International Journal of Computer Sciences and Engineering
Vol.**13**, Issue.**6**, pp.**23-31**, June **2025**
ISSN: 2347-2693 (Online)
Available online at: www.ijcseonline.org

ISSN: 2347-2693 (E)

Review Article

Foundations and Development of Isogeny-Based Cryptography: From Origins to the SIKE Collapse

Krishanu Naskar[1*], Abhishek Dey[2]

[1,2]Dept. of Computer Science, Bethune College, Kolkata, India

**Corresponding Author:* ✉

Received: 25/Apr/2025; **Accepted**: 26/May/2025; **Published**: 30/Jun/2025. **DOI**: https://doi.org/10.26438/ijcse/v13i6.2331

Abstract: Isogeny-based cryptography represents a compelling direction in post-quantum security, distinguished by its exceptionally small key sizes and solid theoretical foundation based on the computational difficulty of finding isogenies between supersingular elliptic curves. This paper traces the foundation and developmental trajectory of isogeny-based cryptography, from its early theoretical proposals to significant advancements leading up to 2022. Special attention is devoted to the period between 2020 and 2022, which witnessed substantial progress in isogeny-based signature schemes, key exchange protocols, and computational optimizations, alongside emerging cryptanalytic challenges. The discussion concludes with a concise summary of the 2022 attack on the Supersingular Isogeny Key Encapsulation (SIKE) scheme, avoiding in-depth technical details, and proceeds to compare isogeny-based cryptography with alternative post-quantum cryptographic approaches.This analysis affirms the ongoing relevance of isogeny-based techniques despite setbacks, while highlighting critical directions for future research.

Keywords: Isogeny-based cryptography, Post-quantum security, Elliptic curves, Isogeny-based signature, Cryptanalysis, SIKE

1. Introduction

The emergence of large-scale quantum computing presents a profound and imminent challenge to the foundations of traditional public-key cryptography. Cryptographic algorithms that currently secure digital communications—such as RSA, Diffie-Hellman, and Elliptic Curve Cryptography (ECC)—derive their security from mathematical problems considered intractable for classical computers, including integer factorization and discrete logarithms. However, the development of quantum algorithms, most notably Shor's algorithm, threatens to upend this security paradigm. Shor's algorithm can solve these problems exponentially faster than the best-known classical methods, enabling a sufficiently powerful quantum computer to efficiently factor large integers and compute discrete logarithms—tasks that would take classical machines an impractical amount of time. As a result, widely used cryptographic systems would be rendered insecure, exposing sensitive data and communications to potential compromise. This looming threat has catalyzed the search for quantum-resistant alternatives, collectively known as post-quantum cryptography, which aim to provide robust security even in the presence of quantum adversaries [1].

In response to the quantum threat, the cryptographic community has turned its focus toward designing post-quantum cryptographic (PQC) schemes capable of withstanding attacks from both classical and quantum adversaries. These emerging cryptosystems are built upon mathematical problems that remain hard even for quantum computers. Among the various PQC candidates, isogeny-based cryptography has attracted particular interest due to its uniquely small key and ciphertext sizes, a feature that distinguishes it from other leading approaches such as lattice-based or code-based cryptography. While many post-quantum schemes require significantly larger cryptographic parameters—posing challenges for storage, transmission, and computational efficiency—isogeny-based systems offer security levels comparable to existing pre-quantum algorithms with key sizes that remain compact. This efficiency makes isogeny-based cryptography especially well-suited for deployment in resource-constrained environments like embedded systems, mobile devices, and the Internet of Things (IoT), where bandwidth and memory are often limited [1].

This paper surveys the development of isogeny-based cryptography from its conceptual origins to its rapid expansion in the early 2020s, concluding with a critical

moment in 2022 when the widely publicized SIKE scheme was broken. The discussion also positions isogeny-based cryptography relative to other PQC families currently under consideration for standardization.

The remainder of this paper is organized as follows. Section 2 reviews the related work on isogeny-based cryptography. Section 3 discusses recent cryptanalytic advancements in the field. Section 4 presents a comparison between isogeny-based cryptography and other post-quantum cryptographic candidates. Section 5 provides a brief overview of the SIKE attack. Finally, Section 6 concludes the paper by summarizing the key insights and highlighting promising avenues for future research.

2. Related Work

The period between 2020 and 2022 marked a significant maturation phase for isogeny-based cryptography. While the early 2010s established foundational protocols such as SIDH and SIKE, this later period saw the emergence of diverse isogeny-based cryptographic primitives addressing critical areas like signature schemes, privacy-preserving protocols, computational optimizations, and hardware acceleration. This section provides a detailed overview of five major areas of innovation, emphasizing both the evolution of cryptographic schemes and the computational infrastructure enabling them.

2.1 SQIsign and Variants

A landmark achievement in the development of isogeny-based digital signatures came with the proposal of SQIsign by De Feo [1]. This scheme introduced a novel approach grounded in the arithmetic of supersingular elliptic curves, specifically exploiting the structure of their endomorphism rings. By incorporating advanced mathematical tools from quaternion algebra and navigating isogeny graphs, SQIsign achieved an unprecedented level of compactness in signature size. Its security is based on the computational difficulty of finding isogenies between supersingular elliptic curves with known endomorphism rings—a problem believed to be hard even in the presence of quantum computing capabilities [2].

