2020 12th International Conference on Cyber Conflict
20/20 Vision: The Next Decade
T. Jančárková, L. Lindström,
M. Signoretti, I. Tolga, G. Visky (Eds.)

Recent Developments in Cryptography

Lubjana Beshaj
Assistant Professor
Army Cyber Institute
United States Military Academy
West Point, New York,
United States of America
Lubjana.Beshaj@westpoint.edu

Andrew O. Hall
Associate Professor and Director
Army Cyber Institute
United States Military Academy
West Point, New York,
United States of America
Andrew.Hall@westpoint.edu

Abstract: In this short note, we briefly describe cryptosystems that are believed to be quantum-resistant and focus on isogeny-based cryptosystems. Recent SIDH (Supersingular Isogeny Diffie-Hellman) developments have focused on (2,2)-reducible Jacobians, where addition is executed via the Kummer surface. While elliptic curve isogenies are easy, explicit, and fast to compute thanks to Velús formulas, this is not the case for higher genus curves. The case of (2,2)-isogenies in genus 2 curves are an exception thanks to the work of Richelot. In addition, some explicit work has been completed in the case of (3,3) and (5,5)-isogenies, which are much more complicated than the case of Richelot isogenies. In this paper, we further investigate the case of (4,4)-reducible Jacobians and explicitly compute the locus $\mathcal{L}_4$.

Keywords: *quantum computing, post quantum cryptography, supersingular elliptic curves, Jacobian surfaces, isogenies, split Jacobians*

1. INTRODUCTION

Quantum computers are powerful machines that take a new approach to processing information and may lead to revolutionary breakthroughs in a variety of areas to include artificial intelligence, drug discovery, materials science, and optimization of complex man-made systems. While increased computational power, such as that offered by quantum computers, can be used for good, these advances do present a threat to public key cryptography. Public key cryptography, and cryptography in general, rely on computational hard or expensive problems. Problems that were extremely hard when only equipped with a pencil and paper are now easily solved with a classical computer. While hard problems for classical computing, like the discrete log problem, ensure the strength of today's current public key cryptography, new quantum algorithms can address these hard problems in polynomial time. Peter Shor, in his paper [37], provided an algorithm to solve the discrete log problem, demonstrating how to use a quantum computer to factor a positive odd integer. With the advent of these quantum algorithms, an adversary could efficiently break the universally adopted public-key cryptographic schemes (e.g. RSA, DSA and elliptic-curve cryptography).

In order to mitigate against this imminent threat, cryptographic schemes that are resistant to increased computing power offered by quantum computers have drawn great attention from both academia and industry. These schemes are collectively referred to as post-quantum cryptography (PQC). Whereas some cryptographic schemes will be rendered obsolete, several existing protocols, (e.g. current symmetric cryptography) do not need to be changed significantly to be considered quantum-resistant (i.e. post-quantum symmetric cryptography).

In April 2016, the National Institute of Science and Technology (NIST) initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. They announced the release of NIST Interagency Report (NISTIR) 8105, a report on Post Quantum Cryptography (see [5] for more details). In this report, they explain the status of quantum computing and post-quantum cryptography, and outline a research plan for future work in these areas. In December 2016, NIST announced a formal call for proposals.

In the first round, 69 algorithms were submitted in response to the call for proposals and competition. Detailed information concerning these algorithms and the comments provided by the world-wide cryptography community are available on the NIST webpage (https://csrc.nist.gov/Projects/Post-Quantum-Cryptography).

As the latest step in the program to develop effective defenses and new standards, NIST has selected 26 of the 69 submitted cryptographic algorithms. There are 17

second round candidates for public-key encryption and key-establishment algorithms and 9 second round candidates for digital signatures. This second round will focus on evaluating submissions performance across a wide variety of systems and platforms as a variety of devices will require effective encryption.

After the completion of the second round of reviews, there still exists the possibility of an additional round of review before NIST announces the post-quantum algorithms that will supplement or replace the most vulnerable cryptosystems currently in use. The state of quantum computer development will determine the requirement for a third round of competition.

A tentative timeline made public by NIST will be given in the following table.

TABLE 1: NIST TIMELINE

Feb 24-26, 2016	NIST Presentation at PQCrypto 2016: Announcement and outline of NIST's Call for Submissions
April 28, 2016	NIST releases NISTIR 8105, Report on Post-Quantum Cryptography
Dec 20, 2016	Formal Call for Proposal
Nov 30, 2017	Deadline for submissions
Dec 4, 2017	NIST Presentation at AsiaCrypt 2017: The Ship Has Sailed: The NIST Post-Quantum Crypto "Competition"
Dec 21, 2017	Round 1 algorithms announced (69 submissions accepted as "complete and proper")
Apr 11, 2018	NIST Presentation at PQCrypto 2018: Let's Get Ready to Rumble – The NIST PQC "Competition"
April 11-13, 2018	First PQC Standardization Conference Submitter's Presentations
2018/2019	Round 2 begins
August 2019	Second PQC Standardization Conference
2020/2021	Round 3 begins or select algorithms
2022/2024	Draft Standards Available

The new algorithms rely on several cryptographic schemes that are believed to be post-quantum-resistant and include the following:

1. Code-based cryptography;
2. Multivariate Cryptography;
3. Lattice-based Cryptography;
4. Hash-based Cryptography;
5. Isogeny-based Cryptography.

Each of these cryptographic schemes has advantages and disadvantages, and the algorithms vary in both their performance measures and maturity. In this paper, we will focus on isogeny-based cryptography.

Supersingular isogeny-based cryptography is one of the more recent advances based on the arithmetic of elliptic curves. In 2011, Jao and De Feo proposed Supersingular Isogeny Diffie-Hellman (SIDH) as a key exchange protocol that would offer post-quantum security. Isogeny-based algorithms rely on the structure of large isogeny graphs, and the cryptographically interesting properties of these graphs are tied to their expansion properties.

In recent developments in supersingular isogeny-based cryptography (SIDH), Costello [8] focuses on (2,2) reducible Jacobians, where addition is executed via Kummer surfaces. More importantly, it seems that the most interesting case is when E_1 is isogenous to E_2. In this case, as the decomposition of the Abelian varieties is determined up to isogeny, the 2-dimensional Jacobian is isogenous to E^2. There are several interesting questions that arise when we consider such Jacobians over the finite field $\mathbb{F}_p$.

