THE SUPERSINGULAR ISOGENY PROBLEM IN TIME AND MEMORY $p^{1/3+o(1)}$

BENJAMIN WESOLOWSKI

Abstract. We prove that under a plausible heuristic assumption (on the smoothness of certain random integers), the supersingular isogeny problem can be solved in time and memory $p^{1/3+o(1)}$. This improves upon the previous best complexity of $p^{1/2} \cdot (\log p)^{O(1)}$.

This problem is arguably *the* central hard problem underlying isogeny-based cryptography, and the cost of its resolution is a major (and often the only) factor in the choice of secure parameters. The impact on concrete parameter sets remains to be clarified, as the asymptotic advantage of the new algorithm is mitigated by a superpolynomial overhead hiding in the $o(1)$ exponent, and by its high memory requirement.

1. Introduction

We prove the following theorem.

Theorem 1.1. *Assuming Heuristic 1, there is a Las Vegas algorithm which, given a supersingular elliptic curve $E/\mathbf{F}_{p^2}$, finds a non-scalar endomorphism $\alpha \in \mathrm{End}(E) \setminus \mathbf{Z}$ in expected time and memory $p^{1/3+o(1)}$.*

As an immediate corollary, applying the computational reductions [35, Theorem 1] and [35, Proposition 8.5], we deduce the following consequences.

Corollary 1.2. *Assuming Heuristic 1, there is a Las Vegas algorithm of expected complexity $p^{1/3+o(1)}$ for the supersingular endomorphism ring problem (given E supersingular, find a basis of $\mathrm{End}(E)$ — see Problem 2.3) and for the supersingular isogeny problem (given E and E' supersingular, find an isogeny $E \to E'$ — see Problem 2.4).*

These three polynomially-equivalent problems constitute the first entry in *The Isogeny Problems* [12]. The previous best algorithms to solve them had complexity $p^{1/2} \cdot (\log p)^{O(1)}$, starting with [21]. This complexity had stayed remarkably stable, with subsequent improvements only impacting the logarithmic cofactor [15, 24, 26, 40].

1.1. Impact on isogeny-based cryptography.

Finding isogenies or endomorphisms of supersingular elliptic curves is arguably the most critical problem in isogeny-based cryptography. The cost of its resolution is a major (and often the only) factor in the choice of secure parameters of schemes of this family, including:

- *(Cryptosystems affected by the attack)* the CGL hash function [14], the SQIsign digital signature family [7, 19, 20, 22, 34] (currently running in the NIST selection process [1] for post-quantum digital signatures), other signature schemes like GPS signatures [28] and PRISM [5], and the $\otimes$-MIKE key exchange [39].

The new algorithm does not constitute a complete break of these cryptosystems, but warrants a careful reevaluation of their concrete security parameters. Note that many other isogeny-based schemes remain *safely out of range* of this algorithm, including:

- *(Cryptosystems safe from the attack)* all group-action-based constructions like CSIDH [13] and (qt-)Pegasis [17, 18] (used in PQarrots [32], planned to be submitted to the NIST call for multi-party threshold schemes), as well as torsion-based key exchanges like M(D)-SIDH [25], FESTA [9] and POKÉ [8].

Indeed, other cryptanalytic algorithms dominate the security analysis of these schemes, already imposing a large enough choice for the characteristic p.

While the new algorithm improves the asymptotic cost from $p^{1/2} \cdot (\log p)^{O(1)}$ to $p^{1/3+o(1)}$, the practical impact is still unclear, as the overhead hiding in the $o(1)$ term is superpolynomial, much larger than the previous $(\log p)^{O(1)}$ cofactor. The algorithm parallelizes perfectly. However, its memory cost is essentially as high as the complexity $p^{1/3+o(1)}$, a serious obstacle for any deployment of the algorithm on instances of cryptographic size. It is currently unclear how to reduce the memory cost without increasing the time: the algorithm essentially resolves a claw-finding problem for two sets of size $N = p^{1/3+o(1)}$. The time-memory tradeoff of van Oorschot–Wiener [43] solves a claw-finding problem of this size in time essentially $\sqrt{N^3/w} = p^{1/2+o(1)}/w^{1/2}$ with memory w. This allows one to interpolate between the $p^{1/3+o(1)}$ high-memory algorithm presented here and the classic $p^{1/2+o(1)}$ algorithms with polynomial memory like [21].

Note that the van Oorschot–Wiener algorithm is also parallelizable, leading to an attack in time $\frac{p^{1/2+o(1)}}{w^{1/2}n}$ with memory w and n parallel processors. We refer the reader to [3, 16] for extensive practical considerations on the van Oorschot-Wiener algorithm (applied to a different context), and to [29] for similar considerations in the quantum setting (suggesting that quantum computation may only be advantageous to reduce the amount of memory, with the same time complexity).

We compute tentative bounds on the concrete cost of the algorithm in Section 4.1. Note that these estimates make optimistic assumptions on the actual cost of certain steps, hence should not be interpreted as accurate predictions.

1.2. **Proof-of-concept implementation.** The author is grateful to Lorenz Panny for swiftly developing a proof-of-concept implementation[1] [36] in SageMath [42].

1.3. **Previous work.** The computational problem of finding isogenies (or, equivalently, endomorphisms) between supersingular elliptic curves can be traced back to Kohel's thesis [30] in 1996: he describes an algorithm of complexity $p \cdot (\log p)^{O(1)}$ [30, Theorem 75] for finding endomorphisms.

The first claim of a complexity of $p^{1/2} \cdot (\log p)^{O(1)}$ for the isogeny problem appears in 2006 in the article [14], where the authors suggest to use a prime p of the order of 2^{256} to achieve 128 bits of security — an estimate that has been used up to this day. A memory-free algorithm with the same complexity was proposed in [21]: the Delfs–Galbraith algorithm.

In 2018, the first heuristic reductions [23] show that finding isogenies is essentially equivalent to finding endomorphisms; as a consequence, the earlier algorithms of complexity $p^{1/2} \cdot (\log p)^{O(1)}$ extend to the supersingular endomorphism problem. The article [24] (as the later refinement [26]) proposes a different algorithm to compute endomorphisms, and introduce an idea that will prove very fruitful: instead of looking for endomorphisms $E \to E$, they look for two distinct (separable) isogenies $\varphi_i : E \to E^{(p)}$ to the Frobenius conjugate of E, and deduce the endomorphism $\hat{\varphi}_2 \circ \varphi_1 \in \mathrm{End}(E)$. They show how to find such isogenies in time $p^{1/2} \cdot (\log p)^{O(1)}$ by generating random isogenies $E \to E'$ until E' is "adjacent" to its conjugate $E'^{(p)}$ — an event which occurs with probability $O(p^{-1/2})$. The idea of using Frobenius conjugates was reused in [40] to accelerate the Delfs–Galbraith algorithm, although still within the $p^{1/2} \cdot (\log p)^{O(1)}$ asymptotic.

1.4. **Overview of the algorithm.** The new algorithm starts from the same idea as [24, 26]: finding a separable isogeny $\varphi : E \to E^{(p)}$, where $E^{(p)}$ is the Frobenius conjugate of E. Then, the composition $\phi \circ \varphi \in \mathrm{End}(E)$ is an endomorphism of E, where $\phi : E^{(p)} \to E$ is the Frobenius isogeny. Since $\phi \circ \varphi$ has inseparable degree p (which is not square), it is a non-scalar endomorphism, and we are done.