What truly distinguishes SQIsign is its ability to deliver highly efficient signatures, with the original implementation producing signatures as small as 336 bytes. This is a significant improvement over many other post-quantum signature schemes, which often involve key and signature sizes in the kilobyte range. As a result, SQIsign presents a compelling option for cryptographic applications where efficiency and compactness are paramount, such as in low-power embedded systems, mobile devices, and secure microcontrollers. Its introduction represents a crucial step forward in making isogeny-based cryptography viable for real-world, resource-constrained environments [2].

In 2022, De Feo and colleagues. revisited SQIsign, introducing a revised version that optimized operational performance, especially in signature verification. The improvements involved refinements in isogeny pathfinding and endomorphism evaluation, significantly reducing the number of isogeny computations required during verification [3].

Further enhancing this line of work, Nakagawa and Onuki [4] introduced SQIsign2DPush, which addressed practical issues around parameter selection and pathfinding efficiency. By proposing a more adaptive and deterministic isogeny walk selection algorithm, SQIsign2DPush reduced signature generation time and improved robustness against implementation-based attacks, offering better performance in constrained environments without compromising security.
These successive advancements within the SQIsign family illustrate the field's ongoing effort to reconcile compactness, efficiency, and security in post-quantum signature design.

2.2 FQIsign and Edwards-Curve Signatures

Alongside the development of SQIsign, the landscape of isogeny-based digital signature schemes continued to evolve with a growing emphasis on improving computational performance while preserving the hallmark advantage of compact signatures. One of the most notable advancements in this direction was the introduction of FQIsign, a scheme designed to address the efficiency challenges that had previously limited the practicality of isogeny-based signatures [5].

FQIsign, and its variant FIBS (Fast Isogeny-Based Signature), builds upon the foundational principles established by SQIsign but incorporates several key innovations to accelerate the signing and verification processes. Specifically, the scheme utilizes an isogeny-based hash function and introduces a range of algorithmic improvements aimed at optimizing isogeny walks—the sequential computation of isogenies between elliptic curves—as well as enhancements in finite field arithmetic.

A central breakthrough in FQIsign is the significantly faster computation of long chains of isogenies, which has historically been a computational bottleneck in isogeny-based cryptographic protocols. By refining the arithmetic operations over finite fields and streamlining the traversal of isogeny graphs, the scheme achieves a substantial reduction in the time required for key cryptographic operations. These advancements were pioneered by Castryck, Decru, and Vercauteren in 2020 [2], who demonstrated that strategic mathematical optimizations could drastically improve the runtime performance of isogeny-based systems.

The performance gains introduced by FQIsign are particularly important given that signature generation and verification are the most computationally intensive tasks in isogeny-based schemes. By addressing these challenges directly, FQIsign enhances the feasibility of deploying isogeny-based digital signatures in real-world scenarios where latency and responsiveness are critical—such as in secure communication protocols, smart cards, and lightweight cryptographic applications. This evolution underscores the growing maturity of isogeny-based cryptography, as research continues to bridge the gap between theoretical security and practical efficiency.

Alongside these efforts, S. Kim, K. Yoon and colleagues [6] introduced a signature scheme based on twisted Edwards curves, a form of elliptic curves known for their efficient point addition and doubling operations. By adapting isogeny-based algorithms to this curve form, the authors achieved significant improvements in computational speed and implementation security. Edwards curves also offered advantages in side-channel resistance, which is essential in hardware and embedded deployments where power and timing analysis attacks are plausible.

These developments demonstrated that innovative curve models and optimized arithmetic frameworks could enhance the performance and security of isogeny-based digital signatures, thereby making them viable competitors against more mature post-quantum schemes.

2.3 Isogeny-Based Blind Signatures

A significant milestone in the advancement of isogeny-based post-quantum cryptography (PQC) was the development of isogeny-based blind signature schemes, which expanded the application scope of isogeny cryptography into the domain of privacy-preserving protocols. Blind signatures are a foundational primitive in cryptographic systems that require message anonymity—they enable a signer to sign a message without seeing its actual content, ensuring that the signature cannot be linked to the specific input by the signer. This functionality is crucial for privacy-sensitive applications such as electronic voting, anonymous credentials, and digital cash systems.

One of the first practical constructions of an isogeny-based blind signature scheme was proposed by Katsumata, Yi-Fu Lai, and collaborators [7], who introduced a provably secure partial blind signature protocol grounded in the hardness of supersingular isogeny problems. Their work demonstrated how to effectively combine the structure of isogeny-based key exchanges with cryptographic blinding techniques, enabling the generation of blind signatures while maintaining strong security guarantees under well-established isogeny assumptions.

The scheme not only preserved the compactness typical of isogeny-based cryptosystems but also achieved competitive performance in terms of both signing speed and signature size—key metrics for usability in constrained environments. Beyond efficiency, the authors placed a strong emphasis on implementation security, offering a detailed security analysis that addressed potential side-channel threats, fault-injection attacks, and ensured message unlinkability, thereby strengthening the protocol's robustness in real-world deployment scenarios.

