



APPLICATIONS OF ARITHMETIC GEOMETRY IN CRYPTOGRAPHY AND COMPUTATIONAL MATHEMATICS: ELLIPTIC CURVES, FINITE FIELDS AND EMERGING DIRECTIONS

Dodiya Nidhiben¹, Dr. Ashok Patel²

ABSTRACT

Arithmetic geometry represents the profound synthesis of algebraic geometry and number theory, emerging as a foundational pillar for both abstract mathematical theory and applied computational science. This report provides an exhaustive investigation into the applications of arithmetic geometry within modern cryptography and computational mathematics, tracking the discipline's evolution from the classical study of Diophantine equations to the frontiers of post-quantum cryptographic infrastructure. The analysis extensively evaluates the integration of elliptic curves over finite fields, emphasizing the critical role of rational points, the Schoof-Elkies-Atkin algorithm, and the Elliptic Curve Discrete Logarithm Problem (ECDLP) in establishing secure communication frameworks. Furthermore, the report critically examines the rapid paradigm shift in isogeny-based cryptography, detailing the catastrophic Castryck-Decru attack on the Supersingular Isogeny Diffie-Hellman (SIDH) protocol—a vulnerability exposed through the arithmetic geometry of abelian surfaces and Richelot isogenies—and the subsequent pivot toward the SQIsign protocol. Beyond cryptography, the analysis explores the deployment of algebraic geometry codes on modular curves that surpass the Gilbert-Varshamov bound. Finally, the report synthesizes emerging theoretical developments shaping the future of computational mathematics, including perfectoid spaces, prismatic cohomology, derived algebraic geometry, and arithmetic statistics, illuminating how the most abstract geometrical frameworks continuously inform and revolutionize applied algorithmic paradigms.

KEYWORDS: Arithmetic Geometry, Elliptic Curve Cryptography, Post-Quantum Cryptography, Supersingular Isogenies, Perfectoid Spaces, Prismatic Cohomology, Algebraic Geometry Codes, Arithmetic Statistics.

How to Cite:

Dodiya Nidhiben
& Dr. Ashok Patel
(2026), Applications of
Arithmetic Geometry
in Cryptography
and Computational
Mathematics:
Elliptic Curves,
Finite Fields and
Emerging Directions,
International
Educational Applied
Scientific & Research
Journal (IEASRJ),
Vol: 11, Issue: 10,
01-07

INTRODUCTION AND BACKGROUND OF THE STUDY

The historical convergence of algebraic geometry and number theory represents one of the most remarkable intellectual achievements in modern mathematics. For centuries, these disciplines operated strictly within their independent silos. Classical number theory occupied itself with the arithmetic properties of integers, prime distribution, congruences, and the explicit numerical solutions of Diophantine equations. Early contributions by mathematicians such as Euclid, Diophantus of Alexandria,

Pierre de Fermat, Leonhard Euler, and Joseph-Louis Lagrange established the fundamental principles governing integer relations, culminating in Carl Friedrich Gauss's *Disquisitiones Arithmeticae*, which formalized the systemic treatment of congruences and quadratic forms. Conversely, classical algebraic geometry investigated the geometric properties of polynomial equations defining curves and surfaces over algebraically closed fields, such as the complex numbers. Initiated by René Descartes' synthesis of algebra and geometry through coordinate systems, the field advanced through the rigorous

geometric methods of Bernhard Riemann, Guido Castelnuovo, and Oscar Zariski, who introduced concepts such as topological genus and commutative algebraic topologies.

