Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-B, pp. 4369–4381
DOI : 10.47974/JDMSC-3058

Isogeny-based cryptosystems for post-quantum security

R. A. Kapgate [†]
Department of Mechatronics Engineering
Sanjivani College of Engineering
Savitribai Phule Pune University
Kopargaon
Ahilyanagar 423603
Maharashtra
India

Dheeravath Raju [*]
Centre for Multidisciplinary Research
Anurag University
Hyderabad 500088
Telangana
India

Chetansinh R. Vaghela [§]
Faculty of Science
Gokul Global University
Sidhpur 384151
Gujarat
India

Neema Sajju Balan [‡]
Department of Computer Science & Engineering
Rungta College of Engineering & Technology
Rungta International Skills University
Bhilai 490024
Chhattisgarh
India

[†] *E-mail:* rakapgate@sanjivani.org.in
[*] *E-mail:* dheeravathraju.dr@rediffmail.com (Corresponding Author)
[§] *E-mail:* crvaghela.maths.gsc@gokuluniversity.ac.in
[‡] *E-mail:* neema@rungta.org

© Taru Publications

Amol Barde [@]
Department of Mechanical Engineering
Vishwakarma Institute of Technology
Pune 411037
Maharashtra
India

Krishna Chaitanya Pidugu [#]
Department of CSE (Artificial Intelligence)
Pragati Engineering College
Surampalem
Kakinada District 533437
Andhra Pradesh
India

Abstract

The fast progress of quantum computing is a serious threat to classical cryptographic schemes like RSA and elliptic curve cryptography, and it is time to come up with safe post-quantum schemes. One of the new solutions is isogeny-based cryptography which has attracted attention because of its good-security basis and comparatively small key sizes. Nevertheless, currently used post-quantum cryptographic (PQC) designs, such as lattice-based and code-based ones, are typically characterized by the high key sizes, high computational costs, or scaling issues, with the necessity to have a well-balanced and efficient cryptographic design. This paper presents a powerful isogeny-based cryptosystem, which can allow safe communication in the post-quantum context. The mathematical complexity of isogenies over supersingular elliptic curves forms the foundation of the proposed framework and it has a structured architecture comprising of parameterization, key generation, encryption/decryption and communication layers. The design of the optimization of algorithms to generate keys, exchange keys securely and encrypt messages using shared secret derivation mechanisms is part of the methodology. Security analysis is also carried out to assess the resistance to quantum attacks and against known cryptanalytic vulnerabilities. The metrics used to conduct performance evaluation are computed cost, key size, and latency, and the results are compared to typical PQC schemes, like lattice-based (Kyber) and code-based (McEliece) systems. The results show that the model proposed has much smaller key sizes (330 bytes public key) with moderate computational efficiency although a little bit more latency than lattice-based methods.

Subject Classification: *68M25, 68M11.*

Keywords: *Post-quantum cryptography (PQC), Isogeny-based cryptography, Supersingular elliptic curves, SIDH, SIKE, Quantum-resistant security, Key exchange, Cryptographic algorithms, Secure communication.*

[@] *E-mail:* **amol.barde1@vit.edu**
[#] *E-mail:* **krishnacp@outlook.com**

I. Introduction

The swift growth of the digital ecosystems such as financial services, healthcare systems, cloud computing, and Internet-of-Things (IoT) networks has caused the need to have strong cryptographic tools to guarantee the safety of communication and data. Many conventional cryptosystems of the public-key type have been used in the past (RSA and Elliptic Curve Cryptography (ECC)) as a foundation of secure digital communication. But this is not the case with the advent of quantum computing that brings a paradigm shift to computational ability and therefore poses a significant threat to such classical systems. The mathematical problems which form the basis of RSA and ECC can be efficiently solved (using quantum algorithms, especially Shors algorithm), and this undermines the security. This has increased interest, leading to a rush in the study of post-quantum cryptography (PQC), to create cryptographic schemes that are resistant to classical and quantum adversaries [3].

