International Journal of Computer Sciences and Engineering
Vol.**13**, Issue.**8**, pp.**68-75**, August **2025**
ISSN: 2347-2693 (Online)
Available online at: www.ijcseonline.org

ISSN: 2347-2693 (E)

Review Article

An Academic Review of the SIKE Attack in Post-Quantum Cryptography Failure

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

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

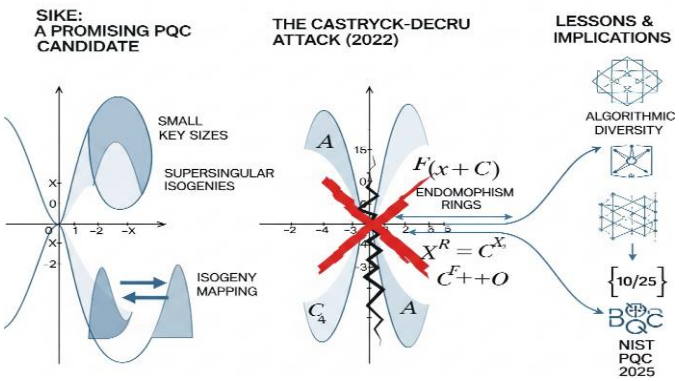
**Corresponding Author:* ✉

Received: 22/Jun/2025; **Accepted**: 24/Jul/2025; **Published**: 31/Aug/2025. **DOI**: https://doi.org/10.26438/ijcse/v13i8.6875

Abstract: Supersingular Isogeny Key Encapsulation (SIKE) was a promising candidate in the National Institute of Standards and Technology (NIST) Post-Quantum Cryptography (PQC) standardization process, as it is distinguished by its exceptionally small key sizes, which makes it attractive for resource-constrained environments, and an elegant mathematical foundation rooted in supersingular elliptic curve isogenies. Its security based on the presumed hardness of computing isogenies between such curves. However, in August 2022, a groundbreaking attack by Castryck and Decru completely compromised SIKE, demonstrating its insecurity with practical polynomial-time complexity. This pivotal event led to SIKE's immediate withdrawal from NIST's standardization efforts, reshaping the evolving landscape of post-quantum cryptography and underscoring essential lessons in cryptographic design, evaluation, and diversity. A comprehensive academic analysis of the SIKE cryptographic scheme methodology and details of the specific nature of the Castryck-Decru attack that rendered it insecure is provided by this paper. It also discusses in brief the far-reaching implications for cryptographic design, standardization processes, and the pursuit of quantum-resistant algorithms, giving particular emphasis on the current state of post-quantum cryptography or PQC standardization as of 2025.

Keywords: Post-Quantum Cryptography, SIKE, Supersingular Isogeny Diffie-Hellman (SIDH), Cryptanalysis, Castryck-Decru Attack, NIST, Elliptic Curves, Isogenies, Endomorphism Rings

Graphical Abstract- (Diagram generated using Google's Gemini AI, based on the textual abstract given as prompt)



1. Introduction

The emergence of large-scale quantum computing presents a profound and imminent challenge to the foundations of traditional public-key cryptography, which primarily rely on the presumed hardness of integer factorization (IFP) and discrete logarithm problems (DLP). These problems are efficiently solvable by Shor's algorithm on a sufficiently large quantum computer. In anticipation of this threat, the National Institute of Standards and Technology (NIST) initiated a comprehensive Post-Quantum Cryptography (PQC) standardization process in 2016 to identify and standardize cryptographic algorithms resilient to such quantum computing attacks [1].

Among the diverse family of candidates in quantum resistant cryptography, Supersingular Isogeny Key Encapsulation (SIKE) emerged as a leading contender, reaching Round 3 of the NIST PQC selection [2]. Based on the Supersingular Isogeny Diffie-Hellman (SIDH) key exchange protocol proposed by Jao and De Feo in 2011 [3], SIKE offered a compelling alternative to lattice-based cryptography, particularly due to its uniquely small public key and ciphertext sizes. With public key sizes of only 330 bytes for SIKE p434 and 564 bytes for SIKE p751, compared to several kilobytes for lattice-based schemes, this characteristic made SIKE an appealing choice for resource-constrained environments and applications where bandwidth efficiency was critical [4,5]. This compact representation stood in stark contrast to many lattice-based proposals, which typically

require significantly larger size keys and arithmetic operations that are more complex. The scheme's security was predicated on the computational difficulty of finding an isogeny between two supersingular elliptic curves when only their starting and ending curves, alongside images of certain torsion points, were known [6]. The details of the development of SIKE has been thoroughly described in a previous article on this topic [7].

