ALGEBRAIC MODELINGS OF THE SUPERSINGULAR ISOGENY PROBLEM

ALESSIO CAMINATA, ANDREA SANGUINETI, AND SILVIA SCONZA

Abstract. We present a new algebraic modeling of the Supersingular Isogeny Problem as a system of multivariate polynomial equations, in the case where the elliptic curves are connected by an isogeny whose degree is a power of 2 or 3. This modeling relies on Renes formulas for elliptic curves in Montgomery form (degree 2) or triangular form (degree 3). We investigate several algebraic properties of these systems: we prove that they are zero-dimensional, compute the dimension of their highest degree part, and show that they are not in generic coordinates. Experimental results show that solving these systems via Gröbner basis techniques is significantly faster than solving the algebraic modeling with modular polynomials.

Introduction

We fix a prime number $p > 3$ and let E and E' be two supersingular elliptic curves defined over $\mathbb{F}_{p^2}$ such that there exists a degree d isogeny $\varphi : E \to E'$. The *Supersingular Isogeny Problem (SIP)* asks to find φ. When d and p are sufficiently large, a random instance of this problem is believed to be computationally difficult to solve, even using a quantum computer. For this reason, it has been used as the underlying problem for several post-quantum cryptographic schemes, such as the signature scheme SQIsign [20], which, at the time of writing, is admitted to Round 3 of the NIST call for post-quantum signature schemes. For this reason, the SIP has been widely studied and several algorithms and methods have been proposed in the literature. We note that, since the degree of isogenies is multiplicative under composition, the main difficulty in solving the SIP arises when the degree d is a power of a prime $\ell \neq p$. In this setting, the most efficient approaches exploit structural properties of the graph of ℓ-isogenies between supersingular elliptic curves [15, 17, 21, 26].

Given the growing importance of post-quantum cryptography, both the cryptanalysis of proposed schemes and the study of the hardness of their underlying problems have received increasing attention in recent years. A comprehensive security assessment requires considering attacks originating from different areas of post-quantum cryptography. In this context, algebraic modeling and algebraic attacks have emerged as important tools. In the literature, several algebraic models have been proposed and studied for problems arising in code-based cryptography [11, 19, 32, 38] and lattice-based cryptography [2, 3, 42]. In contrast, algebraic modeling of problems in isogeny-based cryptography has received comparatively less attention [44].

A natural approach to modeling the Supersingular Isogeny Problem as a system of multivariate polynomial equations is via modular polynomials [48, §10]. Given a positive integer $N \neq p$ the N-th modular polynomial $\Phi_N(X, Y)$ is a polynomial (with integer coefficients) with the property that $\Phi_N(j_1, j_2) = 0$ if and only if j_1, j_2 are the j-invariants of elliptic curves that are related by an isogeny of degree N. So, if $N = \ell^e$, where ℓ is a prime number, given the j-invariants $j_{\text{start}}, j_{\text{finish}}$ of two elliptic curves $E_{\text{start}}, E_{\text{finish}}$ connected by a N-isogeny φ, we can reduce the SIP to several smaller instances of the SIP in degree ℓ by solving a multivariate polynomial system (see Polynomial system 1) with modular polynomials, whose solutions represent all possible paths from

Key words and phrases. Supersingular Isogeny Problem, Gröbner bases, solving degree, algebraic modeling.

E_{start} to E_{finish} in the ℓ-isogeny graph. This approach has been studied in the paper [44]. There, the authors propose the algebraic model and study the complexity of solving the corresponding polynomial system via Gröbner basis techniques.

In this paper, we propose two distinct algebraic models for the SIP: one for isogenies whose degree is a power of 2, and one for isogenies whose degree is a power of 3. These two cases are the most relevant for cryptographic applications. The main ideas, which originate from the works of Renes [35], Burdges–De Feo [10], and Costello–Hisil [16], are as follows. If an elliptic curve E is given in Montgomery form, then the 2-isogenies with domain E can be described explicitly in terms of the x-coordinates of the 2-torsion points of E. More precisely, if $\alpha \in \mathbb{F}_{p^2}$ is the x-coordinate of a 2-torsion point of E, then one can construct a 2-isogeny $\varphi_\alpha : E \to E(\alpha)$, where $E(\alpha)$ can also be expressed in Montgomery form, allowing us to iteratively describe also the 2-isogenies with domain $E(\alpha)$. Moreover, the 2-isogeny with kernel $\langle(0,0)\rangle$ is the dual isogeny of φ_α. By proceeding in this way, we can explicitly construct a non-backtracking path (a sequence in which no two consecutive isogenies are dual to each other) of 2-isogenies starting from E. We use these formulas to derive multivariate polynomials, which we call *Renes polynomials* (Definition 3.7), playing a role analogous to that of modular polynomials for curves in Montgomery form. Using these polynomials, we construct a system of polynomial equations modeling the SIP for curves in Montgomery form and isogenies of degree a power of 2 (Polynomial System 2). One key difference with respect to the modular polynomials setting is that, once a j-invariant is fixed, there exist several non-isomorphic elliptic curves in Montgomery with that j-invariant. As a consequence, the resulting polynomial system contains a polynomial of degree 12, which significantly impacts the efficiency of solving the system. However, this issue can be mitigated by decomposing the problem into six quadratic systems (Polynomial System 3), whose computations can be parallelized.

The case of degree 3 is analogous, with the key difference that, in order to explicitly describe the 3-isogenies with domain an elliptic curve E, the curve must be expressed in triangular form. As in the degree 2 setting, the central idea is to ensure that the point $(0,0)$ is a 3-torsion point. In this framework, the 3-isogenies with kernel $\langle(0,0)\rangle$ correspond to the dual isogenies along the path, and we can exclude them to obtain a non-backtracking path. As before, there exist multiple non-isomorphic curves in triangular form sharing the same j-invariant. Consequently, we construct 12 quadratic systems (Polynomial System 5), whose computations can be parallelized.

Once the algebraic models have been constructed, we analyze the complexity of solving them using Gröbner basis techniques and compare it with that of systems based on modular polynomials. A key parameter for estimating the complexity of solving a multivariate polynomial system $\mathcal{F}$ via linear-algebra-based Gröbner basis algorithms is the solving degree, denoted $\mathrm{sd}(\mathcal{F})$. Informally, the solving degree is the highest degree reached by the polynomials appearing during the computation of a Gröbner basis using such algorithms. Estimating this degree without explicitly solving the system, and thus understanding how it grows with respect to the input parameters (such as the number of variables, the number of equations, and their degrees), is notoriously difficult. Several invariants have been introduced to address this problem, including the degree of regularity [4, 39] and the Castelnuovo-Mumford regularity [12]. The degree of regularity is defined when the highest-degree homogeneous component $\mathcal{F}^{\text{top}}$ of the system is zero-dimensional. However, for the systems arising from the algebraic modeling of the SIP, both with modular and Renes polynomials, we show that this condition does not hold (Proposition 5.4). On the other hand, when a system is in generic coordinates, the solving degree is bounded above by the Castelnuovo-Mumford regularity [12], a fundamental invariant in commutative algebra and algebraic geometry. Nevertheless, we prove that the systems under consideration are not in generic coordinates (Proposition 5.7).

Finally, we perform computational experiments to compare both the running times and the solving degrees of the polynomial systems arising from modular and Renes polynomials (see Section 6). The results show that the approach based on Renes polynomials is significantly faster and typically yields a strictly smaller solving degree. For instance, for a 24-bit prime p, we are able to solve the SIP for isogenies of degree up to 2^{15} with a solving degree of 6. In contrast, for the same parameters using modular polynomials, computations become infeasible beyond degree 2^{12}, with a solving degree of 9.

Structure of the paper. In Section 1, we recall some definitions, notations, and results on elliptic curves and polynomial system solving via Gröbner bases. In Section 2, we recall the algebraic modeling with modular polynomials from [44]. In Section 3 and Section 4 we present our algebraic modelings with Renes polynomials in degrees 2 and 3 respectively. In Section 5, we prove some algebraic properties of these systems and in Section 6 we perform some experiments to compare them.

Acknowledgments. We thank Luca De Feo for bringing Renes' work [35] to our attention. We also thank Giulio Codogni, Ignacio M. Jiménez, Guido Lido, and Marzio Mula for several helpful comments on an earlier version of this paper.

A. Caminata and A. Sanguineti are supported by the PRIN PNRR 2022 grant P2022J4HRR "Mathematical Primitives for Post Quantum Digital Signatures" and by the MUR Excellence Department Project awarded to Dipartimento di Matematica, Università di Genova, CUP D33C23001110001. A. Caminata is supported by the PRIN 2022 grant 2022K48YYP "Unirationality, Hilbert schemes, and singularities".

S. Sconza's research is supported by armasuisse Science and Technology.

1. Preliminaries

Throughout the paper p denotes a prime number greater than 3.

1.1. **Isogeny Problem.** An *elliptic curve* E over a finite field $\mathbb{F}_q$ of characteristic p is a projective plane curve which is defined (in affine coordinates) by a *Weierstrass equation* $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{F}_q$ and *discriminant* $\Delta(E) = 4a^3 + 27b^2 \neq 0$. Its *$j$-invariant* is defined as $j(E) = 1728\frac{4a^3}{4a^3+27b^2}$. Two elliptic curves have the same j-invariant if and only if they are isomorphic (as algebraic curves) over the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$. The set of points of E is endowed with an addition law that makes it into an abelian group whose identity element is $O_E = [0 : 1 : 0]$, the unique point at infinity of the curve. The set $E(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points of E forms a subgroup.

An *isogeny* φ between two elliptic curves E and E' is a morphism $\varphi\colon E \to E'$, which is also a group homomorphism of the underlying group structures. For example, the *multiplication-by-m* map $[m]\colon E \to E$ is an isogeny. Its kernel, denoted by $E[m]$, is the set of m-torsion points of E. The degree of an isogeny is its degree as morphism. We will write ℓ-isogeny to indicate an isogeny of degree ℓ. The degree is multiplicative under composition of isogenies: if φ and ψ are isogenies such that $\varphi \circ \psi$ is defined, then $\deg(\varphi \circ \psi) = \deg(\varphi) \cdot \deg(\psi)$. We say that an isogeny is *cyclic* if its kernel is a cyclic group. We recall that an isogeny is uniquely determined by its kernel, up to isomorphism. For example, when the degree of the isogeny is not divisible by the characteristic of the field, we have $\deg(\varphi) = |\ker(\varphi)|$. In particular, if an isogeny has prime degree, then it is necessarily cyclic. Finally, we recall that given an isogeny $\varphi\colon E \to E'$ of degree ℓ, there exists an isogeny $\widehat{\varphi}\colon E' \to E$ of degree ℓ such that $\varphi \circ \widehat{\varphi} = [\ell]$ and $\widehat{\varphi} \circ \varphi = [\ell]$. Such an isogeny $\widehat{\varphi}$ is called the *dual isogeny* of φ.

Elliptic curves can be partitioned into two disjoint families: ordinary and supersingular elliptic curves. These can be defined in many equivalent ways. For example, we say that an elliptic curve E is *supersingular* if the subgroup of p-torsion points (where p is the characteristic of the base field $\mathbb{F}_q$) is trivial, i.e., $E[p] = \{O_E\}$. Otherwise, E is said to be *ordinary* and in this case $E[p] \cong \mathbb{Z}/p\mathbb{Z}$. A distinctive property of supersingular elliptic curves is that their j-invariants are always defined over $\mathbb{F}_{p^2}$. Whether an elliptic curve is ordinary or supersingular is an isogeny invariant. Namely, if $\varphi\colon E \to E'$ is an isogeny, then E is supersingular (resp. ordinary) if and only if E' is supersingular (resp. ordinary).

We are interested in the following problem.

Problem 1.1 (SIP: Supersingular Isogeny Problem)**.** Given E and E' two supersingular elliptic curves defined over $\mathbb{F}_q$, find (if it exists) an isogeny $\varphi\colon E \to E'$ of degree ℓ.

A key observation in the study of this problem is that any isogeny of degree ℓ can be decomposed into a sequence of isogenies of prime degree, by factoring ℓ into its prime components. Thus, it is often enough to focus on the Supersingular Isogeny Problem when ℓ is a prime power. In practice, chains of isogenies of prime degree 2 or 3 are often considered. Notice that in this setup all the elliptic curves in the intermediate steps of the chain are supersingular.

1.2. **Polynomial system solving via Gröbner bases.** In this section, we give a brief overview on how to solve polynomial systems by using Gröbner bases and the related relevant invariants.