Although much progress has been made, the current methods of PQC, such as lattice-based, code-based, and multivariate cryptography, have some significant shortcomings. Multivariate cryptography has potential but continues to struggle with issues in the security assessment and ability to resist the changing approach of attack techniques [1], [2]. Cryptosystems based on codes, despite their high level of security, can be characterized by big key sizes and lack of efficiency in their real life applications [3]. Likewise, lattice-based schemes are also susceptible to some structural and subversion attacks, given certain circumstances [11].

Due to these shortcomings, isogeny-based cryptography has been proposed as an interesting alternative in PQC field. This method takes advantage of the mathematical intricacy of isogenies between elliptic curves, especially in supersingular isogeny graphs, to create safe cryptographic primitives. These systems are based on the hardness of these problems: isogeny path finding, class group actions, and so on [4], [6]. Moreover, isogeny-based schemes have fairly small key sizes relative to other PQC families, and therefore are resource-friendly. Various constructions have been made with this technique such as the isogeny-based key exchange protocols, password-authenticated key establishment, and the digital signature schemes, which have proven the versatility of this technique [7]-[10].

Nevertheless, recent research has demonstrated some flaws in some of the isogeny-based schemes casting doubt on their long and short-term security as well as practical use [5]. The results highlight the importance of improved designs capable of both addressing new threats and still maintaining the natural benefits of isogeny-based cryptography. As a result, it is still urgent to create strong, efficient and secure isogeny-based cryptosystems that should be suitable to the post-quantum era.

Here, the main goal of this paper is to formulate and discuss a better isogenous based cryptographic system, which limits the drawbacks of the existing methods. The work is aimed at the creation of a secure and efficient system architecture, increased resistance to both classical and quantum attacks and performance optimization in terms of computational complexity and the key size. The most important contributions of this work are as follows: (i) a new isogeny-based cryptosystem framework with enhanced security parameters is introduced; (ii) an optimized algorithm workflow is created to generate keys, encrypt and decrypt messages; (iii) a detailed security assessment is undertaken against known attack vectors; and (iv) a comparative performance analysis is presented to provide an understanding of the effectiveness of the proposed model over existing PQC Together, this work is a step towards the development of scalable and quantum-resilient cryptography solutions to future secure systems.

II. Fundamentals of Isogeny-Based Cryptography

Isogeny-based cryptography, is based on the elliptic curve algebraic structure in finite fields. A finite field Fq the set of rational points on an elliptic curve Eover Fq (an elliptic curve) is often modeled by a Weierstrass equation, and is usually an abelian group with point addition. Cryptographic constructions make use of the fact that it is hard to compute mappings between such curves, called isogenies. An isogeny is a non- constant rational morphism ϕ:E_1-E 2 that maintains the group structure, i.e. it is both a homomorphism, and a mapping of finite degree. Computational complexity of an isogeny is influenced by the degree of an isogeny, which is a key parameter in determining a security parameter. Specifically, a much-utilized type of elliptic curve is the supersingular elliptic curve, a curve with special algebraic properties, which has a rich isogeny structure. These curves create very intertwined graphs with the nodes being elliptic curves and the edges isogenies of degree fixed. The security of an isogeny-based cryptosystems is based on the mathematical difficulty of navigation in these graphs. Isogeny-based methods are based on the difficulty of calculating unknown isogenies between provided curves, unlike traditional elliptic curve cryptography, in which the discrete logarithm problem is in the limelight.

The isogeny-based systems are secure to a number of computationally difficult problems, which are set on supersingular isogeny graphs. The Isogeny Path Problem, finding a sequence of isogenies (a path) between two specified elliptic curves in a big graph is one of the most important. With the start and end nodes only, it is thought to be computationally infeasible to every classical, as well as quantum, adversary to compute the middle path. The Supersingular Isogeny Graph (SSIG) Navigation Problem is another crucial issue where the attacker would need to navigate through an expander-like large graph with no shortcuts, and no efficient ones. These graphs have a high degree of mixing thus random walks are unpredictable

and hard to reverse. Further, issues of the actions of the class groups and endomorphism rings also add to the hardness assumptions in isogeny-based cryptography. They are the problems without an efficient solution in a form of polynomials at the moment, even with known quantum algorithms, that is why they are a good candidate of post-quantum security.

