Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-C, pp. 4753–4763
DOI : 10.47974/JDMSC-3089

A comparative study of isogeny-based and elliptic curve cryptographic protocols for post-quantum secure applications

Prerana Nilesh Khairnar [†]
Department of Computer Engineering
Sir Visveavaraya Institute of Technology
Chincholi
Nashik 422102
Maharashtra
India

Prashant Suryavanshi *
Department of Computer Engineering
HSBPVT'S Parikrama Polytechnic
Kashti
Ahilyanagar 414701
Maharashtra
India

Arti Suryavanshi [§]
Department of Computer Engineering
Faculty of Engineering
HSBPVT's Group of Institutions
Kashti
Ahilyanagar 414701
Maharashtra
India

* *ORCID-ID:* 0009-0000-3623-6726
[§] *ORCID-ID:* 0009-0000-4703-8899

[†] *E-mail:* India.autadeprerana@gmail.com
* *E-mail:* sprashant1234@gmail.com (Corresponding Author)
[§] *E-mail:* artips15@gmail.com

© Taru Publications

Archana Date [‡]
Department of Electronics and Computer Engineering
Faculty of Engineering
HSBPVT's Group of Institutions
Kashti
Ahilyanagar 414701
Maharshtra
India

Rahul Raut [@]
Pratibha Gayke [#]
Department of Information Technology
Dr. Vithalrao Vikhe Patil College of Engineering
Ahilyanagar 414111
Maharashtra
India

Abstract

The fast development of quantum computing presents a major challenge to classical public-key cryptographic systems and especially the Elliptic Curve Cryptography (ECC) which is based on the hardness of the elliptic curve discrete logarithm problem. This paper provides a comparative study of isogeny-based cryptographic protocols with ECC-based schemes of post-quantum secure applications. A SIKE-like protocol is adopted and used to test isogeny-based mechanisms under real-world conditions, in addition to typical ECC protocols. The comparison is based on the size of key, complexity of computation, use of memory and communication latency. Experimental results show that, whereas ECC is more efficient and has lower latency in a classical setting, isogeny-based schemes have a higher resistance to quantum attacks, but with a higher computational cost. The findings show a performance-quantum security trade-off, thus requiring to design optimized hybrid cryptographic frameworks in the future to support a secure communication system.

Subject Classification: *81P94, 94A60.*

Keywords: *Post-quantum cryptography, Isogeny-based cryptography, Elliptic curve cryptography, SIKE, Quantum-resistant security.*

[‡] *ORCID-ID:* **0000-0001-9132-7946**
[@] *ORCID-ID:* **0009-0002-0613-6446**
[#] *ORCID-ID:* **0009-0005-2008-5691**

[‡] *E-mail:* **archanadate@gmail.com**
[@] *E-mail:* **raut_it@enggnagar.com**
[#] *E-mail:* **gayke_it@enggnagar.com**

I. Introduction

The growing development of the quantum computing technologies is a significant threat to the popular public-key cryptographic systems. Classical-based schemes like Elliptic Curve Cryptography (ECC) are based on the computational infeasibility of the elliptic curve discrete logarithm problem, which can be efficiently addressed using quantum algorithms, including the Shor algorithm [1, 2]. This weakness has prompted the increased pace of research in post-quantum cryptography where alternative mathematical frameworks are under consideration in order to provide long-term security of data [3, 4, 5]. Isogeny-based cryptography has come into consideration as one of the promising candidates since it relies on the complexity of the computation of isogenies between elliptic curves, which is considered to be immune to both classical and quantum attacks [6, 7]. This paper is devoted to the comparative analysis of ECC and isogeny-based cryptographic protocols in the framework of the secure communication systems [8, 9]. It looks at the variance of computational efficiency, key size, memory usage and latency in a practical implementation environment [10].

II. System Models and Cryptographic Frameworks

This section identifies system-level architectures that combine ECC and isogeny-based cryptography, emphasizing secure communication model, key exchange schemes, structural variations impacting scalability, interoperability, and robustness. Figure 1 depicts ECC and isogenous cryptographic system architecture.

