{1}{12}$$

$$= \frac{2r}{\ell-1} - \sum_{i=0}^{r-1} \ell^i - \frac{1}{2} \ell^r + \frac{1}{12}$$

$$= \frac{2r}{\ell-1} - \frac{1}{2} \ell^r + \frac{1}{12}$$

Thus, putting everything together, we get that

$$\mathbb{E}_E \left[ C_{E}(\ell^2 r) \right] = \frac{1}{n} \sum_{i=1}^{n} C_{E_i}(\ell^2 r) \leq \frac{\ell^2 r+1}{n(\ell - 1)}.$$ 

Remark 3. In the proof of Theorem 2, we have the upper bound $\sum_{i=1}^{n} C_{E_i}(\ell^2 r) \leq \frac{\ell^2 r+1-\ell^r}{\ell-1} - \frac{1}{2} \ell^r + \frac{1}{12}$. One can ask about how good it is. The only place in (11) were we use an upper bound instead of an equality is at (♦), when we dropped the term $\frac{1}{2} \sum_{0<s^2 \leq 4\ell^2 r-2} H_p(4\ell^2 r-2 - s^2)$ (which has order $\ell^{2r-2}$, so dropping it does not affect things much) and bounded $H_p(D)$ above by $H(D)$. Regarding the latter, we know that the definition of $H_p(D)$ depends on the splitting behaviour of $p$. We thus suspect that $H_p(D)$ is equal to zero half of the time and to $H(D)$ the other half, which leads us to expect that, on average, we have $H_p(D) = \frac{1}{2} H(D)$. Of course, this is not a rigorous statement and we cannot actually prove it, as the actual state of knowledge does not allow us to precisely pin down the average behaviour of the Legendre symbol $\left( \frac{4\ell^2 r-s^2}{p} \right)$ as $s = 0,\ldots,2\ell^r$. So we cannot actually say that our upper bound $\frac{\ell^2 r+1-\ell^r}{\ell-1} - \frac{1}{2} \ell^r + \frac{1}{12}$ is twice the value of $\mathbb{E}_E \left[ C_{E}(\ell^2 r) \right]$, but we can imagine that is should in principal be close. We will discuss this issue further in Section 5.1.2.

We now make use of the bound we have obtained in Lemma 2 to give an estimate of the number of collisions that are expected in a graph.
Theorem 3. We have the following upper bound for the average number of collisions of degree $\ell^e$ in the graph $G_{p^2}(\ell)$:

$$E_E[\#\text{Coll}_{\ell^e}(E)] := \frac{1}{n} \sum_{i=1}^{n} \#\text{Coll}_{\ell^e}(E_i) \leq \frac{\ell^{2e}(\ell + 1)}{n(\ell - 1)}.$$  \hspace{1cm} (12)

The average number of collisions is therefore in $O(1)$.

Proof. By Lemma 2, we know that for all $r \in \mathbb{N}$,

$$E_E[\mathcal{C}_E(\ell^{2r})] \leq \frac{\ell^{2r+1}}{n(\ell - 1)}.$$

Combining this with Lemma 1 we obtain

$$E_E[\#\text{Coll}_{\ell^e}(E)] \leq E_E[\mathcal{C}_E(\ell^{e})] + \sum_{r=1}^{e-1} E_E[\mathcal{C}_E(\ell^{2r})](\ell - 1)\ell^{e-1-r} \leq \frac{\ell^{2e+1}}{n(\ell - 1)} + \sum_{r=1}^{e-1} \frac{\ell^{2r+1}}{n(\ell - 1)}(\ell - 1)\ell^{e-1-r} \leq \frac{\ell^{2e+1}}{n(\ell - 1)} + \frac{\ell^{e}}{n} \sum_{r=1}^{e-1} \ell^{r} \leq \frac{\ell^{2e+1}}{n(\ell - 1)} + \frac{\ell^{e}}{n} \cdot \frac{\ell^{e} - \ell}{\ell - 1} \leq \frac{\ell^{2e}(\ell + 1)}{n(\ell - 1)}.$$

Now that we have found an upper bound, we turn our attention to finding a lower bound.