However, the trajectory of SIKE within the NIST process was dramatically altered on August 1, 2022, when Wouter Castryck and Thomas Decru published a groundbreaking cryptanalytic attack [8]. Their work demonstrated a practical, polynomial-time method to recover the secret isogeny, thereby rendering SIKE insecure. This attack, with quasi-polynomial complexity $O(\log^2 p)$, effectively shattered SIKE's security assumptions across all proposed parameter sets, including the highest security level SIKE p751, which could be broken in approximately one hour on a single CPU core [8,9]. This led to SIKE's immediate removal from NIST's consideration in August 2022 [10].

1.1 Objective of the study

A comprehensive academic review and analysis of the SIKE cryptographic scheme, detailing the specific nature of the Castryck-Decru attack that compromised its security is provided by this paper, alongside exploring the profound implications of the attack on the field of post-quantum cryptography. As the timing of this attack was particularly significant as it occurred just one month after NIST announced its selection of the first four post-quantum cryptographic algorithms for standardization in July 2022, though SIKE was not among them. This demonstrated the continued importance of active cryptanalysis even for algorithms that had progressed through multiple rounds of evaluation.

1.2 Organization

Section 1 gives out a general introduction. After that Section 2 provides essential background on elliptic curves, isogenies, and the SIDH protocol, including a glossary of key terms. Section 3 thoroughly discusses the Castryck-Decru attack, highlighting its core vulnerability and methodology with concrete complexity analysis. Section 4 discusses the immediate impact of the attack and its broader implications for the PQC landscape, including the current state of NIST standardization as of 2025. Section 5 explores the implications specifically for other isogeny-based cryptographic schemes. Section 6 distills critical lessons learned from SIKE's failure, offering insights for future cryptographic design and standardization efforts. Section 7 discusses future research directions and open problems.

2. Background of SIKE and Supersingular Isogeny Cryptography

SIKE's security foundation was derived from the Supersingular Isogeny Diffie-Hellman (SIDH) key exchange protocol. SIDH leverages the intricate mathematical properties of supersingular elliptic curves and isogenies between them to construct a hard computational problem [6].

2.1 Key Terms and Definitions

To aid understanding, we provide key definitions:

- **Elliptic Curve**: A smooth algebraic curve defined by a cubic equation, forming an abelian group under point addition
- **Isogeny**: A rational map between elliptic curves that preserves the group structure
- **Supersingular Curve**: An elliptic curve with a particularly rich endomorphism ring structure
- **Endomorphism Ring**: The set of all isogenies from a curve to itself, forming a ring under composition and addition
- **Torsion Points**: Points of finite order on the elliptic curve group
- **Kernel**: The set of points mapped to the identity by an isogeny

2.2 Elliptic Curves and Isogenies

An elliptic curve E over a finite field F_p is a set of points (x,y) satisfying a Weierstrass equation of the form $y^2 = x^3 + Ax + B$, along with a special point at infinity, denoted O. These points produces an abelian group under a well-defined addition operation. The use of finite fields is pivotal as it allows for discrete, finite mathematical structures essential for cryptographic operations.

An isogeny $\varphi: E_1 \rightarrow E_2$ between two elliptic curves E_1 and E_2 is a non-constant rational map that is also a group homomorphism. Figure 1 provides a visual representation of an elliptic curve and an isogeny mapping between two similar curves. This means it maps the identity element of E_1 to the identity element of E_2 and the group structure is preserved. The degree of an isogeny means its degree as a rational function that is equal to the size of its kernel (the subgroup of points in E_1 counterplotted to O_E_2). One of the pivotal properties is that if G is a finite subgroup of E_1, there exists a unique isogeny $\varphi: E_1 \rightarrow E_1/G$ (up to isomorphism) whose kernel is exactly G. Vélu's formulas give an unequivocal system for constructing such an isogeny if the points in its kernel are given [11].

