EXPLOITING HIGHER DIMENSIONS IN ISOGENY-BASED CRYPTOGRAPHY

SARAH ARPIN AND CHLOE MARTINDALE

1. Introduction

This course covers modern trends using abelian varieties in isogeny-based cryptography, a subfield of post-quantum cryptography. Post-quantum cryptography can be implemented now on classical devices, but is designed to be resistant to a future attacker with access to a quantum computer. Isogeny-based cryptography is an incredibly active research area, with new protocols being proposed every few months, many of which are the only viable post-quantum solution for certain cryptographic tasks. Recent advancements in isogeny-based cryptography are rooted in the arithmetic geometry of abelian varieties over finite fields. In this mini-course, we will cover the mathematical foundations of high-dimensional isogeny-based cryptography.

Isogeny graphs of supersingular elliptic curves are maximal expander graphs, meaning the end vertex of a random walk in the graph very quickly approaches a uniform distribution. The endomorphism rings of supersingular elliptic curves are maximal orders in quaternion algebras, and the classical Deuring correspondence provides in some sense a dictionary between the geometry of elliptic curves and the algebra of the quaternions. As maximal quaternion orders are endomorphism rings of elliptic curves, left ideals of those orders correspond to isogenies of elliptic curves. The computational complexity of the *isogeny problem* underlies the security of isogeny-based cryptographic protocols:

Problem 1 (The isogeny problem)**.** *Given two uniformly random supersingular elliptic curves over a finite field k, find and compute an isogeny between them.*

Much of the existing work in post-quantum cryptography is driven by global standardization efforts, such as those by the National Institute of Standards and Technology (NIST) [21, 20]. In 2024, NIST selected three new cryptographic protocols for standardization, but they are continuing to evaluate and hopefully standardize more protocols. In 2022, NIST continued its efforts with a call for 'additional' post-quantum digital signatures, in which SQISign [1] is a leading round-2 candidate based on the isogeny problem. SQISign is a digital signature built from the Fiat-Shamir Transform of a Σ protocol (depicted in Figure 1).

In the original SQISign [5] Σ protocol, the setup starts with a publicly known elliptic curve E_0 with known endomorphism ring. A *prover* knows a secret isogeny $\tau : E_0 \to E_A$, and they must prove knowledge of this isogeny to a *verifier* who knows E_0 and E_A, without revealing any information about the isogeny τ. The prover computes a random commitment isogeny $\psi : E_0 \to E_1$ and sends ψ and the codomain E_1 to the verifier, who responds with a challenge isogeny $\varphi : E_1 \to E_2$. The prover is now tasked with responding with an isogeny from $E_A \to E_2$ – an instance of the isogeny problem – without revealing anything about the secret isogenies τ and ψ. Crucially:

Date: Arizona Winter School 2026.

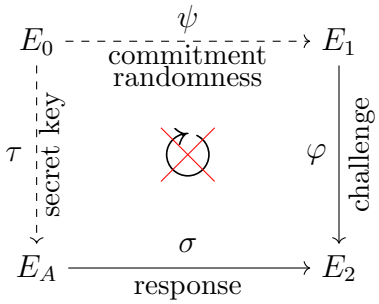

FIGURE 1. A summary of the Σ protocol underlying the original SQIsign.

- Without knowledge of an isogeny $\tau : E_0 \to E_A$, it would be computationally infeasible to produce a response isogeny from E_A to E_2.
- If the prover responds with the isogeny $\varphi \circ \psi \circ \widehat{\tau}$, they reveal enough information to recover τ.

However, via the Deuring correspondence the prover *can* use the knowledge of

$$\varphi \circ \psi \circ \widehat{\tau} : E_A \to E_2$$

to efficiently compute a *random* isogeny $\sigma : E_A \to E_2$, which the prover sends as a response. The isogeny σ does not reveal information about the secret map τ, but it would not be possible for the prover to produce σ without knowledge of τ.