5.1.2 Lower bounds We would like to show that, for a fixed prime $\ell$, the expected number of collisions $\text{Coll}_{\ell^e}(E)$ for an arbitrary prime $p$ and an arbitrary elliptic curve $E$ in the graph $G_{p^2}(\ell)$ is non negligible. By Lemma 3, we only need to focus on $\mathcal{C}_E(\ell^e)$ in order to bound $\text{Coll}_{\ell^e}(E)$. Moreover, in order to get a handle on $\mathcal{C}_E(\ell^e)$ we need to know $\sum_{0<s^{2} \leq 4\ell^{e}} H_p(4\ell^{2r} - s^{2})$. The difficulty lies in relating the sums of modified Hurwitz class numbers $H_p(\cdot)$ to sums of Hurwitz class numbers $H(\cdot)$. As explained in Remark 3, our estimate is that the actual value of $\sum_{0<s^{2} \leq 4\ell^{e}} H_p(4\ell^{2r} - s^{2})$ is roughly $\frac{1}{2} \sum_{0<s^{2} \leq 4\ell^{e}} H(4\ell^{2r} - s^{2})$. However, we cannot prove this as it involves sums of Legendre symbols, and the best bounds for character sums that are known (based the bounds of Burgess in [8–10]) are far from being tight enough for what we need.
What we will do instead, in order to estimate $\text{Coll}_{\ell^e}(E)$, is to model the behaviour of the Legendre symbol $\left( \frac{4\ell^2 - s^2}{p} \right)$ with Bernoulli events. Let

$$
\varepsilon_p(D) := \begin{cases} 
0 & \text{if } p \text{ splits in } O_D; \\
1 & \text{if } p \text{ is inert in } O_{-D} \\
\frac{1}{2} & \text{if } p \text{ is ramified in } O_{-D}
\end{cases}
$$

and does not divide the conductor of $O_{-D}$; (13)

so that

$$
H_p(4\ell^2e - s^2) = \varepsilon_p(4\ell^2e - s^2)H(4\ell^2e - s^2),
$$

for all $4\ell^2e > s^2$. Note that we excluded the last case of the definition of modified Hurwitz Class Numbers in equation (2), which is when $p$ divides the conductor of $O_{s^2 - 4\ell^2e}$, because this case simply does not happen. Indeed, let $f$ denote the conductor of $O_D$ for $D := s^2 - 4\ell^2e$ with $4\ell^2e \geq s^2$ and $-d$ its fundamental discriminant. Then $f = \sqrt{D/d} < 2\ell^e < p$. Hence, $p$ cannot divide the conductor $f$.

In the next lemma, we will replace $\varepsilon_p(4\ell^2e - s^2)$ with Bernoulli random variables, in order to get estimates on $H_p$ and thus on $E_E[\text{Coll}_{\ell^e}(E)]$.

Let $X_0, X_1, ..., X_{2\ell^e}$ be i.i.d. Bern(1/2) random variables with values in $\{0, 1\}$ and set

$$
H^*(4\ell^2e - s^2) = X_s \cdot H(4\ell^2e - s^2),
$$

for all $s = 0, 1, ..., 2\ell^e$. Our goal is for $H^*$, from equation (15), to mimic $H_p$, from equation (14), for all $s^2 < 4\ell^2e$. Now that we have replaced the deterministic (but hard to pin down) behaviour of $H_p(4\ell^2e - s^2)$ by a probabilistic function $H^*(4\ell^2e - s^2)$, we can make probabilistic statements about it.

**Lemma 3.** We have the following expectation for the sum $\sum_{s^2 \leq 4\ell^2e} H^*(4\ell^2e - s^2)$:

$$
E \left[ \sum_{s^2 \leq 4\ell^2e} H^*(4\ell^2e - s^2) \right] = \frac{\ell^{2\ell^e+1} - \ell^e}{\ell - 1} - \frac{1}{2}\ell^e.
$$

**Proof.** First, let $a$ denote the sum $\sum_{s^2 \leq 4\ell^2e} H(4\ell^2e - s^2)$; then

$$
a = 2\sum_{i=0}^{2\ell^e} \ell^i - 2\sum_{i=0}^{2\ell^e-1} \min\{\ell^i, \ell^{2\ell^e-i}\}
\quad = 2\sum_{i=0}^{2\ell^e} \ell^i - 2\sum_{i=0}^{\ell^e-1} \ell^i - \ell^e
\quad = 2\frac{\ell^{2\ell^e+1} - \ell^e}{\ell - 1} - \ell^e.
$$
We then can easily compute the expectation \( \mu := E \left[ \sum_{s^2 \leq 4\ell^2e} H^*(4\ell^2e - s^2) \right] \) as

\[
E \left[ \sum_{s^2 \leq 4\ell^2e} H^*(4\ell^2e - s^2) \right] = \sum_{s^2 \leq 4\ell^2e} H(4\ell^2e - s^2) E[X_s]
\]

\[
= a/2
\]

\[
= \frac{\ell^2 + 1 - \ell e}{\ell - 1} - \frac{1}{2} \ell e.
\]

Now that we know the expectation from Lemma 3, we can ask about how much the sum \( \sum_{s^2 \leq 4\ell^2e} H^*(4\ell^2e - s^2) \) can deviate from its mean \( \mu \). One might initially be tempted to use the central limit theorem, and there are triangular versions of the CLT that allow for the setup we are in (we are not in the presence of a sequence of random variables, but the sequence that we are considering \( \{H^*(4\ell^2e - s^2)\}_{s=0, \ldots, 2\ell e} \) changes for every new \( p \)). However, we would need the Lyapunov or Lindeberg condition, which is not obvious at all to prove rigorously (see Remark 4).