One of the first and most researched isogeny-based key exchange protocols is Supersingular Isogeny Diffie Hellman (SIDH). It generalizes classical DiffieHellman paradigm to use isogeny computations between elliptic curves instead of exponentiation in cyclic groups. In SIDH, the two parties create secret isogenies based on the common initial curve and share auxiliary public parameters, which allows the two parties to compute a shared secret curve. Using SIDH as a basis, Supersingular Isogeny Key Encapsulation (SIKE) protocol was suggested as a useful encryption and key exchange protocol and was a submission in the NIST PQC standardization process. SIKE proposes encapsulation and decapsulation flow of key exchanges with the security of insecure channels. Its key sizes are relatively small in comparison with other PQC schemes, which is a key advantage of this scheme. Nevertheless, cryptanalytic attacks of late have shown weaknesses in SIKE and the algorithm has been dropped out of the NIST competition. Nevertheless, SIDH/SIKE still have a central role to play in the comprehension of constructions based on isogeny and still serve as inspiration in more secure variants.

Isogeny-based cryptography schemes are based on a number of security assumptions that are based on the hardness of mathematical problems. The most noticeable one is that the computation of an isogeny between two randomly selected supersingular elliptic curves is computationally infeasible. Also, assumptions about the hardness of the recovery of secret isogenies given public parameters, sometimes known as the Isogeny Diffie Hellman Problem, are the focus of protocol security. The infeasibility of the calculation of endomorphism ring is another assumption, as well as the impossibility of differentiating the isogenous curves without any supplementary information. Many Isogeny-based schemes are proven to be secure under these assumptions, and may be built in classical or quantum random oracle models. Even though these assumptions are thought to be strong, recent attacks have emphasized the significance of an appropriate parameter selection and protocol design. Consequently, current studies are devoted to enhancing these assumptions and creating resistant constructions that are resistant to classical cryptanalysis and new threats of quantum nature.

III. Proposed Isogeny-Based Cryptosystem Framework

A. *System Model and Design Architecture*

The framework suggests a safe and effective isogeny-based cryptosystem, which can be used in a post-quantum environment. The system is based on client server model of communication in which two

parties are involved or the sender and receiver who create a secure channel over an insecure network. The architecture is designed with four key layers: (i) parameter initialization layer, (ii) key generation layer, (iii) encryption/decryption layer and (iv) communication and verification layer.

The proposed isogeny-based cryptosystem, of a secure post-quantum communication has a layered architecture that is depicted in Figure 1. On top, the parameter initialization layer defines system parameters that are globally shared, such as the supersingular elliptic curve E0, the finite field F(p2), torsion basis and isogeny degrees, which are the core of the cryptographic setup. In the key generation layer, the sender and the receiver both come up with their own secret isogenies (their own private keys) and derive corresponding public keys by mapping the base curve to new elliptic curves; these public parameters are shared across an insecure channel.