This work highlighted the flexibility and expressive power of isogeny-based cryptography, demonstrating its capability to go beyond traditional applications like key encapsulation or static digital signatures. The successful construction of a privacy-preserving primitive such as blind signatures in the isogeny setting marked a critical step forward, suggesting that isogeny-based frameworks can serve as a viable foundation for building secure, privacy-respecting systems in a post-quantum world.

2.4 Isogeny-Based Zero-Knowledge Proof Systems

Zero-knowledge proof systems (ZKPs) are powerful cryptographic protocols that enable a prover to convince a verifier of the truth of a statement without revealing any additional information. The integration of zero-knowledge techniques with isogeny-based cryptography has gained substantial momentum in recent years, driven by the need for privacy-preserving, quantum-resistant cryptographic solutions.

This promising line of research was initiated by Luca De Feo, David Jao, and Jérôme Plût in their landmark 2011 work—commonly referred to as DJP11. In this seminal paper, the authors introduced a novel identification scheme based on the hardness of computing isogenies between supersingular elliptic curves, laying the groundwork for zero-knowledge proofs in the isogeny setting. While the protocol was inherently interactive, it captured the essence of zero-knowledge proofs of knowledge and demonstrated the feasibility of constructing efficient, sound, and compact proof systems grounded in isogeny problems. This construction proved especially relevant for applications such as anonymous identification, verifiable delay functions (VDFs), and privacy-preserving blockchain protocols, where proof size and verification efficiency are critical [8].

Building on this foundation, more recent efforts have explored how modern non-interactive zero-knowledge proof systems, such as zk-SNARKs, can be adapted to isogeny-based contexts. Notably, Cong K., Lai Y. F., and Levin S. demonstrated that isogeny-based relations could be encoded into efficient arithmetic circuits suitable for zk-SNARK frameworks [9]. By optimizing constraint systems and tailoring the underlying arithmetic to reflect the structure of isogeny computations, they significantly improved both proof generation time and verifier efficiency, bringing isogeny-based ZKPs closer to practical deployment.

These developments collectively underscore that isogeny-based cryptography is not only compatible with modern zero-knowledge proof systems, but also well-suited for constructing privacy-enhancing, post-quantum secure applications. The confluence of isogenies and ZKPs opens up promising new research directions in areas such as anonymous credentials, confidential smart contracts, post-quantum zero-knowledge rollups, and decentralized identity systems, pushing the boundaries of what is achievable in secure and private cryptographic design.

2.5 Hardware-Accelerated Implementations

Despite their advantage in offering compact key and signature sizes, isogeny-based cryptographic protocols have long been challenged by relatively slow computation speeds, primarily due to the mathematical complexity of isogeny evaluations. To bridge this performance gap and make isogeny-based cryptography more practical for real-world deployment,

researchers have increasingly turned to hardware acceleration as a viable solution.

In a notable contribution, Guantong Su and Guoqiang Bai (2023) developed a specialized hardware accelerator tailored specifically for supersingular isogeny-based operations [10]. Their design introduced high-performance modular arithmetic units and pipelined isogeny computation modules, resulting in significant improvements in throughput for key exchange and digital signature tasks. Beyond accelerating performance, their architecture also addressed timing-based side-channel vulnerabilities—a critical consideration for cryptographic implementations—by incorporating consistent execution paths and secure arithmetic logic.

Further progress was achieved in 2025 by El Baraka and Ezzouak, who took a novel direction by combining isogeny-based key exchange schemes with error-correcting codes [11]. This hybrid approach aimed to improve the robustness and reliability of isogeny-based communications in noisy or unstable environments, such as wireless networks and satellite communication systems. Their integration demonstrated that isogeny protocols could be effectively adapted to function within real-world communication infrastructures, offering both post-quantum security and enhanced resilience to transmission errors.

Collectively, these innovations highlight the critical role of hardware and systems-level optimizations in advancing the practicality of isogeny-based cryptography. As the demand for efficient and secure post-quantum solutions intensifies—particularly in constrained environments such as embedded devices, mobile platforms, and cloud-based applications—these hardware-oriented efforts are paving the way for broader adoption and deployment of isogeny-based techniques in next-generation cryptographic systems.

3. The Cryptanalytic Developments

While significant progress was made in developing efficient and compact isogeny-based cryptographic schemes between 2020 and 2022, the same period also witnessed intensified cryptanalytic scrutiny. The inherently complex algebraic structures involved in isogeny-based cryptography make it both promising and fragile, requiring careful evaluation against both mathematical and implementation-level attacks. This section reviews the major cryptanalytic advances during this critical period, categorized into classical mathematical attacks, side-channel and fault injection attacks, and investigations into the hardness of endomorphism ring computations.

3.1 Classical Mathematical Attacks

Prior to the pivotal 2022 cryptanalytic breakthrough against the SIKE protocol, the isogeny-based cryptography community had already faced a series of theoretical attacks that revealed subtle weaknesses in the underlying mathematical structures. These early cryptanalytic efforts focused particularly on the Supersingular Isogeny Diffie-Hellman (SIDH) protocol, a widely studied precursor to SIKE, and were instrumental in shaping the understanding of its security assumptions.