The space of genus 2 curves with (n,n) reducible Jacobians, for which $n=2$ or where n is odd, is a 2-dimensional irreducible locus $\mathcal{L}_n$ in the moduli space of curves $\mathcal{M}_2$. For $n=2$, this is the well known locus of curves with extra involutions [23], [24], [35]. In the cases where n is odd, these spaces were computed for the first time in [32], [34], [22].

If E_1 and E_2 are N-isogenous then their j-invariants j_1 and j_2 satisfy the equation of the modular curve $X_0(N)$, say $\mathcal{S}_N := \phi_N(j_1,j_2)=0$. Such a curve can be embedded in $\mathcal{M}_2$. An interesting problem to consider is the study of the intersection between $\mathcal{L}_n$ and $\mathcal{S}_N$ for given n and N. More precisely, for any number field K determines the number of K-rational points of this intersection. For the case when $n=2,3$ this was done in [3]. The case when $n=4$ is more complicated since the locus $\mathcal{L}_4$ is not explicitly computed. The focus of this paper is to compute the locus $\mathcal{L}_4$ and then further inverstigate when the

two elliptic components of the (n,n) reducible 2-dimensional Jacobians are isogenous to each other when $n=4$ and $N=2,3,5,7\ldots..$

The remainder of this paper is organized as follows. First we provide an overivew of quantum computing and briefly explain Shor and Grover's algorithms. In Section 3, we describe each of the cryptosystems mentioned above. Also, we further explain the small changes that should be made to the AES algorithm to allow for its continued use and to ensure its ability to resist exploitation by quantum computers. We briefly explain supersingular isogeny Diffie-Hellman key exchange, and finally explore (n,n)-split Jacobians and compute the locus $\mathcal{L}_4$.

2. QUANTUM COMPUTING

A classical computer has registers that are made up of bits, whereas a quantum computer has a single quantum register that is made up of qubits. Given q classical bits, their state is a binary string in $\{0,1\}^q$, which is a q-dimensional space. Whereas, a q-qubit quantum register is a 2^q -dimensional space. Hence, the dimension of the state space of a quantum computer grows exponentially while that of a classical computer grows linearly. Furthermore, the amount of information stored in a q-qubit quantum register is enormous compared with a classical q-bit computer. However, accessing the information stored in a quantum computer is not as easy as in a classical computer. Information on the quantum state is only gathered through a measurement gate.

One of the main questions regarding quantum computers is the type of algorithms that can be implemented on a quantum computer once they are fielded. There are three known algorithms that can be implemented on a quantum computer: Shor's, Grover's and Simon's algorithms.

In 1994, Peter Shor came up with a quantum algorithm that calculates the prime factors of a large number vastly more efficiently than a classical computer. This poses a threat to all modern cryptographic schemes that rely on the difficulty of factoring prime numbers. More generally, this algorithm poses a threat to all crypto-systems that rely on the difficulty of the discrete logarithm problem.

However, Shor's algorithm's efficiency and power relies on a quantum computer with a large number of quantum bits. It should be noted that Shor's algorithm is only partially executed on a quantum computer. While many have attempted to implement Shor's algorithm on various quantum systems, none have been successful in doing so with more than a few quantum bits or in a scalable way.

Grover's algorithm performs a search over an unordered set of $N=2^n$ items to find the unique element that satisfies some condition. Grover's algorithm performs the search on a quantum computer which is a quadratic speedup ($O(\sqrt{N})$) compared to the best classical algorithm ($O(N)$), i.e. a speedup on the brute force attack. In order to achieve such a speedup, Grover relies on the quantum superposition of states.

It has been shown that applying Grover's algorithm to break a symmetric key algorithm by brute force requires a time roughly $2^{n/2}$, compared to 2^n in the classical case. Hence the symmetric key lengths are halved, i.e. AES 256 would provide the same security level against an attack using Grover's algorithm as AES 128 would provide against a classical attack. Hence, as long as the best-known attack on AES is the brute force attack, we can classify AES as quantum-resistant.

Post-quantum symmetric cryptography does not need to be changed significantly from current symmetric cryptography other than by increasing current security levels. The AES algorithm with appropriate key length will be able to resist attacks launched from quantum computers.

3. POST-QUANTUM CRYPTOGRAPHY

In this section, we describe shortly different cryptosystems that are believed to be quantum-resistant. For more details, see [5] and the NIST webpage on post-quantum cryptosystems.

A. Code-based Cryptography

Code-based cryptosystems are among the most promising candidates to replace quantum-vulnerable primitives such as the Diffie-Hellman key exchange, the Rivest-Shamir-Adleman (RSA), and ElGamal cryptosystems. One of the problems for which no known polynomial time algorithm on a quantum computer exists is the decoding of a general linear code. Conservative and well-understood choices for code-based cryptography are the McEliece cryptosystem [25] and its dual variant by Niederreiter [27] using binary Goppa codes.

B. Multivariate Cryptography

Another potential candidate for PQC is multivariate cryptography. Multivariate cryptography relies on the difficulty of solving a system of m polynomial equations in n variables over a finite field. The complexity of solving a multivariate polynomial system (MP problem) or a multivariate quadratic system (MQ problem) where coefficients of the monomials are independently and uniformly distributed (i.e. random) is well-known to be NP-hard.

An arbitrary MP system can be transformed into an equivalent MQ system by substituting monomials of degree larger than two with new variables and introducing extra equations to the system. Furthermore, a polynomial system over any extension field $\mathbb{F}^{2n}$ can be reduced into an equivalent system over $\mathbb{F}^{2}$ using a Weil descent.

While there have been some proposals for multivariate encryption schemes, multivariate cryptography has historically been more successfully employed as an approach to signatures.