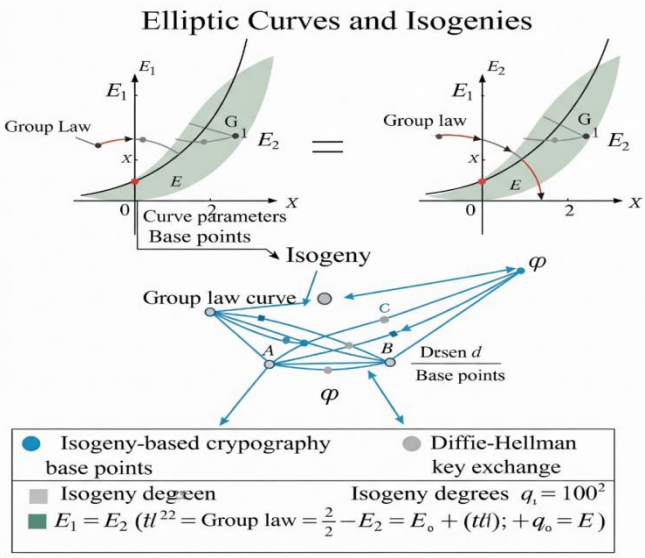


Figure 1: Illustration of Elliptic Curves and Isogenies in Cryptography

Fig. 1 depicts two elliptic curves, E1 and E2, illustrating the group law operation for point addition on an elliptic curve, and an isogeny (ϕ) as a structure-preserving map between E1 and E2.
(Diagram generated using Google's Gemini AI, based on a text prompt describing elliptic curves and isogenies for cryptography.)

2.3 Supersingular Elliptic Curves
Elliptic curves are classified into two types: ordinary and supersingular. Supersingular elliptic curves are characterized by having a particularly rich endomorphism ring, End(E), which is the ring of isogenies from a curve to itself. For a supersingular curve E over F_{p^2} (specifically when $p \equiv 3 \pmod 4$), its endomorphism ring is of rank 4 and non-commutative, isomorphic to a maximal order in a definite quaternion algebra $B_{p,\infty}$ over Q.

This complex algebraic structure of the endomorphism ring is central to isogeny-based cryptography, as it allows for the construction of a hard problem related to navigating the isogeny graph. The richness of the endomorphism ring means that supersingular curves

have many more self-isogenies compared to ordinary curves, creating a highly connected graph structure that was thought to provide security through the difficulty of finding specific paths.

2.4 The SIDH Problem
The security of SIDH, and as a consequence SIKE, is predicated on the computational difficulty of finding a secret isogeny. The core SIDH problem can be described as follows [3]:
Let E_0 be a publicly known supersingular elliptic curve over F_{p^2}. Alice and Bob each choose distinct secret subgroups, G_A and G_B, of E_0's N_A-torsion and N_B-torsion points, respectively (where N_A and N_B are large, coprime integers, typically powers of some small primes).

Alice's Computation: Alice computes her secret isogeny $\varphi_A: E_0 \rightarrow E_A = E_0/G_A$. She then computes the images of Bob's public basis points under her secret isogeny. Her public key consists of E_A and the images of certain N_B-torsion basis points on E_0 under φ_A.

Bob's Computation: Similarly, Bob computes his secret isogeny $\varphi_B: E_0 \rightarrow E_B = E_0/G_B$. He computes the images of Alice's public basis points under his secret isogeny. His public key consists of E_B and the images of certain N_A-torsion basis points on E_0 under φ_B.

Shared Secret Derivation: Alice computes the curve $E_{AB} = E_A/\varphi_A(G_B)$, and Bob computes $E_{BA} = E_B/\varphi_B(G_A)$. Due to the commutativity of isogenies (up to isomorphism) when kernels are disjoint, the property $E_{AB} \cong E_{BA}$ holds. This property allows both parties to arrive at the same shared supersingular elliptic curve (or a derived invariant), which serves as the shared secret.

The computational challenge for an eavesdropper is to derive this shared secret curve without knowledge of Alice's or Bob's secret subgroups. Prior to the Castryck-Decru attack, the best known attacks had exponential complexity (typically O(p^(1/4))), which was supposed to be intractable for cryptographically applicable parameters.

2.5 SIKE as a Key Encapsulation Mechanism
SIKE adapted the SIDH key exchange protocol into a Key Encapsulation Mechanism (KEM) to fit the public-key cryptography paradigm for symmetric key establishment [4]. A KEM typically comprises three algorithms:

- **Key Generation (KeyGen):** A public key and a secret key are generated by a party. In SIKE, Alice (the recipient) generates her secret isogeny from E_0 (defined by her secret subgroup G_A) and publishes the resulting curve E_A and images of specific torsion basis points. Her secret key is effectively her choice of G_A.
- **Encapsulation (Encaps):** A sender (Bob) encapsulates a shared secret by using the recipient's public key. Bob computes his own secret isogeny and then uses Alice's public information to derive the shared secret curve E_{AB}. A symmetric key K is derived from E_{AB} via a key derivation function (KDF), while a ciphertext (CT) is also generated.
- **Decapsulation (Decaps):** The recipient uses her secret key to decapsulate the ciphertext and recover the shared secret. Alice uses her secret isogeny and Bob's public information to compute the same shared secret curve E_{AB}, and then derives K.

SIKE leveraged a variant of the Fujisaki-Okamoto transform to achieve chosen-ciphertext attack (CCA) security from its underlying SIDH primitive [4].

