Final Research Report
INdAM-DP-COFUND 2015 fellowship

Manoj Gyawali

February 3, 2021

1. Introduction

During my fellowship period at my host institution, Department of Mathematics Università degli Studi di Roma Tre, under a supervision of Prof. Luca De Feo, we studied mainly some applications of algebraic geometry to cryptography, in particular to post-quantum cryptography (PQC). One of the main reasons to draw attention toward PQC is the algorithm of Shor [22]. Due to this algorithm, all the public key cryptosystems based on the difficulty of the discrete logarithm or integer factorization problems became vulnerable to polynomial-time attacks by quantum computers. Moreover, a competition organized by the United States government agency National Institute of Standards and Technology (NIST) for new post-quantum cryptographic algorithms [17] and its recent third selection round highlight the important of post-quantum cryptography. Participants of the competition can be classified into lattice-based, code-based, multivariate, hash-based, [11] and isogeny based cryptography. Most of these cryptographic constructions use techniques from algebraic geometry, thereby proving its efficacy in post-quantum cryptography.
Our study was concentrated on two parts. The first part is related to the isogeny problems and the second part is devoted to new key exchange and signature protocols based on hard problems occurred in Veronese variety and secant variety of the Grassmannian.
Isogeny based cryptography is appealing in the area of post-quantum cryptography because of its relatively small key size and underlying beautiful mathematical theory. Many variants of the isogeny problems are used in many existing primitives [12, 1, 4, 10, 9]. There are two main hard problems in isogeny based schemes: finding an isogeny between two elliptic curves and computing the endomorphism ring of an elliptic curve. These two problems are related to each other [14] and there is no sub-exponential algorithm to solve them for supersingular elliptic curves [20]. The computation of a single endomorphism of an elliptic curve E is also closely related to the problem of computing the endomorphism ring of E [13].

2. Main Contributions

(1) We study an endomorphism computation problem for a supersingular elliptic curve defined over a finite field $\mathbb{F}_p$ under the assumption that the action of the endomorphism is known on a torsion subgroup of the elliptic curve. This problem was first posed in [19], where it is reduced to that of solving a Diophantine equation. We use Simon's algorithm [23] to solve such a quadratic equation. We also use a technique from [16] to improve the size of the parameters under some heuristic assumptions.
Let E be a supersingular elliptic curve defined over the finite field $\mathbb{F}_p$. Let ϕ be an endomorphism of E of degree M whose action on N-torsion subgroup of E is known, where $\gcd(N, M) = 1$. Suppose $\pi_p : (x, y) \to (x^p, y^p)$ be the

p^{th}-power Frobenius endomorphism of E. We fix parameters as $N > 2\sqrt{Mp}$. With this parameters restriction, we studied the following problem

Problem 2.1. *Let E be a supersingular elliptic curve defined over a finite field $\mathbb{F}_p$. Let M, N be integers with gcd(M,N)=1 and $N > 2\sqrt{Mp}$. Let ϕ be an endomorphism of E of degree M whose action on N-torsion subgroup of E is known. Compute an efficient expression of ϕ.*

We gave a probabilistic algorithm to solve Problem 2.1.

(2) The transitive and free action of the class group of an imaginary quadratic order $\mathcal{O}$ on the set of elliptic curves with complex multiplication by $\mathcal{O}$ has been used to construct several cryptosystems based on isogenies for example [2, 21, 24, 6]. Classical genus theory gives the structure of the 2-torsion subgroup of the class group of $\mathcal{O}$ via some non-trivial quadratic characters. In [3], an interesting connection between genus theory and isogeny graphs was discovered, and was used to break the analogue of the decisional Diffie-Hellman problem for some isogeny-based cryptosystems. They used characters to find some information of the ideal class to break the decisional Diffie-Hellman problem from just two given elliptic curves.
In our work, we restrict our attention to the values of the non-trivial characters in the 2-torsion subgroup of the class group $cl(\mathcal{O}_K)$ of a maximal order $\mathcal{O}_K$ of an imaginary quadratic field K and observe how these values give colorings in some Cayley and isogeny graphs obtained from the 2-torsion subgroup $cl(\mathcal{O}_K)[2]$ of $cl(\mathcal{O}_K)$.

Characters play an important role in determining the structure of the 2-torsion class group. The following lemma ensures the existence and the uniqueness of the characters in $(\mathbb{Z}/\Delta\mathbb{Z})^*$.