C. Lattice-based Cryptography

A lattice is an infinite arrangement of regularly spaced points, and can be generated as the set of all linear combinations of m independent vectors in $\mathbb{R}^n$, called a basis. Cryptosystems based on lattice problems have received renewed interest. Lattice-based cryptography starts with the work of Ajtai [1] and uses hard problems on lattices as the foundation of secure cryptographic constructions. Exciting new applications (such as fully homomorphic encryption, code obfuscation, and attribute-based encryption) have been made possible using lattice-based cryptography.

Lattice-based cryptographic constructions are mainly based on two well-known problems: the Small Integer Solution problem (SIS) and its Inhomogeneous variant (ISIS) [1], and the Learning With Errors problem (LWE) introduced by Regev [29]. Structured variants of the LWE and SIS problems were proposed [39], called Ring-SIS and Ring-LWE. These problems are preferred in practice since they enjoy smaller storage and faster operations. These two problems can be used to construct many basic cryptographic primitives such as PKE (adapting the schemes from [29]) and signatures [10], [11], [21].

D. Hash-based Cryptography

Cryptographic hash functions are one of the central primitives in cryptography. They are used virtually everywhere: as cryptographically secure checksums to verify the integrity of software or data packages; as building block in security protocols, including TLS, SSH, IPSEC; as part of any efficient variable-input-length signature scheme; to build fully-fledged hash-based signature schemes; and in transformations for CCA-secure encryption.

While all widely deployed means of public-key cryptography may be threatened by the rise of quantum computers, hash functions are believed to be only mildly affected. The reason for this is two-fold. On the one hand, generic quantum attacks achieve at most a square-root speed up compared to their pre-quantum counterparts and can be proven asymptotically optimal [15], [41]. On the other hand, no dedicated quantum

attacks on any specific hash function perform better than generic quantum attacks (except, of course, for hash functions based on number theory, e.g., VSH [6]).

E. Isogeny-based Cryptography

Supersingular isogeny-based cryptography is one of the more recent families of post-quantum proposals. Ever since their introduction to public-key cryptography by Miller [26] and Koblitz [18], elliptic curves have been of interest to the cryptographic community. By using the group of points on an appropriately chosen elliptic curve where the discrete logarithm problem is assumed to be hard, many standard protocols can be instantiated. The efficiency of these curve-based algorithms is largely determined by the scalar multiplication routine, and as a result extensive research has gone into optimizing this operation.

In 2011, Jao and De Feo [17] proposed supersingular isogeny Diffie-Hellman as a key exchange protocol offering post-quantum security.

4. ISOGENY-BASED SUPERSINGULAR ELLIPTIC CURVE CRYPTOGRAPHY

In this section, we will give a brief overview on supersingular isogeny-based cryptography and explain the quantum-resistant supersingular Diffie-Hellman key exchange scheme. Most of the material presented in this section can be found in [2, 4, 7, 12].

A. Isogenies of Elliptic Curves

Let E and E' be elliptic curves defined over field K. An isogeny $\phi{:}E{\to}E'$ is an algebraic morphism satisfying $\phi(\infty){=}\infty$. The degree of the isogeny is its degree as an algebraic map. The endomorphism ring $End\ (E)$ is the set of isogenies from E to itself, together with the constant morphism. This set forms a ring under point-wise addition and composition.

When K is a finite field, the rank of $\mathbb{E}nd(E)$ as a $\mathbb{Z}$-module is either 2 or 4. We say E is *supersingular* if the rank is 4, and ordinary otherwise. A supersingular curve cannot be isogenous to an ordinary curve.

Supersingular curves are all defined over $\mathbb{F}_{p2}$, and for every prime $l\gamma p$ there exist $l{+}1$ isogenies (counting multiplicities) of degree l originating from any given such supersingular curve. Given an elliptic curve E and a finite group G of E, there is up to isomorphism a unique isogeny $E{\to}E'$ having kernel G, [38]. Hence we can identify an isogeny by specifying its kernel, and conversely given a kernel subgroup the

corresponding isogeny can be found using Vélu's formulas, see [40]. Two elliptic curves are called *isogenous* if there exists an isogeny between them.

B. Supersingular Isogeny Diffie-Hellman Key Exchange

In this section, we present briefly a key exchange protocol using supersingular elliptic curves; see [12] for a more complete description of this protocol as well as zero-knowledge proof of identity and a public-key encryption based on supersingular isogenies.

This protocol requires supersingular curves of smooth order. Fix $\mathbb{F}_q=\mathbb{F}_{p2}$, where $p = l_A^{e_A} l_B^{e_B} \cdot f \pm 1$ and l_A, l_B are small primes, and f is a cofactor such that p is prime. Construct a supersingular elliptic curve E defined over $\mathbb{F}_q$ of cardinality $(l_A^{e_A} l_B^{e_B} \cdot f)^2$. By construction, $E[l_A^{e_A}]$ is $\mathbb{F}_q$-rational and contains $l_A^{e_A-1}(l_A+1)$ cyclic subgroups of order $l_A^{e_A}$, each defining a different isogeny; the analogous statement holds for $E[l_B^{e_B}]$.

More precisely, the supersingular isogeny Diffie-Hellman key exchange follows this algorithm. Pick as the public parameters a supersingular elliptic curve E over $\mathbb{F}_{p2}$, and bases $\{P_A,Q_A\}$ and $\{P_B,Q_B\}$ which generate respectively $E[\ell_A^{e_A}] = \langle P_A, Q_A\rangle$, and $E[\ell_B^{e_B}] = \langle P_B, Q_B\rangle$. Then Alice chooses two random numbers $m_A,n_A\in\mathbb{Z}$ not both divisible by l_A, and computes an isogeny $\alpha:E\to E/\langle A\rangle$ with kernel $\langle A\rangle=\langle [m_A]P_A+[n_A]Q_A\rangle$. Alice computes also $\alpha(P_B)$ and $\alpha(Q_B)$ and then sends them to Bob together with E_A.

Bob on the other side chooses two random numbers $m_B,n_B\in\mathbb{Z}$ not both divisible by l_B, and computes an isogeny $\beta:E\to E/\langle B\rangle$ with kernel $\langle B\rangle=\langle [m_B]P_AB+[n_B]Q_B\rangle$ as well as $\beta(P_A)$ and $\beta(Q_A)$ and then sends them to Alice.