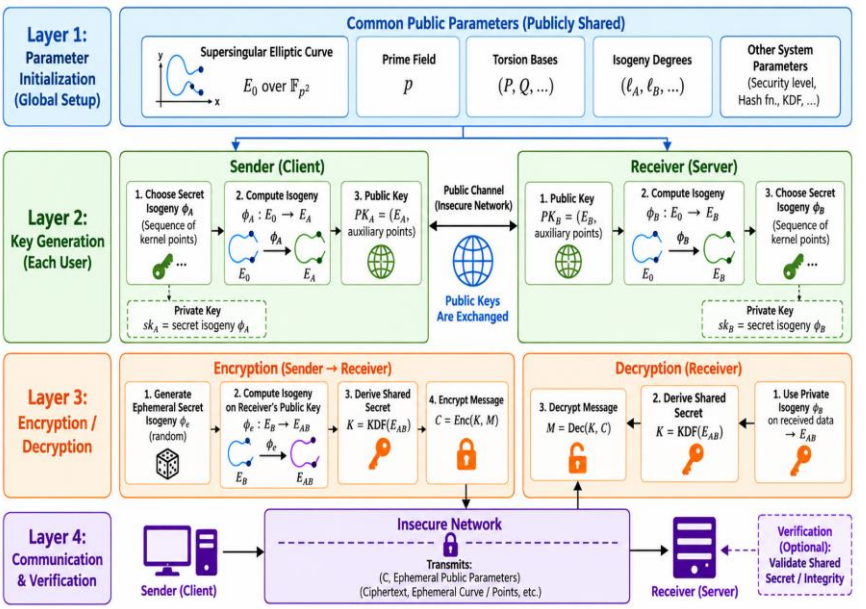


Figure 1
Proposed Isogeny based Cryptosystem Architecture

Lastly, the communication and verification layer entails the flow of encrypted communication over an unsecured network as well as optional mechanisms to authenticate the shared secret and to verify integrity of the data. The architecture, in general, exhibits a secure key exchange protocol, which is isogenous, with isogenous computations, and provides confidentiality and quantum resistance without disclosing any private keys.

B. *Key Generation, Encryption, and Decryption Processes*

Key Generation:

Each user chosen random secret integer or kernel generator of a particular degree in isogeny. With this secret, an isogeny ϕ:E 0 E A is calculated, E Ais is the resulting elliptic curve. The public key is comprised of the curve E A along and support points necessary to perform additional isogeny computations. The key which is kept private is the secret isogeny path or kernel.

Encryption:

The sender uses the public key of the receiver to encrypt a message, and creates a temporary secret isogeny. This results in an intermediate curve and a shared secret is derived using a key derivation function (KDF). A symmetric encryption algorithm (e.g., AES) is used to encrypt the plaintext message with the derived key. The encrypted message and the ephemeral public parameters of the sender are part of the ciphertext.

Decryption:

Later, when the receiver gets the ciphertext, it is reassembled with the help of his or her own key into the shared secret by calculating a compatible isogeny with the public parameters of the sender. The same KDF is used to obtain the symmetric key which is used to decrypt the ciphertext and get the original message.

C. *Algorithmic Workflow and Pseudocode*

The general outline of the work of the suggested cryptosystem is provided in Algorithm 1.

Algorithm 1: Proposed Isogeny-Based Cryptosystem

Input: Public parameters (E0, p, basis points), message M
Output: Ciphertext C, Decrypted message M

// Key Generation (User A)
1. Select random secret sA
2. Compute isogeny φA: E0 → EA using sA
3. Publish public key PK_A = (EA, auxiliary points)

// Key Generation (User B)
4. Select random secret sB
5. Compute isogeny φB: E0 → EB using sB
6. Publish public key PK_B = (EB, auxiliary points)

// Encryption (Sender A → Receiver B)
7. Generate ephemeral secret eA
8. Compute φeA: EB → E_shared
9. Derive shared key K = KDF(E_shared)

10. Encrypt message: C = Enc(K, M)
11. Send (C, ephemeral public parameters)

// Decryption (Receiver B)
12. Compute φB on received parameters to derive E_shared
13. Derive shared key K = KDF(E_shared)
14. Decrypt message: M = Dec(K, C)

This protocol makes sure that the communicating parties derive identical shared secret independently without revealing their private keys. The algorithm outlines a safe communication procedure between two parties based on isogenous cryptography. First, key generation is done independently by the two users as they choose secret isogenies (private keys) and derive respective public keys based on a shared base elliptic curve. This set of public keys are then used in an insecure channel. In the encryption step, the sender creates a temporary (ephemeral) isogeny, and uses that isogeny on the public key of the receiver to create a shared secret. This common secret is transformed into a symmetric key (key derivation function (KDF)) and the message is encrypted with this. During the decryption stage, the receiver applies his or her own isogeny and the received parameters, to independently compute the same shared secret. The ciphertext is then decrypt using the derived key to get back the original message. On the whole, the algorithm secures both sides have a shared secret, without disclosing their private keys to permit secure communication, even across an unsecured network.