3. The Castryck-Decru Attack on SIKE

The security of SIKE was challenged and ultimately broken by the attack published by Wouter Castryck and Thomas Decru on August 1, 2022 [8]. This phenomenal cryptanalytic breakthrough exploited a subtle yet critical vulnerability related to the structure of the endomorphism ring of supersingular elliptic curves and the information leakage through publicly exchanged torsion points.

3.1 The Core Vulnerability: Exploiting Torsion Point Information and the Endomorphism Ring
SIKE's security relied on the assumption that the images of specific public basis points (which actually help define the secret isogenies) revealed insufficient information to reconstruct the secret scalar multipliers used to generate these isogenies. The Castryck-Decru attack, however, demonstrated that these publicly available images, when combined with specific properties of supersingular elliptic curves and their endomorphism rings, leaked just enough information to efficiently recover the secret [8].

The attack highlighted the fact that for any given supersingular elliptic curve E over F_{p^2} (where $p \equiv 3 \pmod$

4)), its endomorphism ring End(E) is known to be isomorphic to a maximal order in the definite quaternion algebra B_p,∞. While the specific maximal order (and thus the endomorphism ring) is not secret and can be computed, it was traditionally believed that leveraging this knowledge to find the secret isogeny was computationally intractable.

The critical insight was that the vulnerability arose from how the public key elements — specifically, the images of certain torsion basis points under the secret isogeny — provided a "handle" into the endomorphism ring structure of an auxiliary curve derived from the public key. This enabled secret recovery by allowing the attacker to construct and exploit a specific endomorphism that revealed information about the secret kernel [8].

3.2 Attack Methodology: Leveraging the Endomorphism Ring and Vélu's Formulas

The Castryck-Decru attack is sophisticated and can be summarized in the following steps [8]:

Step 1: Constructing an Auxiliary Curve with Known Endomorphism Ring

The attacker, given Alice's public key (the curve E_A and the images of N_B-torsion points from Section 2.4), identifies a specific torsion point S on E_A. This point S is chosen such that the curve E_A' = E_A/⟨S⟩ has a known, efficiently computable endomorphism ring. The key insight is selecting S so that E_A' is isomorphic to a curve of the form E_0/⟨G_A, H⟩ where H is related to the public torsion point images, creating a curve with predictable endomorphism ring properties.

The selection of S follows from analyzing the 2-dimensional isogeny structure and identifying points that preserve certain mathematical relationships in the quotient curve. Specifically, S is chosen from the kernel of a carefully constructed 2-isogeny that maintains the desired endomorphism ring structure in the quotient.

Step 2: Exploiting the Endomorphism Ring Structure

Once the auxiliary curve E_A' is constructed, its endomorphism ring End(E_A') can be explicitly computed or is structurally predictable. The attack exploits the fact that the endomorphism ring of E_A' contains non-scalar endomorphisms that can be efficiently computed using knowledge of the curve's construction.

Endomorphisms in this ring correspond to specific self-isogenies on E_A', providing navigable shortcuts within the isogeny graph. By identifying a non-scalar endomorphism ψ ∈ End(E_A'), the attacker gains a powerful tool for extracting information about the secret kernel. The endomorphism ψ acts as a "tracer" that reveals relationships between the secret isogeny and the public torsion point images.

Step 3: Applying Vélu's Formulas and Gluing Techniques

Vélu's formulas allow the explicit construction of an isogeny given its kernel [11]. Castryck and Decru realized that the endomorphism ψ, when applied to carefully chosen public torsion points related to the secret isogeny, provided sufficient information to define the kernel of Alice's secret isogeny φ_A.

The attack uses a technique called "gluing" where the endomorphism ψ is used to connect information from the auxiliary curve E_A' back to the original curve E_A. By examining the action of ψ on the public torsion point images, the attacker can effectively trace back to determine the relationships that define Alice's secret kernel G_A.

Step 4: Reconstructing the Secret Scalar

This process ultimately allows recovery of Alice's secret scalar multiplier — the integer defining her isogeny. The endomorphism ψ provides a system of equations that can be solved to determine the discrete logarithm relationships that define the secret kernel G_A.

With this value, the attacker can compute φ_A from E_0, derive the shared secret curve E_AB, and thus break the SIKE KEM. The reconstruction involves solving a system of linear equations over the appropriate finite field, which can be done efficiently using standard algebraic techniques.

3.3 Complexity Analysis and Practical Implementation

The efficiency of this attack is polynomial in log p, with a remarkable complexity of $O(\log^2 p)$ for the main computational steps. This makes it highly efficient and practical against all parameters proposed for SIKE, in stark contrast to prior attacks which had exponential complexity and were deemed infeasible.