The public-key information of an isomorphism invariant of a supersingular elliptic curve is incredibly efficient to represent, as it is just an element of the (finite!) field of definition k. Isogeny-based cryptography distinguishes itself among post-quantum candidates by offering the smallest key sizes, while maintaining competitive performance.

The current (July 2025) version of SQISign, based on [3, 18, 9], makes use of the fact that we can embed isogenies of elliptic curves into two (or four or eight) dimensions by considering products of elliptic curves. This isogeny representation is compact and achieves superior provable security. This was inspired by the attacks on SIKE [4, 12, 19], which demonstrated the first important cryptographic application of Kani's Reducibility Criterion.

Theorem 2 (Kani's Reducibility Criterion [10, Thm. 2.3])**.** *Let f, A, and B be pairwise coprime integers such that $B = f + A$ and let E, E_A, E_0, F be elliptic curves such that there exist isogenies $\varphi_f, \varphi_A, \varphi, g_A$, and g_f (resp.) of degrees f, A, fA, A, and f (resp.) for which the diagram in Figure 2 commutes. Then, the isogeny*

$$\Phi = \begin{pmatrix} \varphi_f & -\widehat{\varphi}_A \\ g_A & \widehat{g}_f \end{pmatrix} : E \times E_A \to E_0 \times F$$

is a (B, B)-isogeny with respect to the product polarizations on $E \times E_A$ and $E_0 \times F$ with kernel given

$$\ker \Phi = \{([A]P, \varphi(P)) : P \in E[B]\}.$$

This criterion allows us to transport a question about computing isogenies of elliptic curves with potential large non-smooth degree to a question about computing isogenies of abelian surfaces with a degree over which we have some control: typically in practical instantiations we aim for this degree to be a power of two.

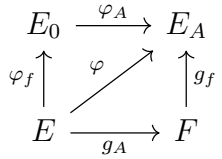

FIGURE 2. Kani's Reducibility Criterion

In summary, Kani's Reducibility Criterion will serve as a central tool in this course, where we will examine its role in the design of cryptographic protocols such as SQISign and in enabling compact representation and efficient computation of isogenies. Along the way, we will also see how principal polarizations of abelian varieties [17], the arithmetic geometry of endomorphism rings [22], and Mumford's theory of theta coordinates [14, 15, 16], enrich our understanding of abelian varieties over finite fields. These techniques motivate advancement of the discipline, in addition to underpinning the state-of-the-art approaches to modern isogeny-based cryptography.

2. Course Outline

(1) Lecture 1: **Introduction to isogeny-based cryptography.**
This lecture will provide an overview of the types of protocols and the mathematical foundations on which they are built: class-group actions, the Deuring correspondence, and Kani's Reducibility Criterion.
(2) Lecture 2: **Efficient representation and evaluation of isogenies.**
In this lecture, we will go into more depth on the applications of Kani's reducibility criterion with a focus on the Clapotis framework.
(3) Lecture 3: **Isogeny-based digital signatures.**
This lecture will describe the details of the SQISign2D digital signature protocol, which makes use of both the Deuring correspondence and Kani's reducibility criterion.
(4) Lecture 4: **Overview of higher dimensional isogeny-based cryptographic applications.**
The tools described in lecture 2 have been used to propose many new isogeny-based protocols. We will provide an overview of the latest developments in this direction along with the state-of-the-art in higher dimensional isogeny computation.

3. Background Reading for Lectures

(1) Luciano Maino. "Factoring Isogenies in Higher Dimension and Applications". Available at `https://research-information.bris.ac.uk/en/studentTheses/factoring-isogenies-in-higher-dimension-and-applications`. PhD thesis. University of Bristol, School of Computer Science, Mar. 2025
(2) Sarah Arpin, Catalina Camacho-Navarro, Kristin Lauter, Joelle Lim, Kristina Nelson, Travis Scholl, and Jana Sotáková. "Adventures in supersingularland". In: *Exp. Math.* 32.2 (2023), pp. 241–268. ISSN: 1058-6458,1944-950X. DOI: `10.1080/10586458.2021.1926009`
(3) Andrea Basso, Pierrick Dartois, Luca De Feo, Antonin Leroux, Luciano Maino, Giacomo Pope, Damien Robert, and Benjamin Wesolowski. "SQIsign2D–West". In: *Advances in cryptology—ASIACRYPT 2024. Part III.* vol. 15486. Lecture Notes

in Comput. Sci. Springer, Singapore, 2025, pp. 339–370. ISBN: 978-981-96-0890-4; 978-981-96-0891-1. DOI: 10.1007/978-981-96-0891-1_11