Finding such a separable isogeny $\varphi : E \to E^{(p)}$ is generally considered a difficult task, and is in fact the bottleneck of the earlier algorithms [24, 26].

However, a recent result [4] proves that there always exists an isogeny $E \to E^{(p)}$ of degree at most $(p/2)^{1/3}$. If one is unlucky, that isogeny could have degree an (unknown) large prime

[1] Available at `https://yx7.cc/files/p-one-third.py`.

$\ell \approx (p/2)^{1/3}$, and finding it would be prohibitively expensive. However, if the degree factors as a product of small primes (i.e., the degree is *smooth*), then it factors as $\varphi = \eta \circ \psi$ where both η and ψ are smooth and of much smaller degree $\approx (p/2)^{1/6}$. One can then hope to find them by listing smooth isogenies from E and from $E^{(p)}$ of degree $\approx (p/2)^{1/6}$, until they "meet in the middle".

To meet this smoothness condition, one can re-randomise the instance of the problem by performing a random walk $E \to E'$, then hoping that the method works for E', and pulling back the solution to E through the walk. This is where we need a heuristic assumption.

1.5. **The heuristic assumption.** The assumption is of a standard kind: we assume that certain random integers have the same smoothness probability as uniformly random integers of the same size. Such heuristics are ubiquitous in computational number theory, yet notoriously difficult to prove.

Heuristic 1. Let p be a prime number, and let $E/\mathbf{F}_{p^2}$ be a uniformly random supersingular elliptic curve. The degree of the smallest isogeny $\varphi : E \to E^{(p)}$ is B-smooth with probability at least $u^{-u(1+o(1))}$, where $u = \frac{\log(p/2)}{3\log(B)}$ (uniformly as $p \to \infty$, if $(\log p)^\varepsilon < u < (\log p)^{1-\varepsilon}$ for a fixed constant ε).

Let us justify this heuristic by showing that $u^{-u+o(1)}$ is indeed the probability one would expect if $\deg(\varphi)$ were to behave like a uniformly random integer of the same size.

Definition 1.3. Fix any $X, B > 0$. An integer is B-smooth if all its prime factors are smaller than B. Write $S(X, B)$ for the set of B-smooth integers smaller than X, and $\Psi(X, B) = \#S(X, B)$.

We have the following classical theorem.

Theorem 1.4 ([10])**.** *Let $X, B > 0$, and $u = \frac{\log X}{\log B}$. Then, $\Psi(X, B) = Xu^{-u(1+o(1))}$ uniformly as $X \to \infty$, if $(\log X)^\varepsilon < u < (\log X)^{1-\varepsilon}$ for a fixed constant ε.*

Furthermore, we have the following bound on $\deg(\varphi)$.

Theorem 1.5 ([4])**.** *Let E be a supersingular elliptic curve over a finite field $\mathbf{F}_{p^2}$. Then there exists an isogeny from E to $E^{(p)}$ of degree less than or equal to $(p/2)^{1/3}$.*

Combining these two results, Heuristic 1 only asks that the degree of the smallest isogeny $E \to E^{(p)}$ has the smoothness probability that one would expect for a random integer of its size. In Section 4, we present computational experiments conducted in SageMath [42] supporting this assumption.

1.6. **Acknowledgements.** The author is grateful to Lorenz Panny for his proof-of-concept implementation [36] of the algorithm, and to Andrea Basso for suggesting a tighter choice of X in Algorithm 2 (replacing B with $\sqrt{B}$). The author further wishes to thank the entire SQIsign team [1], and the authors of [12] for their feedback and for insightful discussions — including proof-reading and suggestions from Luca De Feo, Damien Robert, and Francisco Rodríguez-Henríquez which helped improve the quality of this article.

The author was supported by the European Research Council under grant No. 101116169 (AGATHA CRYPTY), and the Agence Nationale de la Recherche under grants ANR-22-PETQ-0008 (PQ-TLS) and ANR-22-PNCQ-0002 (HQI).

2. Preliminaries

2.1. **Elliptic curves and isogenies.** Fix a finite field k of characteristic $p > 0$, with algebraic closure $\overline{k}$. An *elliptic curve* is an abelian variety of dimension 1. Given an elliptic curve E over k, we write $E(k)$ for its group of k-rational points. Given two elliptic curves E_1 and E_2 over a field k, an *isogeny* $\varphi : E_1 \to E_2$ is a non-constant rational map which is also a group homomorphism $E_1(\overline{k}) \to E_2(\overline{k})$. Its kernel $\ker(\varphi)$ is a finite subgroup of $E_1(\overline{k})$.

The *degree* of an isogeny is its degree as a rational map. The isogeny φ is *separable* if $\deg(\varphi) = \#\ker(\varphi)$. Any isogeny $\varphi : E \to E'$ can be factored as $\varphi = \psi \circ \varphi_{p^n}^E$, where $\varphi_{p^n}^E : E \to E^{(p^n)}$ is the p^n-Frobenius isogeny, and ψ is separable. We then have $\deg(\varphi) = p^n \cdot \#\ker(\varphi)$, and p^n is called

the *inseparable degree* of φ. When $\deg(\varphi) = \ell$ is a prime number, we say that φ is an *ℓ-isogeny*. When $\deg(\varphi) = 1$, then φ is an *isomorphism*.

Given any finite subgroup $G \subset E(\overline{k})$, there exists a separable isogeny $\varphi : E \to E'$ such that $\ker(\varphi) = G$. This isogeny φ is unique up to post-composition by an isomorphism, and we write $E/G := E'$. For any elliptic curve E and any prime number ℓ, there are $\ell + 1$ distinct ℓ-isogenies with domain E, up to post-composition by an isomorphism.

For any non-zero integer m, the multiplication-by-m map $[m] : E \to E$ is an isogeny of degree m^2. Any isogeny $\varphi : E \to E'$ has a unique *dual isogeny* $\hat{\varphi} : E' \to E$ such that $\hat{\varphi} \circ \varphi = [\deg(\varphi)]$.

The kernel of $[m] : E \to E$ is the m-torsion subgroup $E[m]$. The elliptic curve E is *supersingular* if $E[p^i] = \{0\}$ for all $i \geq 0$. Any supersingular elliptic curve over k is isomorphic to a curve defined over $\mathbf{F}_{p^2}$. In this article, we only consider supersingular elliptic curves defined over $\mathbf{F}_{p^2}$.

An *endomorphism* of E is an isogeny $E \to E$, or the zero morphism $[0] : E \to E$. The *endomorphism ring* $\mathrm{End}(E)$ is the collection of all endomorphisms of E. It forms a ring for point-wise addition, and for composition of maps. The map $\mathbf{Z} \to \mathrm{End}(E) : m \mapsto [m]$ is an injection, hence we can see $\mathbf{Z}$ as a subring of $\mathrm{End}(E)$. These elements $\mathbf{Z} \subset \mathrm{End}(E)$ are the *scalar endomorphisms* of E. When E is supersingular, the ring $\mathrm{End}(E)$ is a lattice of rank 4, in which $\mathbf{Z}$ is a primitive sublattice.