Concrete Performance: For the SIKE parameter sets:

- SIKE p434: Attack completes in minutes on a standard laptop
- SIKE p751: Attack completes in approximately one hour on a single CPU core
- SIKE p964: Attack completes in several hours

The attack was successfully implemented and verified against all SIKE parameter sets, demonstrating its practical applicability. The implementation shows that the theoretical polynomial complexity translates to real-world feasibility, making SIKE completely insecure for all proposed security levels [8, 12, 13, 14].

4. Impact and Implications

The Castryck-Decru attack had immediate and profound consequences for SIKE and the broader field of post-quantum cryptography:

4.1 Removal from NIST PQC Standardization

SIKE was a highly-regarded as a candidate in the Round 3 of NIST PQC standardization process [2]. Following the publication of the attack on August 1, 2022, NIST promptly announced SIKE's removal from consideration in August 2022 [10]. This decision highlighted how effective the public and competitive cryptographic evaluation process is. It showed that through a thorough, repeated review,

vulnerabilities can be found, and the integrity of the standardization process can be maintained.

The timing was particularly significant as it occurred just one month after NIST announced the first four algorithms for standardization in July 2022, highlighting the continued importance of active cryptanalysis throughout the standardization process.

4.2 Current State of NIST PQC Standardization (2025)

As of 2025, the NIST Post-Quantum Cryptography standardization process has made significant progress since SIKE's withdrawal. The first set of post-quantum cryptographic standards from NIST's standardization project, namely FIPS 203, FIPS 204, and FIPS 205, were issued on August 13, 2024. These standards define algorithms that come from CRYSTALS-Dilithium, CRYSTALS-KYBER, and SPHINCS+. [15, 16, 17].

The finalized standards include:

- **FIPS 203** (ML-KEM): Module-Lattice-Based Key-Encapsulation Mechanism Standard, derived from CRYSTALS-Kyber [15,18]
- **FIPS 204** (ML-DSA): Module-Lattice-Based Digital Signature Standard, derived from CRYSTALS-Dilithium [16,19]
- **FIPS 205** (SLH-DSA): Stateless Hash-Based Digital Signature Standard, derived from SPHINCS+ [17,20]

Additionally, in a move to ensure robust post-quantum encryption, NIST has chosen **HQC** as a backup to the main **ML-KEM** algorithm. This is significant because **HQC** uses different mathematical foundations than **ML-KEM**, offering a safeguard if vulnerabilities are discovered in **ML-KEM**. This choice highlights NIST's commitment to algorithmic diversity, drawing from past experiences like the **SIKE** failure.

4.3 Validation of Active Cryptanalysis

The attack served as a stark reminder that even well-studied and seemingly robust cryptographic schemes, supported by deep mathematical foundations, can harbor subtle and previously undiscovered vulnerabilities [8]. It highlighted the indispensable role of active cryptanalysis and the collaborative efforts of the global research community in ensuring cryptographic security.

The fact that a fundamentally new attack, rather than an incremental improvement, was discovered emphasizes the value of fresh perspectives and relentless scrutiny. The attack also demonstrated the importance of considering auxiliary mathematical structures that may not be immediately obvious but can provide unexpected attack vectors.

4.4 Impact on PQC Algorithm Diversity

The loss of SIKE significantly altered the composition of the NIST PQC candidates. With SIKE's withdrawal, the set of finalists became heavily concentrated in lattice-based cryptography (ML-KEM, ML-DSA for main algorithms). While other approaches like hash-based (SLH-DSA) and code-based cryptography (HQC) remained [21], SIKE's unique combination of small key sizes and elegant mathematical structure had made it a distinct and attractive option.

Its failure highlighted a temporary reduction in the diversity of underlying mathematical problems within the front-running PQC primitives. By selecting HQC as a backup, an algorithm distinct from ML-KEM in its mathematical foundation, NIST underscores its ongoing commitment to algorithmic diversity [22]. This diversity is recognized as potentially vital should weaknesses emerge in the primary algorithms.

5. Implications for Isogeny-based Cryptography

The Castryck-Decru attack spurred intense research within the isogeny-based cryptography community to understand the specific flaw and assess whether it could be generalized to other isogeny-based constructions [23].

5.1 Impact on Other Isogeny-based Schemes

The attack was specific to the SIDH/SIKE construction and its particular use of torsion point information in the public key. However, this attack does not seem to work on CSIDH or SQISign, as these schemes use different mathematical structures and public key representations.