For consistency with rest of the paper, we fix a finite field $\mathbb{F}_q$ (although everything in this section can be defined over any field), and we work over the polynomial ring $\mathbb{F}_q[x_1, \dots, x_n]$. Let T be the set of terms (i.e., monic monomials) of $\mathbb{F}_q[x_1, \dots, x_n]$. A *term order* $<$ on T is a total order which is compatible with the multiplicative structure, that is $m_1 < m_2$ implies $m_1 m < m_2 m$, and $m_1 \mid m_2$ implies $m_1 \leq m_2$. Given a polynomial f we denote by $\mathrm{LT}_<(f)$ its leading term, i.e., the largest term of f with respect to the chosen term order. Similarly, given an ideal I, we denote by $\mathrm{LT}_<(I) = (\mathrm{LT}_<(f) : f \in I)$, the *initial ideal* of I, which is generated by all leading terms of polynomials of I. If I is generated by polynomials $f_1, \dots, f_m$, then it holds $(\mathrm{LT}_<(f_1), \dots, \mathrm{LT}_<(f_m)) \subseteq \mathrm{LT}_<(I)$, but the inclusion might be strict in general. When equality holds, we say that $f_1, \dots, f_m$ is a *Gröbner basis* of I (with respect to the given term order).

Gröbner bases have a tight connection with polynomial system solving. Namely, the solutions of a zero-dimensional polynomial system $f_i(x_1, \dots, x_n) = 0$ $(i = 1, \dots, m)$ can be read off from a lexicographic Gröbner basis of the corresponding ideal $(f_1, \dots, f_m)$ in $\mathbb{F}_q[x_1, \dots, x_n]$ thanks to the Shape Lemma and its extensions (see e.g. [12]).

There are several methods to compute Gröbner bases in practice. The oldest one is Buchberger's algorithm [9]. Some of the fastest methods in use today are the *linear-algebra algorithms*, such as F4 [23], F5 [24], and XL [18]. The core idea of these algorithms is to compute the Gröbner basis by doing Gaussian reduction on certain matrices, called *Macaulay matrices*. Let $d \in \mathbb{Z}_{\geq 1}$, and let $\mathrm{T}_{\leq d}$ be the set of terms in $\mathbb{F}_q[x_1, \dots, x_n]$ of degree less than or equal to d. The *Macaulay matrix* $\mathcal{M}_{\leq d}$ of $\mathcal{F} = \{f_1, \dots, f_m\}$ is a matrix whose rows are indexed by the polynomials $t_{k,h} f_k$, where $k = 1, \dots, m$ and $t_{k,h}$ ranges through all terms in $\mathrm{T}_{\leq d}$ such that $\deg(t_{k,h} f_k) \leq d$, and columns are indexed by the terms in $\mathrm{T}_{\leq d}$. The (i, j) entry of $\mathcal{M}_{\leq d}$ is the coefficient of the j-th term in the polynomial of the i-th row. When d is large enough, performing Gaussian elimination on $\mathcal{M}_{\leq d}$ provides a Gröbner basis of $(\mathcal{F})$. The smallest d such that this happens is called *solving degree* of $\mathcal{F}$ and we denote it by $\mathrm{sd}_{\leq}(\mathcal{F})$. We often omit the subscript $\leq$ when the term order is clear from the context.

In practice, the linear-algebra-based methods mentioned above make extensive use of this idea, carefully selecting suitable submatrices of the Macaulay matrices in order to minimize the number of

zero entries and avoid unnecessary computations. Moreover, although a Gröbner basis with respect to the lexicographic order is ultimately required to extract the solutions of the system, it is often more efficient to first compute a Gröbner basis with respect to the degree-reverse lexicographic order, and then convert it to lexicographic form using the FGLM algorithm [25] or related techniques. That being said, the main computational bottleneck in solving such systems is typically the Gaussian elimination performed on the largest Macaulay matrix encountered during the computation. The size of this matrix depends on the number of variables n, the number of polynomials m, and the solving degree $\mathrm{sd}_{\leq}(\mathcal{F})$. For this reason, it is crucial to determine, or at least accurately estimate, the solving degree of a polynomial system and understand how it scales with respect to the system's parameters. However, computing the solving degree a priori is generally very difficult. To address this issue, several alternative invariants, often more tractable, have been introduced and related to the solving degree, including the degree of regularity [4], the last fall degree [13, 28], the first fall degree [22], and the Castelnuovo-Mumford regularity [12].

2. Algebraic Modeling with Modular Polynomials

The first natural way to produce an algebraic modeling for the Supersingular Isogeny Problem is using modular polynomials. This was explored by Takahashi et al. [44]. We briefly recall this modeling, which will serve us as a comparison.

2.1. Background on modular polynomials.

We fix a finite field $\mathbb{F}_q$ of characteristic p and let $N > 1$ be an integer coprime with p. Then, there exists a polynomial $\Phi_N \in \mathbb{Z}[X, Y]$, called *$N$-th modular polynomial*, such that for all $j_1, j_2 \in \mathbb{F}_q$ it holds that $\Phi_N(j_1, j_2) = 0$ if and only if j_1, j_2 are the j-invariants of elliptic curves over $\mathbb{F}_q$ that are related by an isogeny of degree N defined over $\overline{\mathbb{F}}_p$ (see e.g. [29, §11.9]).

In the following proposition we collect some useful properties of modular polynomials.

Proposition 2.1. *Let $N > 1$ be an integer. The modular polynomial $\Phi_N(X, Y) \in \mathbb{Z}[X, Y]$ satisfies the following properties:*

(1) $\Phi_N(X, Y) = \Phi_N(Y, X)$;
(2) Φ_N is monic and it has degree $N + 1$ both in X and Y;
(3) If N is prime, then the highest degree form Φ_N^{top} of Φ_N is $-X^N Y^N$.

Proof. The first two properties are well known (see e.g. [43, Lectures 19 and 20]). We address the third. Let N be prime, by combining [43, Theorem 19.14 and Lemma 20.9] we get that $\Phi_N(X, Y)$ is monic in X and in Y and the top degree part of $\Phi_N(X, X)$ is $-X^{2N}$. Therefore, we can write

$$\Phi_N(X, Y) = X^{N+1} + Y^{N+1} - X^N Y^N + \{\text{monomials of degree} < 2N\}.$$

This tells us exactly that $\Phi_N(X, Y)^{\mathrm{top}} = -X^N Y^N$. □

Example 2.2. The first two modular polynomials are the following.

$$\begin{aligned}
\Phi_2(X, Y) &= X^3 + Y^3 - X^2Y^2 + 1488(X^2Y + XY^2) - 162000(X^2 + Y^2) + \\
&\quad + 40773375XY + 8748000000(X + Y) - 157464000000000; \\
\Phi_3(X, Y) &= (X + Y)^4 - X^3Y^3 + 2232X^2Y^2(X + Y) + 36864000(X + Y)^3 + \\
&\quad - 1069960XY(X + Y)^2 + 2590058000X^2Y^2 + \\
&\quad + 8900112384000XY(X + Y) + 452984832000000(X + Y)^2 + \\
&\quad - 771751936000000000XY + 1855425871872000000000(X + Y).
\end{aligned} \tag{1}$$

Higher degree modular polynomials are larger. However, recall that they can be constructed algorithmically, for example by using the procedure outlined in [14].

One subtlety is that the vanishing of $\Phi_N(j_1, j_2)$ is equivalent to the existence of an isogeny which is defined over the algebraic closure $\overline{\mathbb{F}}_q$, while we are interested in working over a finite field. In our setup, this is not a problem. We address it in the following remark.

Remark 2.3. First of all, we recall that every supersingular elliptic curve has j-invariant defined over $\mathbb{F}_{p^2}$ and it is isomorphic (over $\overline{\mathbb{F}}_p$) to an elliptic curve defined over $\mathbb{F}_{p^2}$ ([41, Remark 9.7]). Now, if E_1 and E_2 are two supersingular elliptic curves defined over $\mathbb{F}_{p^2}$ that are connected via an isogeny of degree N over $\overline{\mathbb{F}}_p$, then there exist two elliptic curves E_1', E_2', defined over $\mathbb{F}_{p^2}$, such that $E_1 \cong E_1'$ and $E_2 \cong E_2'$ over $\overline{\mathbb{F}}_p$ and there exists a N-isogeny between E_1' and E_2' defined over $\mathbb{F}_{p^2}$ (see [30, Lemma 5.2]). Therefore, when considering chain of isogenies up to taking those isomorphic curves at the beginning and at the end, we may restrict without loss of generality to work only with supersingular curves and isogenies defined over $\mathbb{F}_{p^2}$.

2.2. **The modeling.** Let $\ell \neq p$ be a prime number. Given two supersingular elliptic curves $E_{\text{start}}, E_{\text{finish}}$ over $\mathbb{F}_{p^2}$ with j-invariants j_{start} and j_{finish} that are connected via an isogeny φ of degree ℓ^m ($m \in \mathbb{Z}_{\geq 1}$), we want to find the j-invariants of the curves in the path that connects them, i.e, the j-invariants of curves $E_1, \dots, E_{m-1}$ such that

$$E_{\text{start}} \xrightarrow{\varphi_1} E_1 \xrightarrow{\varphi_2} E_2 \to \cdots \to E_{m-1} \xrightarrow{\varphi_m} E_{\text{finish}}, \tag{2}$$

where the φ_i's are isogenies of degree ℓ such that

$$\varphi_m \circ \varphi_{m-1} \circ \cdots \circ \varphi_1 = \varphi.$$

Now, we can set up the following polynomial system.

Polynomial system 1: Modular Polynomials

$$S_{m-1} = \mathbb{F}_{p^2}[j_1, \dots, j_{m-1}]$$
$$\mathcal{M}_{\ell,m} = [\Phi_\ell(j_{\text{start}}, j_1), \Phi_\ell(j_1, j_2), \dots, \Phi_\ell(j_{m-2}, j_{m-1}), \Phi_\ell(j_{m-1}, j_{\text{finish}})] \subseteq S_{m-1}$$
$$\begin{cases} \Phi_\ell(j_{\text{start}}, j_1) = 0 \\ \Phi_\ell(j_1, j_2) = 0 \\ \cdots\cdots \\ \Phi_\ell(j_{m-2}, j_{m-1}) = 0 \\ \Phi_\ell(j_{m-1}, j_{\text{finish}}) = 0 \end{cases}$$

The properties of modular polynomials immediately give us the following result.

Theorem 2.4. *Let $E_{\text{start}}, E_{\text{finish}}$ be two supersingular elliptic curves defined over $\mathbb{F}_{p^2}$ which are connected by an ℓ^m-isogeny φ, with ℓ a prime number and $m \in \mathbb{Z}_{>1}$. Let $(\overline{j_1}, \dots, \overline{j_{m-1}}) \in \mathbb{F}_{p^2}^{m-1}$ be a solution of Polynomial system 1, then $\overline{j_1}, \dots, \overline{j_{m-1}}$ are the j-invariants of supersingular elliptic curves in a chain of isogenies of degree ℓ that connects E_{start} and E_{finish} as in (2).*

Theorem 2.4 tells us that finding a solution of Polynomial system 1 allows us to reduce an instance of the Supersingular Isogeny Problem (SIP) of degree ℓ^m between E_{start} and E_{finish} to m instances of the SIP of degree ℓ. When ℓ is small (such as $\ell = 2, 3$) the isogenies φ_i's are easy to find. In fact, we point out that up to $\ell \leq 31$, there exist SageMath libraries [46, 47] that allow the efficient writing of all the ℓ-isogenies of the decomposition.

We postpone to Section 5 and Section 6 an analysis of the algebraic properties of Polynomial system 1 and a report on some experiments that we performed for $\ell = 2, 3$.

3. Algebraic Modeling with Renes Polynomials in degree 2

In this section, we consider chain of isogenies of degree 2. Given a supersingular elliptic curve E we have three isogenies of degree 2 with domain the curve E, indeed the 2-isogeny graph is 3-regular [31]. The kernel of a 2-isogeny is a subgroup of order 2. In other words, we have a degree 2 isogeny associated to each non trivial element of $E[2]$. It turns out that when E is in Montgomery form, these elements and the corresponding isogenies can be explicitly written thanks to Renes formulas [10, 16, 35]. We use these formulas to construct polynomials and build an algebraic modeling for SIP.

3.1. Montgomery curves and Renes formulas.

A supersingular elliptic curve E over $\mathbb{F}_{p^2}$ is written in *Montgomery form* if

$$E\colon By^2 = x^3 + Ax^2 + x,$$

with $A, B \in \mathbb{F}_{p^2}$. It is clear that a nonsingular curve in Montgomery form is elliptic, while not every elliptic curve in Weierstrass form can be transformed into a Montgomery form. A necessary and sufficient condition is given in the following theorem from [33].

Theorem 3.1 ([33])**.** *Let $E\colon y^2 = x^3 + ax + b$ be an elliptic curve defined over $\mathbb{F}_q$. Then E is isomorphic to a Montgomery curve $E'\colon By^2 = x^3 + Ax^2 + x$ over $\mathbb{F}_q$ if and only if*

(1) E has an $\mathbb{F}_q$-rational 2-torsion point $(\alpha, 0)$;
(2) $3\alpha^2 + a = s^2$ for some $s \in \mathbb{F}_q \setminus \{0\}$.