Upon receipt of the respective information, both parties can compute the secret shared key. Alice computes $E/\langle A,B\rangle=E_B/\langle\beta(A)\rangle$ and $\langle\beta(A)\rangle=\langle [m_A]\beta(P_A)+[n_A]\beta(Q_A)\rangle$ and Bob similarly computes $E/\langle A,B\rangle=E_A/\langle\alpha(B)\rangle$ where $\langle\alpha(A)\rangle=\langle [m_B]\alpha(P_B)+[n_B]\alpha(Q_B)\rangle$ so that they have the shared secret key $E/\langle A,B\rangle$. This is summarised in the following table 2.

Given two elliptic curves E, E' over a finite field, isogenous of known degree d, finding an isogeny $\phi:E\to E'$ of degree d is a notoriously difficult problem for which only algorithms exponential in log $\#E$ are known in general.

In [9] they give a precise formulation of the necessary computational assumptions (of supersingular isogeny Diffie-Hellman key exchange, zero-knowledge proof of identity, and a public-key encryption based on supersingular isogenies) along with a discussion of their validity, and prove the security of these protocols under those assumptions.

However, in recent developments in supersingular isogeny-based cryptography (SIDH), Costello [8] focuses on (2,2) reducible Jacobians. As pointed out by Costello in the last paragraph of [8]: *"One hope in this direction is the possibility of pushing odd degree l-isogeny maps from the elliptic curve setting to the Kummer setting. This was difficult in the case of 2-isogenies because the maps themselves are (2, 2)-isogenies, but in the case of odd degree isogenies there is nothing obvious preventing this approach."*

TABLE 2: SUPERSINGULAR ISOGENY DIFFIE-HELLMAN KEY EXCHANGE ALGORITHM

Alice	Bob
Pick $k_{PrA} = \langle A \rangle = \langle [m_A]P_A + [n_A]Q_A \rangle$	Pick $k_{PrB} = \langle B \rangle = \langle [m_B]P_B + [n_B]Q_B \rangle$
Comp. secret isogeny	Comp. secret isogeny
$\alpha : E \to E_A = E/\langle A \rangle$	$\beta : E \to E_B = E/\langle B \rangle$
Send $E_A, \alpha(P_B), \alpha(Q_B)$ ⟶	to Bob
to Alice ⟵	Send $E_B, \beta(P_A), \beta(Q_A)$
Secret shared key: Compute $E/\langle A, B \rangle = E_B/\langle \beta(A) \rangle$ $\langle \beta(A) \rangle = \langle [m_A]\beta(P_A) + [n_A]\beta(Q_A) \rangle$	Secret shared key: Compute $E/\langle A, B \rangle = E_A/\langle \alpha(B) \rangle$ $\langle \alpha(B) \rangle = \langle [m_B]\alpha(P_B) + [n_B]\alpha(Q_B) \rangle$

In the upcoming sections, we focus on n,n-reducible Jacobians, and more precisely when n=4.

5. ISOGENOUS COMPONENTS OF JACOBIAN SURFACES

An Abelian variety defined over k is an absolutely irreducible projective variety defined over k, which is a group scheme. We will denote an Abelian variety defined over a field k by $\mathbb{A}_k$ or simply $\mathbb{A}$. A morphism from the Abelian variety $\mathbb{A}_1$ to the Abelian variety $\mathbb{A}_2$ is a homomorphism if and only if it maps the identity element of $\mathbb{A}_1$ to the identity element of $\mathbb{A}_2$.

An Abelian variety over a field k is called simple if it has no proper non-zero Abelian subvariety over k. It is called *absolutely simple* (*or geometrically simple*) if it is simple over the algebraic closure of k. An Abelian variety of dimension 1 is called an *elliptic curve*.

A homomorphism f:$\mathbb{A}\to\mathcal{H}$ is called an isogeny if $Imgf=\mathcal{H}$ and $\ker f$ is a finite group scheme. If an isogeny $\mathbb{A}\to\mathcal{H}$ exists, we say that $\mathbb{A}$ and $\mathcal{H}$ are isogenous. This relation is symmetric. The degree of an isogeny f:$\mathbb{A}\to\mathcal{H}$ is the degree of the function field extension $\deg f:=[k(\mathbb{A}):f\star k(\mathcal{H})]$. It is equal to the order of the group scheme $\ker(f)$, which is, by definition, the scheme theoretical inverse image $f^{-1}(\{0_{\mathbb{A}}\})$.

The group of $\bar{k}$-rational points has order $\#(\ker f)(\bar{k})=[k(A):f^{\star}k(B)]^{sep}$, where $[k(A):f^{\star}k(B)]^{sep}$ is the degree of the maximally separable extension in $k(A)/f^{\star}k(\mathcal{H})$. We say that f is a *separable isogeny* if and only if $\#\ker f(\bar{k})=\deg f$.

For any Abelian variety $\mathbb{A}/k$ there is a one to one correspondence between the finite subgroup schemes $H\leq\mathbb{A}$ and isogenies f:$\mathbb{A}\to\mathcal{H}$, where $\mathcal{H}$ is determined up to isomorphism. Moreover, $H=\ker f$ and $\mathcal{H}=\mathbb{A}/H$. f is separable if and only if K is étale, and then $\deg f=\#H(\bar{k})$. The following is often called the fundamental theorem of Abelian varieties. Let $\mathbb{A}$ be an Abelian variety. Then $\mathbb{A}$ is isogenous to $\mathbb{A}_1^{n_1}\times\mathbb{A}_2^{n_2}\times\ldots\times\mathbb{A}_r^{n_r}$, where (up to permutation of the factors) $\mathbb{A}_i$, for $i=1,\ldots,r$ are simple, non-isogenous, Abelian varieties. Moreover, up to permutations, the factors $\mathbb{A}_i^{n_i}$ are uniquely determined up to isogenies.

When $k=\bar{k}$, then let f be a non-zero isogeny of $\mathbb{A}$. Its kernel $\ker f$ is a subgroup scheme of $\mathbb{A}$. It contains $0_{\mathbb{A}}$ and so its connected component, which is, by definition, an Abelian variety.