CSIDH (Commutative Supersingular Isogeny Diffie-Hellman):

- Uses mere ordinary elliptic curves instead of supersingular curves
- Based on group actions it employs a different key exchange mechanism
- The public keys do not contain torsion point information that could be exploited by the Castryck-Decru technique
- However, CSIDH faces other challenges, including potential quantum attacks [24,25]

SQISign (Short Quaternion and Isogeny Signature):

- Uses a different mathematical foundation based on quaternion algebras
- The signature scheme does not rely on the same torsion point structure as SIKE
- Recent work continues to develop improvements such as SQIsign2D variants [26]
- Recent research focuses on faster signature schemes using 2-dimensional isogenies

5.2 Ongoing Research and Developments

The isogeny-based cryptography community has responded to SIKE's failure with renewed focus on:

1. **Alternative Constructions:** Development of isogeny-based schemes that avoid the specific vulnerabilities exploited in the Castryck-Decru attack
2. **Enhanced Security Analysis:** More rigorous analysis of information leakage in public key structures
3. **Hybrid Approaches:** Combining isogeny-based techniques with other mathematical foundations

Recent research has focused on optimizing pairings for isogeny-based cryptography, making general techniques more applicable to schemes like CSIDH and SQISign. This work removes previous limitations and enhances the toolkit available for isogeny-based constructions.

5.3 Lessons for Future Isogeny-based Schemes

The SIKE attack has led to several important considerations for future isogeny-based cryptographic schemes:

1. **Torsion Point Information:** Extreme caution is required when including torsion point images in public keys
2. **Endomorphism Ring Structure:** The exploitability of endomorphism ring properties requires careful analysis
3. **Auxiliary Curve Constructions:** The potential for attackers to construct auxiliary curves with favorable properties must be considered
4. **Information Leakage:** A more comprehensive understanding of what information is revealed by public key elements is essential

6. Critical Insights from the SIKE Vulnerability

The Castryck-Decru attack on SIKE provides several critical lessons that resonate across cryptographic design, evaluation, and the development of post-quantum standards:

6.1 Subtlety of Mathematical Vulnerabilities

Even with deep mathematical foundations, subtle interactions between different components of a cryptographic scheme can lead to unexpected and devastating vulnerabilities. The torsion point information leakage in SIKE was not immediately obvious and required sophisticated cryptanalytic insight to uncover and exploit [8].

This underscores the necessity for rigorous and comprehensive scrutiny in the analysis of cryptographic primitives, particularly those relying on intricate mathematical structures. The attack demonstrated that security cannot be assumed merely because the underlying mathematical problem appears hard — the specific way information is structured and revealed in the protocol implementation can create unexpected attack vectors.

6.2 Importance of Public Scrutiny and Continuous Evaluation

The open and competitive nature of the NIST PQC process proved invaluable. By inviting a diverse community of researchers to scrutinize candidates over multiple years, the process effectively allowed for the identification and exposure of flaws that might otherwise have gone unnoticed in a closed development environment.

The fact that the attack was discovered by independent researchers, rather than the original designers, highlights the critical value of collaborative, global cryptanalysis as a cornerstone of robust cryptographic standardization. The timeline also demonstrates that security evaluation must continue even after initial selections are made.

6.3 Diversity in PQC Primitives is Crucial

While the SIKE attack caused a temporary reduction in the diversity of leading PQC candidates, it strongly reinforces the long-term strategic goal of having a portfolio of post-quantum algorithms based on different hard mathematical problems. NIST's recent selection of HQC as a backup algorithm based on different mathematical principles than ML-KEM shows their dedication to keeping a diverse variety of algorithms, which could be crucial if the main ones are found to have vulnerabilities. Efforts also continue to ensure the practical security of various PQC candidates, including digital signature schemes like PICNIC, against side-channel attacks [26].

Over-reliance on a single mathematical family (e.g., lattices) could pose a systemic risk to global digital security if a breakthrough attack on that specific family were to occur. The SIKE failure serves as a concrete example of why this diversity is not just academically interesting but practically essential.

6.4 The Evolving Threat Landscape

Cryptography is an ongoing arms race. As computational power, algorithmic understanding, and cryptanalytic techniques advance, what is considered secure today may not be secure tomorrow. This demands continuous research, proactive cryptanalysis, and the adaptability of cryptographic standards to new threats and insights.

The rapid development of the Castryck-Decru attack from a theoretical possibility to a practical implementation — demonstrates how quickly the security landscape can change. Moving forward, the PQC community must prioritize not only mathematical elegance but also demonstrable resistance against evolving attack methodologies, including those exploiting auxiliary structure leakages.

6.5 Implementation and Standardization Considerations

The SIKE attack also provides lessons for the implementation and deployment of post-quantum cryptography:

1. **Cryptographic Agility:** The need for systems that can quickly transition between different cryptographic algorithms when vulnerabilities are discovered
2. **Hybrid Approaches:** The benefits of using both classical and post-quantum algorithms together while we're still transitioning
3. **Continuous Monitoring:** The importance of ongoing security evaluation even after standardization. This includes rigorous analysis of implementations to ensure resistance against side-channel attacks like physical attacks on digital signature schemes like PICNIC [27].