In order to maximize the practical performance of the proposed cryptosystem, it is optimized using a number of optimization strategies. First, more effective isogeny computation methods, including the formulas of optimized Vélu, and kernel-based isogeny computation are used to minimize computational cost. Second, parameter tuning, including the best choice of isogeny degrees and balanced prime sizes, can be used to trade to some extent security and efficiency. Also, the application of precomputation and caching of commonly utilized elliptic curve operations considerably decreases run time when repeatedly running such operations. Also, independent isogeny computations can be performed by parallelization so that they can be scaled in high-performance settings. Elliptic curves: Elliptic curve points are represented in a memory efficient way and compression of public keys reduces storage and transmission overhead. Lastly, hybrid implementation with symmetric cryptographic primitives is used to enforce the computationally expensive isogeny computations to be restricted to key exchange, and the fast symmetric encryption to perform bulk data processing. All of these optimizations enhance the practicality of isogeny-based cryptosystems deployment in practical scenarios, including resource-constrained systems, such as IoT systems.

IV. Security Analysis and Post-Quantum Resilience

The isogeny-based cryptosystem proposed has good security because of the computational hardness of the isogeny problems in supersingular elliptic curves. This framework is quantum immunity, unlike classical cryptographic schemes that are susceptible to the Shor algorithm, in that it is based not on integer factorization or discrete logarithms. Moreover, the speed-up of the brute force attack by the Grover algorithm is only quadratic, which can be countered by increasing the key size and thus maintain the security level intended in quantum computing environment. In spite of these benefits, recent cryptanalytic studies have shown that some isogeny based schemes like SIKE are susceptible to some attacks like adaptive and side channel attacks. The attacks take advantage of intermediate values leakage or parameter selection weakness to extract secret keys. The framework offered solves these problems by taking into consideration safe parameter selection, the minimization of auxiliary information disclosure, and not depending on already violated constructions. Also, the ephemeral parameters can increase the resistance to chosen-ciphertext and fault-injection attacks.

The system is also forwardly secretive and secure in the exchange of keys by creating a distinct shared secret in every session of communication. This is done by use of ephemeral isogeny computation such that the compromise of long-term private keys have no impact on the past communications. The protocol has the Diffie Hellman-like structure which allows both parties to compute the same shared secret without divulging their own information and hence ensure confidentiality and integrity. Lastly, the cryptosystem is considered in terms of a formal security model, e.g., IND-CPA and IND-CCA, which is resistant to passive and active adversaries. These security guarantees are founded on the difficulty of the isogeny path problem and assumptions. The proposed system, in combination with key derivation and authenticated encryption scheme, offers a system that is comprehensive and resilient to post-quantum secure communication.

V. Performance Evaluation and Comparative Analysis

The suggested isogeny-based cryptosystem is assessed with the help of major cryptographic measures, such as the cost of computation, the key size, and latency. Computation cost is used to determine the time taken to do key generation, encryption and decryption. Key size is an evaluation of memory and bandwidth efficiency, which is important in a limited environment. Latency is a measurement of the overall time it takes to engage in a secure communication (key exchange and processing messages). All these measures ensure the feasibility and viability of the suggested system during practical deployments.

The analysis is done based on a simulated cryptographic environment in Python with optimised finite field arithmetic libraries. The experiments

are carried out in a system that has an Intel i7 processor, 16 GB RAM and Ubuntu Operating System. Fair comparison parameters are chosen: 128-bit post-quantum security level, the size of the message remains constant (256 bits) and testing conditions are always similar across all of the schemes. The suggested isogeny-based is compared to representative lattice-based (e.g., CRYSTALS-Kyber) and code-based (e.g., Classic McEliece) cryptosystems.