A. Jacobian Surfaces

Abelian varieties of dimension 2 are often called Abelian (algebraic) surfaces. We focus on Abelian surfaces which are Jacobian varieties. Let $\mathcal{X}$ be a genus 2 curve defined over a field k. Then its gonality is $\gamma_x=2$. Hence, genus 2 curves are hyperelliptic and we denote the hyperelliptic projection by π:$\mathcal{X}\to\mathbb{P}^1$. By the Hurwitz's formula, this covering has $r=6$ branch points which are images of the Weierstrass points of $\mathcal{X}$. The moduli space has dimension $r-3=3$.

The arithmetic of the moduli space of genus two curves was studied by Igusa in his seminal paper [16] expanding on the work of Clebsch, Bolza, and others. Arithmetic invariants by J_2,J_4,J_6,J_8,J_{10} determine uniquely the isomorphism class of a genus two curve. Two genus two curves $\mathcal{X}$ and $\mathcal{X}'$ are isomorphic over $\bar{k}$ if and only if there exists $\lambda\in\bar{k}^{\star}$ such that $J_{2i}(\mathcal{X})=\lambda^{2i}J_{2i}(\mathcal{X}')$, for $i=1,\ldots,5$. If chark $\neq2$ then the invariant J_8 is not needed.

From now on we assume char $k\neq2$. Then $\mathcal{X}$ has an affine Weierstrass equation

$$y^2=f(x)=a_6x^6+\cdots+a_1x+a_0, \tag{1}$$

over $\bar{k}$, with discriminant $\Delta_f = J_{10} \neq 0$. The moduli space $\mathcal{M}_2$ of genus 2 curves, via the Torelli morphism, can be identified with the moduli space of the principally polarized abelian surfaces $\mathbb{A}_2$ which are not products of elliptic curves. Its compactification $\mathbb{A}_2^\star$ is the weighted projective space $\mathbb{WP}^3_{(2,4,6,10)}(k)$ via the Igusa invariants J_2, J_4, J_6, J_{10}. Hence, $A_2 \cong \mathbb{WP}^3_{(2,4,6,10)}(k) \setminus \{J_{10}=0\}$. Given a moduli point $\mathfrak{p} \in \mathcal{M}_2$, we can recover the equation of the corresponding curve over a minimal field of definition following [23].

It is well known that a map of algebraic curves $f: X \to Y$ induces maps between their Jacobians $f^*: \mathbb{J}ac(Y) \to \mathbb{J}ac(X)$ and $f_*: \mathbb{J}ac(X) \to \mathbb{J}ac(Y)$. When f is maximal then f^* is injective and $\ker(f^*)$ is connected; see [31] for more details.

Let $\mathcal{X}$ be a genus 2 curve and $\psi_1: \mathcal{X} \longrightarrow E_1$ be a degree n maximal covering from $\mathcal{X}$ to an elliptic curve E_1. Then $\psi_1^*: E_1 \to \mathbb{J}ac(\mathcal{X})$ is injective and the kernel of $\psi_{1,*}: \mathbb{J}ac(\mathcal{X}) \to E_1$ is an elliptic curve, which we denote by E_2. For a fixed Weierstrass point $P \in \mathcal{X}$, we can embed $\mathcal{X}$ to its Jacobian via

$$\begin{aligned} &i_p: \mathcal{X} \longrightarrow \mathbb{J}ac(\mathcal{X}) \\ &x \to [(x) - (P)] \end{aligned} \tag{2}$$

Let $g: E_2 \to \mathbb{J}ac(\mathcal{X})$ be the natural embedding of E_2 in $\mathbb{J}ac(\mathcal{X})$, then there exists $g^*: \mathbb{J}ac(\mathcal{X}) \to E_2$. Define $\psi_2 = g^* \circ i_p: \mathcal{X} \to E_2$. So we have the following exact sequence

$$0 \to E_2 g \longrightarrow \mathbb{J}ac(\mathcal{X}) \psi_{1,*} \longrightarrow E_1 \to 0. \tag{3}$$

The dual sequence is also exact $0 \to E_1 \psi_1^* \longrightarrow \mathbb{J}ac(\mathcal{X}) g^* \longrightarrow E_2 \to 0$.
If $\deg(\psi_1) = 2$ or it is an odd number, then the maximal covering $\psi_2: \mathcal{X} \to E_2$ is unique (up to isomorphism of elliptic curves). The Hurwitz space $\mathcal{H}_\sigma$ of such covers is embedded as a subvariety of the moduli space of genus two curves $\mathcal{M}_2$; see [34] for details. It is a 2-dimensional subvariety of $\mathcal{M}_2$ which we denote using $\mathcal{L}_n$. An explicit equation for $\mathcal{L}_n$, in terms of the arithmetic invariants of genus 2 curves, can be found in [35] or [23] for $n=2$, in [34] for $n=3$, and in [22] for $n=5$. From now on, we will say that a genus 2 curve $\mathcal{X}$ has an (n,n)-decomposable Jacobian if $\mathcal{X}$ is as above and the elliptic curves E_i, $i=1,2$ are called the components of $\mathbb{J}ac(\mathcal{X})$.

For every $D := J_{10} > 0$ there is a Humbert hypersurface H_D in $\mathcal{M}_2$ which parametrizes curves $\mathcal{X}$ whose Jacobians admit an optimal action on $\mathcal{O}_D$; see [14]. Points on H_{n^2} parametrize curves whose Jacobian admits an (n,n)-isogeny to a product of two elliptic curves. Such curves are the main focus of our study. In [20, Prop. 2.14] the authors prove that $\mathbb{J}ac(\mathcal{X})$ is a geometrically simple Abelian variety if and only if it is not (n,n)-decomposable for some $n > 1$.

6. (N,N) REDUCIBLE JACOBIANS SURFACES

Genus 2 curves with (n,n)-decomposable Jacobians are the most studied type of genus 2 curves due to work of Jacobi, Hermite, et al. They provide examples of genus two curves with a large Mordell-Weil rank of the Jacobian, many rational points, nice examples of descent [33], etc. Such curves have received new attention lately due to interest in their use on cryptographic applications and their suggested use on post-quantum crypto-systems and the random self-reducibility of discrete logarithm problem; see [8]. A detailed account of applications of such curves in cryptography is provided in [13].