2.2. **Computing with isogenies.** There exist several ways to encode isogenies. They can be explicitly written down as rational maps, or as composable sequences of rational maps (*isogeny paths*). Alternatively, they can be indirectly represented by interpolation data (the image of a few points — sufficiently many to determine the isogeny). In studying computational problems involving isogenies, the exact way in which they are represented is often immaterial: all we need is any encoding that allows to store and evaluate the isogeny φ in polynomial time in $\log(\deg(\varphi))$. Such an encoding is called an *efficient representation* of φ. More formally:

Definition 2.1 (Efficient representation, following [44, Definition 1.3])**.** Let $\mathcal{A}$ be a polynomial time algorithm. It is an *efficient isogeny evaluator* if for any $D \in \{0,1\}^*$ such that $\mathcal{A}(\texttt{validity}, D)$ outputs $\top$, there exists an isogeny $\varphi : E \to E'$ (defined over some finite field $\mathbf{F}_q$) such that:

(1) on input $(\texttt{curves}, D)$, $\mathcal{A}$ returns (E, E'),
(2) on input $(\texttt{degree}, D)$, $\mathcal{A}$ returns $\deg(\varphi)$,
(3) on input $(\texttt{eval}, D, P)$ with $P \in E(\mathbf{F}_{q^k})$, $\mathcal{A}$ returns $\varphi(P)$.

If furthermore D is of polynomial size in $\log(\deg \varphi)$ and $\log q$, then D is an *efficient representation* of φ (with respect to $\mathcal{A}$).

Any representation D of an isogeny (efficient or not) can be converted to an efficient isogeny representation at the cost of polynomially many evaluations — a consequence of the isogeny interpolation algorithm [11, 31, 38]. This property came to be known as the *universality* of the interpolation representation (see [41, Lemma 7.3] for a formalisation of this notion, in the more general context of abelian varieties).

2.3. **Computational problems.** Isogeny-based cryptography rests on a variety of computational problems, all equivalent under polynomial-time reductions. The following are some of the most important ones. In these definitions, the isogenies are encoded in any efficient representation.

The following problem is the object of Theorem 1.1.

Problem 2.2 (OneEnd)**.** Given a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$, find an endomorphism in $\mathrm{End}(E) \setminus \mathbb{Z}$.

The following two problems are the objects of Corollary 1.2.

Problem 2.3 (EndRing)**.** Given a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$, find four endomorphisms generating $\mathrm{End}(E)$ as a $\mathbb{Z}$-module.

Problem 2.4 (Isogeny)**.** Given E and E' two supersingular elliptic curves defined over $\mathbb{F}_{p^2}$, compute an isogeny $\varphi : E \to E'$.

These three problems are computational equivalent under probabilistic polynomial-time reductions. This equivalence is the conclusion of a series of advances starting from heuristic reductions in [23], followed by rigorous reductions under the Generalised Riemann Hypothesis in [45], the introduction of OneEnd into the picture in [35], culminating in a larger network of unconditional equivalencies in [33].

3. Proof of the main result

Definition 3.1. Let E be an elliptic curve, and $X, B > 0$. We define the set of isogenies

$$L(E, X, B) = \{\psi : E \to E' \mid \psi \text{ has cyclic kernel and } \deg(\psi) \in S(X, B)\}.$$

Lemma 3.2. *For any $X > B > 0$, we have $\#L(E, X, B) \leq \Psi(X, B)X(\log(X) + 2)$.*

Proof. For any $x < X$, the number $I(x)$ of isogenies of degree x from E with cyclic kernel is at most $x(\log(x) + 2) \leq X(\log(X) + 2)$ (see the proof of [2, Lemma 5.7]). We then have $\#L(E, X, B) = \sum_{x \in S(X,B)} I(x) \leq \Psi(X, B)X(\log(X) + 2)$, which concludes the proof. □

Algorithm 1 Listing B-smooth isogenies

Require: A supersingular elliptic curve $E/\mathbf{F}_{p^2}$, and parameters B and X.
Ensure: The list $L(E, X, B)$ (Definition 3.1).

$L \leftarrow \emptyset$;
for $\ell \leq B$ **do**
  for $i = 1, \ldots, \lfloor \log_\ell(X) \rfloor$ **do**
    for $\psi \in L$ such that $\ell \deg(\psi) \leq X$ **do**
      Let E' be the codomain of $\psi : E \to E'$;
      $L_{E',\ell} \leftarrow \{(E'', \eta) \mid \eta : E' \to E''$ is an ℓ-isogeny and $\ker(\eta) \not\subset \ker(\hat{\psi})\}$ the list of non-backtracking ℓ-isogenies from E'. *Note that at this stage, it is sufficient to represent the isogenies η as sequences of elliptic curves $(E_0, E_1, \ldots)$, where each E_i is ℓ-isogenous to E_{i+1} for some $\ell \leq B$. In particular, one only needs to compute the codomain of each step η (via modular polynomials).*
      $L \leftarrow L \cup \{\eta \circ \psi \mid \eta \in L_{E',\ell}\}$;
    end for
  end for
end for
return L.

Lemma 3.3. *Algorithm 2 terminates in time $\Psi(X, B) \cdot X^{1+o(1)} \cdot B^{O(1)}$, where $X = B^{1/2} \cdot (p/2)^{1/6}$.*

Proof. From Lemma 3.2, the size of the table L is at most $\Psi(X, B)X(\log(X)+2) = \Psi(X, B)X^{1+o(1)}$. The cost of computing the list (with Algorithm 1) is dominated by the cost, for each batch of $(\leq)\ell + 1$ new entries, of computing these new entries: the non-backtracking ℓ-neighbors of E'. These are precisely the roots of the modular polynomial $\Phi_\ell(j(E'), x) \in \mathbf{F}_{p^2}[x]$ (see [27, Section 25.2]). Computing the polynomial $\Phi_\ell(j(E'), x) \in \mathbf{F}_{p^2}[x]$ and finding its $\ell + 1$ roots requires time [2] $(B + \log p)^{O(1)}$.

The cost of computing the list is thus at most

$$\#L \cdot (B + \log p)^{O(1)} = \Psi(X, B)X^{1+o(1)}B^{O(1)},$$

matching the claimed running time. The cost of the final loop through the table L is dominated by that previous computation. □

Lemma 3.4. *Suppose that the smallest isogeny $E \to E^{(p)}$ is B-smooth. Then, Algorithm 2 returns a separable isogeny $\varphi : E \to E^{(p)}$.*

[2] We do not presently investigate the best possible exponent $O(1)$, because this constant will be absorbed in other asymptotics. It is of course critical for a practical deployment of the algorithm. As suggested by Damien Robert, the fastest way to populate the list might be through *batched evaluations* of these modular polynomials.