Among the earliest and most notable of these was the Galbraith-Hess-Smart (GHS) attack, introduced in the early 2010s [12]. This approach exploited specific configurations within the SIDH framework to reduce the complexity of computing certain isogenies from exponential to subexponential time in highly constrained scenarios [13]. While these attacks did not directly threaten the recommended security parameters in practice, they raised important concerns about structural vulnerabilities and underscored the need for cautious parameter selection and deeper security analysis.

Subsequent research intensified scrutiny on the role of auxiliary torsion points—public parameters in SIDH that are essential to the protocol's functionality but potentially hazardous from a security perspective. These torsion points introduced opportunities for information leakage and side-channel exploitation, particularly when an adversary could observe or manipulate protocol behavior. Though initially theoretical, this line of inquiry gradually exposed a critical flaw in SIDH's design: the asymmetry between public keys and the overconstrained structure imposed by torsion point data.

This growing body of work laid the foundation for the Castryck-Decru attack in 2022 [14], which decisively broke SIKE by demonstrating a polynomial-time algorithm for recovering secret isogenies under specific conditions. The attack exploited mathematical weaknesses inherent to SIDH's use of torsion point information, confirming that previously theoretical concerns could, under the right mathematical constructions, become practical vulnerabilities.

These pre-2022 attacks played a pivotal role in identifying and formalizing the cryptanalytic surface of isogeny-based protocols, particularly those reliant on asymmetric key structures. They also highlighted the importance of protocol design choices, prompting a reassessment of assumptions and leading to increased interest in alternative isogeny-based frameworks with more symmetric architectures and hardened parameter sets.

3.2 Side-Channel and Fault Injection Attacks

Beyond the realm of abstract mathematical attacks, isogeny-based cryptosystems, like all real-world cryptographic implementations, are vulnerable to physical side-channel attacks (SCAs) and fault injection techniques. These attacks exploit unintended information leakage from the physical execution of cryptographic algorithms—rather than weaknesses in the underlying mathematics—to compromise sensitive data such as secret keys or intermediate values.

Early side-channel analyses of isogeny-based schemes, particularly those targeting the SIKE protocol, focused on Differential Power Analysis (DPA). These attacks leverage correlations in power consumption traces during isogeny computations to recover information about secret scalars. For

instance, an attacker observing repeated scalar multiplications could infer certain bits of the private key based on subtle variations in power usage patterns [15]. In response, developers implemented countermeasures such as coordinate randomization, constant-time field arithmetic, and blinded isogeny walks, which significantly raised the difficulty of mounting naïve power analysis attacks.

However, more advanced side-channel strategies soon emerged. A particularly noteworthy development came in 2022, when De Feo et al. introduced zero-value side-channel attacks targeting SIKE implementations [16]. This class of attacks exploited the fact that elliptic curve point operations resulting in the identity element (the point at infinity) produce distinctive power consumption signatures. By carefully crafting input points and monitoring the resulting power traces, attackers could infer when these zero-value conditions occurred—revealing structural information about the secret scalar. Alarmingly, these attacks were effective even in the presence of coordinate randomization, challenging the efficacy of previously established countermeasures.

In parallel, researchers explored the potential of fault injection attacks, a form of active cryptanalysis wherein an adversary intentionally introduces faults into the computation—such as through voltage glitches, electromagnetic interference, or laser pulses. While more invasive and difficult to execute in practice, such attacks can force a cryptographic device to produce incorrect intermediate values, which may leak secret information or allow for algebraic fault analysis leading to partial key recovery. When applied to isogeny-based protocols, fault attacks have shown potential for bypassing certain protections by manipulating sensitive isogeny or point operations at critical stages.

Together, these physical-layer attacks underscore the reality that the security of isogeny-based cryptography cannot be evaluated in isolation from its implementation. As such protocols transition from theoretical models to deployment in embedded systems, smart cards, and networked environments, securing them against SCAs and fault-based threats becomes essential. These findings have prompted a shift toward implementation-aware cryptographic design, where hardware robustness, side-channel resistance, and fault tolerance are treated as first-class security considerations in the post-quantum era.

3.3 Attacks on Endomorphism Ring Computation

Another important area of cryptanalytic research between 2020 and 2022 targeted the computational hardness of endomorphism ring problems. Many isogeny-based schemes rely on the assumption that computing the endomorphism ring of a supersingular elliptic curve is infeasible. If this problem could be efficiently solved, it would severely weaken the foundational assumptions of several isogeny-PQC proposals, including variants of SIDH, CSIDH [17], and isogeny-based signatures [5].

Bernstein, Kizhakkumkara, Lange & Wester in 2020 conducted extensive theoretical analysis of the computational hardness of determining endomorphism rings, assessing both known algorithms and potential quantum improvements [18]. Their results reinforced the assumption's hardness for recommended parameter sizes but also highlighted areas where improvements could potentially reduce security margins.

Later works proposed secure constructions of supersingular curves with unknown endomorphism rings as a countermeasure against potential future attacks [19]. Ensuring that no efficient algorithms could compute these rings remained a priority, as any progress in this domain could have cascading effects on isogeny-based protocol security.