Let $\mathcal{X}$ be a genus 2 curve defined over an algebraically closed field k, $chark=0$, K the function field of $\mathcal{X}$, and $\psi_1:\mathcal{X}\longrightarrow E_1$ a degree n covering from $\mathcal{X}$ to an elliptic curve E; see [31] for the basic definitions. The covering $\psi_1:\mathcal{X}\longrightarrow E$ is called a *maximal covering* if it does not factor through a nontrivial isogeny. We call E a *degree n elliptic subcover* of $\mathcal{X}$. Degree n elliptic subcovers occur in pairs, say (E_1,E_2). It is well known that there is an isogeny of degree n^2 between the Jacobian $\mathbb{J}ac(\mathcal{X})$ and the product $E_1\times E_2$. Such curve $\mathcal{X}$ is said to have (n,n)-decomposable (or (n,n)-split) Jacobian. The focus of this paper is on isogenies among the elliptic curves E_1 and E_2.

The locus of genus 2 curves $\mathcal{X}$ with (n,n)-decomposable Jacobian it is denoted by $\mathcal{L}_n$. When $n=2$ or n an odd integer, $\mathcal{L}_n$ is a 2-dimensional algebraic subvariety of the moduli space $\mathcal{M}_2$ of genus two curves; see [31] for details. Hence, we can get an explicit equation of $\mathcal{L}_n$ in terms of the Igusa invariants J_2,J_4,J_6,J_{10}; see [35] for $\mathcal{L}_2$, [34] for $\mathcal{L}_3$, [36] for $\mathcal{L}_4$, and [22] for $\mathcal{L}_5$. There is a more recent paper on the subject [19] where results of [22, 34] are confirmed and equations for $n>5$ are studied.

A. Computing the Locus $\mathcal{L}_4$ in $\mathcal{M}_2$

When $\deg(\phi)=4$ to compute the locus $\mathcal{L}_4(\sigma)$ one has to consider two cases. There is one generic case and one degenerate case with possible ramification structures:

1. $(2,2,2,2^2,2)$ (generic)
2. $(2,2,2,4)$ (degenerate)

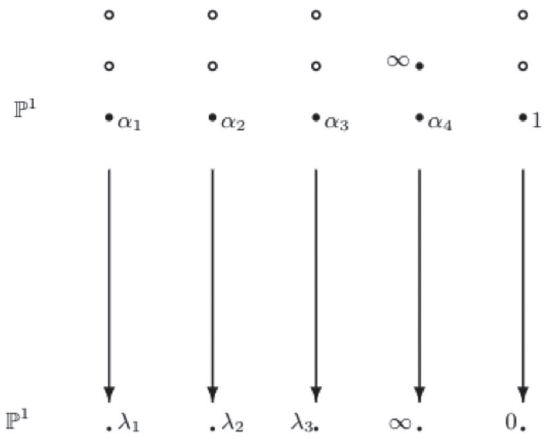
In this paper, we will focus only on the generic case. For a complete treatment of the degenerate case see [28, 36].

B. Non-degenerate Case

Let $\psi:C\longrightarrow E$ be a covering of degree 4, where C is a genus 2 curve and E is an elliptic curve. Let ϕ be the Frey-Kani covering with $\deg(\phi)=4$ such that $\phi(1)=0$, $\phi(\infty)=\infty$,

$\phi(p)=\infty$ and the roots of $f(x)=x^2+ax+b$ be in the fiber of 0. In the following figure, bullets (resp., circles) represent places of ramification index 2 (resp., 1).

FIGURE 2: DEGREE 4 COVERING FOR GENERIC CASE



Then the cover can be given by

$$\phi(x) = \frac{k(x-1)^2(x^2 + ax + b)}{(x-\alpha_4)^2}. \tag{4}$$

Let $\lambda_1,\lambda_2,\lambda_3$ and ∞ be the Weierstrass points of E. Then

$$\begin{cases} \phi(x) - \lambda_1 = k\dfrac{(x-\alpha_1)^2(x^2 - a_1x + b_1)}{(x-\alpha_4)^2} \\ \phi(x) - \lambda_2 = k\dfrac{(x-\alpha_2)^2(x^2 - a_2x + b_2)}{(x-\alpha_4)^2} \\ \phi(x) - \lambda_3 = k\dfrac{(x-\alpha_3)^2(x^2 - a_3x + b_3)}{(x-\alpha_4)^2} \end{cases}$$

Next, let $\lambda_1,\lambda_2,\lambda_3$ and 0 be the Weierstrass points of E. Then

$$\begin{cases} \phi(x) - \lambda_1 = k\,x\,(x-\alpha_1)^2(x^2 - a_1x + b_1) \\ \phi(x) - \lambda_2 = k\,x\,(x-\alpha_2)^2(x^2 - a_2x + b_2) \\ \phi(x) - \lambda_3 = k\,x\,(x-\alpha_3)^2(x^2 - a_3x + b_3) \end{cases}$$

By clearing the denomirators and equaling the coefficients of quartics to zero, we get a system of equations in terms of parameters a,b,a_1,b_1,a_2,b_2,a_3,b_3,$\alpha 1$,...$\alpha 4$, λ_1,λ_2,λ_3,k. We solve this equation to get

$$\begin{cases} \alpha_1 = -3\,a + 2 + A \\ \alpha_2 = -3\,a + 2 + A \\ \alpha_3 = -3\,a + 2 + A \\ \lambda_1 = aA^{3/2} - 27\,a^4 + 18\,a^2A - 72\,a^3 + 144\,a^2b + 8\,aA - 64\,bA - 56\,a^2 + 320\,ba \\ \qquad -128\,b^2 + 8\,A + 32\,a + 320\,b + 16 \\ \lambda_2 = aA^{3/2} - 27\,a^4 + 18\,a^2A - 72\,a^3 + 144\,a^2b + 8\,aA - 64\,bA - 56\,a^2 + 320\,ba \\ \qquad -128\,b^2 + 8\,A + 32\,a + 320\,b + 16 \\ \lambda_3 = aA^{3/2} - 27\,a^4 + 18\,a^2A - 72\,a^3 + 144\,a^2b + 8\,aA - 64\,bA - 56\,a^2 + 320\,ba \\ \qquad -128\,b^2 + 8\,A + 32\,a + 320\,b + 16 \end{cases}$$

where $A = \sqrt{9\,a^2 + 4\,a - 32\,b + 4}$. The equation of the genus 2 curve is

$$y^2 = (x-1)\prod_{i=1}^{4}(x-\alpha_i),$$

and elliptic curves have equations

$$E_1: y^2 = \prod_{i=1}^{3}(x-\lambda_i), \qquad E_2: y^2 = x\prod_{i=1}^{3}(x-\lambda_i).$$