The realization that polynomial equations simultaneously possess algebraic, geometric, and arithmetic interpretations fundamentally transformed both disciplines. The decisive paradigm shift occurred in the mid-twentieth century, spearheaded by Alexander Grothendieck's introduction of scheme theory. By generalizing classical algebraic varieties to geometric objects defined over arbitrary commutative rings, scheme theory allowed arithmetic objects—such as the ring of integers and finite fields—to be studied using sophisticated geometric intuition. Grothendieck's framework, combined with his development of étale cohomology, provided the essential machinery that enabled Pierre Deligne to prove the Weil Conjectures in 1974. Deligne's landmark proof established a profound topological analogue for the Riemann Hypothesis over finite fields, demonstrating that the number of rational points on algebraic varieties over finite fields is governed by cohomological invariants and the eigenvalues of the Frobenius endomorphism.

This theoretical unification birthed modern arithmetic geometry. As researchers began interpreting classical number-theoretic problems through the lens of geometric structures, the study of elliptic curves assumed a central role. Possessing an intrinsic abelian group structure, elliptic curves allowed mathematicians to utilize both geometric morphisms and arithmetic group laws to resolve ancient queries, most notably culminating in Andrew Wiles' 1995 proof of Fermat's Last Theorem via the Modularity Theorem, which established a profound equivalence between elliptic curves and modular forms. Similarly, Gerd Faltings' 1983 proof of the Mordell Conjecture demonstrated that every smooth projective curve of genus greater than one defined over a number field possesses only finitely many rational points, fundamentally relying on abelian varieties and arithmetic intersection theory.

Simultaneously, the late twentieth century witnessed an unprecedented integration of arithmetic geometry into computational mathematics.

Abstract theoretical constructs suddenly yielded immense practical utility. The finite generation of rational points on elliptic curves, coupled with the computational hardness of specific group-theoretic problems, revolutionized public-key cryptography. Error-correcting codes derived from algebraic curves over finite fields resolved critical bottlenecks in digital information transmission. Today, as the advent of quantum computing threatens classical cryptographic architectures, arithmetic geometry remains the vanguard of defense, pivoting toward advanced constructs such as supersingular isogeny graphs and abelian surfaces to construct quantum-resistant protocols.

AIMS & OBJECTIVES

The primary objective of this report is to provide a comprehensive, expert-level synthesis of the applications of arithmetic geometry in computational mathematics and cryptography. Specifically, the analysis seeks to examine the fundamental algebraic and geometric structures—such as elliptic curves and finite fields—that undergird modern public-key cryptographic protocols and algorithmic coding theory. Furthermore, the report aims to evaluate the trajectory of isogeny-based cryptography, with a critical focus on the mathematical mechanisms of the Castryck-Decru attack and its implications for post-quantum cryptographic standardization. To bridge abstract theory with applied methodologies, the analysis details the computational infrastructure and algorithmic techniques that facilitate the practical deployment of arithmetic geometry. Ultimately, the report synthesizes emerging, highly abstract theoretical frameworks—including perfectoid spaces, prismatic cohomology, derived algebraic geometry, and arithmetic statistics—assessing their potential to dictate the future of computational mathematics and secure digital infrastructure.

RESEARCH APPROACH AND COMPUTATIONAL INFRASTRUCTURE

The methodology guiding this analysis is rooted in a deductive, theoretical evaluation of the contemporary mathematical landscape. The study synthesizes formal geometric structures—such as schemes, sheaves, abelian varieties, and Galois representations—and analyzes their algorithmic implementation across computational domains.

The approach examines the transition from classical explicit computation to structural analysis, analyzing how geometric invariants determine arithmetic behavior across highly complex polynomial systems. The bridge between abstract arithmetic geometry and applied computational science is entirely reliant on modern mathematical software. The sheer complexity of symbolic computation, high-degree polynomial systems, and immense prime fields requires robust algorithmic ecosystems. Below is an overview of the core computational infrastructure that powers experimental and applied arithmetic geometry.