In this case, the coefficients of E' are $A = 3\alpha s^{-1}$ and $B = s^{-1}$.

Remark 3.2. If $E\colon By^2 = x^3 + Ax^2 + x$ is an elliptic curve in Montgomery form over $\mathbb{F}_{p^2}$, then it is isomorphic (over $\mathbb{F}_{p^4}$) to the curve $E'\colon y^2 = x^3 + Ax^2 + x$, which is a quadratic twist of E. Thus, for simplicity in what follows we will restrict to curves in Montgomery form with $B = 1$ and $A \in \mathbb{F}_{p^2}$.

We consider a supersingular elliptic curve E written in Montgomery form as

$$E : y^2 = x^3 + Ax^2 + x. \tag{3}$$

The 2-torsion points of E are

$$E[2] = \{O_E, (0,0), (\alpha, 0), (\alpha^{-1}, 0)\},$$

where $\alpha \in \mathbb{F}_{p^4}$ is a root of $x^2 + Ax + 1$, and $A = -\alpha - \alpha^{-1}$. For curves with j-invariant $\neq 0, 1728$ the roots α, α^{-1} of $x^2 + Ax + 1$ are indeed in $\mathbb{F}_{p^2}$.

Lemma 3.3. *Let E be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$ such that $|E(\mathbb{F}_{p^2})| = (p \pm 1)^2$. Then $E[2] \subseteq E(\mathbb{F}_{p^2})$, i.e., the 2-torsion points of E are $\mathbb{F}_{p^2}$-rational.*

Proof. Thanks to [40, Lemma 4.8 (ii)], we have that $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}/(p+1)\mathbb{Z} \times \mathbb{Z}/(p+1)\mathbb{Z}$ or $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z}$. On the other hand, we have that $E[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Since $2 \mid p \pm 1$, it holds that $\mathbb{Z}/(p \pm 1)\mathbb{Z}$ has a subgroup of order 2, and it must be $\mathbb{Z}/2\mathbb{Z}$. So we must have that $E[2] \subseteq E(\mathbb{F}_{p^2})$. □

Remark 3.4. The condition $|E(\mathbb{F}_{p^2})| = (p \pm 1)^2$ in Lemma 3.3 may seem restrictive, however it is satisfied by any supersingular elliptic curve E with $j(E) \neq 0, 1728$. Indeed, let $t = p^2 + 1 - |E(\mathbb{F}_{p^2})|$ be the trace of the Frobenius endomorphism ϕ_{p^2} on E. Since E is supersingular, by Hasse's bound we have that $t \in \{0, \pm p, \pm 2p\}$. If $t = 0$, then the characteristic polynomial of the Frobenius ϕ_{p^2} is $h(x) = x^2 + p^2$. Since $h(x)$ has a root ϕ_{p^2} in $\mathrm{End}(E)$, its discriminant $\Delta = -4p^2$ must be a square. This implies that E has a nontrivial automorphism of order 4. Since the characteristic of the field is $\neq 2, 3$, this happens only if $j(E) = 1728$ [41, Theorem 10.1]. With a similar argument one can show that $t = \pm p$ forces $j(E) = 0$. Thus, if $j(E) \neq 0, 1728$, we have $t = \pm 2p$ and $|E(\mathbb{F}_{p^2})| = (p \pm 1)^2$ (see also [1]).

Now, we consider a supersingular elliptic curve E over $\mathbb{F}_{p^2}$ written in Montgomery form as in (3) with $|E(\mathbb{F}_{p^2})| = (p \pm 1)^2$. By Lemma 3.3, the 2-torsion points of E are in $\mathbb{F}_{p^2}$. Thus, we can factor the polynomial $x^2 + Ax + 1$ over $\mathbb{F}_{p^2}$ and write E in *simplified Montgomery form* [10]:

$$E\colon y^2 = x(x - \alpha)(x - \alpha^{-1}),$$

with $\alpha \in \mathbb{F}_{p^2}$. The subgroups of order 2 $\langle(\alpha, 0)\rangle$ and $\langle(\alpha^{-1}, 0)\rangle$ are the kernels of two distinct 2-isogenies φ_1 and φ_2 with domain E. It turns out that the codomain elliptic curves of φ_1 and φ_2 can also be written in simplified Montgomery form.

The following lemma due to Renes [35, Proposition 2] formalizes our claims.

Lemma 3.5 (Renes formulas, degree 2)**.** *Let E be a supersingular elliptic curve over $\mathbb{F}_{p^2}$ written in simplified Montgomery form $y^2 = x(x - \alpha)(x - \alpha^{-1})$. Then, there exist two 2-isogenies $\varphi_1\colon E \to E_1$, $\varphi_2\colon E \to E_2$ defined over $\mathbb{F}_{p^2}$ such that E_1, E_2 are defined over $\mathbb{F}_{p^2}$ and can be written in Montgomery form as*

$$E_1\colon y^2 = x^3 + A_1x^2 + x, \quad E_2\colon y^2 = x^3 + A_2x^2 + x,$$

where $A_1 = 2 - 4\alpha^2$ and $A_2 = 2 - 4(\alpha^{-1})^2$.

Remark 3.6. The remaining 2-isogeny with domain E is the one with kernel $\langle(0, 0)\rangle$. We will not keep track of this isogeny in the algebraic modeling we are going to construct. This is because when we have a chain of 2-isogenies, the isogeny with kernel $\langle(0, 0)\rangle$ (apart from the first step of the chain) is the backtracking isogeny, i.e., the dual isogeny to the previous step in the chain (see [35, Corollary 1]).

3.2. **Renes polynomials.** We are going to use Renes formulas to construct polynomials which we will use in our modeling. First, we define them and then we explain their properties.

Definition 3.7. The *Renes polynomials of degree* 2 are the following polynomials in $\mathbb{Z}[X, Y]$:

$$\begin{aligned}
\Psi_1(X, Y) &= XY + Y^2 + 1;\\
\Psi_2(X, Y) &= -4X^2Y + Y^2 + 2Y + 1;\\
\Psi_3(X, Y) &= 65536X^{12} - 196608X^{10} + 208896X^8 - 90112X^6 - X^4Y + 13056X^4 +\\
&\quad + X^2Y - 768X^2 + 16.
\end{aligned}$$

Proposition 3.8. *Let E be a supersingular elliptic curve over $\mathbb{F}_{p^2}$ such that $|E(\mathbb{F}_{p^2})| = (p \pm 1)^2$ written in Montgomery form $E : y^2 = x^3 + Ax^2 + x$. Let $\varphi_1\colon E \to E_1$, $\varphi_2\colon E \to E_2$ be two degree 2 isogenies (defined over $\mathbb{F}_{p^2}$) with kernel $\neq \langle(0, 0)\rangle$. The following facts hold.*

(1) *Let $\alpha, \alpha^{-1} \in \mathbb{F}_{p^2}$ be the roots of $\Psi_1(A, Y)$. Then, the simplified Montgomery form of E is $y^2 = x(x-\alpha)(x-\alpha^{-1})$.*
(2) *Let $\gamma_1, \gamma_2, \gamma_3, \gamma_4$ be the four roots of $\Psi_2(\alpha, Y)$ and $\Psi_2(\alpha^{-1}, Y)$. Then, up to relabeling, $\gamma_3 = \gamma_1^{-1}$, $\gamma_4 = \gamma_2^{-1}$ and the simplified Montgomery forms of E_1 and E_2 are*

$$E_i \colon y^2 = x(x-\gamma_i)(x-\gamma_i^{-1}).$$

Proof. (1) This is clear from the discussion in §3.1. Notice that $\alpha, \alpha^{-1} \in \mathbb{F}_{p^2}$ by Lemma 3.3.
(2) Let $i \in \{1, 2\}$. By Lemma 3.5, also E_i can be written in Montgomery form. Moreover, Tate's Theorem ([45, Section 3 Theorem 1]) yields $|E_i(\mathbb{F}_q)| = |E(\mathbb{F}_q)| = (p \pm 1)^2$. Thus, by Lemma 3.3 E_i can be written in simplified Montgomery form

$$E_i \colon y^2 = x(x-\gamma)(x-\gamma^{-1}),$$

where γ is a root of $x^2 + (2 - 4\beta^2)x + 1$ with $\beta \in \{\alpha, \alpha^{-1}\}$. So, we have

$$\gamma_i = -1 + 2\beta^2 + c_i, \quad i = 1, 2, \tag{4}$$

where the c_i's are the two square roots of the discriminant $4\beta^4 - 4\beta^2$. If we isolate c_i in (4) and square both sides we get that γ must satisfy

$$-4\beta^2\gamma + \gamma^2 + 2\gamma + 1 = 0, \tag{5}$$

that is γ is a root of $\Psi_2(\beta, Y)$.

□

Proposition 3.9. *Let E be a supersingular elliptic curve over $\mathbb{F}_{p^2}$ in Montgomery form. Let $\delta \in \mathbb{F}_{p^2}$ be a root of $\Psi_3(X, j(E))$. Then there exists an isogeny of degree 2 (defined over $\mathbb{F}_{p^2}$) from $y^2 = x(x-\delta)(x-\delta^{-1})$ to an elliptic curve $y^2 = x^3 + (2 - 4\delta^2)x^2 + x$ with j-invariant $j(E)$.*

Proof. We recall that we have six possible elliptic curves in Montgomery form with the same j-invariant of E. Indeed, their A's are given by the relation

$$j(E) = 256\frac{(A^2-3)^3}{A^2-4}.$$

Clearing the denominator in the previous equation we get that the roots of the polynomial $f(Z) = (Z^2-4)j(E) - 256(Z^2-3)^3$ are precisely these six possible A's. Now, let $g(X, Z) = 2 - 4X^2 - Z$ be the polynomial obtained from Renes formulas (Lemma 3.5). In particular, for a fixed value δ, the roots of $g(X, \delta)$ are precisely the A-coefficients of the Montgomery forms of the codomain elliptic curves of the 2-isogenies from $y^2 = x(x-\delta)(x-\delta^{-1})$. We consider the elimination ideal $I = (g(X, Z), f(Z)) \cap \mathbb{Q}[X]$. A computation shows that I is generated by the polynomial

$$65536X^{12} - 196608X^{10} + 208896X^8 - 90112X^6 - X^4 j(E) + 13056X^4 + \\ + X^2 j(E) - 768X^2 + 16 \in \mathbb{Z}[X].$$

This is exactly $\Psi_3(X, j(E))$. Alternatively, one can check that $\Psi_3(X, j(E)) = -\frac{1}{16} f(2 - 4X^2)$.

Now, let $\delta \in \mathbb{F}_{p^2}$ be a root of $\Psi_3(X, j(E))$. By construction, δ satisfies $f(2 - 4\delta^2) = 0$. Thus, $A' = 2 - 4\delta^2$ is one of the six possible Montgomery coefficients A's coming from $j(E)$. From what is said above, we know that there exists an isogeny of degree 2 (defined over $\mathbb{F}_{p^2}$) from $y^2 = x(x-\delta)(x-\delta^{-1})$ to the elliptic curve $y^2 = x^3 + A'x^2 + x$ with j-invariant $j(E)$. □

Remark 3.10. Notice that the curve $y^2 = x(x-\delta)(x-\delta^{-1})$ of Proposition 3.9 is not an elliptic curve iff $\delta \in \{0, \pm 1\}$. Indeed, if $\delta \in \{0, \pm 1\}$ then $A' \in \{\pm 2\}$ which implies that $j(E)$ is not well-defined.

3.3. **The modeling.** We assume the following setup. We have two supersingular elliptic curves E_{start} and E_{finish} over $\mathbb{F}_{p^2}$ in Montgomery form (with $B = 1$) that are connected via an isogeny φ of degree 2^m ($m \in \mathbb{Z}_{\geq 1}$). Moreover, suppose $|E_{\text{start}}(\mathbb{F}_{p^2})| = (p \pm 1)^2$, thus by Lemma 3.3, E_{start} can be put in simplified Montgomery form, and by Tate's Theorem the same applies to E_{finish} and all elliptic curves in the chain. Finally, we assume that the first 2-isogeny (the one with domain E_{start}) in the decomposition of φ is not the one associated with the 2-torsion point $(0, 0)$. Let $A_{\text{start}}, A_{\text{finish}} \in \mathbb{F}_{p^2}$ be their Montgomery x^2-coefficients and $j(E_{\text{finish}})$ the j-invariant of E_{finish} computed from A_{finish}. Using Renes polynomials, we construct a polynomial system whose solutions correspond to all possible degree 2^m isogenies from E_{start} to an elliptic curve with j-invariant $j(E_{\text{finish}})$.

To make things more precise, we introduce the following definition which will be important also for the degree 3 case.