7. Future Research Directions and Open Problems

The recent attack on the Supersingular Isogeny Key Encapsulation (SIKE) protocol has highlighted critical areas requiring further exploration in post-quantum cryptography. The incident has not only revealed vulnerabilities in specific

cryptographic constructions but has also opened new directions for research. These directions can be categorized into three broad areas: isogeny-based cryptography, general post-quantum cryptographic development, and cryptanalysis and security evaluation.

7.1 Isogeny-based Cryptography Research

1. There is a need to develop new isogeny-based cryptographic schemes that are resilient to the types of vulnerabilities exploited in the SIKE attack. These new constructions should aim to retain the key advantage of isogeny-based systems such as their compact key sizes.
2. Further research is required to deepen the understanding of endomorphism ring structures and how they can either be leveraged in cryptographic attacks or protected against in secure cryptographic designs.
3. Exploring alternative hard problems in isogeny-based cryptography, beyond the conventional Supersingular Isogeny Diffie–Hellman (SIDH) framework, may provide new foundations for secure and efficient post-quantum protocols.

7.2 General Post-Quantum Cryptography

1. It is important to develop hybrid security models that address the challenges of transitioning from classical to post-quantum cryptographic systems. Such models should ensure secure interoperability during this transitional phase.
2. Ongoing efforts must focus on optimizing the performance of post-quantum algorithms. The goal is to make these algorithms more computationally efficient while preserving their resistance to both classical and quantum attacks.
3. The standardization processes for post-quantum cryptography need to be refined. Improved evaluation methodologies are necessary to detect subtle and complex vulnerabilities, such as those that compromised SIKE.

7.3 Cryptanalysis and Security Evaluation

1. There is significant potential in developing automated tools and techniques for systematically discovering vulnerabilities in cryptographic schemes. Such tools can enhance the robustness of cryptographic design and validation processes.
2. Researchers should focus on gaining a deeper understanding of how auxiliary mathematical structures, often embedded in cryptographic protocols, can be exploited by adversaries.
3. It is essential to improve existing methods for assessing information leakage. Specifically, there should be a stronger focus on evaluating the extent to which public key structures and protocol transcripts reveal sensitive information.

8. Conclusion

The Castryck-Decru attack on SIKE represents a pivotal moment in the history of post-quantum cryptography. Though the immediate impact was the elimination of a promising candidate from NIST standardization, but the broader implications extend far beyond a single algorithm's failure. The attack showed the critical importance of open, collaborative cryptanalysis and the value of maintaining diversity in cryptographic approaches. It demonstrated the subtlety of mathematical vulnerabilities and the need for continued vigilance in security evaluation, even for well-studied schemes with elegant mathematical foundations. As the field moves forward with the finalized NIST standards of 2024-2025, including the strategic selection of backup algorithms like HQC, the lessons learned from SIKE's failure continue to inform best practices in cryptographic design and standardization. The ongoing research in isogeny-based cryptography, while more cautious than before, demonstrates the resilience of the cryptographic community in learning from failures and pursuing new approaches to quantum-resistant security. The SIKE attack ultimately serves as a valuable case study that strengthens the overall post-quantum cryptography ecosystem by emphasizing the importance of rigorous analysis, algorithmic diversity, and continuous evaluation in the face of evolving threats.

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] National Institute of Standards and Technology, "Post-Quantum Cryptography Standardization: Announcement and Requirements", Federal Register, December, Vol.**81**, No.**244**, pp. **92787--92788**, **2016**.

[2] National Institute of Standards and Technology, "NIST Post-Quantum Cryptography (PQC) Standardization Process: Status Update", August **2022**.

[3] J. De Feo, D. Jao, and J. Plut, "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies", in *Post-Quantum Cryptography: 4th International Workshop, PQCrypto*, Taipei, Taiwan, **2011.**

[4] R. Azarderakhsh *et al.*, "Supersingular Isogeny Key Encapsulation (SIKE)", NIST Post-Quantum Cryptography Standardization Process, **2020**.

[5] D. Jao, R. Azarderakhsh, M. Campagna, C. Costello, L. De Feo, B. Hess, A. Jalali, B. Koziel, B. LaMacchia, P. Longa, M. Naehrig, J. Renes, V. Soukharev, and D. Urbanik, "SIKE: Supersingular Isogeny Key Encapsulation", NIST Post-Quantum Cryptography Standardization, Round 3 Submission, **2020**.