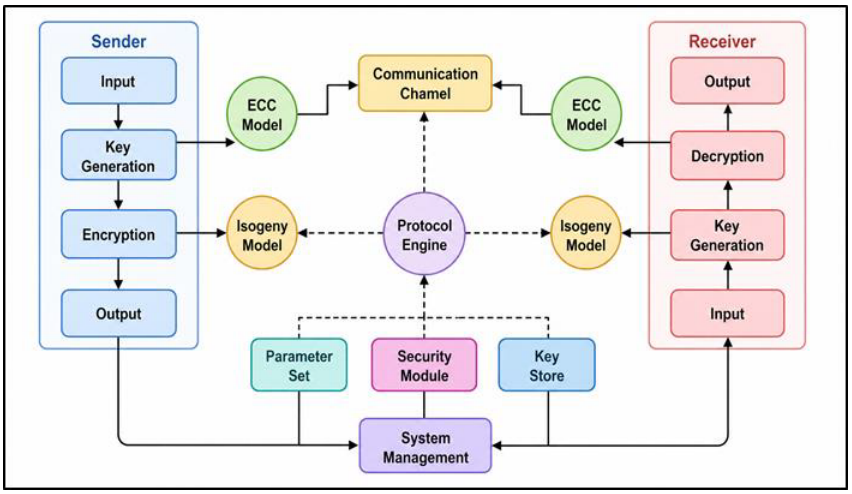


Figure 1

System Architecture for ECC and Isogeny-Based Cryptographic Frameworks

A. *System architecture for ECC-based secure communication*

ECC architecture uses the key generation, encryption, and decryption modules with the use of elliptic curve, lightweight keys and secure channels and the effective computational structures to use in real time communication systems.

$$d = \int^{01} (r(t) mod\ n)\, dt \tag{1}$$

This step is a model step to generate private keys where a randomized function is restricted to a finite group and this method generates uniformly distributed secret scalar to perform the secure elliptic curve operations (Eq. 1).

$$Q = \int^{01} [\, d \cdot G(t)]\, dt \tag{2}$$

It involves taking the public key as a result of scalar multiplication of the secret key and a specific generator point, thus permitting secure key exchange protocols (Eq. 2).

$$C^1 = \int^{01} [\, k \cdot G(t)]\, dt \tag{3}$$

$$C^2 = \int^{01} [\, M + k \cdot Q(t)]\, dt \tag{4}$$

The stage produces the initial ciphertext element with the help of an ephemeral random value which adds randomness and increases forward secrecy in the encryption procedure (Eq. 3). The result of this step is the second ciphertext block, which is a combination of the message and the public key of the receiver, and is secured by providing security through secure mathematical masking (Eq. 4).

$$M = \int^{01} [\, C^2 - d \cdot C^1(t)]\, dt \tag{5}$$

This step is used to restore the original message in such a way that it reverses the encryption transformation with the help of the private key and data sent over the network are recovered correctly and securely (Eq. 5).

$$S = \int^{01} \sqrt{\sum_{\mathrm{i}}^{=1\mathrm{n}} \left(C_{recv_{\mathrm{i}}} - C_{sent_{\mathrm{i}}} \right)^2}\, dt \tag{6}$$

This action ensures integrity of communication by determining the deviation between the sent and received values, error detection, consistency and reliability in a secure communication channel (Eq. 6).

B. *Communication and computation workflow comparison*

In this subsection, the workflows of ECC and isogeny are compared, the steps of encryption are analyzed, the process of key exchange is analyzed, the complexity of calculations and the efficiency of data transmission in different network and processing conditions are analyzed.

$$M_{\mathrm{e}} = \int^{01} [\, \sum_{\mathrm{i}}^{=1\mathrm{n}} m_{\mathrm{i}} \cdot \varphi_{\mathrm{i}}(t)]\, dt \tag{7}$$

This operation codes input data through the combination of weighted basis functions with time, converting discrete message bits to a continuous form to be used in cryptography (Eq. 7).

$$E_{ECC} = \int^{01} \sqrt{(kG)^2 + (kQ)^2}\, dt \tag{8}$$

This equation is an approximation of computational effort of ECC in terms of scalar multiplication of generator and public keys and is a reflection of the complexity of processing in general when performing encryption and key exchange processes (Eq. 8).

$$E_{ISO} = \int^{01} [\, \varphi(E^1 \rightarrow E^2)(t)]\, dt \tag{9}$$

This operation is a transformation of elliptic curves by isogeny mapping, which captures structural changes that can allow key exchange that is resistant to quantum-based computational attacks (Eq. 9).

$$C_{comp} = \int^{01} \sqrt{E_{ECC}^2 + E_{ISO}^2}\, dt \tag{10}$$

This is a hybrid of ECC and isogeny computational complexities, which offers a complete measure of overall cost of cryptographic processing in hybrid systems (Eq. 10).

$$\Psi = \int^{01} \sqrt{\frac{C_{comp}^2}{(C_{comm}^2 + \sum_{i=1}^{n} L_i^2)}}\, dt \tag{11}$$

It is a measure of efficiency in the system by providing a tradeoff between computational complexity and communication overhead and latency considerations and provides a combined performance measure of secure communication systems (Eq. 11).