Table 1
Computation Cost Comparison (ms)

Scheme	Key Generation	Encryption	Decryption
Proposed Isogeny-Based	120	95	100
Lattice-Based (Kyber)	15	10	12
Code-Based (McEliece)	200	5	6

Table 1 compares the time of key generation, encryption and decryption of various post quantum cryptographic schemes. The isogeny-based system suggested has a moderate-to-high computation cost, especially in key generation, as the isogeny computations are very complex. By contrast, lattice-based schemes including Kyber exhibit much lower computation times, and are therefore very useful in real-time applications. Code-based systems such as McEliece are fast when it comes to encryption and decryption but comparatively expensive to produce keys. In general, the table indicates that isogeny-based cryptography is computationally more expensive, but can be implemented with optimization.

Table 2
Key Size Comparison

Scheme	Public Key Size	Private Key Size
Proposed Isogeny-Based	330 bytes	48 bytes
Lattice-Based (Kyber)	1.5 KB	3.2 KB

This Table 2 compares the public and the private key sizes of the various schemes. The size of keys in the proposed isogeny-based cryptosystem is very compact particularly when compared to code-based schemes, which have very large public keys (in the order of hundreds of kilobytes). In lattice-based schemes, the keys are larger than isogeny-based schemes are. This shows one of the main benefits of isogeny-based cryptography: it is resource-efficient in memory and bandwidth, and is therefore suitable to the IoT and resource-constrained setting.

Table 3
Latency Comparison (ms)

Scheme	Total Latency
Proposed Isogeny-Based	315
Lattice-Based (Kyber)	37
Code-Based (McEliece)	211

In this Table 3, the overall latency is described, which is a sum of time taken to carry out a secure communication, including key exchange and cryptographic communication. The proposed scheme has a greater latency than lattice-based schemes because of the computational complexity of isogeny operations. Nevertheless, it does not fare worse with respect to total communication delay as compared to code-based schemes.

The graphical analysis of the Performance Evaluation of the model in Figure 2 is where Figure 1 (Computation Cost Comparison) indicates the trade-offs among various post-quantum cryptographic schemes based on operational efficiency. The suggested isogeny-based cryptosystem exhibits significantly longer computation times in key generation, encryption, and decryption stages than lattice-based protocols, like Kyber. This is mainly because of the intricacy of computations of isogeny on elliptic curves. Nevertheless, compared to the systems written in code, such as McEliece, the offered approach shows a more balanced performance, in particular, at the stages of encryption and decryption, as it does not imply drastic computational inequity. This means that the methods based on isogeny are computationally heavier than lattice-based methods, but are still viable with optimization and less skewed than code-based method.



Figure 2
Graphical Analysis of the results

One of the most evident strengths of isogeny-based cryptography, which is evidenced by the analysis of Figure 2 (Key Size Comparison) is the small size of keys. The scheme proposed has much smaller public and private keys than both lattice-based and code-based systems. Specifically, code-based schemes have very large public keys, and thus, are less appropriate in bandwidth-constrained settings. Lattice-based techniques are in the middle of the range but demand larger storage than the isogeny-based techniques. This small size renders the proposed system very efficient in the memory consumption and transmission overhead that is particularly useful in the case of the IoT devices and embedded systems.