Instead, we need to revert to the use of concentration inequalities that do not use limits, such as Hoeffding’s bound (see Proposition 2.5 in [40]).

**Proposition 1.** Let \( \varepsilon > 0 \), there is a positive constant \( c_\varepsilon := 1 - e^{-\varepsilon^2/2} \) only depending on \( \varepsilon \) such that

\[
P \left( \left| \frac{\sum_{s^2 \leq 4\ell^2e} H^*(4\ell^2e - s^2)}{\mu} - 1 \right| \leq \varepsilon \right) \geq c_\varepsilon.
\]

**Proof.** Let \( \varepsilon > 0 \). Using Hoeffding’s bound, we can rewrite the probability

\[
P \left( \left| \frac{\sum_{s^2 \leq 4\ell^2e} H^*(4\ell^2e - s^2)}{\mu} - 1 \right| \leq \varepsilon \right) =
\]

\[
= \mathbb{P} \left( \left| \sum_{s^2 \leq 4\ell^2e} H^*(4\ell^2e - s^2) - \mu \right| \leq \varepsilon \mu \right)
\]

\[
= \mathbb{P} \left( \left| \sum_{s^2 \leq 4\ell^2e} H(4\ell^2e - s^2) X_s - \mu \right| \leq \varepsilon \mu \right)
\]

\[
\geq 1 - \exp \left[ -\frac{\varepsilon^2 \mu^2}{2 \cdot \sum_{s^2 \leq 4\ell^2e} \text{Var}(H(4\ell^2e - s^2) X_s)} \right]
\]

\[
= 1 - \exp \left[ -\frac{\varepsilon^2 \mu^2}{2 \cdot \sum_{s^2 \leq 4\ell^2e} (H(4\ell^2e - s^2))^2 \text{Var}(X_s)} \right]
\]
con. It then follows that most 2
\( \frac{\sum_{s^2 \leq 4\ell^2e} H(4\ell^2e - s^2)}{\sum_{s^2 \leq 4\ell^2e} H(4\ell^2e - s^2)^2} \)
\( > 1 - \exp \left[ -\frac{2\varepsilon^2 \mu^2}{a^2} \right] \)
\( = 1 - e^{-\varepsilon^2/2}. \)

\[ \square \]

This shows the quantity \( \sum_{s^2 \leq 4\ell^2e} H^*(4\ell^2e - s^2) \) is close to \( p/2 \) a positive proportion of the time. Indeed, if we take \( \varepsilon = 0.5 \), then \( \sum_{s^2 \leq 4\ell^2e} H^*(4\ell^2e - s^2) \) is between 0.5\( \mu \) and 1.5\( \mu \) with probability \( \geq 11\% \) which is non-negligible. This provides more evidence to the fact that we can think of \( \mu \) as being close to \( \mu = \frac{1}{2} \sum_{s^2 \leq 4\ell^2e} H(4\ell^2e - s^2) \).

Note that for proving Proposition 1, we could have also used Markov’s inequality, which gives slightly better bounds for certain values of \( \varepsilon \).

Remark 4. One can actually do much better than the bound provided in Proposition 1. Indeed, in step (❼) of the proof of the above proposition, we bound
\[ \frac{(\sum_{s^2 \leq 4\ell^2e} H(4\ell^2e - s^2))^2}{\sum_{s^2 \leq 4\ell^2e} H(4\ell^2e - s^2)^2} \]
above by 1. However, we believe that this quantity should tend to zero as \( p \) goes to infinity. Indeed, as \( \sum_{s^2 \leq 4\ell^2e} H(4\ell^2e - s^2) \in \Theta(p) \) (by the proof of Lemma 2), we only need to explain why \( \sum_{s^2 \leq 4\ell^2e} H(4\ell^2e - s^2)^2 \) is on \( o(p^2) \). By the Brauer-Siegel theorem \[7\], we have that for all \( \varepsilon > 0 \) there is some \( c_\varepsilon > 0 \) such that \( h(-d) < c_\varepsilon d^{1/2+\varepsilon} \). In addition, we know that there are at most \( 2d^{1/4} \) square divisors of \( d \) for all \( d \); or even better: there are \( o(d^\varepsilon) \) divisors for \( d \) for all \( \varepsilon \). This gives us a small enough bound on \( H(D) \), especially when \( D \) is big, which is the case in the majority of the values \( D = 4\ell^2e - s^2 \) that we consider. It then follows that \( \sum_{s^2 \leq 4\ell^2e} H(4\ell^2e - s^2)^2 \) is \( o(\ell^4e^\varepsilon) = o(p^2) \).