Software System	Primary Mathematical Applications	Role in Arithmetic Geometry & Cryptography
SageMath	Open-source symbolic computation, algebra, number theory.	Integrates multiple libraries for elliptic curve point counting, finite field arithmetic, and post-quantum cryptographic protocol simulation.
Magma	High-performance computational algebra, finite groups, geometry.	Provides highly optimized algorithms for modular forms, L-functions, hyperelliptic curve Jacobians, and Galois representations.
PARI/GP	Computational number theory, algebraic number fields.	Specializes in prime testing, integer factorization, class group computations, and extremely rapid arbitrary-precision arithmetic.
Macaulay2	Commutative algebra, algebraic geometry, homological algebra.	Computes Gröbner bases, syzygies, sheaf cohomology, and intersection theory; vital for analyzing high-dimensional varieties.

This computational foundation ensures that purely theoretical conjectures—such as the Birch and Swinnerton-Dyer Conjecture or the distribution of class groups under the Cohen-Lenstra heuristics—can be empirically tested across massive datasets of mathematical objects.

RESULTS & DISCUSSION

Elliptic Curves and Finite Fields in Cryptography

Elliptic curves serve as the paramount example of arithmetic geometry's practical utility. An elliptic curve defined over a field with characteristic distinct from 2 and 3 can be canonically represented by the

short Weierstrass equation, where the variables satisfy a non-singularity condition dictating that the discriminant is non-zero. From the perspective of algebraic geometry, this forms a smooth projective curve of genus one. However, its true power lies in its arithmetic properties: the rational points on an elliptic curve naturally form an abelian group under a chord-and-tangent addition law. The identity element of this group is the distinguished point at infinity, and the group operations are defined entirely through geometric intersections.

When defined over a finite field, the set of rational points forms a finite abelian group. The cardinality of this group is tightly constrained by Hasse's Theorem, a fundamental precursor to the Weil conjectures, which bounds the number of rational points relative to the size of the finite field. The establishment of Elliptic Curve Cryptography (ECC) in the 1980s leveraged the difficulty of the Elliptic Curve Discrete Logarithm Problem (ECDLP): given a base point and a scalar multiple of that point, retrieving the scalar integer is computationally intractable for appropriately chosen curves. ECC achieves robust security with substantially smaller key sizes compared to legacy systems like RSA. For instance, a 256-bit ECC key offers comparable cryptographic strength to a 3072-bit RSA key, thereby drastically reducing computational overhead, memory consumption, and transmission bandwidth in modern digital infrastructures.

The practical implementation of ECC required immense advancements in computational number theory, specifically in algorithms for point counting over finite fields to ascertain the precise group order and avoid mathematically vulnerable curves. The Schoof-Elkies-Atkin (SEA) algorithm revolutionized this process. By calculating the trace of the Frobenius endomorphism modulo various small primes and subsequently utilizing the Chinese Remainder Theorem, the SEA algorithm performs deterministic point counting in polynomial time, rendering the generation of cryptographically secure curves highly efficient.

Isogeny-Based Cryptography and the Post-Quantum Paradigm

The advent of quantum computing, specifically the

theoretical realization of Shor's algorithm, threatens to dismantle classical public-key cryptography by solving both integer factorization and the ECDLP in polynomial time. In response, the cryptographic community turned once again to arithmetic geometry, specifically to the complex structures of isogeny graphs, to construct post-quantum cryptographic protocols.

An isogeny is a non-constant algebraic morphism between two elliptic curves that preserves the point at infinity, effectively acting as a group homomorphism. Because it is a rational map with a finite kernel, an isogeny is entirely defined by its kernel up to an isomorphism of the target curve. The post-quantum paradigm heavily relies on supersingular elliptic curves. An elliptic curve over a field of characteristic greater than zero is supersingular if its group of p -torsion points over the algebraic closure is trivial. The graph formed by supersingular elliptic curves (represented as vertices by their j -invariants) and isogenies of a fixed prime degree (acting as edges) constitutes a regular Ramanujan graph, which exhibits optimal expansion and rapid mixing properties.