4. Projects

The Project Assistant will be Luciano Maino. We will have several options for project problems, all using the arithmetic geometry of abelian varieties over finite fields to study problems motivated by isogeny-based cryptography. The project problem options will involve varying amounts of cryptography. Students in our project group should arrive at Arizona Winter School having read through the recommended background.

The projects will be on two themes: structural questions on graphs in higher dimensions and explicit computation of higher dimensional isogenies. The precise projects will be fixed a later point in time: the research in this area moves *very* fast and things may change in the meantime!

If you are more interested in the first theme, we recommend reading [2] and [7] on the dimension 1 case, and [13, Chapter 3] for a particularly simple dimension g case. If you are more interested in the second theme, we recommend reading [6] on computing (3,3)-isogenies, [11, Chapter 4] on the theta model and (2,2)-isogenies, [8] on computing cyclic isogenies, and [11, Chapter 7] on computing cyclic isogenies using Kani's lemma.

References

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

[2] Sarah Arpin, Catalina Camacho-Navarro, Kristin Lauter, Joelle Lim, Kristina Nelson, Travis Scholl, and Jana Sotáková. "Adventures in supersingularland". In: *Exp. Math.* 32.2 (2023), pp. 241–268. ISSN: 1058-6458,1944-950X. DOI: 10.1080/10586458.2021.1926009.

[3] Andrea Basso, Pierrick Dartois, Luca De Feo, Antonin Leroux, Luciano Maino, Giacomo Pope, Damien Robert, and Benjamin Wesolowski. "SQIsign2D–West". In: *Advances in cryptology—ASIACRYPT 2024. Part III*. Vol. 15486. Lecture Notes in Comput. Sci. Springer, Singapore, 2025, pp. 339–370. ISBN: 978-981-96-0890-4; 978-981-96-0891-1. DOI: 10.1007/978-981-96-0891-1_11.

[4] Wouter Castryck and Thomas Decru. "An efficient key recovery attack on SIDH". In: *Advances in cryptology—EUROCRYPT 2023. Part V*. Vol. 14008. Lecture Notes in Comput. Sci. Springer, Cham, 2023, pp. 423–447. ISBN: 978-3-031-30588-7; 978-3-031-30589-4. DOI: 10.1007/978-3-031-30589-4_15.

[5] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. "SQISign: Compact Post-quantum Signatures from Quaternions and Isogenies". In: *Advances in Cryptology – ASIACRYPT 2020*. Ed. by Shiho Moriai and Huaxiong Wang. Cham: Springer International Publishing, 2020, pp. 64–93. ISBN: 978-3-030-64837-4.

[6] Thomas Decru and Sabrina Kunzweiler. "Efficient computation of $(3^n, 3^n)$-isogenies". In: *Progress in cryptology—AFRICACRYPT 2023*. Vol. 14064. Lecture Notes in Comput. Sci. Springer, Cham, 2023, pp. 53–78. ISBN: 978-3-031-37678-8; 978-3-031-37679-5. DOI: 10.1007/978-3-031-37679-5_3.

[7] Christina Delfs and Steven D. Galbraith. "Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$". In: *Des. Codes Cryptogr.* 78.2 (2016), pp. 425–440. ISSN: 0925-1022,1573-7586. DOI: 10.1007/s10623-014-0010-1.