3.4 Prelude to the SIKE Collapse

By 2021, researchers were increasingly concerned about the potential for exploiting auxiliary torsion points in SIDH and SIKE public keys. These points, while necessary for ensuring protocol correctness and security against active adversaries, introduced subtle leakages.

The final blow came in July 2022 when Castryck and Decru in 2022 [14] demonstrated a practical, polynomial-time classical attack on SIKE. Exploiting the structure of torsion point images in public keys, the attack recovered the secret isogeny by reconstructing the corresponding kernel generator. The method required no quantum hardware and broke SIKE's recommended parameter sets in hours to days on a single-core classical computer.

While the technical intricacies of this attack fall outside the scope of this section, its significance cannot be overstated. The success of this attack exposed a fundamental structural flaw in SIDH and SIKE, unrelated to parameter selection or implementation errors. As a result, SIKE was formally withdrawn from the NIST PQC standardization process later that year [20], marking a pivotal turning point in the field.

4. Isogeny Based Cryptography Vs Other Post-Quantum Cryptography Candidates

In the global effort to design cryptographic systems that remain secure against both classical and quantum adversaries, five major mathematical frameworks have emerged as frontrunners for post-quantum cryptographic (PQC) standardization: lattice-based, code-based, hash-based, multivariate, and isogeny-based cryptography. Each paradigm offers unique strengths and faces distinct trade-offs across dimensions such as computational efficiency, key and signature sizes, underlying security assumptions, and practical deployability.

This section provides a comparative analysis of isogeny-based cryptography relative to its four leading counterparts, with a focus on performance, resource demands, and quantum resistance.

4.1 Lattice-Based Cryptography

Lattice-based cryptography is currently the most mature and well-studied PQC paradigm. Its security relies on hard mathematical problems such as Learning With Errors (LWE), Short Integer Solution (SIS), and Ring-LWE, which are conjectured to be resistant to attacks from both classical and quantum algorithms. A key theoretical advantage is the existence of worst-case to average-case reductions, offering strong evidence for the robustness of these assumptions [21].

Prominent schemes like Kyber (for key encapsulation) and Dilithium (for digital signatures), both selected in NIST's PQC standardization process, exhibit high computational efficiency, parallelizability, and support for high-throughput environments. These properties make them ideal for cloud systems, web protocols, and general-purpose cryptographic libraries.

However, a common drawback is their large public key and signature sizes, typically ranging from 1 to 3 kilobytes, which poses challenges for bandwidth-constrained or memory-limited devices, such as embedded systems or IoT nodes.

By contrast, isogeny-based cryptography offers significantly smaller key and ciphertext sizes—often as small as a few hundred bytes. This compactness makes it more suitable for use cases where data size and transmission efficiency are critical. Nevertheless, isogeny-based schemes typically suffer from slower signing and verification speeds, particularly in software-only implementations, due to the high cost of isogeny computations.

Post-quantum security: both paradigms are built on problems believed to resist quantum attacks. However, lattice problems have been extensively analyzed over decades and benefit from a broader community consensus on their hardness. In contrast, isogeny-based cryptography is based on narrower and more specialized assumptions, and while promising, it has a relatively shorter history of cryptanalytic scrutiny.

4.2 Code-Based Cryptography

Code-based cryptography derives its security from the difficulty of decoding linear error-correcting codes—a problem that has resisted both classical and quantum cryptanalysis for over four decades. The syndrome decoding problem underpins classic schemes such as McEliece, and more modern proposals like BIKE and HQC.

A key strength of code-based schemes is their remarkable cryptanalytic resilience. The McEliece cryptosystem, for instance, has withstood rigorous public scrutiny since the 1970s, offering strong post-quantum assurances based on time-tested assumptions.

However, this security comes at a cost: very large public key sizes. Typical implementations require key sizes of 50–100 kilobytes or more to achieve 128-bit post-quantum security. While structural variants attempt to reduce this overhead, they often introduce additional assumptions or potential vulnerabilities.

In contrast, isogeny-based schemes maintain the advantage of ultra-compact keys and ciphertexts, drawing comparisons to Elliptic Curve Cryptography (ECC) in the pre-quantum era. This makes isogeny protocols attractive for space-constrained environments and systems requiring lightweight cryptographic primitives.

On the downside, code-based cryptosystems often outperform isogeny-based ones in terms of raw computational speed, especially for encryption and decryption of large messages. Additionally, they benefit from simpler arithmetic operations, avoiding the complexity of navigating isogeny graphs or handling elliptic curve arithmetic.

Post-quantum security: Code-based cryptography remains one of the most conservatively trusted paradigms, with a proven track record of resistance to quantum and classical attacks. In contrast, isogeny-based schemes are newer and less mature, and their security assumptions have not yet been tested over decades, although they are backed by mathematically well-defined hard problems.

4.3 Hash-Based Signatures

Hash-based cryptography relies exclusively on the security of cryptographic hash functions, particularly their pre-image resistance, second pre-image resistance, and collision resistance. This design philosophy makes it one of the most conservative and well-understood approaches in the post-quantum landscape. The flagship scheme in this category, SPHINCS+, was selected for standardization by NIST and serves as a stateless, quantum-resistant digital signature scheme.