Now, recall from equations (2) and (3) that
\[ E_E \left[ \ell^2e(\ell^2e) \right] := \frac{1}{n} \sum_{i=1}^n \ell^{2e_i}(\ell^2e) \]
\[ = \frac{1}{2} \sum_{0 < s^2 < 4\ell^2e} H_p(4\ell^2e - s^2) - \frac{1}{2} \sum_{0 < s^2 < 4\ell^2e-2} H_p(4\ell^2e-2 - s^2) \]
\[ = \frac{1}{2} \sum_{s^2 \leq 4\ell^2e} H_p(4\ell^2e - s^2) - \frac{1}{2} \sum_{s^2 \leq 4\ell^2e-2} H_p(4\ell^2e-2 - s^2). \]
Let us define
\[ \ell^2e(\ell^2e) := \frac{1}{2} \sum_{s^2 \leq 4\ell^2e} H^*(4\ell^2e - s^2) - \frac{1}{2} \sum_{s^2 \leq 4\ell^2e-2} H^*(4\ell^2e-2 - s^2) \]
which should approximate the total number of collisions \( \sum_{i=1}^{n} C_{E_i}(\ell^2e) \) defined in (9). As in (16), we can compute

\[
\mathbb{E}[C^*(\ell^2e)] = \frac{1}{2} \mathbb{E} \left[ \sum_{s^2 \leq 4\ell^2e} H^*(4\ell^2e - s^2) \right] - \frac{1}{2} \mathbb{E} \left[ \sum_{s^2 \leq 4\ell^2e - 2} H^*(4\ell^2e - 2 - s^2) \right] \\
= \frac{\ell^{2e+1} - \ell^e}{\ell - 1} - \frac{1}{2} \ell^e - \left( \frac{\ell^{2e-1} - \ell^{e-1}}{\ell - 1} - \frac{1}{2} \ell^{e-1} \right) \\
= \frac{\ell^{2e+1} - \ell^e}{\ell - 1} - \frac{1}{2} \ell^e - \frac{\ell^{2e-1} - \ell^{e-1}}{\ell - 1} + \frac{1}{2} \ell^{e-1} \\
= \frac{1}{2} \ell^{e-1}(\ell + 1)(2\ell^e - 1).
\]

Using Lemma [1] we conclude the proof of the following theorem.

**Theorem 4.** Using the Bernoulli model introduced in Section 5.1.2 we expect that for an arbitrary supersingular isogeny graph \( G_{p^2}(\ell) \), the number of collisions of degree \( \ell^e \) is bounded below by \( \frac{1}{2} \ell^{e-1}(\ell + 1)(2\ell^e - 1) \). In particular, this model predicts the number of collisions starting at a given elliptic curve to be \( \Omega(1) \).

### 5.2 Double Collisions

The second problem we consider is directly related with the first one.

**Problem 6.** Assuming the scenario described in Problem 5, determine the probability of having two more isogenies (not necessarily distinct this time), \( \psi_A, \psi_B : E_1 \to E_2 \) of degree \( q^f \), and cyclic kernel, where \( q \) is a small prime and \( f \in \mathbb{N} \), with \( p \approx q^{2f} \), such that there exists \( R \in E_0 \) for which \( R_A := \varphi_A(R) \) and \( R_B := \varphi_B(R) \) are generators for the kernels of \( \psi_A \) and \( \psi_B \), respectively.

![Fig. 6: Isogenies of the same degrees sending \( E_0 \) in \( E_1 \), and \( E_1 \) in \( E_2 \).](image)

Let us compute the average number of pairs of isogenies from \( E_1 \) to some \( E_2 \), as in Problem 6. We can rephrase this problem as follows: determine the probability of finding two points \( R_A, R_B \in E_1[q^f] \) of maximal order, such that
$E_1/\langle R_A \rangle \cong E_1/\langle R_B \rangle$ and $R_i = \varphi_i(R)$ for $i = A, B$. Let $\text{Coll}^\perp_{E,q'}(E_0, E_1)$ denote the set

$$\left\{ (R_A, R_B) \in (E_1[q'])_{\text{max}}^2/((X, Y) \sim (Y, X)) \text{ such that } E_1/\langle R_A \rangle \cong E_1/\langle R_B \rangle; R_i = \varphi_i(R) \text{ for some } R \in E_0[q']_{\text{max}} \right\}$$

of desired pairs $(R_A, R_B)$ up to equivalence, where $E_1[q']_{\text{max}}$ denotes the set of point of maximal order in $E_1[q']_{\sim}$. Let also $\text{Coll}^\parallel_{E,q'}(E_1)$ denote the set:

$$\{(R_A, R_B) \in (E_1[q']_{\text{max}}^2/((X, Y) \sim (Y, X)) : E_1/\langle R_A \rangle \cong E_1/\langle R_B \rangle \}.$$