VI. Conclusion and Future Directions

Although this type of cryptography offers promising benefits, isogeny-based cryptography has a number of critical issues that affect its implementation in real-life applications. High computational complexity of the isogeny operations is one of the main constraints that lead to a higher latency than lattice-based schemes. The practical application of isogeny calculations (especially with large parameter space) is still a considerable bottleneck. Moreover, the advent of cryptanalytic attacks on schemes like SIKE has cast doubt on the strength of some of their constructions, as well as the importance of stronger security assumptions, and careful protocol design. The other issue is the management and selection of key parameters whose inappropriate settings can result to weakness, or low performance. Going forward, further studies need to be directed towards creation of hybrid cryptographic models that integrate isogeny-based methods with other PQC methods in order to achieve better security and efficiency. The use of algorithmic optimization and hardware acceleration (e.g., FPGA and GPU-based implementations) can greatly decrease the amount of computation. It is important to investigate quantum-resistant versions and novel isogeny constructions to deal with the new attack vectors. Also, the standardization and interoperability framework research will help to expand its applicability in a real system.

References

[1] G. Alagic, D. Cooper, Q. Dang, T. Dang, J. M. Kelsey, J. Lichtinger, Y.-K. Liu, C. A. Miller, D. Moody, R. Peralta, R. Perlner, A. Robinson, D. Smith-Tone, and D. Apon, “Status report on the third round of the NIST post-quantum cryptography standardization process,” *National Institute of Standards and Technology,* Gaithersburg, MD, USA, NISTIR 8413 (2022), doi: 10.6028/NIST.IR.8413.

[2] C. Balamurugan, K. Singh, G. Ganesan, and M. Rajarajan, “Post-quantum and code-based cryptography—Some prospective research directions,”

Cryptography, vol. 5, no. 4, Art. no. 38 (2021), doi: 10.3390/cryptography5040038.

[3] W. Beullens, L. De Feo, S. D. Galbraith, and C. Petit, "Proving knowledge of isogenies: A survey," *Des. Codes Cryptogr.*, vol. 91, no. 11, pp. 3425–3456 (2023), doi: 10.1007/s10623-023-01243-3.

[4] R. C. Poonia, R. Almakki, A. K. J. Saudagar, A. Altameem, and M. Albathan, "An optimization approach for real-time object detection in IoT devices through edge computing and deep learning," *J. Inf. Optim. Sci.,* vol. 45, no. 5, pp. 1465–1475 (2024), doi: 10.47974/JIOS-1768.

[5] D. Boneh, D. Kogan, and K. Woo, "Oblivious pseudorandom functions from isogenies," in *Advances in Cryptology—ASIACRYPT 2020*, S. Moriai and H. Wang, Eds., Lecture Notes in Computer Science, vol. 12492. Cham, Switzerland: Springer (2020).

[6] J. Dey and R. Dutta, "Progress in multivariate cryptography: Systematic review, challenges, and research directions," *ACM Comput. Surv.*, vol. 55, no. 12, pp. 1–34 (2023), doi: 10.1145/3571071.

[7] B. Drzazga and Ł. Krzywiecki, "Review of chosen isogeny-based cryptographic schemes," *Cryptography*, vol. 6, no. 2, Art. no. 27 (2022), doi: 10.3390/cryptography6020027.

[8] M. Fukumitsu and S. Hasegawa, "A lattice-based provably secure multisignature scheme in quantum random oracle model," in *Proc. Int. Conf. Provable Security (ProvSec)*, pp. 45–64 (2020).

[9] J. J. Mershia Rabuni, R. Mehala Devi, S. Subhalakshmi, and J. Sudha, "Analysis of operation on spherical fuzzy soft topology and its application," *J. Interdiscip. Math.*, vol. 28, no. 7, pp. 2707–2732 (2025), doi: 10.47974/JIM-2329.

[10] S. Uygun and E. Akıncı, "A new method for coding theory by third order Jacobsthal sequence," *J. Discrete Math. Sci. Cryptogr.*, vol. 29, no. 3, pp. 1267–1278 (2026), doi: 10.47974/JDMSC-2233.

[11] S. Limkar, S. Singh, W. V. Ashok, V. Wadne, R. Phursule, and S. N. Ajani, "Modified elliptic curve cryptography for efficient data protection in wireless sensor network," *J. Discrete Math. Sci. Cryptogr.*, vol. 27, no. 2-A, pp. 305–316 (2024).

Received April, 2026