Notice that we write the equation of genus 2 curve in terms of only 2 unknowns. We denote the Igusa invariants of C by J_2,J_4,J_6, and J_{10}. The absolute invariants of C are given in terms of these classical invariants:

$$i_1 = 144\frac{J_4}{J_2^2}, \quad i_2 = -1728\frac{J_2J_4 - 3J_6}{J_2^3}, \quad i_3 = 486\frac{J_{10}}{J_2^5}.$$

Two genus 2 curves with $J_2 \neq 0$ are isomorphic if and only if they have the same absolute invariants. Notice that these invariants of our genus 2 curve are polynomials in a and b. By using a computational symbolic package (as Maple), we eliminate a and b to determine the equation for the non-degenerate locus $\mathcal{L}_4$. The result is very long. We do not display it here.

7. FINAL REMARKS AND FUTURE WORK

Let $\mathcal{X}$ be a genus 2 curve defined over a field K, $charK=p\geq 0$, and $\mathbb{J}ac(\mathcal{X},\iota)$ its Jacobian, where ι is the principal polarization of $\mathbb{J}ac(\mathcal{X})$ attached to $\mathcal{X}$. Assume that $\mathbb{J}ac(\mathcal{X})$ is (n,n)- geometrically reducible with E_1 and E_2 its elliptic components.

In an upcoming project, we would like to study pairs of (E_1,E_2) elliptic components and try to determine their number (up to isomorphism over $\bar{k}$) when they are isogenous of degree N, for an integer $N\geq 2$. We denote by $\phi_N(x,y)$ the N-th modular polynomial. Two elliptic curves with j-invariants j_1 and j_2 are N-isogenous if and only if $\phi_N(j_1,j_2)=0$. The equation $\phi_N(x,y)=0$ is the canonical equation of the modular curve $X_0(N)$. The equations of $X_0(N)$ are well-known.

In [3], Beshaj et al. prove that there are only finitely many curves $\mathcal{X}$ (up to isomorphism) defined over K such that E_1 and E_2 are N-isogenous for $n=2$ and $N=2,3,5,7$ with $\mathrm{Aut}(\mathbb{J}ac\mathcal{X}) \cong V_4$ or $n=2$, $N=3,5,7$ with $\mathrm{Aut}(\mathbb{J}ac(\mathcal{X})) \cong D_4$. The same holds if $n=3$ and $N=5$. Furthermore, by determining the Kummer and the Shioda-Inose surfaces for the above $\mathbb{J}ac(\mathcal{X})$ we can show how such results in positive characteristic $p>2$ suggest nice applications in cryptography. Now that we have computed the locus $\mathcal{L}_4$, it would be interesting to explore the same problem when $n=4$ and $N=2,3,5,7$.

ACKNOWLEDGMENTS

The authors would like to thank our supportive colleagues at the Army Cyber Institute at West Point.

REFERENCES

[1] M. Ajtai, "*Generating hard instances of lattice problems (extended abstract)*," In Proc. Twenty-eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, PA, 1996, ACM, New York, 1996, pp. 99–108. MR 1427503.

[2] J. Alwen, *What is lattice-based cryptography and why should you care*. Publication details? 2018.

[3] L. Beshaj, A. Elezi and T. Shaska, "Isogenous components of jacobian surfaces," *European Journal of Mathematics*, 2019.

[4] Charles, D., & Lauter, K. (2005). Computing Modular Polynomials. LMS Journal of Computation and Mathematics, 8, 195-204. doi:10.1112/S1461157000000954.

[5] L. Chen, S. Jordan, Y. Liu, D. Moody, R. Peralta and D. Smith-Tone, "Report on post-quantum cryptography," National Institute of Standards and Technology Internal Report, NIST.IR.8105. 2016.

[6] S. Contini, A. K. Lenstra and Ron Steinfeld, "VSH, an efficient and provable collision-resistant hash function," Advances in cryptology – EUROCRYPT 2006, Lecture Notes in Comput. Sci., vol. 4004, Springer, Berlin, 2006, pp. 165–182. MR 2423542.

[7] C. Costello and H Hisil, "A simple and compact algorithm for sidh with arbitrary degree isogenies," presented at International Conference on the Theory and Application of Cryptology and Information Security ASIACRYPT, Advances in Cryptology ASIACRYPT (2017), 303–329.