Taking a sufficiently long random walk through a supersingular isogeny graph produces an output curve that is virtually indistinguishable from a curve drawn from a uniform distribution. The foundational security assumption of this paradigm is the computational hardness of the path-finding problem: given two randomly selected supersingular elliptic curves, it is exponentially difficult for both classical and quantum computers to determine the specific sequence of isogenies connecting them.

This mathematical framework birthed the Supersingular Isogeny Diffie-Hellman (SIDH) protocol, later encapsulated by the National Institute of Standards and Technology (NIST) as SIKE (Supersingular Isogeny Key Encapsulation). In SIDH, two parties initiate random walks on the isogeny graph from a public starting curve, using isogenies of smooth, coprime degrees. To allow the parties to complete a commutative key-exchange square, SIDH requires the transmission of auxiliary information: each party must send the images of the other's torsion basis points evaluated under their own secret isogeny.

The Castryck-Decru Attack: An Arithmetic Geometry Collapse

The transmission of these auxiliary torsion points was long scrutinized but generally deemed safe until a catastrophic vulnerability was exposed. In 2022, Wouter Castryck and Thomas Decru published an efficient, polynomial-time key recovery attack that entirely broke SIDH, forcing its immediate deprecation from the NIST post-quantum standardization process.

The brilliance of the Castryck-Decru attack resides not in quantum computing algorithms, but in the sophisticated application of high-dimensional arithmetic geometry. Because the protocol required the transmission of the images of torsion points, the attacker possessed exact knowledge of how the secret isogeny acted on a large torsion subgroup. The attack leveraged Ernst Kani's "glue-and-split" theorem, which dictates that two elliptic curves coupled with a specific isogeny between them can be embedded into the Jacobian of a genus 2 curve, effectively forming an abelian surface.

Castryck and Decru realized that by mapping the public and intermediate curves into a two-dimensional abelian surface, the exposed torsion data provided a deterministic pathway to compute a known endomorphism. By walking the isogeny graph of abelian surfaces using Richelot isogenies—generalized isogenies applicable to hyperelliptic curves—the attacker could iteratively test whether a hypothesized step in the secret isogeny walk was correct. If the attacker's guess was correct, the resulting abelian surface would geometrically "split" back into the product of two elliptic curves; if incorrect, it would remain the Jacobian of a hyperelliptic curve. This binary geometric oracle allowed attackers to recover the secret isogeny key bit-by-bit, solving the supposedly intractable problem in mere minutes on a standard commercial processor.

The collapse of SIDH underscores a vital insight: lifting one-dimensional cryptographic problems (elliptic curves) into higher-dimensional arithmetic spaces (abelian surfaces) can expose profound structural weaknesses. Following this event, the cryptographic community pivoted to alternative isogeny protocols, most notably SQIsign (Short Quantum Isogenies).

SQIsign circumvents the Castryck-Decru attack by completely abandoning the transmission of auxiliary torsion points. Instead, it relies on the Deuring correspondence, which establishes a structural equivalence between supersingular elliptic curves over finite fields and maximal orders in quaternion algebras. By translating the isogeny path-finding problem into algebraic tasks within quaternion rings, SQIsign preserves the quantum resistance of isogenies without exposing geometric vulnerabilities.

Algebraic Geometry Codes and Information Theory

Beyond cryptography, the structural properties of arithmetic geometry have deeply penetrated information and coding theory. Classical Reed-Solomon codes, though highly effective for data transmission, are fundamentally constrained because their block length cannot exceed the cardinality of the underlying finite field. To surpass this limitation, V.D. Goppa leveraged the theory of algebraic curves to invent Algebraic Geometry (AG) codes.

An AG code is constructed using a smooth projective curve defined over a finite field. By defining a divisor consisting of distinct rational points on the curve, and a secondary divisor with disjoint support, the code evaluates functions derived from the Riemann-Roch space at the specified rational points. The Riemann-Roch theorem provides precise mathematical lower bounds on the dimension of the resulting code, while the degree of the secondary divisor bounds the number of roots, thereby rigorously guaranteeing the minimum Hamming distance of the code.