Note that $\text{Coll}^\perp_{E,q'}(E_1) \subseteq \text{Coll}^\parallel_{E,q'}(E_1)$. Now, since we are allowing $R_A \sim R_B$, we can split $\text{Coll}^\perp_{E,q'}(E_1)$ and $\text{Coll}^\parallel_{E,q'}(E_1)$ into two disjoint subsets:

$$\text{Coll}^\perp_{E,q'}(E_0, E_1) = \text{Coll}_{E,q'}^\perp(E_0, E_1) \cup \text{Coll}_{E,q'}^\parallel(E_0, E_1),$$

where $\text{Coll}_{E,q'}^\perp(E_0, E_1)$ is the set

$$\left\{ (R_A, R_B) \in (E_1[q']_{\text{max}}^2/((X, Y) \sim (Y, X)) \text{ such that } E_1/\langle R_A \rangle \cong E_1/\langle R_B \rangle; R_A \neq R_B, R_i = \varphi_i(R) \text{ for some } R \in E_0[q']_{\text{max}} \right\},$$

$\text{Coll}_{E,q'}^\parallel(E_0, E_1)$ is the set

$$\left\{ (R_A, R_B) \in (E_1[q']_{\text{max}}^2/((X, Y) \sim (Y, X)) \text{ such that } E_1/\langle R_A \rangle \cong E_1/\langle R_B \rangle; R_A = R_B, R_i = \varphi_i(R) \text{ for some } R \in E_0[q']_{\text{max}} \right\} \cong \{R_A \in E_1[q']_{\text{max}} | R_A = \varphi_A(R) = \varphi_B(R) \text{ for some } R \in E_0[q']_{\text{max}} \},$$

$\text{Coll}_{E,q'}^\perp(E_1)$ is the set

$$\{(R_A, R_B) \in (E_1[q']_{\text{max}}^2/((X, Y) \sim (Y, X)) | E_1/\langle R_A \rangle \cong E_1/\langle R_B \rangle, R_A \neq R_B \}$$

and $\text{Coll}_{E,q'}^\parallel(E_1)$ is the set

$$\{(R_A, R_B) \in (E_1[q']_{\text{max}}^2/((X, Y) \sim (Y, X)) | E_1/\langle R_A \rangle \cong E_1/\langle R_B \rangle, R_A = R_B \} \cong \{R_A \in E_1[q']_{\text{max}} \}.$$

It is known that the size of the torsion subgroup $E_1[q']$ is $q^{2f}$ and that the number of subgroups of $E_1[q']$ having order $q^f$ (i.e. the number of points with maximal order, up to equivalence) is $q^f + q^{f-1}$. We can now prove that the expected number of double collisions in a supersingular isogeny graph for a fixed initial curve is 1.

**Proposition 2.** We have that

$$\mathbb{E}[\# \text{Coll}_{E,q'}^\parallel(E_0, E_1)] = 1.$$
Thus, \( \varphi^\dagger \). The justification for step (\( \text{Coll} \)) is again, as in the first step of this proof, that \( \varphi_i : E_0 \to E_1 \) restricts to an isomorphism \( \varphi_i : E_0[q^f]_{\max} \to E_1[q^f]_{\max} \). Hence,

\[
\mathbb{P}_{R_A, R_B \in E_1[q^f]_{\max}} \left( R_i = \varphi_i(R) \text{ for some } R \in E_0[q^f]_{\max} \right) = \mathbb{P}_{R_A, R_B \in E_1[q^f]_{\max}} \left( \varphi_A^{-1}(R_A) = \varphi_B^{-1}(R_B) \right).
\]

So the cardinality of \( \text{Coll}^{e, q^f}_v(E_0, E_1) \) is equal to

\[
\sum_{R_A, R_B \in E_1[q^f]_{\max}} \mathbb{I}_{(E_1/R_A) \cong (E_1/R_B), R_A = R_B, R_i = \varphi_i(R) \text{ for some } R \in E_0[q^f]_{\max}}
= \sum_{R_A \in E_1[q^f]_{\max}} \mathbb{I}_{\varphi_A^{-1}(R_A) = \varphi_B^{-1}(R_A)}.
\]