Lemma 2.2. [5, Lemma 1.14] *Let $\Delta \equiv 0, 1 \mod 4$ be a nonzero integer. There exists a unique homomorphism $\chi : (\mathbb{Z}/\Delta\mathbb{Z})^* \to \{\pm 1\}$ given by Legendre symbol as $\chi([p]) = \left(\frac{\Delta}{p}\right)$ for odd primes not dividing Δ and $\chi([-1]) = \pm 1$ according to $\Delta > 0$ and $\Delta < 0$.*

The following theorem tells when a value in $(\mathbb{Z}/\Delta\mathbb{Z})^*$ is represented by a quadratic from of discriminant Δ.

Theorem 2.3. [5] *Let $\Delta \equiv 0, 1 \mod 4$ be a negative integer and χ be the character as in Lemma 2.2. Then for an odd prime not dividing Δ, $[p] \in ker(\chi)$ if and only if p is represented by one of the quadratic forms in $cl(\Delta)$. Furthermore, the values in $(\mathbb{Z}/\Delta\mathbb{Z})^*$ represented by the principal form of discriminant Δ form a subgroup H of $ker(\chi)$.*

Lemma 2.4. [5, Lemma 3.13] *The map $\Phi : cl(\Delta) \to ker(\chi)/H$ sending the class of a quadratic form of discriminant Δ to the values it represents in $(\mathbb{Z}/\Delta\mathbb{Z})^*$ i.e. the coset of H in $ker(\chi)$, is a group homomorphism.*

The following proposition gives the cardinality of the 2-torsion subgroup of the class group $cl(\Delta)$.

Proposition 2.5. [5, Proposition 3.11] *Let $\Delta \equiv 0, 1 \mod 4$ be a negative integer, and r be the number of odd primes dividing Δ. Define the number of assigned characters μ as follows: if $\Delta \equiv 1 \mod 4$, then $\mu = r$ and if $\Delta \equiv 0$*

mod 4, *then* $\Delta = -4n$, *where* $n > 0$, *and* μ *id determined by the following table*

n	μ	*assigned characters*
$n \equiv 3 \mod 4$	r	$\chi_1, \ldots, \chi_r$
$n \equiv 1 \mod 4$	$r+1$	$\chi_1, \ldots, \chi_r, \delta$
$n \equiv 2 \mod 8$	$r+1$	$\chi_1, \ldots, \chi_r, \delta\epsilon$
$n \equiv 6 \mod 8$	$r+1$	$\chi_1, \ldots, \chi_r, \epsilon$
$n \equiv 4 \mod 8$	$r+1$	$\chi_1, \ldots, \chi_r, \delta$
$n \equiv 0 \mod 8$	$r+2$	$\chi_1, \ldots, \chi_r, \delta, \epsilon$

where

$$\begin{aligned} \chi_i(a) &= \left(\frac{a}{p_i}\right) \text{ defined for a prime to } p_i, i = 1, \ldots, r \\ \delta(a) &= (-1)^{(a-1)/2} \text{ defined for a odd} \\ \epsilon(a) &= (-1)^{(a^2-1)/8} \text{ defined for a odd.} \end{aligned}$$

Then the class group $cl(\Delta)$ *has exactly* $2^{\mu-1}$ *elements of order* ≤ 2.

The *principal genus*, the genus consisting the principal form, corresponds to the classes of squares in the class group by the following theorem.

All the μ characters defined in Proposition 2.5 constitute a map

$$\Psi : (\mathbb{Z}/\Delta\mathbb{Z})^* \to \{\pm 1\}^\mu$$

defined by all the μ characters in its coordinates i.e.

$$[a] \mapsto (\chi_1(a), \ldots, \chi_\mu(a)),$$

where $\chi_i = \epsilon, \delta,$ or $\delta\epsilon$ for $r < i \leq \mu$ according to Proposition 2.5. An important observation is that Ψ is a homomorphism.

Lemma 2.6. [5, Lemma 3.17] *The homomorphism* $\Psi : (\mathbb{Z}/\Delta\mathbb{Z})^* \to \{\pm 1\}^\mu$ *is surjective and its kernel is the subgroup* H *of values represented by the principal form and hence* Ψ *induces an isomorphism*

$$(\mathbb{Z}/\Delta\mathbb{Z})^*/H \xrightarrow{\sim} \{\pm 1\}^\mu.$$

This lemma guarantees that the map Ψ is uniquely determined by the values in $(\mathbb{Z}/\Delta\mathbb{Z})^*$ up to the values that are represented by the principal form of discriminant Δ.