Algorithm 2 Finding a separable isogeny to the conjugate

Require: A supersingular elliptic curve $E/\mathbf{F}_{p^2}$, a parameter $0 < B < p$.
Ensure: A separable isogeny $\alpha : E \to E^{(p)}$.
1: $X \leftarrow B^{1/2} \cdot (p/2)^{1/6}$;
2: $L(E, X, B) \leftarrow$ the list of B-smooth isogenies from E, of cyclic kernel and degree at most X (computed with Algorithm 1);
3: $L \leftarrow$ a table containing each entry $\psi : E \to E'$ of $L(E, X, B)$, keyed by the codomain E' (let us write them as pairs $(E', \psi) \in L$).
4: **for** $(E', \psi) \in L$ **do**
5: **if** $(E')^{(p)}$ is the key of an entry $((E')^{(p)}, \chi) \in L$ **then**
6: **return** $\hat{\chi}^{(p)} \circ \psi : E \to E^{(p)}$; *Note that if the entries of L were represented as sequences of elliptic curves (see the note in Algorithm 1), one may want to convert this final isogeny to a more explicit form: using Vélu's formulas for each step, then computing an efficient representation by interpolation.*
7: **end if**
8: **end for**
9: **return** $\perp$.

Proof. Write $\deg(\varphi) = \prod_{i=1}^{n} \ell_i$ the degree of φ (where the ℓ_i values are prime numbers smaller than B, not necessarily distinct). From Theorem 1.5, we have that $\deg(\varphi) \leq (p/2)^{1/3}$. Let k be the largest index such that $\prod_{i=1}^{k} \ell_i \leq X = B^{1/2}(p/2)^{1/6}$. Let $\varphi = \eta \circ \psi$ be any decomposition of φ such that $\deg(\psi) = \prod_{i=1}^{k} \ell_i$ and $\deg(\eta) = \prod_{i=k+1}^{n} \ell_i$. Note that by minimality of φ, it must have cyclic kernel, hence ψ and η also have cyclic kernel. By construction, $\deg(\psi) \leq X$, and $\deg(\psi)$ is B-smooth, and the domain of ψ is E, hence $\psi \in L(E, X, B)$.

Now, let us prove that $\deg(\eta) \leq X$. If $k = n$, then $\deg(\eta) = 1 \leq X$ and we are done. Otherwise, by maximality of k, we have $\deg(\psi)\ell_{k+1} > X$. Therefore

$$\deg(\eta) = \frac{\deg(\varphi)}{\deg(\psi)} \leq \frac{\ell_{k+1}(p/2)^{1/3}}{X} \leq \frac{B(p/2)^{1/3}}{B^{1/2}(p/2)^{1/6}} = B^{1/2}(p/2)^{1/6} = X.$$

Let $\chi = \hat{\eta}^{(p)}$. The codomain of η is $E^{(p)}$, so the domain of χ is $E^{(p^2)} = E$. Furthermore, $\deg(\chi) = \deg(\eta)$ is B-smooth and smaller than X, so $\chi \in L(E, X, B)$.

Finally, $\varphi = \eta \circ \psi$ so the codomain of ψ equals the domain of η; let it be E'. We have proved that both (E', ψ) and $(E'^{(p)}, \chi)$ are entries in the table L, so the algorithm will find a matching entry. □

Lemma 3.5. *Suppose that E is a uniformly random supersingular elliptic curve over $\mathbf{F}_{p^2}$. Assuming Heuristic 1, Algorithm 2 successfully returns an isogeny with probability at least $u^{-u(1+o(1))}$, where $u = \frac{\log(p/2)}{3\log(B)}$.*

Proof. By Lemma 3.4, the algorithm succeeds when the smallest isogeny $E \to E^{(p)}$ is B-smooth, and by Heuristic 1, this probability is at least $u^{-u(1+o(1))}$, where $u = \frac{\log(p/2)}{3\log(B)}$. □

Remark 1. Lemma 3.5 is a simple lower bound on the probability, and is not expected to be optimal. Indeed, it considers the single smallest isogeny $E \to E^{(p)}$, and estimates its smoothness probability; but there are generally multiple small (non-cyclic) isogenies $E \to E^{(p)}$, and it is sufficient for any one of them to be smooth. This has already been observed experimentally by Panny through his proof-of-concept implementation [36]. While practically relevant, this phenomenon is absorbed in the hidden term of the asymptotic complexity.

Proof of Theorem 1.1. The algorithm is described in Algorithm 3. It repeatedly calls Algorithm 2 on uniformly random curves E', with the smoothness parameter $B = e^{\frac{1}{3}\sqrt{\log(p/2)}} = p^{o(1)}$, until a success is hit. We fix the length n of the random walk to ensure that E' is indistinguishable from uniform. Following [37] or the more explicit [6, Lemma 14], we can ensure that $n = O(\log(p))$.

Algorithm 3 Finding a non-scalar endomorphism

Require: A supersingular elliptic curve $E/\mathbf{F}_{p^2}$.
Ensure: A non-scalar endomorphism $\alpha \in \mathrm{End}(E) \setminus \mathbf{Z}$.

1: $B \leftarrow e^{\frac{1}{3}\sqrt{\log(p/2)}}$; *Note that in practice, one may instead precompute an optimal choice of B minimizing the total expected cost of the algorithm.*
2: **while** `true` **do**
3: $\omega \leftarrow$ a non-backtracking random walk $\varphi : E \to E'$ of length n in the 2-isogeny graph *(see the proof for the choice of n)*;
4: $\varphi \leftarrow$ the output of Algorithm 2 on input E' and B;
5: **if** $\varphi \neq \perp$ **then**
6: Let $\phi : E'^{(p)} \to E'$ be the p-Frobenius isogeny from $E'^{(p)}$ to $E'^{(p^2)} = E'$;
7: **return** $\hat{\omega} \circ \phi \circ \varphi \circ \omega$;
8: **end if**
9: **end while**

By Lemma 3.5, and thanks to Heuristic 1, the success probability of one attempt is $\mathbb{P}_0 \geq u^{-u(1+o(1))}$, where $u = \frac{\log(p/2)}{3\log(B)} = \sqrt{\log(p/2)}$, hence

$$\mathbb{P}_0 = \sqrt{\log(p/2)}^{-\sqrt{\log(p/2)}(1+o(1))} = p^{\frac{-\log(\sqrt{\log(p/2)})\sqrt{\log(p/2)}}{\log p}(1+o(1))} = p^{o(1)}.$$

By Lemma 3.3, each attempt takes time $\Psi(X,B)X^{1+o(1)}B^{O(1)}$, where $X = B^{1/2} \cdot (p/2)^{1/6} = p^{1/6+o(1)}$. Writing $w = \frac{\log(X)}{\log(B)} = \frac{\frac{1}{2}\log B + \frac{1}{6}\log(p/2)}{\log B} = \frac{1}{2} + \frac{1}{2}\sqrt{\log(p/2)}$, Theorem 1.4 implies

$$\Psi(X,B) = Xw^{-w(1+o(1))} = p^{1/6+o(1)}p^{o(1)} = p^{1/6+o(1)}.$$

We deduce that each attempt costs $\Psi(X,B)X^{1+o(1)}B^{O(1)} = p^{1/6+o(1)}p^{1/6+o(1)}p^{o(1)} = p^{1/3+o(1)}$. The total expected cost of Algorithm 3 is therefore this latter quantity multiplied by $\mathbb{P}_0^{-1}$, which is $p^{1/3+o(1)}$, as claimed.