Definition 3.11. Let $d \geq 2$, $m \geq 1$ be integers and let E_{start} and E_{finish} be two supersingular elliptic curves which are connected via an isogeny of degree d^m. We define the set

$$P(d, m, E_{\text{start}}, j(E_{\text{finish}})) = \{E_{\text{start}} \xrightarrow{\varphi_0} E_1 \xrightarrow{\varphi_1} \cdots \xrightarrow{\varphi_{m-1}} E_m \mid \text{non-backtracking}, \ker \varphi_0 \neq \langle (0,0) \rangle,\ \deg(\varphi_i) = d \ \ \forall i,\ j(E_m) = j(E_{\text{finish}})\}/\sim \tag{6}$$

where $E_{\text{start}} \xrightarrow{\varphi_0} E_1 \xrightarrow{\varphi_1} \cdots \xrightarrow{\varphi_{m-1}} E_m$ and $E_{\text{start}} \xrightarrow{\varphi'_0} E'_1 \xrightarrow{\varphi'_1} \cdots \xrightarrow{\varphi'_{m-1}} E'_m$ are equivalent under $\sim$ if and only if for $i = 1, \ldots, m$ there exist isomorphisms $\psi_i : E_i \xrightarrow{\cong} E'_i$ such that the following diagram commutes

$$\begin{array}{ccccccccc} E_{\text{start}} & \xrightarrow{\varphi_0} & E_1 & \longrightarrow & \cdots & \longrightarrow & E_{m-1} & \xrightarrow{\varphi_{m-1}} & E_m \\ \downarrow{\scriptstyle \text{id}} & & \downarrow{\scriptstyle \psi_1} & & & & \downarrow{\scriptstyle \psi_{m-1}} & & \downarrow{\scriptstyle \psi_m} \\ E_{\text{start}} & \xrightarrow{\varphi'_0} & E'_1 & \longrightarrow & \cdots & \longrightarrow & E'_{m-1} & \xrightarrow{\varphi'_{m-1}} & E'_m \end{array}$$

In particular, we have $j(E_i) = j(E'_i)$ and $\ker(\varphi_i) = \ker(\varphi'_i \circ \psi_i)$ for all $i = 1, \ldots, m$.

The set $P(d, m, E_{\text{start}}, j(E_{\text{finish}}))$ parametrizes all possible non-backtracking paths of degree d isogenies of length m that start from E_{start} and end into a supersingular elliptic curve with the same j-invariant as E_{finish}. We recall that by non-backtracking we mean that we do not allow two consecutive isogenies in the path to be dual to each other. The additional condition that the kernel of the first isogeny is not generated by the point $(0, 0)$ guarantees that when the curve E_{start} is in Montgomery form and $d = 2$, then these paths can be obtained from the solutions of the following polynomial system build up from Renes polynomials.

Polynomial system 2: Renes Formulas for 2-isogenies, complete

$R_m = \mathbb{F}_{p^2}[\alpha_0, \ldots, \alpha_{m-1}]$

$\mathcal{F}_{2\text{-Renes},m} = [\Psi_1(A_{\text{start}}, \alpha_0), \Psi_2(\alpha_0, \alpha_1), \ldots, \Psi_2(\alpha_{m-2}, \alpha_{m-1}), \Psi_3(\alpha_{m-1}, j(E_{\text{finish}}))] \subseteq R_m$

$$\begin{cases} \Psi_1(A_{\text{start}}, \alpha_0) = 0 \\ \Psi_2(\alpha_0, \alpha_1) = 0 \\ \Psi_2(\alpha_1, \alpha_2) = 0 \\ \cdots \\ \Psi_2(\alpha_{m-2}, \alpha_{m-1}) = 0 \\ \Psi_3(\alpha_{m-1}, j(E_{\text{finish}})) = 0. \end{cases}$$

Theorem 3.12. *Let $E_{\text{start}}, E_{\text{finish}}$ be two supersingular elliptic curves in Montgomery form over $\mathbb{F}_{p^2}$ (with the y^2-coefficient equal to 1). Suppose that $|E_{\text{start}}(\mathbb{F}_{p^2})| = (p \pm 1)^2$. Then, given $m \in \mathbb{Z}_{\geq 1}$, there is a bijective map*

$$\Theta_2 : V_{\mathbb{F}_{p^2}}(\mathcal{F}_{2\text{-}Renes,m}) \longrightarrow P(2, m, E_{\text{start}}, j(E_{\text{finish}})),$$

where $V_{\mathbb{F}_{p^2}}(\mathcal{F}_{2\text{-}Renes,m})$ is the set of $\mathbb{F}_{p^2}$-rational solutions to Polynomial system 2.

Proof. First, let $(\alpha_0, \ldots, \alpha_{m-1}) \in (\mathbb{F}_{p^2})^m$ be a solution of Polynomial system 2. Then, by Proposition 3.8, the simplified Montgomery form of E_{start} is $y^2 = x(x - \alpha_0)(x - \alpha_0^{-1})$ and we have a degree 2 isogeny $\varphi_0 : E_{\text{start}} \to E_1$, with $E_1 : y^2 = x(x - \alpha_1)(x - \alpha_1^{-1})$ and $\ker \varphi_0 \neq \langle (0,0) \rangle$. Applying Proposition 3.8 to E_1 and then recursively, we obtain a chain $E_{\text{start}} \xrightarrow{\varphi_0} E_1 \xrightarrow{\varphi_1} \cdots \xrightarrow{\varphi_{m-1}} E_m$, where each curve in the path has simplified Montgomery form $y^2 = x(x - \alpha_i)(x - \alpha_i^{-1})$, $\deg \varphi_i = 2$, and $\ker \varphi_i \neq \langle (0,0) \rangle$. The last condition guarantees that the path is non-backtracking. Also, by Proposition 3.9, we obtain that $j(E_m) = j(E_{\text{finish}})$. Thus, we have constructed an element of the set $P(2, m, E_{\text{start}}, j(E_{\text{finish}}))$. This construction defines the desired map Θ_2.

Now, we construct an inverse map Λ_2 in the opposite direction. Suppose that we have a path φ of m degree 2 non-backtracking isogenies between E_{start} and E_m with $j(E_{\text{finish}}) = j(E_m)$ and $\ker \varphi_0 \neq \langle (0,0) \rangle$:

$$\varphi : E_{\text{start}} \xrightarrow{\varphi_0} E_1 \xrightarrow{\varphi_1} \cdots \xrightarrow{\varphi_{m-1}} E_m.$$

We select an appropriate representative in the equivalence class of φ in $P(2, m, E_{\text{start}}, j(E_{\text{finish}}))$ and we use this representative to construct an element $(\alpha_0, \ldots, \alpha_{m-1}) \in V_{\mathbb{F}_{p^2}}(\mathcal{F}_{2\text{-Renes},m})$. Since E_{start} is in Montgomery form, then $\ker(\varphi_0)$ is generated by a point $(\alpha_0, 0)$, where α_0 is one of the two distinct (since E_{start} is an elliptic curve) solutions of the equation $\Psi_1(A_{\text{start}}, Y) = Y^2 + A_{\text{start}} Y + 1 = 0$. Notice that $\alpha_0 \in \mathbb{F}_{p^2}$ by Lemma 3.3. Thanks to Renes formulas (Lemma 3.5), each 2-torsion point $(\alpha, 0)$ defines a distinct 2-isogeny from E_{start} to an elliptic curve $E(\alpha)$ in Montgomery form defined by the coefficient $A = 2 - 4\alpha^2$. In particular, the codomain curve $E(\alpha_0)$ is isomorphic over $\overline{\mathbb{F}}_p$ to the curve E_1 in the fixed path φ, thus $j(E_1) = j(E(\alpha_0))$. Therefore, by composing with an isomorphism $\psi_1 : E_1 \to E(\alpha_0)$ we may replace E_1 by $E(\alpha_0)$, which is in Montgomery form, without changing the equivalence class of the path φ. Since the path is non-backtracking, the kernel of φ_1 is generated by a point $(\alpha_1, 0)$, where by Proposition 3.8 α_1 is a solution to the equation $\Psi_2(\alpha_0, Y) = Y^2 + (2 - 4\alpha_0^2)Y + 1 = 0$. We observe that $\alpha_1 \in \mathbb{F}_{p^2}$ since $|E(\alpha_0)(\mathbb{F}_{p^2})| = (p \pm 1)^2$ by Tate's theorem. As before, we may compose with an isomorphism $\psi_2 : E_2 \to E(\alpha_1)$ and replace E_2 with a curve in Montgomery form $E(\alpha_1)$ without changing the representative class of the path φ. Proceeding in this way, we obtain elements $\alpha_0, \ldots, \alpha_{m-1} \in \mathbb{F}_{p^2}$ which satisfy the equations involving the polynomials Ψ_1 and Ψ_2 of Polynomial system 2. Notice that, since the path is non-backtracking, at each step we do not have to consider the isogeny with kernel generated by $(0, 0)$. At the last step, from the condition $j(E_{\text{finish}}) = j(E(\alpha_{m-1}))$, we also obtain that α_{m-1} is a solution to the equation $\Psi_3(X, j(E_{\text{finish}})) = 0$ by Proposition 3.9. Therefore, $(\alpha_0, \ldots, \alpha_{m-1})$ is a solution of Polynomial system 2. In particular, this construction defines a map $\Lambda_2 : P(2, m, E_{\text{start}}, j(E_{\text{finish}})) \longrightarrow V_{\mathbb{F}_{p^2}}(\mathcal{F}_{2\text{-Renes},m})$ which is the inverse of the map Θ_2 defined above, hence Θ_2 is bijective. □

Remark 3.13 (Comparison with modular polynomials)**.** We point out some distinctions between the approach with Renes polynomials and with modular polynomials.

(1) Once we have a solution of Polynomial system 2, we are able to directly recover the explicit curves (in simplified Montgomery form) that are in the path of the 2^m-isogeny, while this is

not immediate with modular polynomials. Moreover, we can also give a precise description of the 2-isogenies in the path. Those formulas can be found in [35, Proposition 2].

(2) It is not true in this setting that there exists a 2-isogeny between two elliptic curves in simplified Montgomery form with parameters α_1 and α_2 if and only if $\Psi_2(\alpha_1, \alpha_2) = 0$. This is due to the fact that Renes polynomials do not take into account the different representations of the curves, which may have different Montgomery forms isomorphic to each other. Moreover, Renes polynomials do not consider the backtracking isogeny, associated to the 2-torsion point $(0, 0)$. Indeed, $\Psi_2(X, Y)$ is not a symmetric polynomial.

3.4. **The (compact) modeling.** From a computational point of view, the presence of the degree 12 polynomial Ψ_3 in Polynomial System 2 makes it harder to solve. To fix this issue, we consider 6 systems where the last equation is replaced by $(2 - 4\alpha_{m-1}^2) - A = 0$, where A is one of the 6 possible roots of the polynomial that codifies all the possible A's of a curve in Montgomery form with fixed j-invariant $j(E_{\text{finish}})$. Explicitly, we precompute those A's as the roots of $256(X^2-3)^3 - j(E_{\text{finish}})(X^2-4) \in \mathbb{F}_{p^2}[X]$ and we plug them into the polynomial

$$\Psi_4 = -4X^2 - Y + 2 \in \mathbb{Z}[X].$$

We obtain 6 equations $\Psi_4(\alpha_{m-1}, A) = 0$, which give rise to 6 new polynomial systems of the following form.

Polynomial system 3: Renes Formulas for 2-isogenies, compact

$R_m = \mathbb{F}_{p^2}[\alpha_0, \dots, \alpha_{m-1}]$
$\mathcal{R}_{2,m} = [\Psi_1(A_{\text{start}}, \alpha_0), \Psi_2(\alpha_0, \alpha_1), \dots, \Psi_2(\alpha_{m-2}, \alpha_{m-1}), \Psi_4(\alpha_{m-1}, A)] \subseteq R_m$

$$\begin{cases} \Psi_1(A_{\text{start}}, \alpha_0) = 0 \\ \Psi_2(\alpha_0, \alpha_1) = 0 \\ \Psi_2(\alpha_1, \alpha_2) = 0 \\ \dots \\ \Psi_2(\alpha_{m-2}, \alpha_{m-1}) = 0 \\ \Psi_4(\alpha_{m-1}, A) = 0. \end{cases}$$

Now, the degree of the last polynomial is 2 instead of 12. Moreover, only one of these 6 systems will have a solution, but the computations can be parallelized and, once a solution is found, all other computations can be aborted. Notice that, since we already have A_{finish} and we know that $-A_{\text{finish}}$ is also an admissible A, to find the other A's we can now find the roots of a polynomial of degree 4. This means that the pre-computation of the A's is computationally irrelevant with respect to the computation of a Gröbner basis.

For these reasons, we will focus on Polynomial System 3 rather than Polynomial System 2. We postpone to Section 5 and Section 6 an analysis of its algebraic properties and a report on some computational experiments.