[6] P. Stratil, S. Hasegawa, and H. Shizuya, "Supersingular Isogeny-based Cryptography: A Survey", *Cryptology Interdisciplinary Information Sciences*, Vol.**27**, No.**1**, **2021**.

[7] K. Naskar and A. Dey, "Foundations and Development of Isogeny-Based Cryptography: From Origins to the SIKE Collapse" International Journal of Computer Sciences and Engineering Vol.**13**, Issue.**6**, pp.**23**-**31**, **2025**.

[8] W. Castryck and T. Decru, "An efficient key recovery attack on SIDH", in *CRYPTO 2022: 42nd International Cryptology Conference*, Santa Barbara, CA, USA, Aug. pp.**15**-**19**, **2022.**

[9] W. Castryck and T. Decru, "CSIDH on the surface", in *Post-Quantum Cryptography: 13th International Workshop, PQCrypto 2022*, J. Ding and J.-P. Tillich, Eds. Cham: Springer International Publishing, pp. **111**-**129, 2022**.

[10] "The SIKE teams acknowledges that SIKE and SIDH are insecure and should not be used". NIST Post-Quantum Cryptography-Round 4 Submissions: Public-key Encryption and Key-establishment Algorithms, History of Round 4 updates, **2017**.

[11] J. Vélu, "Isogénies entre courbes elliptiques", *Comptes Rendus de l'Académie des Sciences, Série A et B*, Vol.**273**, No.**1**, pp.**55**-**58**, **1971**.

[12] A. Adj, L. Rivera-Zamarripa, and J. A. López-Ramos, "An attack on SIDH with arbitrary starting curve", *Cryptology ePrint Archive*, pp.**10**-**26, 2022**.

[13] L. Maino and C. Martindale, "An attack on SIDH with arbitrary starting curve", *Cryptology ePrint Archive*, **2022**.

[14] D. Robert, "Breaking SIDH in polynomial time", in *Advances in Cryptology -- EUROCRYPT* pp.**472**-**503, 2023**.

[15] National Institute of Standards and Technology, "Module-Lattice-Based Key-Encapsulation Mechanism Standard", FIPS **203**, **2024**.

[16] National Institute of Standards and Technology, "Module-Lattice-Based Digital Signature Standard", FIPS 204, August **2024**.

[17] National Institute of Standards and Technology, "Stateless Hash-Based Digital Signature Standard", FIPS 205, August **2024**.

[18] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehlé, "CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM", in *IEEE European Symposium on Security and Privacy*, pp.**353**-**367, 2018**.

[19] L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé, "CRYSTALS-Dilithium: A lattice-based digital signature scheme", *IACR Transactions on Cryptographic Hardware and Embedded Systems*, Vol.**2018**, No.**1**, pp.**238**-**268**, **2018**.

[20] D. J. Bernstein, A. Hülsing, S. Kölbl, R. Niederhagen, J. Rijneveld, and P. Schwabe, "The SPHINCS+ signature framework", in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pp.**2129**-**2146, 2019**.

[21] T. Chou, "QcBits: Constant-time small-key code-based cryptography", in *Cryptographic Hardware and Embedded Systems – CHES*, pp.**280**-**300, 2016**.

[22] C. Aguilar-Melchor, N. Aragon, S. Bettaieb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, A. Hauteville, and G. Zémor, "HQC: Hamming Quasi-Cyclic", NIST Post-Quantum Cryptography Standardization, Round 4 Submission, **2023**.

[23] W. Beullens, J. De Feo, S. D. Galbraith, and C. Petit, "Proving knowledge of isogenies-A survey", IACR Cryptology ePrint Archive, pp.**671, 2023**.

[24] W. Castryck, T. Lange, C. Martindale, L. Panny, and J. Renes, "CSIDH: An efficient post-quantum commutative group action", in *Advances in Cryptology -ASIACRYPT*, pp.**395**-**427, 2018**.

[25] P. Longa, "A note on the security of CSIDH", *Cryptology ePrint Archive*, pp.**11**-**98, 2018**.

[26] L. De Feo, D. Kohel, A. Leroux, C. Petit, and B. Wesolowski, "SQISign: Compact post-quantum signatures from quaternions and isogenies", in *Advances in Cryptology - ASIACRYPT*, pp.**64**-**93, 2020**.

[27] D. Cervantes-Vázquez, M. Chenu, J.-J. Chi-Domínguez, L. De Feo, F. Rodríguez-Henríquez, and B. Smith, "Stronger and faster side-channel protections for PICNIC signatures", in *Progress in Cryptology - LATINCRYPT*, pp.**391**-**412, 2019**.

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 2000 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.