It remains to prove correctness. When a success occurs, we get a separable isogeny $\varphi : E' \to E'^{(p)}$ (with cyclic kernel). Now, $\phi : E'^{(p)} \to E'$ is the Frobenius isogeny. We clearly have $\phi \circ \varphi \in \mathrm{End}(E')$, and it has inseparable degree p (which is not a square), so it cannot be in the subring $\mathbf{Z}$. In particular, $\hat{\omega}\circ\phi\circ\varphi\circ\omega \in \mathrm{End}(E)$ is also non-scalar — which concludes the proof. □

4. Experimental results

4.1. **Rough estimation of the concrete cost.** Let us estimate a lower bound on the concrete cost of the algorithm (under the assumption that the bound on the success probability derived in Lemma 3.5 is tight). Consider B to be an optimizable parameter, and let $X = B^{1/2} \cdot (p/2)^{1/6}$. The size of the tables constructed in Algorithm 2 is at least

$$M = \Psi(X,B)X.$$

This is derived like the upper bound from Lemma 3.2, but using that the number of isogenies of degree d is *at least* d. Now, let us be conservative and assume that constructing a table costs a single $\mathbf{F}_{p^2}$-operation per entry, so a total of M $\mathbf{F}_{p^2}$-operations per table. In doing so, we anticipate that Algorithm 1 is not optimal. Now, the memory cost of the algorithm is $\approx M$, and its time cost is $\approx M/\mathbb{P}_0$ $\mathbf{F}_{p^2}$-operations, where $\mathbb{P}_0$ is the probability of success of one iteration of Algorithm 3. We estimate $\mathbb{P}_0$ as in Lemma 3.5.

With these estimates, and optimizing B for best time, we obtain the following costs:

- For $\log_2(p) \approx 256$ (SQIsign NIST-I): $\geq 2^{106.5}$ $\mathbf{F}_{p^2}$-operations and memory $\geq 2^{92.5}$; (previous methods: $\approx 2^{128}$ $\mathbf{F}_{p^2}$-operations and negligible memory);
- For $\log_2(p) \approx 384$ (SQIsign NIST-III): $\geq 2^{157.5}$ $\mathbf{F}_{p^2}$-operations and memory $\geq 2^{138.6}$; (previous methods: $\approx 2^{192}$ $\mathbf{F}_{p^2}$-operations and negligible memory);
- For $\log_2(p) \approx 512$ (SQIsign NIST-V): $\geq 2^{204.2}$ $\mathbf{F}_{p^2}$-operations and memory $\geq 2^{181.3}$; (previous methods: $\approx 2^{256}$ $\mathbf{F}_{p^2}$-operations and negligible memory);

- For $\log_2(p) \approx 576$: $\geq 2^{230.9}$ $\mathbf{F}_{p^2}$-operations and memory $\geq 2^{206.0}$;
  (previous methods: $\approx 2^{288}$ $\mathbf{F}_{p^2}$-operations and negligible memory);
- For $\log_2(p) \approx 768$: $\geq 2^{302.4}$ $\mathbf{F}_{p^2}$-operations and memory $\geq 2^{272.2}$;
  (previous methods: $\approx 2^{384}$ $\mathbf{F}_{p^2}$-operations and negligible memory).

We emphasize again that these numbers are obtained via a rough *under*estimation of the size of the table and the cost of its generation. On the other hand, we are assuming here that the bound of Lemma 3.5 is tight: the above numbers may be *over*estimating the factor $1/\mathbb{P}_0$ (see Remark 1).

4.2. **Supporting the heuristic assumption.** This section presents computational experiments conducted in SageMath [42] supporting Heuristic 1. Fix a prime number p. Given a random elliptic curve E, computing the degree of the shortest isogeny $E \to E^{(p)}$ is generally extremely costly. To perform experiments with large p, we exploit the Deuring correspondence: instead of a random elliptic curve E, we generate a random maximal order $\mathcal{O}$ in the quaternion algebra $B_{p,\infty}$ ramified at p and ∞. Through the Deuring correspondence, E corresponds to a maximal order $\mathcal{O}$. Then, the lattice of isogenies $\mathrm{Hom}(E, E^{(p)})$ (with the quadratic form deg) is isometric to the unique two-sided ideal P of reduced norm p in $\mathcal{O}$ (with the quadratic form $\frac{\mathrm{Nrd}}{p}$).

Therefore, we sample random maximal orders (uniformly random up to conjugation), compute the ideal P, and find the smallest vector in P. Its norm corresponds to the degree of the smallest isogeny $E \to E^{(p)}$ for a uniformly random E. We then factor this norm, and record its largest prime factor ℓ. The corresponding isogeny is B-smooth for any $B \geq \ell$.

After gathering a large number of data points, we are then able to compare the probability of the degree being B-smooth against the prediction of Heuristic 1. Our results for 100,000 samples over the field $\mathbf{F}_{p^2}$, $p = 5 \cdot 2^{248} - 1$ (i.e., the security level I of SQIsign [1]) are represented in Figure 1. The same experiment conducted for $p = 27 \cdot 2^{500} - 1$ (i.e., security level V of SQIsign [1]) with 10,000 samples is represented in Figure 2. In all cases, the data points closely align with the prediction of Heuristic 1.

In the case $p = 5 \cdot 2^{248} - 1$, the smoothest sample out of 100,000 is 12589-smooth. The predicted probability to be 12589-smooth is $\rho(u) \approx \frac{1}{69232}$, consistent with the observation.

In the case $p = 27 \cdot 2^{500} - 1$, the smoothest sample out of 10,000 is e^{23}-smooth. The predicted probability to be e^{23}-smooth is $\rho(u) \approx \frac{1}{3312}$, consistent with the observation.

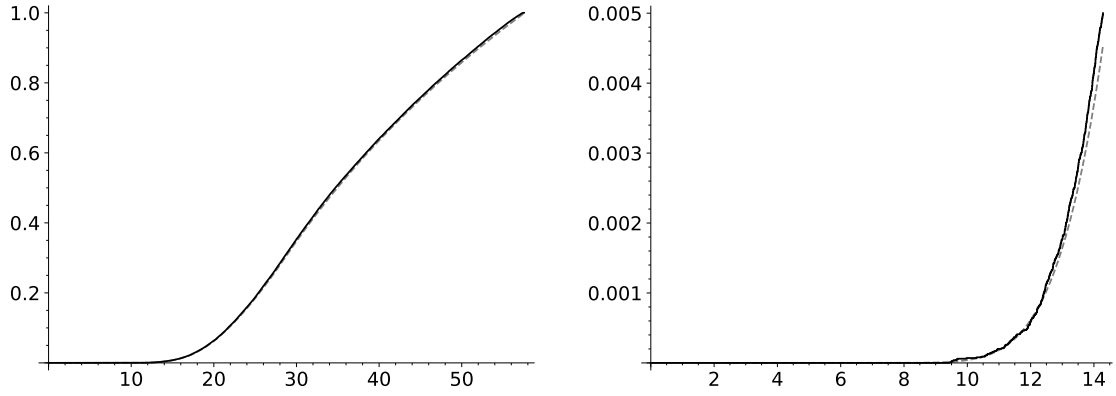


FIGURE 1. Cumulative distribution of the logarithm of the largest prime factor dividing the degree of the smallest isogeny $E \to E^{(p)}$, for 100,000 supersingular elliptic curves $E/\mathbf{F}_{p^2}$ sampled uniformly at random, for $p = 5 \cdot 2^{248} - 1$ (i.e., the prime used for the first security level of SQIsign [1]). For each abscissa x, the black line plots the proportion of samples which are e^x-smooth. The dotted grey line represents the theoretical prediction $\rho(u) \sim u^{-u(1+o(1))}$, where $u = \frac{\log(p/2)}{3x}$ (with ρ the Dickman-de Bruijn function).
The plot on the left represents the whole data, and the plot on the right is a focus on the 500 smoothest isogenies.