The most spectacular success of AG codes occurred when mathematicians Tsfasman, Vladut, and Zink demonstrated that codes derived from modular curves and Shimura curves possess sufficiently many rational points relative to their genus that they exceed the Gilbert-Varshamov bound. This bound was previously believed by information theorists to be the absolute theoretical limit for the asymptotic performance of error-correcting codes. Today, AG codes are actively researched for integration into post-quantum cryptography, specifically as drop-in replacements for standard Goppa codes in the McEliece public-key encryption system, offering reduced public key sizes without sacrificing security

margins.

EMERGING THEORETICAL FRAMEWORKS IN ARITHMETIC GEOMETRY

While elliptic curves and modular curves have firmly established their applied utility in computation, the vanguard of pure arithmetic geometry is currently exploring highly abstract frontiers. These emerging frameworks—while seemingly detached from current computational implementation—historically serve as the incubators for the next generation of algorithmic tools.

Perfectoid Spaces and p -adic Geometry

Introduced by Peter Scholze in 2012, perfectoid geometry resolves some of the most intractable barriers in mixed-characteristic arithmetic. Classical p -adic geometry struggled to compare mathematical objects defined over characteristic zero (such as p -adic fields) with those defined over characteristic p (such as Laurent series over finite fields). A perfectoid field is a highly complete non-Archimedean field featuring a non-discrete valuation of rank 1, wherein the Frobenius map is surjective modulo p .

Scholze's crowning innovation within this framework is the "tilting equivalence." The tilting process establishes a strict categorical isomorphism between perfectoid spaces over a mixed-characteristic perfectoid field and those over its characteristic p tilt. This equivalence allows mathematicians to translate brutally complex geometric and cohomological problems from characteristic 0 down to characteristic p , solve them utilizing the robust, highly developed tools of positive characteristic algebra, and lift the solutions back to characteristic 0.

The geometrization of the local Langlands correspondence heavily relies on this foundation. By constructing the Fargues-Fontaine curve—an arithmetic curve that behaves analogously to a compact Riemann surface but operates entirely within a p -adic framework—mathematicians Laurent Fargues and Peter Scholze have provided a purely geometric theater for studying p -adic Galois representations and automorphic forms.

Prismatic Cohomology and Syntomic Methods

Building upon the success of perfectoid spaces,

Bhargav Bhatt and Peter Scholze introduced prismatic cohomology, an abstract theory that unifies several historically disparate cohomological frameworks—namely de Rham, crystalline, and étale cohomology—under a single structural umbrella. Prismatic cohomology evaluates algebraic varieties relative to a “prism,” which is a highly structured commutative ring equipped with a Frobenius lift and a distinguished ideal. This construction acts effectively as a q -deformation of classical de Rham cohomology, allowing geometric invariants to be tracked across different mathematical topologies.

Furthermore, the integration of topological cyclic homology and prismatic cohomology has yielded profound results in syntomic cohomology. By applying trace methods and the Bhatt-Morrow-Scholze motivic filtration, researchers can compute previously inaccessible algebraic K-groups. Recently, mathematicians Shachar Carmeli and Tony Feng constructed the “syntomic Steenrod algebra,” applying spectral prismatic F-gauges to definitively resolve Tate’s 1966 conjecture regarding the existence of symplectic forms on the Brauer groups of smooth proper surfaces over finite fields. This breakthrough demonstrates the remarkable capacity of modern cohomological abstraction to solve classical, concrete arithmetic conjectures.

Derived Algebraic Geometry and Motive Theory

Derived algebraic geometry, spearheaded heavily by Jacob Lurie, extends Grothendieck’s scheme theory by replacing standard commutative rings with ∞ -categories of animated rings or E_∞ -ring spectra. In classical algebraic geometry, intersections of varieties can be highly pathological, often yielding singular spaces that lose dimensional data. Derived algebraic geometry resolves this by retaining higher homotopical data in the structure sheaf; derived intersections fundamentally “remember” how they were formed, thus smoothing out intersection theory and allowing robust analysis of derived moduli stacks.