Definition 2.7. *(Genus coloring map) A map* $T : cl(\Delta_K) \to \{\pm 1\}^\mu$ *defined by the composition* $T = \Psi' \circ \Phi$, *where* $\Phi : cl(\Delta_K) \to \ ker(\chi)/H$ *sends the class of a quadratic form of discriminant* Δ_K *to the coset it represents and* Ψ' *is an isomorphism deduced from* Ψ *from Lemma 2.6. The map* T, *which gives* μ *tuple of values in* $\{\pm 1\}^\mu$, *is defined as a genus coloring map.*

Definition 2.8. *(Cayley graph)* [15] *Let* G *be a group and* X *be a generating set of* G *such that* X *does not contain the identity element of* G *and* $X = X^{-1} = \{x^{-1} : x \in X\}$. *Then the Cayley graph* $\Gamma = (G, E)$ *is an undirected graph in which the vertices are the elements of* G *and edges set* E *consists the edges joining* g *and* gx *for any* $g \in G$ *and* $x \in X$, *i.e.* $E = \{(g, gx) : g \in G, x \in X\}$.

Now we define the Cayley graph in our context. We construct Cayley graph with the group $G = cl(\mathcal{O}_K)[2]$ and the generating set $X = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ of G, where $\mathfrak{p}_i$ are the primes above the ramified primes p_i in K for $i = 1, \ldots, n$. We color the vertices of the Cayley graph by the map T, then T assigns values to each of the ideal classes in G which we say coloring of the vertices.
We name the Cayley graph constructed by taking the group $G = \langle \mathfrak{p}_1, \ldots, \mathfrak{p}_n \rangle$ and the generating set $X = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ as a $\{p_1, \ldots, p_n\}$ graph. Mainly we observed the followings

Theorem 2.9. *Let $\Delta_K \equiv 1 \mod 4$ be the discriminant of the imaginary quadratic field K. Let $p_1, \ldots, p_r$ be the odd prime divisors of the discriminant Δ_K of K and $\mathcal{O}_K$ be the maximal order of K. Let $(p_i) = \mathfrak{p}_i^2$ in $\mathcal{O}_K$. Then, there are the following possible cases if the coloring is done by the coloring map T.*

i. *From p_i's, consider any set with $r-1$ elements, without loss of generality, let this set be $\{p_1, \ldots, p_{r-1}\}$. Then the $\{p_1, \ldots, p_{r-1}\}$ graph is $(r-1)$ hypercube graph Q_{r-1}. If $\mathfrak{p}_i \notin cl(\mathcal{O}_K)^2$ for $i = 1, \ldots, r-1$ then the coloring is valid and attains the chromatic number of the $(r-1)$-hypercube if all the $\mathfrak{p}_i$ belong to the same genus.*
ii. *The $\{p_1, \ldots, p_r\}$ graph is $(r-1)$-hypercube with longest diagonals Q_{r-1}^d. Suppose $\mathfrak{p}_i \notin cl(\mathcal{O}_K)^2$ for $i = 1, \ldots, r$ and $r \geq 2$. Then the coloring is valid, the chromatic number is 2 when r is even and all of these r prime ideals belong to a non-principal genus; and the chromatic number is 4 when r is odd and these r prime ideals belong to two different non-principal genus.*

Theorem 2.10. *Let $\Delta_K \equiv 0 \mod 4$ be the discriminant of imaginary quadratic field $K = Q(\sqrt{d_K})$. Let $p_1, \ldots, p_r$ be the odd prime divisors of the discriminant Δ_K of the maximal order $\mathcal{O}_K$. Let $(p_i) = \mathfrak{p}_i^2$, $(2) = \mathfrak{c}^2$ in $\mathcal{O}_K$. Write $\Delta_K = 4d_K$.*