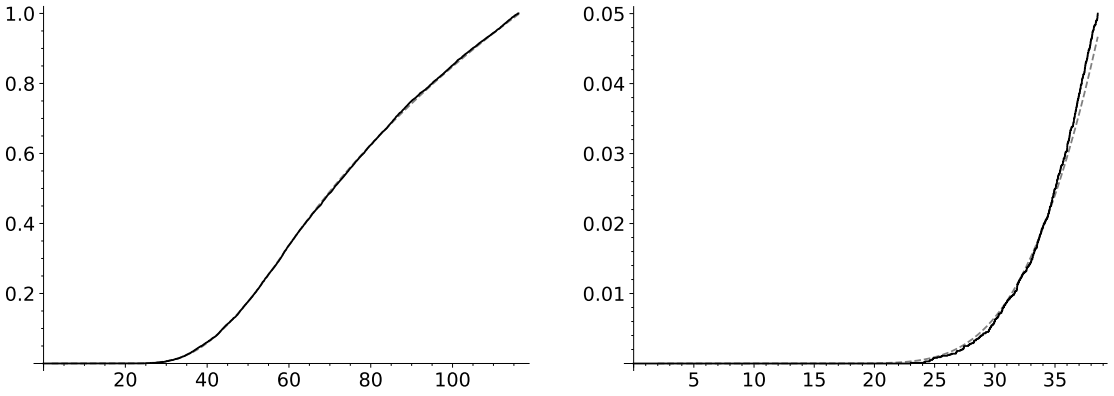


FIGURE 2. Same experiments as Figure 2, but for $p = 27 \cdot 2^{500} - 1$ (i.e., security level V of SQIsign [1]). The plot on the left represents the whole data (10,000 samples), and the plot on the right is a focus on the 500 smoothest isogenies.

REFERENCES

[1] Marius A. Aardal, Gora Adj, Diego F. Aranha, Andrea Basso, Isaac Andrés Canales Martínez, Jorge Chávez-Saab, Maria Corte-Real Santos, Pierrick Dartois, Luca De Feo, Max Duparc, Jonathan Komada Eriksen, Tako Boris Fouotsa, Décio Luiz Gazzoni Filho, Basil Hess, David Kohel, Antonin Leroux, Patrick Longa, Luciano Maino, Michael Meyer, Kohei Nakagawa, Hiroshi Onuki, Lorenz Panny, Sikhar Patranabis, Christophe Petit, Giacomo Pope, Krijn Reijnders, Damien Robert, Francisco Rodríguez-Henríquez, Sina Schaeffler, and Benjamin Wesolowski. *SQIsign*. Tech. rep. National Institute of Standards and Technology, 2025. URL: https://sqisign.org.

[2] Marius A. Aardal, Andrea Basso, Luca De Feo, Sikhar Patranabis, and Benjamin Wesolowski. "A Complete Security Proof of SQIsign". In: *Advances in Cryptology - CRYPTO 2025*. Ed. by Yael Tauman Kalai and Seny F. Kamara. Vol. 16005. Lecture Notes in Computer Science. Springer, 2025, pp. 190–222. DOI: 10.1007/978-3-032-01887-8_7. URL: https://doi.org/10.1007/978-3-032-01887-8_7.

[3] Gora Adj, Daniel Cervantes-Vázquez, Jesús-Javier Chi-Domínguez, Alfred Menezes, and Francisco Rodríguez-Henríquez. "On the Cost of Computing Isogenies Between Supersingular Elliptic Curves". In: *SAC 2018: 25th Annual International Workshop on Selected Areas in Cryptography*. Ed. by Carlos Cid and Michael J.: Jacobson Jr. Vol. 11349. Lecture Notes in Computer Science. Calgary, AB, Canada: Springer, Cham, Switzerland, 2019, pp. 322–343. DOI: 10.1007/978-3-030-10970-7_15.

[4] Yves Aubry, Roger Oyono, and Christelle Vincent. *Minimal degree of an isogeny between a supersingular elliptic curve and its conjugate*. 2026. arXiv: 2607.14624 [math.NT]. URL: https://arxiv.org/abs/2607.14624.

[5] Andrea Basso, Giacomo Borin, Wouter Castryck, Maria Corte-Real Santos, Riccardo Invernizzi, Antonin Leroux, Luciano Maino, Frederik Vercauteren, and Benjamin Wesolowski. "PRISM: Simple and Compact Identification and Signatures from Large Prime Degree Isogenies". In: *PKC 2025: 28th International Conference on Theory and Practice of Public Key Cryptography, Part III*. Ed. by Tibor Jager and Jiaxin Pan. Vol. 15676. Lecture Notes in Computer Science. Røros, Norway: Springer, Cham, Switzerland, 2025, pp. 300–332. DOI: 10.1007/978-3-031-91826-1_10.

[6] Andrea Basso, Giulio Codogni, Deirdre Connolly, Luca De Feo, Tako Boris Fouotsa, Guido Maria Lido, Travis Morrison, Lorenz Panny, Sikhar Patranabis, and Benjamin Wesolowski. "Supersingular Curves You Can Trust". In: *Advances in Cryptology – EUROCRYPT 2023*. Ed. by Carmit Hazay and Martijn Stam. Vol. 14005. Lecture Notes in Computer Science. Springer, 2023, pp. 405–437. DOI: 10.1007/978-3-031-30617-4_14. URL: https://doi.org/10.1007/978-3-031-30617-4_14.

[7] Andrea Basso, Pierrick Dartois, Luca De Feo, Antonin Leroux, Luciano Maino, Giacomo Pope, Damien Robert, and Benjamin Wesolowski. "SQIsign2D-West - The Fast, the Small, and the Safer". In: *Advances in Cryptology – ASIACRYPT 2024, Part III*. Ed. by Kai-Min Chung and Yu Sasaki. Vol. 15486. Lecture Notes in Computer Science. Kolkata, India: Springer, Singapore, Singapore, 2024, pp. 339–370. DOI: 10.1007/978-981-96-0891-1_11.

[8] Andrea Basso and Luciano Maino. "POKÉ: A Compact and Efficient PKE from Higher-Dimensional Isogenies". In: *Advances in Cryptology – EUROCRYPT 2025, Part II*. Ed. by Serge Fehr and Pierre-Alain Fouque. Vol. 15602. Lecture Notes in Computer Science. Madrid, Spain: Springer, Cham, Switzerland, 2025, pp. 94–123. DOI: 10.1007/978-3-031-91124-8_4.