Thus,

\[
\mathbb{E}[\# \text{Coll}^{e, q^f}_v(E_0, E_1)] = \mathbb{E} \sum_{R_A \in E_1[q^f]_{\max}} \mathbb{I}_{\varphi_A^{-1}(R_A) = \varphi_B^{-1}(R_A)}
= \sum_{R_A \in E_1[q^f]_{\max}} \mathbb{P}(\varphi_A^{-1}(R_A) = \varphi_B^{-1}(R_A))
= \mathbb{E}_{E_0} \left[ \text{Coll}^{e, q^f}_v(E_0) \right] \cdot \mathbb{E}_{E_0, E_1} \left[ \text{Coll}^{e, q^f}_v(E_0, E_1) \right]
\]

We are finally ready to give an answer to Problem 6: we want to estimate how many double collisions we can have in the graph \( G_{p^2}(\ell) \). We have found estimates for lower bounds on the number of first collisions that could occur in subsection 5.1.2 and we have found the expected number of certain kinds of second collisions in Proposition 2. We now argue that we can combine these two results together. Indeed, the first collision has degree \( \ell^e \) and the second has degree \( q^f \). Thus, we can assume without loss of generality that the events of having a first collision and having a second collision are independent. This allows us to write that the expectation of this event is

\[
\mathbb{E}_{E_0} \left[ \text{Coll}^{e}_v(E_0) \right] \cdot \mathbb{E}_{E_0, E_1} \left[ \text{Coll}^{e, q^f}_v(E_0, E_1) \right]
\geq \mathbb{E}_{E_0} \left[ \text{Coll}^{e}_v(E_0) \right] \cdot \mathbb{E}_{E_0, E_1} \left[ \text{Coll}^{e, q^f}_v(E_0, E_1) \right]
= \mathbb{E}_{E_0} \left[ \text{Coll}^{e}_v(E_0) \right].
\]

However, as amply discussed in Section 5.1.2 we cannot directly bound the quantity \( \mathbb{E}_{E_0} \left[ \text{Coll}^{e}_v(E_0) \right] \) from below (without getting the trivial bound zero!). We therefore revert to using our Bernoulli model for approximating Legendre symbols. We then get the following result.
Theorem 5. Fix an arbitrary supersingular isogeny graph as in Problems 5 and 6 and pick an arbitrary elliptic curves $E_0$ on it. Then, using the Bernoulli model introduced in Section 2.1.2 to estimate Legendre symbols, we expect that the number of double collisions starting at $E_0$ is non negligible. More precisely, it is in $\Omega(1)$.

Remark 5. The above result uses a statistical model to approximate a deterministic event. This means that the bound is not necessarily always true, and that one could potentially hope to manufacture a prime $p$ specifically tailored in order to ensure that the graph $G_p^\ell$ has fewer collisions. However, Bernoulli events are a very good way of approximating Legendre symbols, and therefore, on average, our bound should provide a very good indicator for what is actually happening.

6 Collisions in Isogeny-based Cryptography

When bounding the average number of collisions in Theorem 3 of Section 5, we fixed the starting elliptic curve and allowed the image curve to be any vertex on the graph. However, one can also consider the average number of collisions starting at a given elliptic curve $E$ and colliding at another fixed elliptic curve $E'$. This would drastically change the order of magnitude of our final answer, and we would then get a much smaller quantity. This fact is sometimes implicitly assumed in the literature, with scarce formal justifications.

In the analysis of claw-finding algorithms for the CSSI problem of [13] - and in particular in Section 2.2. - the focus is on finding an isogeny $\varphi$ from $E_0$ to $E_1$. It is claimed that, once an elliptic curve $E'$, with isogenies $f_1 : E_0 \to E'$ and $g_1 : E_1 \to E'$ is found, the composition $g_1 \circ f_1$ would return $\varphi$. This argument assumes that it is impossible (or at least extremely unlikely) to have collisions $f_1, f_2 : E_0 \to E'$ or $g_1, g_2 : E_1 \to E'$, with $f_1 \neq f_2$ and $g_1 \neq g_2$. If such collisions happen, all the isogenies $g_i \circ f_j$, with $i, j \in \{1, 2\}$, would be different, and the recovered isogeny would not necessarily be equal to $\varphi$.

Also in [23, Sec. 3.1], it is claimed that if two curves $E/G_1$ and $E/G_2$ are isomorphic, then one could safely assume $G_1 = G_2$. In other words, if two isogenies of the same sufficiently small degree start at the same curve and have the same codomain, then they are equivalent. This argument is mentioned in the adaptive attack developed in [23] and assumes that collisions are extremely unlikely.

We now use the calculations done in Section 5 to provide a more rigorous proof of this assumption. Let $\text{Coll}_e(E, E')$ denote the number of collisions between $E$ and $E'$ of degree $\ell^e$ in the graph $G_p^\ell$, with $p \approx \ell^2e$. The number of elliptic curves that one can obtain starting from $E$ and taking a path of length $e$ is $\Theta(\ell^e) = \Theta(\sqrt{p})$. Therefore, we would get that $\text{Coll}_e(E, E') \approx O(1/\ell^e)$ which is negligible. The details of this argument are proven in the following theorem.