Simultaneously, Alexander Grothendieck’s Motive Theory continues to shape the underlying philosophy of arithmetic geometry. Grothendieck posited that the myriad cohomology theories applicable to algebraic varieties are mere “realizations” of a singular, universal, underlying geometric essence called a

“motive”. While the full, unconditioned theory of mixed motives remains conjectural—contingent upon the resolution of the Standard Conjectures on Algebraic Cycles—motives increasingly dictate the analysis of L-functions and the mapping of the motivic Galois group. This structural view acts as the ultimate compass guiding the global Langlands Program, asserting that all arithmetic symmetry stems from universal geometric kernels.

Arithmetic Statistics

Whereas classical number theory is intensely deterministic—asking whether a specific Diophantine equation has explicit solutions—the emerging field of Arithmetic Statistics adopts a probabilistic approach, inquiring about the distribution, density, and average behavior of arithmetic properties across massive families of objects.

The cornerstone of this statistical approach lies in the Cohen-Lenstra heuristics, which successfully predicted the distribution of the odd-prime parts of ideal class groups in imaginary quadratic fields. The heuristics model these class groups as random finite abelian groups weighted inversely by their number of automorphisms. However, the 2-part of class groups historically resisted this modeling due to the overriding influence of Gauss’s genus theory constraints.

Recent breakthroughs have dramatically propelled this field forward. Manjul Bhargava’s revolutionary work on the geometry of numbers established precise bounds on the 2-Selmer groups of hyperelliptic curves, proving unconditionally that a positive proportion of elliptic curves have rank 0, and another positive proportion have rank 1, validating massive swathes of the Birch and Swinnerton-Dyer conjecture. Concurrently, Alexander Smith resolved the long-standing mystery surrounding the 2-part of class groups and the distribution of 2^∞ -Selmer groups, validating Gerth’s modification of the Cohen-Lenstra heuristics for the prime $p=2$. Furthermore, investigations into Malle’s conjecture on the distribution of Galois extensions have been refined following the discovery of critical counterexamples by Klüners, pushing the discipline to account for previously unmapped local behavioral dependencies. These statistical frameworks are

heavily dependent on vast computational databases, such as the LMFDB (L-functions and Modular Forms Database), illuminating the symbiotic cycle between theoretical probability, geometric bounds, and raw computational data mining.

CONCLUSION

Arithmetic geometry stands as the preeminent unifying framework in modern mathematics, seamlessly binding the disparate realms of topology, geometry, algebra, and number theory. As demonstrated throughout this report, the implications of this convergence extend far beyond abstract theoretical elegance. The instantiation of elliptic curves and algebraic geometry codes over finite fields has fundamentally dictated the architecture of global cryptographic infrastructure and digital communication. The evolutionary trajectory of isogeny-based cryptography provides a sobering yet illuminating testament to the power of these mathematical structures. The catastrophic collapse of the SIDH protocol via the Castryck-Decru attack was not orchestrated through brute computational force or nascent quantum hardware, but through the profound structural insights of higher-dimensional arithmetic geometry—specifically abelian surfaces, Kani’s glue-and-split theorem, and Richelot isogenies. It serves as a stark reminder that as cryptographic protocols venture into post-quantum mathematical domains, evaluating their security demands an exceptionally deep mastery of arithmetic geometry. Looking forward, the frontiers of mathematical abstraction—perfectoid spaces, prismatic cohomology, derived algebraic geometry, and arithmetic statistics—will inevitably precipitate the next technological revolution. Just as Riemann surfaces and modular curves once seemed entirely divorced from applied computational science only to eventually undergird public-key cryptography and information theory, the highly abstract topological machinations of today will invariably translate into the optimized computational algorithms and quantum-resistant infrastructures of tomorrow. By continuing to explore the interplay between pure theoretical abstraction and rigorous computational modeling, arithmetic geometry will undoubtedly dictate the future paradigm of both applied mathematics and global cybersecurity.