[9] Andrea Basso, Luciano Maino, and Giacomo Pope. "FESTA: Fast Encryption from Supersingular Torsion Attacks". In: *Advances in Cryptology – ASIACRYPT 2023, Part VII*. Ed. by Jian Guo and Ron Steinfeld. Vol. 14444. Lecture Notes in Computer Science. Guangzhou, China: Springer, Singapore, Singapore, 2023, pp. 98–126. DOI: 10.1007/978-981-99-8739-9_4.

[10] E Rodney Canfield, Paul Erdös, and Carl Pomerance. "On a problem of Oppenheim concerning "factorisatio numerorum"". In: *Journal of number theory* 17.1 (1983), pp. 1–28.

[11] Wouter Castryck and Thomas Decru. "An Efficient Key Recovery Attack on SIDH". In: *Advances in Cryptology – EUROCRYPT 2023, Part V*. Ed. by Carmit Hazay and Martijn Stam. Vol. 14008. Lecture Notes in Computer Science. Lyon, France: Springer, Cham, Switzerland, 2023, pp. 423–447. DOI: 10.1007/978-3-031-30589-4_15.

[12] Wouter Castryck, Luca De Feo, Steven D. Galbraith, Péter Kutas, Krijn Reijnders, and Benjamin Wesolowski. *The Isogeny Problems*. Cryptology ePrint Archive, Paper 2026/1431. 2026. URL: https://eprint.iacr.org/2026/1431.

[13] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. "CSIDH: An Efficient Post-Quantum Commutative Group Action". In: *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security*. Ed. by Thomas Peyrin and Steven D. Galbraith. Vol. 11274. Lecture Notes in Computer Science. Springer, 2018, pp. 395–427. DOI: 10.1007/978-3-030-03332-3_15.

[14] Denis X. Charles, Kristin E. Lauter, and Eyal Z. Goren. "Cryptographic Hash Functions from Expander Graphs". In: *Journal of Cryptology* 22.1 (2009), pp. 93–113. ISSN: 1432-1378. DOI: 10.1007/s00145-007-9002-x.

[15] Maria Corte-Real Santos, Craig Costello, and Jia Shi. "Accelerating the Delfs-Galbraith Algorithm with Fast Subfield Root Detection". In: *Advances in Cryptology – CRYPTO 2022, Part III*. Ed. by Yevgeniy Dodis and Thomas Shrimpton. Vol. 13509. Lecture Notes in Computer Science. Santa Barbara, CA, USA: Springer, Cham, Switzerland, 2022, pp. 285–314. DOI: 10.1007/978-3-031-15982-4_10.

[16] Craig Costello, Patrick Longa, Michael Naehrig, Joost Renes, and Fernando Virdia. "Improved Classical Cryptanalysis of SIKE in Practice". In: *PKC 2020: 23rd International Conference on Theory and Practice of Public Key Cryptography, Part II*. Ed. by Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas. Vol. 12111. Lecture Notes in Computer Science. Edinburgh, UK: Springer, Cham, Switzerland, 2020, pp. 505–534. DOI: 10.1007/978-3-030-45388-6_18.

[17] Pierrick Dartois, Jonathan Komada Eriksen, Tako Boris Fouotsa, Arthur Herlédan Le Merdy, Riccardo Invernizzi, Damien Robert, Ryan Rueger, Frederik Vercauteren, and Benjamin

Wesolowski. “PEGASIS: Practical Effective Class Group Action using 4-Dimensional Isogenies”. In: *Advances in Cryptology – CRYPTO 2025, Part I*. Ed. by Yael Tauman Kalai and Seny F. Kamara. Vol. 16000. Lecture Notes in Computer Science. Santa Barbara, CA, USA: Springer, Cham, Switzerland, 2025, pp. 67–99. DOI: 10.1007/978-3-032-01855-7_3.

[18] Pierrick Dartois, Jonathan Komada Eriksen, Riccardo Invernizzi, and Frederik Vercauteren. “sfqt-sfPegasis: Simpler and Faster Effective Class Group Actions”. In: *Advances in Cryptology – EUROCRYPT 2026, Part IV*. Ed. by Joan Daemen and Emmanuel Thomé. Vol. 16545. Lecture Notes in Computer Science. Rome, Italy: Springer, Cham, Switzerland, 2026, pp. 636–665. DOI: 10.1007/978-3-032-25327-9_22.

[19] Pierrick Dartois, Antonin Leroux, Damien Robert, and Benjamin Wesolowski. “SQIsignHD: New Dimensions in Cryptography”. In: *Advances in Cryptology – EUROCRYPT 2024, Part I*. Ed. by Marc Joye and Gregor Leander. Vol. 14651. Lecture Notes in Computer Science. Zurich, Switzerland: Springer, Cham, Switzerland, 2024, pp. 3–32. DOI: 10.1007/978-3-031-58716-0_1.

[20] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. “SQISign: Compact Post-quantum Signatures from Quaternions and Isogenies”. In: *Advances in Cryptology – ASIACRYPT 2020, Part I*. Ed. by Shiho Moriai and Huaxiong Wang. Vol. 12491. Lecture Notes in Computer Science. Daejeon, South Korea: Springer, Cham, Switzerland, 2020, pp. 64–93. DOI: 10.1007/978-3-030-64837-4_3.

[21] Christina Delfs and Steven D Galbraith. “Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$”. In: *Designs, Codes and Cryptography* 78.2 (2016), pp. 425–440.

[22] Max Duparc and Tako Boris Fouotsa. “SQIPrime: A Dimension 2 Variant of SQISignHD with Non-smooth Challenge Isogenies”. In: *Advances in Cryptology – ASIACRYPT 2024, Part III*. Ed. by Kai-Min Chung and Yu Sasaki. Vol. 15486. Lecture Notes in Computer Science. Kolkata, India: Springer, Singapore, Singapore, 2024, pp. 396–429. DOI: 10.1007/978-981-96-0891-1_13.

[23] Kirsten Eisenträger, Sean Hallgren, Kristin E. Lauter, Travis Morrison, and Christophe Petit. “Supersingular Isogeny Graphs and Endomorphism Rings: Reductions and Solutions”. In: *Advances in Cryptology – EUROCRYPT 2018, Part III*. Ed. by Jesper Buus Nielsen and Vincent Rijmen. Vol. 10822. Lecture Notes in Computer Science. Tel Aviv, Israel: Springer, Cham, Switzerland, 2018, pp. 329–368. DOI: 10.1007/978-3-319-78372-7_11.

[24] Kirsten Eisenträger, Sean Hallgren, Chris Leonardi, Travis Morrison, and Jennifer Park. “Computing endomorphism rings of supersingular elliptic curves and connections to path-finding in isogeny graphs”. In: *ANTS XIV: Proceedings of the Fourteenth Algorithmic Number Theory Symposium, Open Book Series* 4.1 (2020), pp. 215–232.

[25] Tako Boris Fouotsa, Tomoki Moriya, and Christophe Petit. “M-SIDH and MD-SIDH: Countering SIDH Attacks by Masking Information”. In: *Advances in Cryptology – EUROCRYPT 2023, Part V*. Ed. by Carmit Hazay and Martijn Stam. Vol. 14008. Lecture Notes in Computer Science. Lyon, France: Springer, Cham, Switzerland, 2023, pp. 282–309. DOI: 10.1007/978-3-031-30589-4_10.