Theorem 6. Given a supersingular graph $G_p^\ell$, pick uniformly at random two elliptic curves $E, E'$ in $G_p^\ell$ and assume that there is an isogeny of degree $\ell^e$ with no backtracking between them. Then, the expected number of collisions of degree $\ell^e$ from $E$ to $E'$ in the graph $G_p^\ell$ is $O(1/\sqrt{p})$. 

Proof. We know from Theorem 3 that there are, on average, $O(1)$ collisions starting at $E$. Let $m_E$ be the number of elliptic curves that are connected to $E$ via a path of length $e$ without backtracking. Let $m_E = \ell^e + \ell^{e-1}$ be the number of non-equivalent isogenies of degree $\ell^e$ with no backtracking starting from $E$. Note that $m_E$ is not exactly the same as $m_E$. This is because it possible for two non-equivalent isogenies of degree $\ell^e$ starting from $E$ to arrive to the same elliptic curve $E'$, thus forming a collision. We have shown that the number of such collisions is $O(1)$. Thus, $0 \leq m_E - m_E$ is $O(1)$, and

$$E_{E,E'}[\text{Coll}_{e'}(E, E')] := \frac{1}{n} \sum_{i=1}^{n} \frac{1}{m_{E_i}} \sum_{E' \in D} \text{Coll}_{e'}(E_i, E')$$

$$\leq \frac{1}{n} \sum_{i=1}^{n} \frac{\text{Coll}_{e'}(E_i)}{m_{E_i}}$$

$$\leq \frac{1}{n} \sum_{i=1}^{n} \frac{\text{Coll}_{e'}(E_i)}{m_{E_i} - (m_{E_i} - m_{E_i})}$$

(18)

Now, from the last line of Equation (18), we know that $E_{E}[\text{Coll}_{e'}(E)] \in O(1)$, $m_{E_i} = \ell^e + \ell^{e-1} \in \Theta(\sqrt{p})$ and $m_{E_i} - m_{E_i} \in O(1)$ for all $i$. Thus,

$$E_{E,E'}[\text{Coll}_{e'}(E, E')] \in O(1/\sqrt{p}).$$

\[\square\]

7 Conclusion

In this paper, we disputed the validity of the existing proofs for the special soundness property of the SIDH-based identification protocol $\text{ID}_{\text{SIDH}}$. In addition to providing concrete examples for two scenarios where the proposed extraction algorithm $\text{Ex}_{\text{SIDH}}$ fails, we also made a careful study of the number of collisions that occur in supersingular isogeny graphs. Our analysis shows that one can always expect the existence of certain single and double collisions, exactly those that make $\text{Ex}_{\text{SIDH}}$ fail. We also used our calculations to give upper bounds on the number of certain collisions in the supersingular isogeny graph $G_{p^2}(\ell)$ for fixed primes $p$ and $\ell$, thus providing a rigorous justification to some informal claims which have appeared in the literature. Our calculations are general and could be exploited in many contexts within Isogeny-based Cryptography. We leave the improvement of the bounds we provided on the number of collisions for future work, as this would require developing new number theoretic tools.

Despite the fact we showed that the issue with the previous special-soundness proofs does not impact the security of the SIDH-based signature scheme that have been proposed so far, formalising the security properties of $\text{ID}_{\text{SIDH}}$ seems to be important to avoid any misconceptions or unnecessary flaws in existing and future isogeny-based cryptosystems.
References


8 Appendix

In order to find a meaningful example for the scenario depicted in Section 3.2, we follow the same approach adopted by Onuki, Aikawa and Takagi \cite{32} do determine the existence of endomorphisms of prescribed degree in supersingular isogeny graphs for SIKE parameters. The general ideal is the following:

1. since \( p \equiv 15 \pmod{16} \) in our study case, we know the explicit description of \( \text{End}(E_0) \), we know that there is a unique 2-isogeny that maps \( E_0 \) to a distinct curve, which we call \( E_6 \), and by Lemma 1 of \cite{32} we know the explicit description of \( \text{End}(E_6) \). In particular, any endomorphism of \( E_6 \) can be written as
   \[
   \alpha = a + b(2i) + c\frac{1+j}{2} + d\frac{i+k}{4},
   \]
   with \( a, b, c, d \in \mathbb{Z} \) (at least one of which not divisible by \( \ell \)) and \( i, j, k \) such that \( i^2 = -1, j^2 = -p, ij = k = -ji \).