4. Algebraic Modeling with Renes Polynomials in degree 3

In this section, we consider chain of isogenies of degree 3. Given a supersingular elliptic curve E we have four isogenies of degree 3 with domain the curve E, and the kernel of a 3-isogeny is a subgroup of $E[3]$ of order 3. In [35], Renes gives a description for degree 3-isogenies similar to

the degree 2 in the previous subsection. We use it to construct polynomials and build an algebraic modeling for SIP.

4.1. **Triangular curves and Renes formulas.** A supersingular elliptic curve E is in *triangular form* if it is given by an equation

$$E\colon\ y^2 + axy + by = x^3,$$

for some $a, b \in \mathbb{F}_{p^2}$. If b is a cube in $\mathbb{F}_{p^2}$, then writing $b = \beta^3$ for some $\beta \in \mathbb{F}_{p^2}$, we obtain $b = 1$ through the transformation $(x, y) \mapsto (x/\beta^2, y/\beta^3)$. For simplicity, in the following, we will always assume that the elliptic curve admits a triangular form with $b = 1$. We recall that in this case the condition of being non-singular is equivalent to $a^3 \neq 27$.

As for Montgomery curves, not every supersingular elliptic curve can be put into triangular form. However, if the curve $E/\mathbb{F}_{p^2}$ contains a rational point of order 3, then it can be written in triangular form (see [6, Theorem 5.2]). We point out that when an elliptic curve is in triangular form, the point $(0, 0)$ has order 3. The following lemma, whose proof is analogous to the proof of Lemma 3.3, gives a sufficient criterion for the rationality of points of order 3.

Lemma 4.1. *Let E be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$. Assume that $|E(\mathbb{F}_{p^2})| = (p-1)^2$ if $p \equiv 1 \mod 3$ and $|E(\mathbb{F}_{p^2})| = (p+1)^2$ if $p \equiv 2 \mod 3$. Then $E[3] \subseteq E(\mathbb{F}_{p^2})$, i.e., the 3-torsion points of E are $\mathbb{F}_{p^2}$-rational.*

Remark 4.2. Notice that, if we are in a case for a curve E as in Lemma 4.1 where $p \equiv 1 \mod 3$ but $|E(\mathbb{F}_{p^2})| = (p+1)^2$ (resp. $p \equiv 2 \mod 3$ but $|E(\mathbb{F}_{p^2})| = (p-1)^2$), we can pass to a twist E_{qt} of E such that $|E_{qt}(\mathbb{F}_{p^2})| = (p-1)^2$ (resp. $|E_{qt}(\mathbb{F}_{p^2})| = (p+1)^2$) and work with E_{qt}. Therefore, up to a twist, we can always apply Lemma 4.1.

As for the degree 2 case, if E is a supersingular elliptic curve in triangular form and $\varphi : E \to E'$ is a degree 3 isogeny with $\ker\varphi \neq \langle(0,0)\rangle$, then also E' can be put in triangular form and the $\mathbb{F}_{p^2}$-rationality of the 3-torsion points is preserved. More precisely, the 3-isogenies with domain E can be explicitly described by *Renes formulas* as follows (cf. [35, Proposition 4, Corollary 3]).

Lemma 4.3 (Renes formulas, degree 3)**.** *Given a supersingular elliptic curve $E\colon y^2 + axy + y = x^3$ in triangular form and $(x_P, y_P) \in E(\mathbb{F}_{p^2})$ a 3-torsion point distinct from $(0, 0)$, then we have a 3-isogeny $\varphi : E \to E'$, where $E'\colon y^2 + Axy + y = x^3$ with $A = -3(2 + ax_P)$. Moreover, the dual isogeny $\hat{\varphi} : E' \to E$ is the one with kernel $\langle(0, 0)\rangle$.*

4.2. **Renes polynomials.** We are going to use Renes formulas to construct polynomials which we will use in our modeling. First, we define them and then we explain their properties.

Definition 4.4. The *Renes polynomials of degree* 3 are the following polynomials in $\mathbb{Z}[X, Y]$:

$$\Gamma_1(X, Y) = X^3Y^2 + 3X^3Y + 9X^3 - Y^3 - 18Y^2 - 108Y - 216;$$
$$\Gamma_2(X, Y) = X^{12} - 72X^9 + 1728X^6 - X^3Y - 13824X^3 + 27Y.$$

Proposition 4.5. *Let E be a supersingular elliptic curve over $\mathbb{F}_{p^2}$ written in triangular form as $y^2 + axy + y = x^3$. Assume that $|E(\mathbb{F}_{p^2})| = (p-1)^2$ if $p \equiv 1 \mod 3$ and $|E(\mathbb{F}_{p^2})| = (p+1)^2$ if $p \equiv 2 \mod 3$. For $i \in \{1, 2, 3\}$, let $\varphi_i\colon E \to E_i$ be the three degree 3 isogenies (defined over $\mathbb{F}_{p^2}$) with kernel $\neq \langle(0, 0)\rangle$. Let $\gamma_1, \gamma_2, \gamma_3 \in \mathbb{F}_{p^2}$ be the roots of $\Gamma_1(a, Y)$. Then, (up to relabeling) the triangular form of E_i is $y^2 + \gamma_i xy + y = x^3$.*

Proof. The assumption on the number of rational points of E guarantees that the 3-torsion points of E are rational by Lemma 4.1. Then, by Lemma 4.3 each 3-torsion point $(x_i, y_i) \neq (0,0)$ gives a degree 3 isogeny to an elliptic curve in triangular form $E'\colon y^2+\gamma_i xy+y = x^3$ with $\gamma_i = -3(2+ax_i)$. Thus, it is enough to prove that $\gamma_1, \gamma_2, \gamma_3$ are precisely the three roots of $\Gamma_1(a, Y)$.

First, we recall that the x-coordinates of the 3-torsion points of E are the roots of the 3-division polynomial

$$\psi_3(a, Z) = 3Z^4 + a^2Z^3 + 3aZ^2 + 3Z.$$

Notice, that $\psi_3(a, 0) = 0$, since $(0, 0)$ is always a 3-torsion point. Since we are not interested in the isogeny with kernel $\langle(0, 0)\rangle$, we divide by Z and consider the polynomial with integer coefficients

$$\widetilde{\psi_3}(X, Z) = 3Z^3 + Z^2X^2 + 3XZ + 3.$$

The roots of $\widetilde{\psi_3}(a, Z)$ are the x-coordinates of the 3-torsion points of E distinct from $(0, 0)$. We also introduce the polynomial

$$\theta(X, Y, Z) = 3XZ + Y + 6 \in \mathbb{Z}[X, Y, Z]$$

with the property that for any root z of $\widetilde{\psi_3}(a, Z)$ the root of $\theta(a, Y, z)$ is one of $\gamma_1, \gamma_2, \gamma_3$ by Lemma 4.3. Now, we consider the elimination ideal

$$I = (\widetilde{\psi_3}(X, Z), \theta(X, Y, Z)) \cap \mathbb{Q}[X, Y].$$

A computation shows that the ideal I is principally generated by the polynomial $\Gamma_1(X, Y) = X^3Y^2 + 3X^3Y + 9X^3 - Y^3 - 18Y^2 - 108Y - 216$. Thus, the roots of $\Gamma_1(a, Y)$ are precisely $\gamma_1, \gamma_2, \gamma_3$ as required. □

Proposition 4.6. *Let E be a supersingular elliptic curve over $\mathbb{F}_{p^2}$ in triangular form. Let $\delta \in \mathbb{F}_{p^2}$ be a root of $\Gamma_2(X, j(E))$, then the elliptic curve $y^2 + \delta xy + y = x^3$ has j-invariant $j(E)$.*

Proof. Let $y^2 + axy + y = x^3$ be the triangular form of E with $a \in \mathbb{F}_{p^2}$, $a^3 \neq 27$. We recall that the j-invariant of E is given by the formula

$$j(E) = \frac{a^3(a^3 - 24)^3}{a^3 - 27}.$$

Thus, there are 12 possible a's giving an elliptic curve in triangular form with j-invariant $j(E)$. By clearing denominators, these can be expressed as the roots of the polynomial $\Gamma_2(X, j(E))$, where

$$\Gamma_2(X, Y) = X^{12} - 72X^9 + 1728X^6 - X^3Y - 13824X^3 + 27Y \in \mathbb{Z}[X, Y].$$

□

4.3. **The modeling.** We assume the following setup. We have two supersingular elliptic curves E_{start} and E_{finish} over $\mathbb{F}_{p^2}$ in triangular form that are connected via an isogeny φ of degree 3^m ($m \in \mathbb{Z}_{\geq 1}$) and suppose that the first 3-isogeny in the decomposition of φ has kernel $\neq \langle(0, 0)\rangle$. We assume further that $|E_{\text{start}}(\mathbb{F}_{p^2})| = (p - 1)^2$ if $p \equiv 1 \mod 3$ and $|E_{\text{start}}(\mathbb{F}_{p^2})| = (p + 1)^2$ if $p \equiv 2 \mod 3$. Let a_{start} be the xy-coefficient of the triangular form of E_{start} and let $j(E_{\text{finish}})$ be the j-invariant of E_{finish}. Using Renes polynomials (Definition 4.4), we construct a polynomial system whose solutions represent the a's of the triangular forms of the elliptic curves in the path that connects E_{start} and E_{finish}. Notice that Tate's theorem ensures that all curves in the path will have the same number of rational points as E_{start}, and thus can be put in triangular form as well by Lemma 4.1.

Polynomial system 4: Renes Formulas for 3-isogenies, complete

$U_m = \mathbb{F}_{p^2}[a_1, \dots, a_m]$
$\mathcal{F}_{3\text{-Renes},m} = [\Gamma_1(a_{\text{start}}, a_1), \Gamma_1(a_1, a_2), \cdots, \Gamma_1(a_{m-1}, a_m), \Gamma_2(a_m, j(E_{\text{finish}}))] \subseteq U_m$

$$\begin{cases} \Gamma_1(a_{\text{start}}, a_1) = 0 \\ \Gamma_1(a_1, a_2) = 0 \\ \cdots\cdots \\ \Gamma_1(a_{m-2}, a_{m-1}) = 0 \\ \Gamma_1(a_{m-1}, a_m) = 0 \\ \Gamma_2(a_m, j(E_{\text{finish}})) = 0 \end{cases}$$

The solutions of Polynomial system 4 are in bijection with the set $P(3, m, E_{\text{start}}, j(E_{\text{finish}}))$ of Definition 3.11 which parametrizes all possible non-backtracking paths of degree 3 isogenies of length m that start from E_{start} and ends into a supersingular elliptic curve with the same j-invariant as E_{finish}. We state this in the next theorem. The proof is analogous to the proof of Theorem 3.12, where Lemma 4.1, Lemma 4.3, Proposition 4.5, and Proposition 4.6 shall be used.

Theorem 4.7. *Let $E_{\text{start}}, E_{\text{finish}}$ be two supersingular elliptic curves in triangular form over $\mathbb{F}_{p^2}$ (with the y-coefficient equal to 1). Assume that $|E_{\text{start}}(\mathbb{F}_{p^2})| = (p-1)^2$ if $p \equiv 1 \mod 3$ and $|E_{\text{start}}(\mathbb{F}_{p^2})| = (p+1)^2$ if $p \equiv 2 \mod 3$. Then, given $m \in \mathbb{Z}_{\geq 1}$, there is a one to one correspondence between the set of $\mathbb{F}_{p^2}$-rational solutions to Polynomial system 4 and the set $P(3, m, E_{\text{start}}, j(E_{\text{finish}}))$.*

As for the degree 2 case, this complete polynomial system is difficult to solve with Gröbner bases because the polynomial $\Gamma_2(a_m, j(E_{\text{finish}}))$ has degree 12. So, as before, we replace the complete system with 12 compact ones, replacing the last equation with $\Gamma_1(a_{m-1}, a)$, where the a's are the roots of the polynomial $\Gamma_2(X, j(E_{\text{finish}}))$. We obtain the following systems, which we will focus our analysis on.

Polynomial system 5: Renes Formulas for 3-isogenies, compact

$U_{m-1} = \mathbb{F}_{p^2}[a_1, \dots, a_{m-1}]$
$\mathcal{R}_{3,m} = [\Gamma_1(a_{\text{start}}, a_1), \Gamma_1(a_1, a_2), \cdots, \Gamma_1(a_{m-2}, a_{m-1}), \Gamma_1(a_{m-1}, a)] \subseteq U_{m-1}$

$$\begin{cases} \Gamma_1(a_{\text{start}}, a_1) = 0 \\ \Gamma_1(a_1, a_2) = 0 \\ \cdots\cdots \\ \Gamma_1(a_{m-2}, a_{m-1}) = 0 \\ \Gamma_1(a_{m-1}, a) = 0 \end{cases}$$

5. Algebraic Analysis

In this section, we study some algebraic properties of the systems introduced:

- the system of modular polynomials $\mathcal{M}_{\ell,m}$, where $\ell \neq p$ is a prime number (Polynomial system 1);
- the system of (compact) Renes polynomials $\mathcal{R}_{2,m-1}$ in degree 2 (Polynomial System 3);
- the system of (compact) Renes polynomials $\mathcal{R}_{3,m}$ in degree 3 (Polynomial System 5).