III. Methodology and Experimental Design

A. *Implementation of isogeny-based schemes (SIKE-like framework)*

Isogeny-based isogenous implementation: SIKE-like protocols are implemented using supersingular elliptic curves, isogeny computations, and key exchange is secure, but is not hardened for quantum adversaries that can structure their algorithm design.

$$E^0 = \int^{1} [\, y^2 = x^3 + ax + b \bmod p\,]\, dt \tag{12}$$

This is the step that defines the initial elliptic curve in the context of finite field, and hence, the algebraic structure and the choice of parameters to carry out secure cryptography (Eq. 12).

$$K_s = \int^{1} [\, \langle P + [m]Q \rangle]\, dt \tag{13}$$

The computation yields a secret kernel whose basis (base points and scalar multiplication) is the foundation of the construction of secure isogeny-based transformations (Eq. 13).

$$\varphi : E^0 \rightarrow E^1 = \int^{01} [\, \varphi_{Ks}(x, y)]\, dt \tag{14}$$

The step is an isogeny whereby an elliptic curve is transformed into another using a kernel-computed isogeny that makes the secure structural transformation required by quantum-resistant key exchange protocols (Eq. 14).

$$PK = \int^{1} \left[\left(E^{1}, \varphi(P'), \varphi(Q') \right) \right] dt \tag{15}$$

This equation derives the public key, it involves an isogenic map of base points and leads to sharing of shared parameter, which is not secure in the event that the shared parameter is shared across the insecure communication channels (Eq. 15).

$$V_{iso} = \int^{1} \sqrt{\sum_{\mathrm{i}}^{=1\mathrm{n}} (SS_{\mathrm{i}}^{A} - SS_{\mathrm{i}}^{B})^{2}}\, dt \tag{16}$$

This test is applied to test accuracy by verifying the deviation of independently computed joint secrets which is both sides incur the same key and integrity of communication is achieved (Eq. 16).

B. *Performance metrics: key size, computation time, memory, latency*

The important size efficiency of cryptographic schemes, their computation time, and memory usage and communication latency are also taken into account, with the assistance of performance evaluation, and, as a result, it will be feasible to compare cryptographic schemes in terms of their practicability in the field of implementation and in resource-constrained environments in general.

$$K_{size} = \int^{1} [\, \sum_{\mathrm{i}}^{=1\mathrm{n}} k_{\mathrm{i}} \,]\, dt \tag{17}$$

It is a total key size equation that adds up the key components by domain that determine the storage needs and scaling properties of cryptographic key constructions (Eq. 17).

$$M_{usage} = \int^{1} \sqrt{\sum_{\mathrm{i}}^{=1\mathrm{n}} m_{\mathrm{i}}^{2}}\, dt \tag{18}$$

This step assesses memory utilization by aggregating memory components (root-sum square) that represents the total storage utilization during cryptographic computations and protocol execution procedures (Eq. 18).

$$L_{comm} = \int^{0\,\mathrm{T}} \left[\left(\frac{d(t)}{bw} \right) + \delta \right] dt \tag{19}$$

This equation is used to estimate the latency through the integration of the transmission delay and constant overhead versus time which takes into consideration bandwidth constraints and propagation delays in communication channels (Eq. 19).

$$C_{res} = \int^{0\,\mathrm{T}} \sqrt{T_{comp}^{2} + M_{usage}^{2}}\, dt \tag{20}$$

This step is a model of total resource cost as it involves a combination of computational effort and memory consumption, which gives a single presentation of energy consumption in cryptographic operations (Eq. 20).

$$\Psi_{perf} = \int^{0}{}^{\mathrm{T}} \sqrt{\frac{K_{size}^2}{\left(T_{comp}^2 + L_{comm}^2 + \sum_{i=1}^{n} m_i^2\right)}}\, dt \tag{21}$$

The measure is a quantification of efficiency in relation to key size and a combination of other important computation, latency, and memory metrics, which provides an overall performance measure in cryptographic system optimization (Eq. 21).