2. we then consider the corresponding norm equation
   \[
   \ell^n \equiv \frac{1}{16} \left( (4a + 2c)^2 + (8b + d)^2 + (4c^2 + d^2)p \right) \quad (19)
   \]
   where \( \ell^n \) is the norm of the endomorphism \( \alpha \). By Theorem 1 in \cite{32}, we can focus on integers \( n \) such that \( \frac{p+1}{16} < \ell^n \leq \ell^2 \), and by rearranging Equation \( 19 \) and replacing \( A = 4a + 2c \) and \( B = 8b + d \), we reduce the problem to solving the following Diophantine equation
   \[
   16\ell^n - (4c^2 + d^2)p = A^2 + B^2 \quad (20)
   \]
   with \( c \) and \( d \) not both 0, and \( A, B \) such that \( a = \frac{A-2c}{4} \in \mathbb{Z}, b = \frac{B-d}{8} \in \mathbb{Z} \).

The authors provide results for the first two parameter sets of SIKE, namely a collision of \( 3^{e_2} \)-isogenies for \( p^{434} \) and no collisions for \( p^{503} \). They could not examine the remaining parameter sets because of a lack of computational resources. With our implementation, we could investigate the two remaining parameter sets, running the code on a laptop mounting a Coffee Lake 2.2 GHz Intel i7 processor and 12GB of RAM. The result is that there exist no cycles (and thus no collisions) for \( p^{610} \) neither of degree \( 2^{e_1} \) nor \( 3^{e_2} \). For \( p^{751} \) there are no collisions of \( 2^{e_1} \)-isogenies, while there exist two pairs of colliding \( 3^{e_2} \)-isogenies, which we now present.

Let \( e_1 = 372, e_2 = 239 \) and \( p^{751} = 2^{e_1} \cdot 3^{e_2} - 1 \). Let \( \eta \) be a primitive element of \( \mathbb{F}_{p^{e_1}} \) with minimal polynomial \( x^2 + 1 \); given the \( E_6[3^{e_2}] \) torsion basis

\[
P_2 = \left\{ (8412791055464618046864991152137622977409634695645810034532197, 170119753830282998639717315851968048398639566308956037522600551905, 715721966592107851870816915611798787993698296708629746037186926706, 864439421128729040655630231, 2328323397749860472782995125935431844, 906025806012863155618480480941189811779357793741107399715583024436 \right\}
\]
the kernels of two distinct isogenies colliding in curves of \( j \)-invariant 367483248146527414370377344994980543168691447497832891959594848980770518959999
2095468628645832999930993954329220632137251116916741555717141232468270
095522907986594462515809975777276460889605379454261659270550521004
94910843 \cdot \eta + 21591927837304995784124378975633208329639309170229661310
7402562987941377339210306577392886841850729538629166862620501988346
3152635938117824557617902828758668352682365984162219942133146159837
6727469297778450637325459 are generated by the points

\[ K_1 = 193262648327552634362057829832895638371956375167641154459552249 \]
\[ 8055086645899366678565722236003305074981600179788901 \cdot P_2 + 398140788 \]
\[ 12909453073616618563048908428001097524649905086708128521669460981 \]
\[ 8660510059680733336819941831934627498 \cdot Q_2 \]

and

\[ K_2 = 8831526910052987014763504409048916666528834642174726130546931940 \]
\[ 78697241064121690098335862704399965485326427935366 \cdot P_2 + 398140788 \]
\[ 12909453073616618563048908428001097524649905086708128521669460981 \]
\[ 8660510059680733336819941831934627503 \cdot Q_2 \]

respectively. The other pair of isogenies colliding in curves of \( j \)-invariant 667988526030402783860739089287182477825842819805123828715659483073908421726
\[ 478925458196610102368094930593776867768968860922036926879290931 \]
\[ 61476119952617805089545375532460262696634387873185640825191720946820 \]
\[ 565156665988 \cdot \eta + 2159192778373049957841243789756332083296393091702296 \]
\[ 61310740526289784137733921030657739288684185072953862916686262050194 \]
\[ 88346315263593811782455761790282875866835268236598416221994213314616 \]
\[ 598376727469282977798450603737325459 \]

is given by the two kernels generated by

\[ K_1 = 193262648327552634362057829832895638371956375167641154459552249 \]
\[ 9805508664589936678565722236003305074981600179788901 \cdot P_2 + 1036601 \]
\[ 260520760882764971660274383964728991918771729449781337774031412 \]
91329669744484840555673967909895094673096769 \cdot Q_2

and

K_2 = 88315269100529870147635044900489166652883464217472613054693194
0786972410641216900983358627043999654855326427935366 \cdot P_2 + 103660
126052076088276479166027473839647278991981771729449781337774031412
91329669744484840555673967909895094673096764 \cdot Q_2

respectively.