[8] Costello C. (2018) Computing Supersingular Isogenies on Kummer Surfaces. In: Peyrin T., Galbraith S. (eds) Advances in Cryptology – ASIACRYPT 2018. ASIACRYPT 2018. Lecture Notes in Computer Science, vol 11274. Springer, Cham.
[9] L. De Feo, D. Jao and J. Plút, "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies," *J. Math. Cryptol*., vol. 8, pp. 209–247, 2014.
[10] L. Ducas, A. Durmus, T. Lepoint and V. Lyubashevsky, "*Lattice signatures and bimodal Gaussians*," Advances in cryptology – CRYPTO 2013. Part I, Lecture Notes in Comput. Sci., vol. 8042, Springer, Heidelberg, 2013, pp. 40–56. MR 3126416.
[11] L. Ducas and D. Micciancio, "Improved short lattice signatures in the standard model," Advances in cryptology – CRYPTO 2014. Part I, Lecture Notes in Comput. Sci., vol. 8616, Springer, Heidelberg, 2014, pp. 335–352. MR 3239444.
[12] L. Feo, *Mathematics of isogeny based cryptography*, Arxiv, 2017.
[13] G. Frey and T. Shaska, "Curves, Jacobians, and Cryptography, Algebraic curves and their applications" (L. Beshaj, ed.), Contemporary Math., vol. 724, American Mathematical Society, 2019, pp. 280–350.
[14] K. Hashimoto and N. Murabayashi, "Shimura curves as intersections of Humbert surfaces and defining equations of QM-curves of genus two," *Tohoku Math*. J., vol. 2, no. 47, pp. 271–296, 1995. MR 1329525.
[15] A. Hülsing, J. Rijneveld and F. Song, *Mitigating multi-target attacks in hash-based signatures*, Public-key cryptography – PKC 2016. Part I, Lecture Notes in Comput. Sci., vol. 9614, Springer, [Cham], 2016, pp. 387–416. MR 3492589.
[16] J. Igusa, "*Arithmetic variety of moduli for genus two*," Ann. of Math., vol. 2, no. 72, pp. 612–649, 1960. MR 0114819.
[17] D. Jao and L. De Feo, "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies," Post-quantum cryptography, Lecture Notes in Comput. Sci., vol. 7071, Springer, Heidelberg, 2011, pp. 19–34. MR 2931459.
[18] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comp*., vol. 48, no. 177, pp. 203–209, 1987. MR 866109.
[19] A. Kumar, "Hilbert modular surfaces for square discriminants and elliptic subfields of genus 2 function fields," *Res. Math. Sci*., vol. 2, Art. 24, 46, 2015. MR 3427148.
[20] D. Lombardo, *Computing the geometric endomorphism ring of a genus 2 jacobian* Math. Comp. 88 (2019), 889-929.
[21] V. Lyubashevsky, "Lattice signatures without trapdoors," Advances in cryptology – EUROCRYPT 2012, Lecture Notes in Comput. Sci., vol. 7237, Springer, Heidelberg, 2012, pp. 738–755. MR 2972929.
[22] K. Magaard, T. Shaska, and H. Völklein, "*Genus 2 curves that admit a degree 5 map to an elliptic curve*," *Forum Math*., vol. 21, no. 3, pp. 547–566, 2009. MR 2526800.
[23] A. Malmendier and T. Shaska, A universal genus-two curve from Siegel modular forms, SIGMA. Symmetry, Integrability and Geometry. Methods and Applications, vol 13 (2017), no. 089, 17 pages. MR 3731039.
[24] A. Malmendier and T. Shaska, "From hyperelliptic to superelliptic curves," *Albanian J. Math*., vol. 13, no. 1, pp. 107–200, 2019. MR 3978315.
[25] R. J. McEliece, A Public-key cryptosystem based on algebraic coding theory, DSN Progress Report, Jet Propulsion Laboratory, Pasadena, CA (Jan./Feb. 1978) pp. 114–116.
[26] V. S. Miller, "Use of elliptic curves in cryptography," Advances in cryptology – CRYPTO '85 (Santa Barbara, Calif., 1985), Lecture Notes in Comput. Sci., vol. 218, Springer, Berlin, 1986, pp. 417–426.
[27] H. Niederreiter, "*Knapsack-type cryptosystems and algebraic coding theory," Problems Control Inform. Theory/Problemy Upravlen. Teor. Inform*., vol. 15, no. 2, pp. 159–166, 1986. MR 851173.
[28] N. Pjerro, M. Ramosaco and T. Shaska, "Degree even covering of elliptic curves by genus 2 curves," *Albanian Journal of Mathematics*, vol. 2, no. 3, pp. 241–248, 2008.
[29] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," J. ACM, vol. 56, no. 6, art. 34, p. 40, 2009. MR 2572935.
[30] F. Richelot, "Essai sur une methode generale pour determiner la valuer des integrales ultra-elliptiques, fondee sur des transformations remarquables des ce transcendantes," *CR Acad. Sc. Paris*, vol. 2, pp. 622–627, 1836.
[31] T. Shaska, "Curves of genus 2 with (N,N) decomposable Jacobians," *J. Symbolic Comput*., vol. 31, no. 5, pp. 603–617, 2001. MR 1828706.
[32] T. Shaska, "Curves of genus two covering elliptic curves," ProQuest LLC, Ann Arbor, MI, Thesis (Ph.D.), University of Florida, 2001.
[33] T. Shaska, "Genus 2 curves with (3,3)-split Jacobian and large automorphism group," *Algorithmic number theory*, Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, pp. 205–218, 2002.

[34] T. Shaska, “Genus 2 fields with degree 3 elliptic subfields,” *Forum Math*., vol. 16, no. 2, pp. 263–280, 2004. MR 2039100.
[35] T. Shaska and H. Völklein, “Elliptic subfields and automorphisms of genus 2 function fields,” *Algebra, arithmetic and geometry with applications*, Springer, Berlin, pp. 703–723, 2004. MR 2037120.
[36] T. Shaska, G. S. Wijesiri, S. Wolf, and L. Woodland, “Degree 4 covering of elliptic curves by genus 2 curves,” *Albanian Journal of Mathematics*, vol. 2, no. 4, pp. 307–318, 2008.
[37] Peter W. Shor, “Algorithms for quantum computation: discrete logarithms and factoring” 35th Annual Symposium on Foundations of Computer Science (Santa Fe, NM, 1994), IEEE Comput. Soc. Press, Los Alamitos, CA, 1994, pp. 124–134. MR 1489242.
[38] J. Silverman and J. Tate, Rational points on elliptic curves, ISBN: 978-3-319-18587-3, Number of Pages : XXII, 332, 2nd edition, 2015.
[39] Stehlé D., Steinfeld R., Tanaka K., Xagawa K. (2009) Efficient Public Key Encryption Based on Ideal Lattices. In: Matsui M. (eds) Advances in Cryptology – ASIACRYPT 2009. ASIACRYPT 2009. Lecture Notes in Computer Science, vol 5912, pg 617-635. Springer, Berlin, Heidelberg.
[40] L. C. Washington, *Elliptic Curves: Number Theory and Cryptography*, second edition, London: Chapman and Hall/CRC, 2008.
[42] M. Zhandry, “A note on the quantum collision and set equality problems,” *Quantum Inf. Comput*., vol. 15, no. 7-8, pp. 557–567, 2015.