C. *ECC–Isogeny Secure Key Exchange Protocol*

The proposed communication protocol is a comparative communication protocol by means of secure keys, which is based on Elliptic Curve Cryptography (ECC) and isogeny-based cryptographic mechanisms for post-quantum secure communication environments. The protocol allows establishment of an authenticated secure session between the sender and receiver entities by performing lightweight ECC operations and isogeny transformations that are quantum resistant.

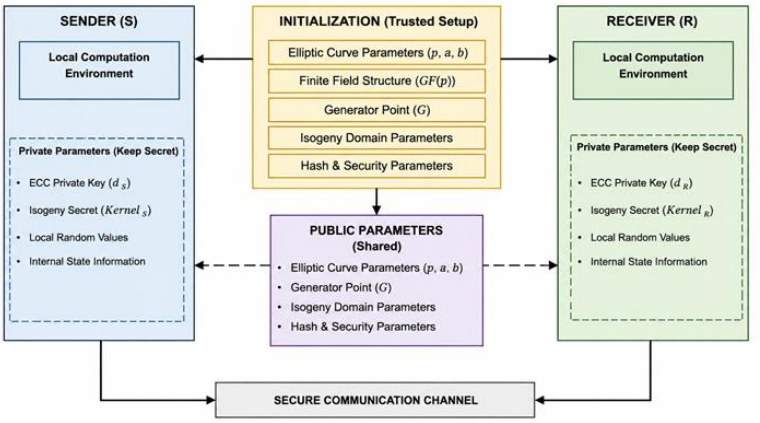


Figure 2

ECC–Isogeny Secure Key Exchange Workflow for Post-Quantum Communication

The system initialization, public/private key generation, exchange of ciphertexts, derivation of shared secret, verification of authentication and establishment of session key steps are included in the framework. The "classical" communication systems that use ECC operations are more efficient, while isogeny-based transformations offer greater resistance to adversarial attacks using quantum computers. In the proposed communication framework, the secure key exchange through the ECC–isogeny is shown in Figure 2. The proposed protocol contains 2 communication entities namely sender S and receiver R in the environment of ECC based and isogeny based cryptography. When initializing, elliptic

curve parameters, finite field structures, generator points and the domain parameters of the isogeny domain are created, which ensure secure communication channels. Public cryptographic parameters are distributed by trusted initialization procedure and private parameters are kept confidential in local computation environments.

IV. Algebraic structure of elliptic curves over finite fields

This chapter describes algebraic properties of elliptic curves on finite fields, group operations, addition of points, multiplication of scalars, and mathematical properties that make elliptic curve cryptography and computationally efficient.

$$E(F_p) = \int^{1} [\, y^2 = x^3 + ax + b \bmod p \,]\, dt \tag{22}$$

$$P + Q = \int^{01} [\, (x^3, y^3)]\, dt \tag{23}$$

The equation illustrates the elliptic curve in finite field Fp which guarantees correct algebraic structure and parameter bounds needed to execute secure cryptographic functionality (Eq. 22). This operation is the addition of two points on an elliptic curve, to generate a third point on the curve, keeping the closure and allowing them to be used in group-based cryptographic operations (Eq. 23).

$$2P = \int^{1} \left[\left(\frac{3x^{12} + a}{2y^{1}}, y^3 \right) \right] dt \tag{24}$$

This equation is a doubling of a point on elliptic curve, calculating tangent-based result, which is a fundamental operation in cryptographic algorithms in calculating scalar multiplication (Eq. 24).

$$G_E = \int^{1} \sqrt{\sum_{\mathrm{i}}^{=1\,\mathrm{n}} P_{\mathrm{i}}^{\,2}}\, dt \tag{25}$$

This procedure checks elliptic curve group properties by summing point magnitudes, which guarantee closure, associativity, identity and invertibility needed to perform secure algebraic operations (Eq. 25).

$$H_{ECDLP} = \int^{1} \sqrt{(Q - kP)^2 + \sum_{\mathrm{i}}^{=1\,\mathrm{n}} r_{\mathrm{i}}^{\,2}}\, dt \tag{26}$$

This equation is a model of difficulty of solving elliptic curve discrete logarithm problem, which is a combination of unknown scalar and randomness, which is highly computational hard against adversarial attacks (Eq. 26).

V. Result and Discussion

Results give comparative analysis of ECC and isogeny schemes, and remark on the performance disparity, security, and trade-offs, and real-world practicability of post-quantum safe communication systems under different circumstances.