i. *When $d_K \equiv 3 \mod 4$,*
   - *Let $\mathfrak{c}, \mathfrak{p}_i \notin cl(\mathcal{O}_K)^2$ for $i = 1, \ldots, r-1$. The $\{2, p_1 \ldots, p_{r-1}\}$ graph is Q_r and coloring is valid for any choice of $r-1$ odd prime divisors and the chromatic number 2 is attained when all the prime ideals belong to the same non-principal genus.*
   - *Let $\mathfrak{c}, \mathfrak{p}_i \notin cl(\mathcal{O}_K)^2$ for $i = 1, \ldots, r$. Then the $\{2, p_1 \ldots, p_r\}$ graph is $Q_r^{d,r-1}$ and the coloring is valid. Moreover, when r and all the prime ideals belong to the same genus, then the chromatic number is 2. When r is odd, and if one of the prime ideals in $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ belongs to a genus which is different from the genus of the remaining ideals, then the graph attains 4 colors.*

ii. *When $d_K \equiv 2 \mod 8$, coloring in $\{2, p_1, \ldots, p_r\}$ graph and any r subset graph have similar cases as in Theorem 2.9 for $\mu = r + 1$.*
iii. *When $d_K \equiv 6 \mod 8$, coloring behavior is similar in $\{2, p_1, \ldots, p_r\}$ graph as in the case of Theorem 2.9 for $\mu = r + 1$.*

(3) We proposed a new candidate for a key exchange protocol that we call QSI key exchange, joint work with Daniele Di Tullio [26], and an encryption scheme

derived from it. The key exchange is, mainly, based on the difficulty of recovering a Veronese variety, which is hidden by an automorphism of the ambient space. This problem reduces to a problem of solving a large system of high degree polynomial equations in many variables or finding the primary decomposition of an ideal generated by some multivariate polynomials, which we claim a post-quantum problem. We leave the detail security analysis and an optimization of the proposed scheme towards an efficient key exchange candidate for future research.
We have implemented our algorithm in a computer algebra system SageMath [7] and is available at
`https://github.com/mgyawali/QSI-Key-Exchange`.

(4) Multivariate public key authentication schemes like Rainbow [8], one of the three NIST post-quantum signature finalists [18], is known for relatively fast signing and verification but large public key size in comparison to other post-quantum signature schemes. We purposed a new multivariate signature scheme, a joint work with Daniele Di Tullio [27], based on the difficulty of finding points inside the shifted secant variety of the Grassmannian when only the implicit equations are known. A purpose of the proposed signature scheme is to start a new line of work toward an efficient signature scheme with small key size.
The main idea of the signature scheme can be summarized as follows:
   (a) Alice chooses a secret projective variety Y, which is a shifted (through an automorphism of the ambient space) Secant variety of the Grassmannian.
   (b) She publishes a set of equations vanishing on the variety.
   (c) A message is encoded into a linear subspace L of the ambient space. A signature is a point P lying in the intersection $Y \cap L$.
   (d) Alice can quickly sign a message by using the Plücker embedding of the Grassmannian and her secret automorphism.
   (e) Signature P can be verified easily by checking whether it satisfies or not the set of public equations and the system of linear equations defining L.

We summarize our main contributions in the following list:

- Elliptic Curve of Nearly Prime Order (accepted for the Computing Conference 2021, UK, London) [25].
- A post-quantum key exchange protocol from the intersection of quadric surfaces (arXiv:2005.13606) [26].
- A post-quantum signature scheme from the secant variety of the Grassmannian (Cryptology ePrint Archive: Report 2020/1141) [27]
- An implementation of the key exchange in Sagemath [7]
  `https://github.com/mgyawali/QSI-Key-Exchange`
- An implementation of the signature scheme in Sagemath `https://github.com/mgyawali/SSGrass`

3. Acknowledgments

I am grateful to the whole INdAM-DP COFUND family members including president Prof. Giorgio Patrizio, Dr. Elisabetta Esposito, Dr. Daniela Evangelista, Dr. Giovanni Feliciangeli for an outstanding support during the fellowship period not only to the academic arrangements but also for the bureaucratic supports while coming my wife Srijana Karki to Italy.

References

[1] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: An efficient post-quantum commutative group action. In Thomas Peyrin and Steven D. Galbraith, editors, *Advances in Cryptology – ASIACRYPT 2018*, pages 395–427. Springer International Publishing, 2018.

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

[3] Wouter Castryck, Jana Sotáková, and Frederik Vercauteren. Breaking the decisional Diffie-Hellman problem for class group actions using genus theory. In Ristenpart T. Micciancio D., editor, *Advances in Cryptology -CRYPTO 2020*, Lecture Notes in Computer Science, vol 12171, pages 92–120. Springer, Cham, 2020.