One of the key strengths of hash-based schemes is their minimal reliance on complex or untested mathematical assumptions. Since their security depends solely on the hardness of inverting secure hash functions—such as SHA-2 or SHA-3—they are broadly considered among the most trustworthy and implementation-friendly post-quantum primitives. Additionally, the use of standard hash function evaluations provides a natural resistance to side-channel attacks, particularly timing and fault injection, due to their deterministic and uniform operation profiles.

However, this conservative approach comes with trade-offs. Hash-based signatures tend to have large signature sizes, often in the range of 8–20 kilobytes, depending on the desired security level and scheme configuration. This makes them less suited for bandwidth-limited applications or environments where message size is a limiting factor. Signing speed is also generally slower than that of lattice- or code-based systems, especially when implemented in constrained devices, due to the large number of hash evaluations required. In comparison, isogeny-based signature schemes such as SQIsign offer significantly more compact public keys and signatures, often well under 1 kilobyte, making them more practical for resource-constrained platforms such as IoT nodes, smart cards, and embedded devices. However, isogeny schemes tend to have more complex and computation-heavy

implementations, which may pose challenges in highly constrained hardware environments.

Post-quantum security: Hash-based cryptography is often regarded as the most conservative option among post-quantum candidates. As long as the underlying hash functions remain secure, the scheme itself inherits their robustness. This makes hash-based signatures a compelling choice for long-term digital signatures and applications where simplicity, transparency, and auditability are valued over performance.

4.4 Multivariate Cryptography

Multivariate cryptography is founded on the computational hardness of solving systems of multivariate quadratic equations over finite fields—a problem known to be NP-hard. This algebraic structure offers a fertile ground for constructing digital signature schemes, and has led to proposals such as Rainbow, GeMSS, and MQDSS, which were contenders in the NIST post-quantum cryptography standardization process.

A key advantage of multivariate schemes is their efficiency in signature generation and verification. These operations are typically fast and require relatively low computational overhead, making multivariate systems attractive for real-time applications and constrained devices. Their public key sizes generally fall in the range of several kilobytes to tens of kilobytes, and signature sizes are often smaller than those produced by hash-based schemes.

However, the security landscape of multivariate cryptography remains less mature and more volatile than that of other PQC families. Although the underlying mathematical problem is well-known, its cryptographic instantiations have proven sensitive to structural weaknesses. Notably, several multivariate schemes have been broken or significantly weakened by recent algebraic cryptanalysis. The Rainbow signature scheme, once considered a strong candidate for standardization, was invalidated by a practical key-recovery attack that exploited the predictable structure of its central map. Similar vulnerabilities have emerged in other proposals, underscoring the challenges of designing secure parameter sets in this domain.

In contrast, isogeny-based cryptography avoids these algebraic pitfalls by basing security on an entirely different mathematical foundation: the difficulty of finding isogenies between supersingular elliptic curves. This geometric and number-theoretic approach introduces unique hardness assumptions that do not overlap with those of lattice-, code-, or multivariate-based schemes. While isogeny-based systems typically involve higher computational costs, especially in signature generation and key exchange, they offer the benefit of ultra-compact key and signature sizes, and are not known to suffer from the algebraic vulnerabilities that have compromised several multivariate designs.

Post-quantum security: Multivariate cryptographic schemes remain an active area of research, but their security is still regarded as relatively speculative, given their shorter history of public scrutiny and recent cryptanalytic setbacks. By contrast, although isogeny-based cryptography is also a younger field, it has shown greater resilience to structural attacks thus far and benefits from an orthogonal security foundation that contributes to the diversity and robustness of the overall post-quantum ecosystem.

4.5 Strengths and Limitations of Isogeny-Based Cryptography

Isogeny-based cryptography presents a unique and valuable contribution to the post-quantum cryptographic ecosystem, particularly in scenarios where resource constraints and compactness are critical. One of its most compelling advantages is the exceptionally small size of public keys, ciphertexts, and signatures—often just a few hundred bytes—making it highly suitable for bandwidth-limited environments, embedded systems, smart cards, and IoT devices, where minimizing data transfer and memory usage is essential.

Moreover, isogeny-based schemes are built on a mathematically distinct security assumption: the hardness of computing isogenies between supersingular elliptic curves. This problem lies in a different complexity class from those used in lattice-, code-, or hash-based cryptography, thereby enhancing the algorithmic diversity of post-quantum security options. Such diversity is particularly valuable in a post-quantum world, where the risk of breakthrough quantum algorithms could affect some—but not necessarily all—cryptographic assumptions.

Beyond foundational cryptographic functions, the isogeny framework also supports the construction of advanced primitives such as zero-knowledge proofs, blind signatures, and anonymous identification schemes. These capabilities expand its relevance to privacy-preserving applications, including digital identity, secure voting, and decentralized finance (DeFi), where both confidentiality and post-quantum security are paramount.