Notice, that for degree 2 we consider the system $\mathcal{R}_{2,m-1}$ parametrizing paths of length $m-1$ since it has $m-1$ variables as the system $\mathcal{R}_{3,m}$ of degree 3 (which parametrizes paths of length m).

First, we prove that the systems are zero-dimensional, i.e., they admit a finite number of solutions over the algebraic closure $\overline{\mathbb{F}}_p$. For modular polynomials, this was already observed in [44]. First, we need the following lemma.

Lemma 5.1. *Let $S = K[x_1, \dots, x_n]$ be a polynomial ring over a field K and let $I = (f_1, \dots, f_{n+1}) \subseteq S$ be an ideal. If, up to reordering the generators of I, there exists a term order $<$ on S such that $\mathrm{LT}_<(f_1), \dots, \mathrm{LT}_<(f_n)$ are coprime and of degree ≥ 1, then I is zero-dimensional and $f_1, \dots, f_n$ is a regular sequence of (maximal) length n in I.*

Proof. Since $\mathrm{LT}_<(f_1), \dots, \mathrm{LT}_<(f_n)$ are coprime, the polynomials $f_1, \dots, f_n$ form a reduced Gröbner basis for the ideal $\tilde{I} = (f_1, \dots, f_n)$. Moreover, since $\mathrm{LT}_<(f_1), \dots, \mathrm{LT}_<(f_n)$ are precisely n and of degree ≥ 1, there exists a permutation $\sigma \in \mathfrak{S}_n$ such that $\mathrm{LT}_<(f_i) = x_{\sigma(i)}^{\deg(\mathrm{LT}_<(f_i))}$ for all $i = 1, \dots, n$. So, the ideal $\tilde{I}$ is zero-dimensional and $\mathrm{LT}_<(f_1), \dots, \mathrm{LT}_<(f_n)$ is a regular sequence of maximal length n in $\tilde{I}$. Macaulay Basis Theorem (see e.g. [36, Theorem 1.5.7]) yields that the ideal $\tilde{I}$ is zero-dimensional, hence I is zero-dimensional as well. Finally, by [37, Tutorial 54], we obtain that $f_1, \dots, f_n$ is a regular sequence of maximal length n in I. □

Proposition 5.2. *Let $m \geq 2$. The ideals $(\mathcal{M}_{\ell,m})$, $(\mathcal{R}_{2,m-1})$, and $(\mathcal{R}_{3,m})$ are zero-dimensional and contain a regular sequence of (maximal) length $m-1$.*

Proof. For every statement, we want to use Lemma 5.1 to conclude. For $(\mathcal{M}_{\ell,m})$, we consider a Lex term order $<$ with $j_{m-1} > j_{m-2} > \cdots > j_1$. Then, the leading terms of the first $m-1$ polynomials of $\mathcal{M}_{\ell,m}$ are $j_1^{\ell+1}, j_2^{\ell+1}, \dots, j_{m-1}^{\ell+1}$, which are coprime and of degree ≥ 1. For $(\mathcal{R}_{2,m-1})$, we consider a Lex term order $<$ with $\alpha_{m-2} > \alpha_{m-3} > \cdots > \alpha_0$. Then, the leading terms of the first $m-1$ polynomials of $\mathcal{R}_{2,m-1}$ are $\alpha_0^2, \alpha_1^2, \dots, \alpha_{m-2}^2$, which are coprime and of degree ≥ 1. For $(\mathcal{R}_{3,m})$ we consider a Lex term order $<$ with $a_{m-1} > a_{m-2} > \cdots > a_1$. Then, the leading terms of the first $m-1$ polynomials of $\mathcal{R}_{3,m}$ are $a_1^3, a_2^3, \dots, a_{m-1}^3$, which are coprime and of degree ≥ 1. □

The notion of degree of regularity was introduced in [4] as a way to measure the complexity of solving a polynomial system via linear-algebra based algorithms. Indeed, under suitable assumptions the degree of regularity provides an upper bound on the solving degree [39]. In a nutshell, given a polynomial system $\mathcal{F} = \{f_1, \dots, f_s\}$ the degree of regularity d_{reg} is the minimum integer d such that the homogeneous degree d piece of the ideal $(f_1^{\mathrm{top}}, \dots, f_s^{\mathrm{top}})$ coincides with the polynomial ring in degree d. If this minimum does not exists, i.e., when the ideal $(f_1^{\mathrm{top}}, \dots, f_s^{\mathrm{top}})$ is not zero-dimensional, then the degree of regularity is not defined or is set to be ∞, depending on the convention. Thus, when $(f_1^{\mathrm{top}}, \dots, f_s^{\mathrm{top}})$ is not zero-dimensional the degree of regularity does not provide an immediate insight on the complexity of solving the related system. We prove that this is the case for the systems under study. More precisely, in Proposition 5.4 we compute the Krull dimension of the ideal generated by the top part of the system. We need a technical lemma.

Lemma 5.3. *Let K be a field, and let $S = K[x_1, \dots, x_n]$ be a polynomial ring. We consider the monomial ideal $I = (x_1, x_1x_2, \dots, x_{n-1}x_n, x_n)$. Then, we have*

$$\dim(S/I) = \begin{cases} \frac{n-2}{2} & \text{if } n \text{ even} \\ \frac{n-1}{2} & \text{if } n \text{ odd.} \end{cases}$$

Proof. If $n = 1$ or 2, then $\dim(S/I) = \dim(K) = 0$, since K is a field. Let $n \geq 3$, then

$$\dim(S/I) = \dim(K[x_2, \ldots, x_{n-1}]/(x_2x_3, \ldots, x_{n-2}x_{n-1})).$$

Thus, for computing the Krull dimension we may replace the polynomial ring by $S = K[y_1, \ldots, y_t]$ and the ideal by $I = (y_1y_2, \ldots, y_{t-1}y_t)$. Now, the dimension of I can be computed as

$$\dim S/I = t - \min\{\mathrm{ht}(P) \mid P \in \mathrm{Min}(I)\},$$

where $\mathrm{Min}(I)$ is the set of minimal primes of I. Now, let $t = 2k$ be even ($k \in \mathbb{Z}_{\geq 1}$). We claim that the ideal $\mathcal{P} = (y_2, y_4, \ldots, y_{2k})$ of height k is the minimal prime ideal over I that realizes the minimum above.

By [27, Theorem 1.3.1, Corollary 1.3.4] an irredundant presentation of I is given by

$$I = \bigcap_{i=1,\ldots,s} V_i,$$

where each V_i is a (prime) ideal of variables with $\mathrm{ht}(V_i) = \mu(V_i)$. Moreover, since I is squarefree (hence radical), we can write

$$I = \bigcap_{P \in \mathrm{Min}(I)} P.$$

For any $i = 1, \ldots, 2k-1$, we have $y_i \mid y_iy_{i+1}$ and $y_{i+1} \mid y_iy_{i+1}$ and either i or $i+1$ is even, thus the prime ideal $\mathcal{P}$ contains I. We claim that it does not exist a minimal prime ideal $\mathcal{P}'$ of I such that $\mathrm{ht}(\mathcal{P}') < \mathrm{ht}(\mathcal{P})$. Once the claim is proved, then we are done since $\mathcal{P}$ will be minimal and of the smallest possible height.

Assume by contradiction, that such a $\mathcal{P}'$ exists. Thanks to the decompositions above, we have

$$I = \bigcap_{i=1,\ldots,s} V_i = \bigcap_{P \in \mathrm{Min}(I)} P.$$

By properties of the irredundant decomposition (see [27, Lemma 1.3.5]), for every $P \in \mathrm{Min}(I)$ there exists $i \in \{1, \ldots, s\}$ such that $P = V_i$. Then, for some $h \in \{1, \ldots, s\}$, we have $\mathcal{P}' = V_h$. In particular, $\mathcal{P}'$ is an ideal of variables, so $\mu(\mathcal{P}') = \mathrm{ht}(\mathcal{P}') < k$. This tells us that there exist two consecutive variables y_c, y_{c+1} (for some $c \in \{1, \ldots, 2k-1\}$) such that $y_c, y_{c+1} \notin \mathcal{P}'$. But $y_cy_{c+1} \in I$, so $I \not\subseteq \mathcal{P}'$, and this is a contradiction. So, the Krull dimension of $\tilde{I}$ is $t - k = 2k - k = k = \frac{n-2}{2}$.

For $t = 2k - 1$ odd the argument is the same but $\mathcal{P} = (y_2, y_4, \ldots, y_{2k-2})$ is the minimal prime ideal which realizes the height. □

Proposition 5.4. *Let $m \geq 2$. The (Krull) dimension of the ideals $(\mathcal{M}^{\mathrm{top}}_{\ell,m})$,$(\mathcal{R}^{\mathrm{top}}_{2,m-1})$ and $(\mathcal{R}^{\mathrm{top}}_{3,m})$ coincides and it is equal to*

$$\begin{cases} \frac{m-2}{2} & \text{if } m \text{ even} \\ \frac{m-3}{2} & \text{if } m \text{ odd.} \end{cases}$$

In particular, if $m \geq 4$, these ideals are not zero-dimensional.

Proof. For every statement, we use Lemma 5.3 with $n = m - 1$ to conclude. For $(\mathcal{M}^{\mathrm{top}}_{\ell,m})$, we have that $(\mathcal{M}^{\mathrm{top}}_{\ell,m}) = (j_1^{\ell+1}, j_1^{\ell}j_2^{\ell}, \ldots, j_{m-2}^{\ell}j_{m-1}^{\ell}, j_{m-1}^{\ell+1})$. Passing to the radical the Krull dimension does not change and $\sqrt{(\mathcal{M}^{\mathrm{top}}_{\ell,m})} = (j_1, j_1j_2, \ldots, j_{m-2}j_{m-1}, j_{m-1})$ has the shape of Lemma 5.3. Similarly, we have that $\sqrt{(\mathcal{R}^{\mathrm{top}}_{2,m-1})} = (\alpha_0, \alpha_0\alpha_1, \ldots, \alpha_{m-3}\alpha_{m-2}, \alpha_{m-2})$, and $\sqrt{(\mathcal{R}^{\mathrm{top}}_{3,m})} = (a_1, a_1a_2, \ldots, a_{m-2}a_{m-1}, a_{m-1})$. □

Another consequence of Proposition 5.4 is that when $m \geq 4$ the polynomial systems are not semi-regular [4, 7, 34].

Corollary 5.5. *For every $m \geq 4$, we have that $\mathcal{M}^{\text{top}}_{\ell,m}$, $\mathcal{R}^{\text{top}}_{2,m-1}$ and $\mathcal{R}^{\text{top}}_{3,m}$ are not semi-regular sequences.*

Another invariant which can be used as a proxy for the solving degree is the Castelnuovo–Mumford regularity. Indeed, when the ideal is in generic coordinates in the sense of Bayer and Stillman [5], then the regularity of the ideal generated by the homogenized polynomials of the system is greater or equal than the solving degree of the system by [12]. On the other hand, in Proposition 5.7, we prove that the systems $\mathcal{M}_{\ell,m}$, $\mathcal{R}_{2,m-1}$ and $\mathcal{R}_{3,m}$ are not in generic coordinates.

For the convenience of the reader, we recall here the relevant definitions and notations. Let K be a field and let $S = K[x_1, \dots, x_n]$ be a polynomial ring. For a polynomial $f \in S$, we denote by $f^h \in R = S[t]$ its homogenization with respect to an extra variable t, that is

$$f^h = t^{\deg(f)} \cdot f\left(\frac{x_1}{t}, \dots, \frac{x_n}{t}\right).$$

For a list of polynomials $\mathcal{F} = [f_1, \dots, f_s]$ in S, we denote by $\mathcal{F}^h = [f_1^h, \dots, f_s^h]$ the list of the homogenized polynomials in R. If $I \subseteq S$ is an ideal, we denote by I^h the ideal generated by all the homogenizations of elements in I, that is $I^h = (f^h \mid f \in I)$. Clearly, we have $(\mathcal{F}^h) \subseteq (\mathcal{F})^h$, but the inclusion may be strict.

Given a homogeneous ideal J of R, the *saturation* of J with respect to the irrelevant maximal ideal $\mathfrak{m} = (x_1, \dots, x_n, t)$ of R is

$$J^{\text{sat}} = \bigcup_{d \geq 0} \{f \in R \mid fm \in J \ \forall m \in R_d\} = \bigcup_{d \geq 0} (J : \mathfrak{m}^d).$$

We stress that the condition $fm \in J \ \forall m \in R_d$ can be checked only on the monomials of R_d, since they form a K-basis for R_d and J is an ideal. Moreover, we always have that $J \subseteq J^{\text{sat}}$. Now, let $\overline{J} = J\overline{K}[x_1, \dots, x_n, t]$ be the extension of the ideal J over the algebraic closure $\overline{K}$ of K. We say that J is in *generic coordinates* over $\overline{K}$ if $|\mathcal{Z}_+(\overline{J})| < \infty$ and either $|\mathcal{Z}_+(\overline{J})| = 0$ or $t \nmid 0$ modulo $\overline{J}^{\text{sat}}$.