[8] Alina Dudeanu, Dimitar Jetchev, Damien Robert, and Marius Vuille. "Cyclic isogenies for abelian varieties with real multiplication". In: *Mosc. Math. J.* 22.4 (2022), pp. 613–655. ISSN: 1609-3321,1609-4514. DOI: 10.17323/1609-4514-2022-22-4-613-655.

[9] Max Duparc and Tako Boris Fouotsa. *SQIPrime: A dimension 2 variant of SQISignHD with non-smooth challenge isogenies*. Cryptology ePrint Archive, Paper 2024/773. 2024. URL: https://eprint.iacr.org/2024/773.

[10] Ernst Kani. "The number of curves of genus two with elliptic differentials." In: *Journal für die reine und angewandte Mathematik* 1997.485 (1997), pp. 93–122. DOI: doi:10.1515/crll.1997.485.93.

[11] Luciano Maino. "Factoring Isogenies in Higher Dimension and Applications". Available at https://research-information.bris.ac.uk/en/studentTheses/factoring-isogenies-in-higher-dimension-and-applications. PhD thesis. University of Bristol, School of Computer Science, Mar. 2025.

[12] Luciano Maino, Chloe Martindale, Lorenz Panny, Giacomo Pope, and Benjamin Wesolowski. "A direct key recovery attack on SIDH". In: *Advances in cryptology—EUROCRYPT 2023. Part V*. Vol. 14008. Lecture Notes in Comput. Sci. Springer, Cham, 2023, pp. 448–471. ISBN: 978-3-031-30588-7; 978-3-031-30589-4. DOI: 10.1007/978-3-031-30589-4_16.

[13] Chloe Martindale. "Isogeny graphs, modular polynomials, and applications". Universiteit Leiden and Bordeaux University. PhD thesis. 2018. URL: https://www.martindale.info/research/Thesis.pdf.

[14] D. Mumford. "On the equations defining abelian varieties. I". In: *Invent. Math.* 1 (1966), pp. 287–354. ISSN: 0020-9910,1432-1297. DOI: 10.1007/BF01389737. URL: https://doi.org/10.1007/BF01389737.

[15] D. Mumford. "On the equations defining abelian varieties. II". In: *Invent. Math.* 3 (1967), pp. 75–135. ISSN: 0020-9910,1432-1297. DOI: 10.1007/BF01389741. URL: https://doi.org/10.1007/BF01389741.

[16] D. Mumford. "On the equations defining abelian varieties. III". In: *Invent. Math.* 3 (1967), pp. 215–244. ISSN: 0020-9910,1432-1297. DOI: 10.1007/BF01425401. URL: https://doi.org/10.1007/BF01425401.

[17] David Mumford. *Abelian varieties*. Vol. 5. Tata Institute of Fundamental Research Studies in Mathematics. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition. Tata Institute of Fundamental Research, Bombay; by Hindustan Book Agency, New Delhi, 2008, pp. xii+263. ISBN: 978-81-85931-86-9; 81-85931-86-0.

[18] Kohei Nakagawa and Hiroshi Onuki. *SQIsign2D-East: A New Signature Scheme Using 2-dimensional Isogenies*. Cryptology ePrint Archive, Paper 2024/771. 2024. URL: https://eprint.iacr.org/2024/771.

[19] Damien Robert. "Breaking SIDH in polynomial time". In: *Advances in cryptology—EUROCRYPT 2023. Part V*. Vol. 14008. Lecture Notes in Comput. Sci. Springer, Cham, 2023, pp. 472–503. ISBN: 978-3-031-30588-7; 978-3-031-30589-4. DOI: 10.1007/978-3-031-30589-4_17.

[20] National Institute of Standards and Technology. *Post-quantum cryptography standardization*. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography. 2016.

[21] National Institute of Standards and Technology. *Post-Quantum Cryptography: Additional Digital Signature Schemes*. https://csrc.nist.gov/projects/pqc-dig-sig. 2022.

[22] John Tate. "Endomorphisms of abelian varieties over finite fields". In: *Invent. Math.* 2 (1966), pp. 134–144. ISSN: 0020-9910,1432-1297. DOI: 10.1007/BF01404549.