REFERENCES

1. Hartshorne, R. (1977). *Algebraic geometry*. Springer.
2. Silverman, J. H. (2009). *The arithmetic of elliptic curves* (2nd ed.). Springer.
3. Gauss, C. F. (1986). *Disquisitiones arithmeticae* (A. A. Clarke, Trans.). Springer. (Original work published 1801).
4. Grothendieck, A., & Dieudonné, J. A. (1960–1967). *Éléments de géométrie algébrique* (Vols. I–IV). Publications Mathématiques de l’IHÉS.
5. Corn, P. (2021). *Arithmetic geometry*. American Mathematical Society.
6. Milne, J. S. (1986). *Arithmetic duality theorems*. Academic Press.
7. Lang, S. (1983). *Fundamentals of Diophantine geometry*. Springer.
8. Bombieri, E., & Gubler, W. (2006). *Heights in Diophantine geometry*. Cambridge University Press.
9. Wiles, A. (1995). Modular elliptic curves and Fermat’s Last Theorem. *Annals of Mathematics*, 141(3), 443–551.
10. Weil, A. (1949). Numbers of solutions of equations in finite fields. *Bulletin of the American Mathematical Society*, 55(5), 497–508.
11. Deligne, P. (1974). La conjecture de Weil: I. *Publications Mathématiques de l’IHÉS*, 43, 273–307.
12. Faltings, G. (1983). Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Inventiones Mathematicae*, 73(3), 349–366.
13. Langlands, R. P. (1970). *Problems in the theory of automorphic forms*. Springer.
14. Frenkel, E. (2013). *Love and math: The heart of hidden reality*. Basic Books.
15. Scholze, P. (2012). Perfectoid spaces. *Publications Mathématiques de l’IHÉS*, 116(1), 245–313.
16. Cohen, H. (1993). *A course in computational algebraic number theory*. Springer.
17. Cremona, J. E. (1997). *Algorithms for modular elliptic curves* (2nd ed.). Cambridge University Press.
18. Washington, L. C. (2008). *Elliptic curves: Number theory and cryptography* (2nd ed.). Chapman & Hall/CRC.
19. Descartes, R. (1954). *The geometry of René Descartes* (D. E. Smith & M. L. Latham, Trans.). Dover Publications. (Original work published 1637).
20. Neukirch, J. (1999). *Algebraic number theory*. Springer.
21. Cox, D., Little, J., & O’Shea, D. (2015). *Ideals, varieties, and algorithms: An introduction to computational algebraic geometry and commutative algebra* (4th ed.). Springer.
22. Bhatt, B., & Scholze, P. (2022). Prisms and prismatic cohomology. *Annals of Mathematics*, 196(3), 1135–1275.
23. Castryck, W., & Decru, T. (2022). An efficient key recovery attack on SIDH. *Cryptology ePrint Archive*.
24. Lurie, J. (2009). *Higher topos theory*. Princeton University Press.
25. Smith, A. (2017). 2∞ -Selmer groups, 2∞ -class groups, and Goldfeld’s conjecture. *arXiv preprint arXiv:1702.02325*.
26. Klüners, J. (2005). A counter example to Malle’s conjecture on the asymptotics of discriminants. *C. R. Math. Acad. Sci. Paris*, 340(6), 411–414.
27. Fargues, L., & Scholze, P. (2021). Geometrization of the local Langlands correspondence. *arXiv preprint arXiv:2102.13459*.
28. Tsfasman, M. A., Vlăduț, S. G., & Zink, T. (1982). Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound. *Mathematische Nachrichten*, 109, 21–28.
29. De Feo, L., Jao, D., & Plüt, J. (2014). Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *Journal of Mathematical Cryptology*, 8(3), 209–247.