Lemma 5.6. *Let K be an algebraically closed field and let $S = K[x_1, \dots, x_n]$ be a polynomial ring. Let $\mathcal{F} = [f_1, \dots, f_m]$ be a list of non-homogeneous polynomials such that $|\mathcal{Z}(\mathcal{F})| = 1$. Assume that there exists $i \in \{1, \dots, n\}$ such that for all integers $a \geq 1$ we have $x_i^a \notin \text{Supp}(\mathcal{F}^h) = \bigcup_{c=1}^{m} \text{Supp}(f_c^h)$. Then, the ideal $(\mathcal{F}^h)$ is not in generic coordinates over K.*

Proof. Let $\mathcal{Z}(\mathcal{F}) = \{(a_1, \dots, a_n)\} \subseteq K^n$. Thanks to the Shape Lemma (see e.g. [12]), we get that $\text{LexGB}((\mathcal{F})) = [x_1 - a_1, \dots, x_n - a_n]$. Since $(\mathcal{F})$ is zero-dimensional, $[x_1 - a_1, \dots, x_n - a_n]$ is also the reduced Gröbner basis with respect to DegRevLex. Thanks to [37, Proposition 4.3.21], the homogenized ideal $(\mathcal{F})^h$ is generated by the homogenization of this basis, that is

$$(\mathcal{F})^h = (x_1 - a_1 t, \dots, x_n - a_n t) \subseteq S[t] = R.$$

From now on, we equip R with the DegRevLex term order with $x_1 > \cdots > x_n > t$. Moreover, we have that $(\mathcal{F}^h) \subseteq (\mathcal{F}^h)^{\text{sat}} \subseteq (\mathcal{F})^h$, where the former follows from the definition of saturation and the latter from the fact that

$$(\mathcal{F}^h)^{\text{sat}} = \bigcup_{d \geq 0} ((\mathcal{F}^h) : \mathfrak{m}^d), \qquad (\mathcal{F})^h = \bigcup_{d \geq 0} ((\mathcal{F}^h) : (t)^d), \qquad \text{and } (t) \subseteq \mathfrak{m}.$$

Now, we claim that $t \mid 0$ modulo $(\mathcal{F}^h)^{\text{sat}}$. By assumption, we can fix $i \in \{1,\dots,n\}$ such that $x_i^a \notin \text{Supp}(\mathcal{F}^h)\ \forall a \in \mathbb{Z}_{\geq 1}$ and we know that $x_i - a_i t \in (\mathcal{F})^h$. So, again since $(\mathcal{F})^h = \bigcup_{d\geq 0}((\mathcal{F}^h) : (t)^d)$, there exists $\tilde{d} \in \mathbb{Z}_{\geq 1}$ such that

$$(x_i - a_i t) \cdot t^{\tilde{d}} \in (\mathcal{F}^h) \subseteq (\mathcal{F}^h)^{\text{sat}}.$$

Note that $\tilde{d}$ cannot be 0. In fact, since by assumption $x_i^a \notin \text{Supp}(\mathcal{F}^h)$ for all $a \in \mathbb{Z}_{\geq 1}$, then $x_i \in \text{Supp}(x_i - a_i t)$ cannot be written as a polynomial combination of the generators $\mathcal{F}^h$.

If we prove that $x_i - a_i t \notin (\mathcal{F}^h)^{\text{sat}}$, the claim follows. Suppose by contradiction that $x_i - a_i t \in (\mathcal{F}^h)^{\text{sat}}$. Then, by definition of saturation, there exists $d' \in \mathbb{Z}_{\geq 0}$ such that $x_i - a_i t \in [(\mathcal{F}^h) : \mathfrak{m}^{d'}]$. Now, $x_i^{d'} \in \mathfrak{m}^{d'}$, so

$$f = (x_i - a_i t) \cdot x_i^{d'} = x_i^{d'+1} - a_i x_i^{d'} t \in (\mathcal{F}^h).$$

But, since by assumption $x_i^a \notin \text{Supp}(\mathcal{F}^h)$ for all $a \in \mathbb{Z}_{\geq 1}$, again $x_i^{d'+1} \in \text{Supp}(f)$ cannot be written as a polynomial combination of the generators $\mathcal{F}^h$. Therefore $f \notin (\mathcal{F}^h)$ and we get a contradiction, which proves the claim.

Finally, since $(a_1,\dots,a_n) \in \mathcal{Z}(\mathcal{F})$, we get that $[a_1 : \cdots : a_n : 1] \in \mathcal{Z}_+(\mathcal{F}^h)$, so $|\mathcal{Z}_+(\mathcal{F}^h)| > 0$. This concludes the proof. □

Proposition 5.7. *Let $m \geq 4$ and let $\mathcal{F} = \mathcal{M}_{\ell,m}$, $\mathcal{R}_{2,m-1}$, or $\mathcal{R}_{3,m}$. If $|\mathcal{Z}(\mathcal{F})| = 1$, then $(\mathcal{F}^h)$ is not in generic coordinates over $\overline{\mathbb{F}}_p$.*

Proof. Let $\mathcal{F} = \mathcal{M}_{\ell,m}$. Since $m \geq 4$, we have that $j_2^b \notin \text{Supp}(\mathcal{M}_{\ell,m}^h)$ for all $b \in \mathbb{Z}_{\geq 1}$. So, we conclude using Lemma 5.6. Similarly, for $\mathcal{R}_{2,m-1}$, it holds $\alpha_1^b \notin \text{Supp}(\mathcal{M}_{2,m-1}^h)$ for all $b \in \mathbb{Z}_{\geq 1}$ and for $\mathcal{R}_{3,m}$ it holds $a_2^b \notin \text{Supp}(\mathcal{M}_{3,m}^h)$ for all $b \in \mathbb{Z}_{\geq 1}$, so in both cases we conclude using again Lemma 5.6. □

Remark 5.8. If $m \geq 6$ for $\mathcal{F} = \mathcal{M}_{\ell,m}$, $\mathcal{R}_{2,m-1}$, or $\mathcal{R}_{3,m}$, it is easier to check that $(\mathcal{F}^h)$ is not in generic coordinates over $\overline{\mathbb{F}}_p$. In fact, one can show that $|\mathcal{Z}_+(\overline{\mathcal{F}^h})| = \infty$. Indeed, $[0 : v_1 : 0 : \cdots : 0 : v_2 : 0] \in \mathcal{Z}_+(\overline{\mathcal{F}^h})$ for all $v_1, v_2 \in \overline{\mathbb{F}}_p$ linearly independent.

6. Experimental Results

We solved the polynomial systems arising from the previous modelings using Gröbner bases in order to compare the modeling based on Renes polynomials with that based on modular polynomials. All computations were performed using Magma V2.28-13 [8], on a Dell Inc. Precision 7875 Tower, with 64 GB of RAM and processor AMD ®Ryzen threadripper pro 7975wx 32-cores x 64.

We constructed the test examples as follows. Let $d = 2, 3$ be the degree. We selected a random supersingular elliptic curve E_{start} in Montgomery form (for degree $d = 2$) or triangular form (for degree $d = 3$) and we constructed a non-backtracking path of length m of isogenies obtaining the curve E_{finish}. Then, we built the system $\mathcal{M}_{d,m}$ of modular polynomials (Polynomial system 1) and $\mathcal{R}_{d,m}$ of Renes polynomials (Polynomial System 3 and Polynomial System 5) to recover the path from E_{start} to E_{finish}. These systems were solved using Magma's implementation of F4 [23]. We recorded the CPU time and the maximal degree reached during the Gröbner basis computation (used as a proxy for the solving degree).

We repeated these computations for nine different values of the underlying prime p, ranging from 10 to 32 bits. For each set of parameters, we performed 10 tests. In Table 1 and Table 2, we report the results for degrees 2 and 3, respectively. The results show that the solving degree is consistently smaller for Renes polynomials than for modular polynomials. Moreover, the average solving times

are two to three orders of magnitude lower for Renes polynomials. This allows us to solve paths of isogenies of length up to 16 in degree 2 for small primes, whereas we are limited to length 12 when using modular polynomials. A similar trend is observed in degree 3.

Remark 6.1. To solve longer paths of degree 3 isogenies described by the modular polynomial systems $\mathcal{M}_{3,m}$, Takahashi et al. [44] split the system into two halves and compute a Gröbner basis for each of them. Then, by eliminating variables, they find the solutions. This technique can also be applied to the polynomial systems $\mathcal{R}_{2,m}$ and $\mathcal{R}_{3,m}$ with Renes polynomials, allowing one to recover longer isogeny paths. However, to enable a clearer comparison of the systems, we chose not to apply this splitting technique to any of the computations performed in this paper.

m	$\mathrm{tm}(\mathcal{M}_{2,m})$	$\mathrm{tm}(\mathcal{R}_{2,m})$	$\mathrm{sd}(\mathcal{M}_{2,m})$	$\mathrm{sd}(\mathcal{R}_{2,m})$	m	$\mathrm{tm}(\mathcal{M}_{2,m})$	$\mathrm{tm}(\mathcal{R}_{2,m})$	$\mathrm{sd}(\mathcal{M}_{2,m})$	$\mathrm{sd}(\mathcal{R}_{2,m})$
$p = 587417, 20$ bits					$p = 919447, 20$ bits				
6	0.02	0.003	6	4	6	0.02	0.002	6	4
7	0.514	0.018	7	5	7	0.671	0.02	7	5
8	1.722	0.09	7	5	8	2.612	0.102	7	5
9	66.563	0.298	8	5	9	135.981	0.375	8	5
10	78.454	2.008	8	5	10	179.822	3.009	8	5
11	3040.88	15.958	9	5	11	10055.526	27.815	9	5
12	3359.307	50.588	9	5	12	11223.916	96.897	9	5
13	> 7 hrs	104.499		6	13	> 7 hrs	213.71		6
14		434.435		6	14		1016.976		6
15		7632.326		6	15		> 7 hrs		
16		23416.61		6	16				
17		> 7 hrs			17				
$p = 15739441, 24$ bits					$p = 16541149, 24$ bits				
6	0.02	0.001	6	4	6	0.02	0.001	6	4
7	0.502	0.018	7	5	7	0.506	0.019	7	5
8	1.738	0.09	7	5	8	1.716	0.08	7	5
9	67.766	0.309	8	5	9	67.375	0.276	8	5
10	76.685	2.019	8	5	10	77.189	1.951	8	5
11	2710.243	15.68	9	5	11	2692.042	15.635	9	5
12	2618.765	50.162	9	5	12	2610.953	50.164	9	5
13	> 7 hrs	104.273		6	13	> 7 hrs	103.944		6
14		437.867		6	14		438.755		6
15		7582.87		6	15		7703.542		6
16		23514.02		6	16		> 7 hrs		
17		> 7 hrs			17				
$p = 266545607, 28$ bits					$p = 2757059413, 32$ bits				
6	0.022	0.003	6	4	6	0.086	0.01	6	4
7	0.704	0.02	7	5	7	2.333	0.06	7	5
8	2.674	0.102	7	5	8	8.678	0.387	7	5
9	129.268	0.371	8	5	9	390.104	1.361	8	5
10	168.687	2.923	8	5	10	476.839	10.147	8	5
11	9739.063	27.347	9	5	11	21743.386	86.571	9	5
12	11001.887	95.651	9	5	12	22894.691	284.438	9	5
13	> 7 hrs	207.348		6	13	> 7 hrs	612.507		6
14		1000.487		6	14		2762.891		6
15		> 7 hrs			15		> 7 hrs		

TABLE 1. Timings and solving degrees for polynomial systems modeling a SIP of degree 2^m. The values $\mathrm{tm}(\mathcal{M}_{2,m})$ and $\mathrm{tm}(\mathcal{R}_{2,m})$ record the average time (in seconds) of solving the polynomial systems $\mathcal{M}_{2,m}$ (modular polynomials) and $\mathcal{R}_{2,m}$ (Renes polynomials) modeling a SIP of degree 2^m; $\mathrm{sd}(\mathcal{M}_{2,m})$ and $\mathrm{sd}(\mathcal{R}_{2,m})$ are the highest step degrees obtained during the computation by using Magma F4 implementation.