[26] Jenny Fuselier, Annamaria Iezzi, Mark Kozek, Travis Morrison, and Changningphaabi Namoijam. “Computing supersingular endomorphism rings using inseparable endomorphisms”. In: *Journal of Algebra* 668 (2025), pp. 145–189.

[27] Steven D Galbraith. *Mathematics of public key cryptography*. Cambridge University Press, 2012.

[28] Steven D. Galbraith, Christophe Petit, and Javier Silva. “Identification Protocols and Signature Schemes Based on Supersingular Isogeny Problems”. In: *Advances in Cryptology – ASIACRYPT 2017, Part I*. Ed. by Tsuyoshi Takagi and Thomas Peyrin. Vol. 10624. Lecture Notes in Computer Science. Hong Kong, China: Springer, Cham, Switzerland, 2017, pp. 3–33. DOI: 10.1007/978-3-319-70694-8_1.

[29] Samuel Jaques and John M. Schanck. “Quantum Cryptanalysis in the RAM Model: Claw-Finding Attacks on SIKE”. In: *Advances in Cryptology – CRYPTO 2019, Part I*. Ed. by

Alexandra Boldyreva and Daniele Micciancio. Vol. 11692. Lecture Notes in Computer Science. Santa Barbara, CA, USA: Springer, Cham, Switzerland, 2019, pp. 32–61. DOI: 10.1007/978-3-030-26948-7_2.

[30] David Kohel. "Endomorphism rings of elliptic curves over finite fields". PhD thesis. University of California, Berkeley, 1996. ISBN: 978-0591-32123-4.

[31] Luciano Maino, Chloe Martindale, Lorenz Panny, Giacomo Pope, and Benjamin Wesolowski. "A Direct Key Recovery Attack on SIDH". In: *Advances in Cryptology – EUROCRYPT 2023, Part V*. Ed. by Carmit Hazay and Martijn Stam. Vol. 14008. Lecture Notes in Computer Science. Lyon, France: Springer, Cham, Switzerland, 2023, pp. 448–471. DOI: 10.1007/978-3-031-30589-4_16.

[32] Marius A. Aardal and Shahla Atapoor and Karim Baghery and Andrea Basso and Xavier Bonnetain and Giacomo Borin and Daniele Cozzo and Pierrick Dartois and Luca De Feo and Max Duparc and Jonathan K. Eriksen and Tako Boris Fouotsa and Arthur Herlédan Le Merdy and Riccardo Invernizzi and Samuel Jaques and Yi-Fu Lai and Dania Lazzarini and Jason T. LeGrow and Luciano Maino and Jonas Meers and Michael Meyer and Sikhar Patranabis and Robi Pedersen and Giacomo Pope and Doreen Riepel and Damien Robert and Ryan Rueger and Sina Schaeffler and André Schrottenloher and Frederik Vercauteren. *PQarrots: Macaw, Kea and Kakapo; Threshold primitives from isogeny-based group actions*. NIST First Call for Multi-Party Threshold Schemes, Preview Writeup. Accessed: July 20 2026. 2026. URL: https://csrc.nist.gov/csrc/media/Projects/threshold-cryptography/documents/TCall-1/PQarrots-PW01.pdf.

[33] Arthur Herlédan Le Merdy and Benjamin Wesolowski. "Unconditional Foundations for Supersingular Isogeny-Based Cryptography". In: *TCC 2025: 23rd Theory of Cryptography Conference, Part III*. Ed. by Benny Applebaum and Huijia (Rachel) Lin. Vol. 16270. Lecture Notes in Computer Science. Aarhus, Denmark: Springer, Cham, Switzerland, 2025, pp. 266–297. DOI: 10.1007/978-3-032-12296-4_9.

[34] Kohei Nakagawa, Hiroshi Onuki, Wouter Castryck, Mingjie Chen, Riccardo Invernizzi, Gioella Lorenzon, and Frederik Vercauteren. "SQIsign2D-East: A New Signature Scheme Using 2-Dimensional Isogenies". In: *Advances in Cryptology – ASIACRYPT 2024, Part III*. Ed. by Kai-Min Chung and Yu Sasaki. Vol. 15486. Lecture Notes in Computer Science. Kolkata, India: Springer, Singapore, Singapore, 2024, pp. 272–303. DOI: 10.1007/978-981-96-0891-1_9.

[35] Aurel Page and Benjamin Wesolowski. "The Supersingular Endomorphism Ring and One Endomorphism Problems are Equivalent". In: *Advances in Cryptology – EUROCRYPT 2024, Part VI*. Ed. by Marc Joye and Gregor Leander. Vol. 14656. Lecture Notes in Computer Science. Zurich, Switzerland: Springer, Cham, Switzerland, 2024, pp. 388–417. DOI: 10.1007/978-3-031-58751-1_14.

[36] Lorenz Panny. *Proof-of-concept implementation of Benjamin Wesolowski's 2026 attack against the OneEnd problem with time complexity $p^{1/3+o(1)}$*. Python script. Accessed: July 20 2026. 2026. URL: https://yx7.cc/files/p-one-third.py.

[37] Arnold K Pizer. "Ramanujan graphs and Hecke operators". In: *Bulletin of the American Mathematical Society* 23.1 (1990), pp. 127–137.

[38] Damien Robert. "Breaking SIDH in Polynomial Time". In: *Advances in Cryptology – EUROCRYPT 2023, Part V*. Ed. by Carmit Hazay and Martijn Stam. Vol. 14008. Lecture Notes in Computer Science. Lyon, France: Springer, Cham, Switzerland, 2023, pp. 472–503. DOI: 10.1007/978-3-031-30589-4_17.

[39] Damien Robert. *The module action for isogeny based cryptography*. Cryptology ePrint Archive, Paper 2024/1556. 2024. URL: https://eprint.iacr.org/2024/1556.

[40] Maria Corte-Real Santos, Arthur Herlédan Le Merdy, Joseph Macula, Michael Meyer, Travis Morrison, and Eli Orvis. *Algorithms for solving the isogeny problem with oriented elliptic curves*. Cryptology ePrint Archive, Paper 2026/1219. 2026. URL: https://eprint.iacr.org/2026/1219.

[41] Maria Corte-Real Santos, Etienne Piasecki, and Benjamin Wesolowski. *A computational framework for principally polarized abelian varieties and applications*. Cryptology ePrint Archive, Paper 2026/1142. 2026. URL: https://eprint.iacr.org/2026/1142.

[42] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 10.7)*. https://www.sagemath.org. Computer software. 2025.

[43] Paul C. Van Oorschot and Michael J. Wiener. "Parallel collision search with cryptanalytic applications". In: *Journal of cryptology* 12.1 (1999), pp. 1–28.

[44] Benjamin Wesolowski. "Random Walks in Number-theoretic Cryptology". HDR Thesis. ENS Lyon, 2024. URL: https://bweso.com/hdr.pdf.

[45] Benjamin Wesolowski. "The supersingular isogeny path and endomorphism ring problems are equivalent". In: *62nd Annual Symposium on Foundations of Computer Science*. Denver, CO, USA: IEEE Computer Society Press, 2022, pp. 1100–1111. DOI: 10.1109/FOCS52979.2021.00109.

ENS de Lyon, CNRS, UMPA, UMR 5669, Lyon, France