However, these benefits are tempered by several important limitations that currently hinder broader adoption. Chief among them is computational performance: isogeny-based protocols tend to be significantly slower than their lattice- or code-based counterparts, particularly in signature generation and key exchange operations. This performance gap becomes more pronounced in software-only implementations, where complex elliptic curve arithmetic and isogeny path computations dominate runtime.

Another concern is the relative immaturity of the field. While the underlying mathematical problems are well-defined, isogeny-based cryptography has a shorter history of cryptanalytic analysis compared to more established paradigms like lattice or code-based schemes. This uncertainty was exemplified by the 2022 cryptanalytic attack on SIKE—a NIST candidate based on the SIDH protocol—which revealed exploitable structural weaknesses and rendered the scheme insecure. The attack underscored the

importance of careful protocol design, robust parameter selection, and continued scrutiny as the field evolves.

In summary, isogeny-based cryptography offers a compact, privacy-friendly, and mathematically diverse option for post-quantum security. While it shows considerable promise—especially in constrained and specialized applications—its current limitations in efficiency and maturity of analysis highlight the need for further research, optimization, and cryptographic engineering to reach its full potential.

5. The SIKE Attack: A Brief Mention

In July 2022, a pivotal moment in the field of post-quantum cryptography occurred when Wouter Castryck and Thomas Decru unveiled a polynomial-time classical attack on the Supersingular Isogeny Key Encapsulation (SIKE) protocol [4]. Their attack exploited auxiliary torsion point information embedded in public keys, a fundamental component of the underlying SIDH construction. By leveraging this structural feature, the authors demonstrated a method to efficiently recover the secret isogeny on a classical computer, undermining the core security assumption of the scheme.

Although the intricate technical mechanics of the attack lie beyond the scope of this paper, its impact was both immediate and far-reaching. The SIKE proposal, once a promising finalist in the NIST Post-Quantum Cryptography Standardization process, was formally withdrawn [22]. This event triggered a broad reassessment of isogeny-based cryptographic constructions, especially those relying on torsion point-based public key architectures, which were shown to be inherently fragile under specific conditions.

Importantly, not all isogeny-based protocols were equally affected. Schemes that do not depend on SIDH-style torsion point disclosures, such as those using hard homogeneous spaces or leveraging different instantiations of the isogeny problem, remain intact and are still considered viable. The 2022 break thus served less as a categorical dismissal of isogeny-based cryptography and more as a cautionary signal—highlighting the importance of careful protocol design, rigorous cryptanalytic vetting, and continued diversification of mathematical assumptions in the post-quantum cryptographic landscape.

6. Conclusion and Future Scope

The period between 2020 and 2022 showcased both significant advancements and a stark re-evaluation for isogeny-based cryptography. Initially praised for its compact key sizes and strong security, this field saw a boom in research across various cryptographic applications, including signature schemes like SQIsign and FQIsign, and even hardware implementations. Its adaptability was evident in accommodating real-world challenges, making it viable for bandwidth- and memory-constrained environments such as embedded systems and IoT. However, this optimism was significantly impacted by the Castryck-Decru attack in July 2022. This attack classically undermined the security of SIDH and SIKE, a leading NIST post-quantum cryptography candidate, by exploiting weaknesses related to disclosed auxiliary torsion point information. Consequently, SIKE was withdrawn from the NIST process, prompting a critical re-evaluation of security assumptions in isogeny-based designs [23].

Despite the setback with SIKE, isogeny-based cryptography remains a valuable and innovative area within the broader post-quantum cryptography landscape. Its unique combination of compact key sizes and advanced algebraic structures makes it ideal for applications where communication bandwidth and storage efficiency are crucial. Future research is focused on developing new Castryck-Decru-resistant schemes, exploring genus-2 isogenies and higher-genus structures, and integrating these techniques into privacy-preserving frameworks [22]. Additionally, optimizing hardware implementations for robustness and considering hybrid schemes that combine isogeny-based and lattice-based primitives are key directions [24]. In summary, while recent challenges have tested its resilience, isogeny-based cryptography remains a lightweight and adaptable contender in the evolving landscape of post-quantum security.

Funding Source
No funding was received for this study.

Authors' Contributions
The first author, Krishanu Naskar, was primarily responsible for the comprehensive literature review, including the collection and critical analysis of relevant research papers, and for drafting the initial manuscript and subsequent revised drafts. This foundational work established the thematic scope and initial content framework of the submission.

The second author, Abhishek Dey, provided invaluable critical oversight and substantive revisions to the preliminary draft, contributing significantly to the refinement of its intellectual content and argument structure. Additionally, Abhishek Dey was instrumental in formalizing the manuscript to adhere to academic standards and ensuring its proper formatting for submission.

Conflict of Interest
The authors declare that there is no conflict of interest regarding the publication of this research paper.

Data Availability
No datasets were generated or analyzed during the current study.