m	$\mathrm{tm}(\mathcal{M}_{3,m})$	$\mathrm{tm}(\mathcal{R}_{3,m})$	$\mathrm{sd}(\mathcal{M}_{3,m})$	$\mathrm{sd}(\mathcal{R}_{3,m})$	m	$\mathrm{tm}(\mathcal{M}_{3,m})$	$\mathrm{tm}(\mathcal{R}_{3,m})$	$\mathrm{sd}(\mathcal{M}_{3,m})$	$\mathrm{sd}(\mathcal{R}_{3,m})$
$p = 919447, 20$ bits					$p = 15739441, 24$ bits				
6	0.901	0.074	8	6	6	0.648	0.06	8	6
7	76.149	1.345	10	7	7	43.406	0.916	10	7
8	1887.466	30.398	10	7	8	724.222	17.511	10	7
9	> 7 hrs	42.104		8	9	11580.257	203.132	11	8
10		2620.534		8	10	$m > 9$	1000.555		8
11		> 7 hrs			11		17300.334		9
12					12		> 7 hrs		
$p = 16541149, 24$ bits					$p = 12239911, 24$ bits				
6	0.652	0.06	8	6	6	0.906	0.074	8	6
7	43.066	0.912	10	7	7	74.625	1.304	10	7
8	726.928	17.443	10	7	8	1721.217	29.82	10	7
9	11609.202	202.294	11	8	9	> 7 hrs	411.02		8
10	> 7 hrs	1001.411		8	10		2531.694		8
11		17303.164		9	11		> 7 hrs		
12		> 7 hrs			12				
$p = 266545607, 28$ bits					$p = 2757059413, 32$ bits				
6	0.897	0.073	8	6	6	2.968	0.283	8	6
7	75.404	1.302	10	7	7	241.397	4.486	10	7
8	1766.141	30.031	10	7	8	4705.333	95.73	10	7
9	> 7 hrs	419.066		8	9	> 7 hrs	1225.204		8
10		2579.288		8	10		6568.001		8
11		> 7 hrs			11		> 7 hrs		

TABLE 2. Timings and solving degrees for polynomial systems modeling a SIP of degree 3^m. The values $\mathrm{tm}(\mathcal{M}_{3,m})$ and $\mathrm{tm}(\mathcal{R}_{3,m})$ record the average time (in seconds) of solving the polynomial systems $\mathcal{M}_{3,m}$ (modular polynomials) and $\mathcal{R}_{3,m}$ (Renes polynomials) modeling a SIP of degree 3^m. $\mathrm{sd}(\mathcal{M}_{3,m})$ and $\mathrm{sd}(\mathcal{R}_{3,m})$ are the highest step degrees obtained during the computation by using Magma F4 implementation.

REFERENCES

[1] G. ADJ, O. AHMADI, AND A. MENEZES, *On isogeny graphs of supersingular elliptic curves over finite fields*, Finite Fields Appl., 55 (2019), pp. 268–283. 8

[2] M. R. ALBRECHT, C. CID, J.-C. FAUGÈRE, R. FITZPATRICK, AND L. PERRET, *Algebraic Algorithms for LWE Problems*, ACM Commun. Comput. Algebra, 49 (2015), p. 62. 1

[3] S. ARORA AND R. GE, *New Algorithms for Learning in Presence of Errors*, in Automata, Languages and Programming, L. Aceto, M. Henzinger, and J. Sgall, eds., Berlin, Heidelberg, 2011, Springer Berlin Heidelberg, pp. 403–415. 1

[4] M. BARDET, J. C. FAUGÈRE, AND B. SALVY, *On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations*, in ICPPSS International Conference on Polynomial System Solving, 2004. 2, 5, 16, 18

[5] D. BAYER AND M. STILLMAN, *A criterion for detecting m-regularity*, Invent. Math., 87 (1987), pp. 1–11. 18

[6] D. J. BERNSTEIN, C. CHUENGSATIANSUP, D. KOHEL, AND T. LANGE, *Twisted Hessian curves*, in Progress in cryptology—LATINCRYPT 2015, vol. 9230 of Lecture Notes in Comput. Sci., Springer, Cham, 2015, pp. 269–294. 13

[7] M. Bigdeli, E. De Negri, M. M. Dizdarevic, E. Gorla, R. Minko, and S. Tsakou, *Semi-regular sequences and other random systems of equations*, in Women in numbers Europe III—research directions in number theory, vol. 24 of Assoc. Women Math. Ser., Springer, Cham, [2021] ©2021, pp. 75–114. 18

[8] W. Bosma, J. Cannon, and C. Playoust, *The Magma Algebra System. I. The User Language*, vol. 24, 1997, pp. 235–265. Computational algebra and number theory (London, 1993). 19

[9] B. Buchberger, *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*, PhD thesis, University of Innsbruck, 1965. 4

[10] J. Burdges and L. De Feo, *Delay Encryption*, in Advances in cryptology—EUROCRYPT 2021. Part I, vol. 12696 of Lecture Notes in Comput. Sci., Springer, Cham, [2021] ©2021, pp. 302–326. 2, 7, 8

[11] A. Caminata, R. Cartor, A. Meneghetti, R. Mora, and A. Pellegrini, *Quadratic Modelings of Syndrome Decoding*, in Post-quantum cryptography. Part I, vol. 15577 of Lecture Notes in Comput. Sci., Springer, Cham, [2025] ©2025, pp. 35–70. 1

[12] A. Caminata and E. Gorla, *Solving multivariate polynomial systems and an invariant from commutative algebra*, in Arithmetic of finite fields, vol. 12542 of Lecture Notes in Comput. Sci., Springer, Cham, [2021] ©2021, pp. 3–36. 2, 4, 5, 18

[13] ———, *Solving degree, last fall degree, and related invariants*, J. Symbolic Comput., 114 (2023), pp. 322–335. 5

[14] D. Charles and K. Lauter, *Computing Modular Polynomials*, LMS J. Comput. Math., 8 (2005), pp. 195–204. 6

[15] M. Corte-Real Santos, C. Costello, and J. Shi, *Accelerating the Delfs-Galbraith Algorithm with Fast Subfield Root Detection*, in Annual International Cryptology Conference, Springer, 2022, pp. 285–314. 1

[16] C. Costello and H. Hisil, *A simple and compact algorithm for SIDH with arbitrary degree isogenies*, in Advances in cryptology—ASIACRYPT 2017. Part II, vol. 10625 of Lecture Notes in Comput. Sci., Springer, Cham, 2017, pp. 303–329. 2, 7

[17] C. Costello and B. Smith, *The Supersingular Isogeny Problem in Genus 2 and Beyond*, in Post-quantum cryptography, vol. 12100 of Lecture Notes in Comput. Sci., Springer, Cham, [2020] ©2020, pp. 151–168. 1

[18] N. Courtois, A. Klimov, J. Patarin, and A. Shamir, *Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations*, in Advances in cryptology—EUROCRYPT 2000 (Bruges), vol. 1807 of Lecture Notes in Comput. Sci., Springer, Berlin, 2000, pp. 392–407. 4

[19] G. D'Alconzo, A. Gangemi, L. Romano, and G. Romeo, *Rethinking r-PKP: a New Formulation for the Relaxed Permuted Kernel Problem*. Cryptology ePrint Archive, Paper 2026/631, 2026. 1

[20] L. De Feo, D. Kohel, A. Leroux, C. Petit, and B. Wesolowski, *SQISign: compact post-quantum signatures from quaternions and isogenies*, in Advances in cryptology—ASIACRYPT 2020. Part I, vol. 12491 of Lecture Notes in Comput. Sci., Springer, Cham, [2020] ©2020, pp. 64–93. 1

[21] C. Delfs and S. D. Galbraith, *Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$*, Des. Codes Cryptogr., 78 (2016), pp. 425–440. 1

[22] V. Dubois and N. Gama, *The Degree of Regularity of HFE Systems*, in Advances in cryptology—ASIACRYPT 2010, vol. 6477 of Lecture Notes in Comput. Sci., Springer, Berlin, 2010, pp. 557–576. 5

[23] J.-C. Faugére, *A new efficient algorithm for computing Gröbner bases* (F_4), vol. 139, 1999, pp. 61–88. Effective methods in algebraic geometry (Saint-Malo, 1998). 4, 19

[24] J.-C. Faugère, *A new efficient algorithm for computing Gröbner bases without reduction to zero* (F_5), in Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation, ACM, New York, 2002, pp. 75–83. 4

[25] J. C. Faugère, P. Gianni, D. Lazard, and T. Mora, *Efficient Computation of Zero-dimensional Gröbner Bases by Change of Ordering*, J. Symbolic Comput., 16 (1993), pp. 329–344. 5

[26] S. D. Galbraith, C. Petit, and J. Silva, *Identification Protocols and Signature Schemes Based on Supersingular Isogeny Problems*, J. Cryptology, 33 (2020), pp. 130–175. 1

[27] J. Herzog and T. Hibi, *Monomial Ideals*, Springer, 2011. 17

[28] M.-D. A. Huang, M. Kosters, Y. Yang, and S. L. Yeo, *On the last fall degree of zero-dimensional Weil descent systems*, J. Symbolic Comput., 87 (2018), pp. 207–226. 5

[29] D. Husemöller, *Elliptic Curves*, vol. 111 of Graduate Texts in Mathematics, Springer-Verlag, New York, second ed., 2004. With appendices by Otto Forster, Ruth Lawrence and Stefan Theisen. 5

[30] B. W. Jordan, A. G. Keeton, B. Poonen, E. M. Rains, N. Shepherd-Barron, and J. T. Tate, *Abelian varieties isogenous to a power of an elliptic curve*, Compositio Mathematica, 154 (2018), p. 934–959. 6

[31] D. R. Kohel, *Endomorphism rings of elliptic curves over finite fields*, PhD thesis, University of California, Berkeley, 1996. 7
[32] A. Meneghetti, A. Pellegrini, and M. Sala, *On the equivalence of two post-quantum cryptographic families*, Ann. Mat. Pura Appl. (4), 202 (2023), pp. 967–991. 1
[33] K. Okeya, H. Kurumatani, and K. Sakurai, *Elliptic Curves with the Montgomery-Form and Their Cryptographic Applications*, in Public key cryptography (Melbourne, 2000), vol. 1751 of Lecture Notes in Comput. Sci., Springer, Berlin, 2000, pp. 238–257. 7
[34] K. Pardue, *Generic sequences of polynomials*, J. Algebra, 324 (2010), pp. 579–590. 18
[35] J. Renes, *Computing Isogenies Between Montgomery Curves Using the Action of* $(0,0)$, in Post-quantum cryptography, vol. 10786 of Lecture Notes in Comput. Sci., Springer, Cham, 2018, pp. 229–247. 2, 3, 7, 8, 12, 13
[36] L. Robbiano and M. Kreuzer, *Computational Commutative Algebra 1*, Springer-Verlag, Berlin Heidelberg, 2000. 16
[37] ———, *Computational Commutative Algebra 2*, Springer-Verlag, Berlin Heidelberg, 2005. 16, 18
[38] M. A. Saeed, *Algebraic Approach for Code Equivalence*, PhD thesis, Normandie Université; University of Khartoum, 2017. 1
[39] F. Salizzoni, *An upper bound for the solving degree in terms of the degree of regularity*, Transactions on Mathematical Cryptology, 5 (2025), pp. 1–7. 2, 16
[40] R. Schoof, *Nonsingular Plane Cubic Curves over Finite Fields*, J. Combin. Theory Ser. A, 46 (1987), pp. 183–211. 7
[41] J. H. Silverman, *The Arithmetic of Elliptic Curves*, vol. 106 of Graduate Texts in Mathematics, Springer-Verlag, New York, 1986. 6, 8
[42] M. J. Steiner, *The Complexity of Algebraic Algorithms for LWE*, in Advances in cryptology—EUROCRYPT 2024. Part III, vol. 14653 of Lecture Notes in Comput. Sci., Springer, Cham, [2024] ©2024, pp. 375–403. 1
[43] A. Sutherland, *MIT Lecture Notes, 18.783 - Spring 2021*, tech. rep., MIT, 2021. 5
[44] Y. Takahashi, M. Kudo, R. Fukasaku, Y. Ikematsu, M. Yasuda, and K. Yokoyama, *Algebraic approaches for solving isogeny problems of prime power degrees*, J. Math. Cryptol., 15 (2021), pp. 31–44. 1, 2, 3, 5, 16, 20
[45] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math., 2 (1966), pp. 134–144. 9
[46] The Sage Developers, *SageMath, the Sage Mathematics Software System (Version x.y.z)*, 2025. `https://www.sagemath.org`. 6
[47] K. Tsukazaki, *Explicit isogenies of elliptic curves*, PhD thesis, University of Warwick, 2013. 6
[48] L. C. Washington, *Elliptic Curves*, Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, second ed., 2008. Number theory and cryptography. 1

Dipartimento di Matematica, Università di Genova, via Dodecaneso 35, 16146, Genova, Italy
Email address: `alessio.caminata@unige.it`

Dipartimento di Matematica, Università di Genova, via Dodecaneso 35, 16146, Genova, Italy
Email address: `andrea.o.sanguineti@gmail.com`

Institute of Mathematics, University of Zurich, Zurich, Switzerland
Email address: `silvia.sconza@math.uzh.ch`