[4] Denis X. Charles, Eyal Z. Goren, and Kristin E. Lauter. Cryptographic hash functions from expander graphs. *Journal of Cryptology*, 22(1):93–113, January 2009.

[5] David A. Cox. *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication.* Pure and Applied Mathematics. Wiley, second edition, 2013.

[6] Luca De Feo, Jean Kieffer, and Benjamin Smith. Towards practical key exchange from ordinary isogeny graphs. Cryptology ePrint Archive, Report 2018/485, 2018.

[7] The Sage Developers. The sage mathematics software system (version 9.0), 2020. `https://www.sagemath.org`.

[8] Jintai Ding and Dieter Schmidt. Rainbow, a new multivariate polynomial signature scheme. In J. Ioannidis, A. Keromytis, and M. Yung, editors, *Applied Cryptography and Network Security. ACNS 2005. Lecture Notes in Computer Science*, volume 3531, pages 164–175. Springer, Heidelberg, 2005.

[9] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. SQISign: Compact post-quantum signatures from quaternions and isogenies. In Moriai S. and Wang H., editors, *Advances in Cryptology âĂŞ ASIACRYPT 2020. Lecture Notes in Computer Science*, volume 12491, pages 64–93. Springer, Cham., 2020.

[10] Steven D. Galbraith, Christophe Petit, and Javier Silva. Identification protocols and signature schemes based on supersingular isogeny problems. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology – ASIACRYPT 2017*, pages 3–33. Springer International Publishing, 2017.

[11] Bernstein D. J., Buchmann J., and Dahmen E. Post-quantum cryptography, 2009.

[12] David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In Yang BY., editor, *Post-Quantum Cryptography. PQCrypto 2011*, volume 7071, pages 19–34, Springer, Berlin, Heidelberg, 2011. Lecture Notes in Computer Science.

[13] David Kohel. Endomorphism rings of elliptic curve over finite fields. PhD thesis, University of California, Berkeley, 1996. `http://iml.univ-mrs.fr/~kohel/pub/thesis.pdf`.

[14] David R. Kohel, Kristin Lauter, Christophe Petit, and Jean-Pierre Tignol. On the quaternion-isogeny path problem. *LMS Journal of Computation and Mathematics*, 17(A):418–432, 2014.

[15] Elena Konstantinova. Some problems on cayley graphs. *Linear Algebra and its Applications*, 429(11-12):2754–2769, 2008.

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

[17] National Institute of Standards and Technology. Post-quantum cryptography standardization, August 2016. `https://csrc.nist.gov/News/2016/Post-Quantum-Cryptography-Proposed-Requirements`.

[18] National Institute of Standards and Technology. Post-quantum cryptography standardization, July 2020. `https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization`.

[19] Christophe Petit. Faster algorithms for isogeny problems using torsion point images. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology – ASIACRYPT 2017*, pages 330–353. Springer International Publishing, 2017.

[20] Christophe Petit and Kristin Lauter. Hard and easy problems for supersingular isogeny graphs. Cryptology ePrint Archive, Report 2017/962, 2017.

[21] Alexander Rostovtsev and Anton Stolbunov. Public-key cryptosystem based on isogenies. Cryptology ePrint Archive, Report 2006/145, April 2006.

[22] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997. `https://arxiv.org/abs/quant-ph/9508027`.

[23] Denis Simon. Quadratic equations in dimensions 4, 5 and more. Preprint, 2005.

[24] Anton Stolbunov. Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves. *Advances in Mathematics of Communications*, 4(2), 2010.

[25] Daniele Di Tullio and Manoj Gyawali. Elliptic curves of nearly prime order. Cryptology ePrint Archive: Report 2020/001, 2020. `https://eprint.iacr.org/2020/001`.

[26] Daniele Di Tullio and Manoj Gyawali. A post-quantum key exchange protocol from the intersection of quadric surfaces. Cryptology ePrint Archive, Report 2020/628, 2020. `https://eprint.iacr.org/2020/628.pdf`.

[27] Daniele Di Tullio and Manoj Gyawali. A post-quantum signature scheme from the secant variety of the grassmannian. Cryptology ePrint Archive, Report 2020/1141, 2020. `https://eprint.iacr.org/2020/1141`.