References

[1] L. De Feo, D. Kohel, A. Leroux, C. Petit, and B. Wesolowski, "SQIsign: Compact post-quantum signatures from quaternions and isogenies," IACR Cryptology ePrint Archive, 438, **2020**.
[2] W. Castryck, T. Decru, and F. Vercauteren, "Radical Isogenies," IACR Cryptology ePrint Archive, 1108, **2020**.
[3] L. De Feo, A. Leroux, P. Longa, and B. Wesolowski, "New algorithms for the Deuring correspondence: Towards practical and secure SQISign signatures," IACR Cryptology ePrint

Archive, 234, **2022**.
[4] K. Nakagawa and H. Onuki, "SQIsign2DPush: Faster Signature Scheme Using 2-Dimensional Isogenies," IACR Cryptology ePrint Archive, 897, **2025**.
[5] S. Kim, Y. Lee, and K. Yoon, "Performance Evaluation of Isogeny-Based Digital Signature Algorithms: Introducing FIBS -- Fast Isogeny Based Digital Signature," The Journal of Supercomputing, **2025**.
[6] J. Kim, C. Yoon, H. Jo, and J. H. Cheon, "New Hybrid Method for Isogeny-Based Cryptosystems Using Edwards Curves," IACR Cryptology ePrint Archive, 1215, **2018**.
[7] S. Katsumata, Y. F. Lai, J. T. LeGrow, and L. Qin, "CSI-Otter: Isogeny-Based (Partially) Blind Signatures from the Class Group Action with a Twist," IACR Cryptology ePrint Archive, 1239, **2023**.
[8] D. Beullens, L. De Feo, S. D. Galbraith, and C. Petit, "Proving knowledge of isogenies – A survey," IACR Cryptology ePrint Archive, 671, **2023**.
[9] K. Cong, Y. F. Lai, and S. Levin, "Efficient isogeny proofs using generic techniques," IACR Cryptology ePrint Archive, 037, 2023.
[10] G. Su and G. Bai, "Towards High-Performance Supersingular Isogeny Hardware Accelerator Design," Electronics, Vol.**12**, No.**5**, pp.**1235**, **2023**.
[11] M. El Baraka and S. Ezzouak, "Proposal of a New Isogeny-Based Cryptographic Protocol: Formal Analysis and Comparison," Mathematics Interdisciplinary Research, Vol.**10**, No.**1**, pp.**111-132, 2025.**
[12] D. Jao and L. De Feo, "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies," IACR Cryptology ePrint Archive, 506, **2011**.
[13] S. D. Galbraith, S. Barak, B. T. Yan, and C. Petit, "On the security of supersingular isogeny cryptosystems," IACR Cryptology ePrint Archive, 859, **2016**.
[14] W. Castryck and T. Decru, "An efficient key recovery attack on SIDH," IACR Cryptology ePrint Archive, 975, **2022**.
[15] A. Denis, "Side-channel attacks on SIKE," Master's thesis, EPFL, **2023**.
[16] L. De Feo et al., "SIKE channels: Zero-value side-channel attacks on SIKE," IACR Cryptology ePrint Archive, 54, **2022**.
[17] F. Campos, M. Meyer, and S. Reith, "On Lions and Elligators: An Efficient Constant Time Implementation of CSIDH," IACR Cryptology ePrint Archive, 1198, **2018**.
[18] D. J. Bernstein, A. Kizhakkumkara, T. Lange, and B. Wester, "On the hardness of computing endomorphism rings," IACR Cryptology ePrint Archive, 986, **2017**.
[19] Y. Mokrani and D. Jao, "Generating supersingular elliptic curves over FP with unknown endomorphism ring," IACR Cryptology ePrint Archive, 984, **2023**.
[20] NIST, "Status report on the fourth round of the PQC standardization process," NIST IR 8545, **2025**.
[21] S. Du, X. Li, M. Lin, and R. Tang, "A Review of Chosen Isogeny-Based Cryptographic Schemes," Sensors, Vol.**22**, No.**18**, pp.**7057**, **2022**.
[22] E. V. Flynn and Y. B. Ti, "Genus 2 isogeny cryptography," IACR Cryptology ePrint Archive, 177, **2019**.
[23] P. Dartois et al., "SQIsignHD: New dimensions in cryptography," IACR Cryptology ePrint Archive, 436, **2023**.
[24] C. Costello and B. Wester, "Fast and fault-tolerant isogeny-based key exchange," IACR Cryptology ePrint Archive, 1271, **2020**.

AUTHORS PROFILE

Krishanu Naskar completed his Masters in Computer Application from IISER, Shibpur Kolkata (Erstwhile Bengal Engineering College, B.E. College) in 2003 after graduating from Calcutta University in the year 200 with Physics Honours. He also qualified in NET 2012 (December) and NET 2018 (June) and joined Bethune College under Calcutta University as Assistant Professor of Computer Science in 2019. His research interests include Computational Mathematics specially Graph Theory, Algorithm Development, Information Theory, Cryptography and Quantum Information Processing.

Abhishek Dey received his B.Sc. in Computer Science (Honours) from Scottish Church College, University of Calcutta, Kolkata, India, in 2011. He obtained his M.Sc. in Computer and Information Science from the University of Calcutta in 2013, followed by an M.Tech. in Computer Science and Engineering from the same institution in 2015. He is currently serving as an Assistant Professor in the Department of Computer Science at Bethune College, Kolkata, India. His research interests include Image Processing, Machine Learning, Artificial Intelligence, and Computer Vision.