Table 1

Comparative Performance Evaluation of ECC and Isogeny-Based Cryptographic Protocols

Metric	ECC-Based Protocol	Isogeny-Based Protocol (SIKE-like)
Key Size (bytes)	32	330
Public Key Size (bytes)	64	564
Private Key Size (bytes)	32	48
Computation Time (ms)	2.8	45.6
Key Exchange Time (ms)	3.5	52.3

In Table 1 of results, it is indicated that the ECC-based protocols are much more efficient than the isogeny-based protocols. Variable sizes, performance and performance comparisons are visualized in Figure 3.

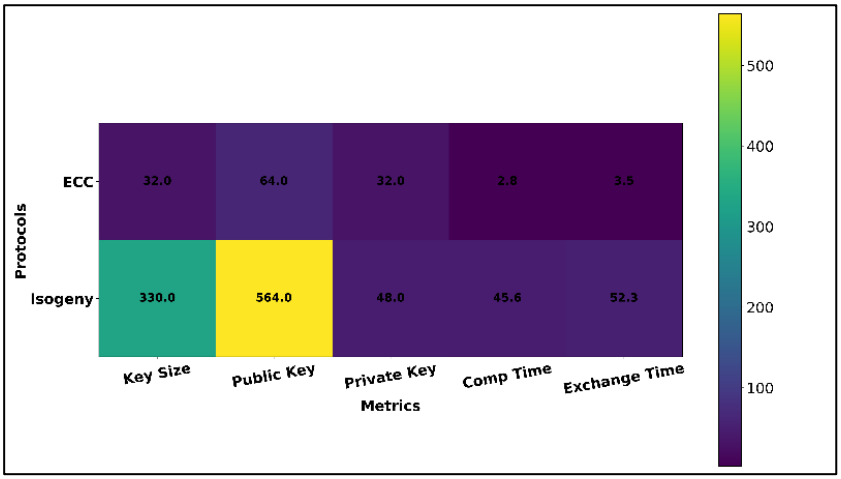


Figure 3

Visualization of Key Size, Performance, and Efficiency Metrics in Cryptographic Protocols

The sizes of key of ECC are very small (32-64 bytes), computation and exchange of key are also very small therefore it is used in real time applications. Conversely, the SIKE-like protocols need large keys and have high computation time, which introduce latency.

Figure 4 indicates the ECC, and isogeny protocol performance. This overhead is however offset with their higher resistance to quantum attacks and it is clear that there is a trade off between the performance efficiency and the post-quantum security assurance.

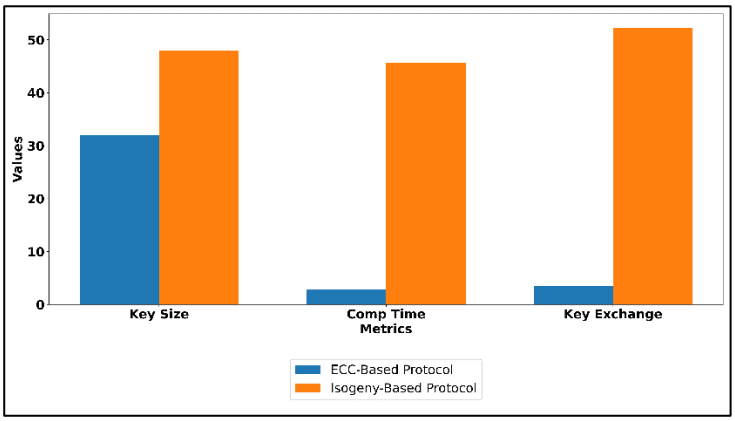


Figure 4
Comparative Performance of ECC-Based and Isogeny-Based Cryptographic Protocols

VI. Conclusion

This was a comparative analysis of isogeny cryptographic protocol and elliptic curve in postquantum secure application. The results indicate that Elliptic Curve Cryptography (ECC) is extremely effective in terms of its speed of computing, memory, and low latency that can be implemented in the current real-time systems. It may however be susceptible to quantum attacks thereby restricting its use in long run. Comparatively, cryptographic constructions that are based on isogeny, especially SIKE-like, are resistant to quantum adversaries to a significant extent, as they are based on mathematical hardness. They are costlier to compute, and they need more resources, but may prove to be a possible solution in the security field. On the whole, the paper discusses the necessity to introduce hybrid crypto-techniques, which are efficient and quantum resistant in order to improve the future safe communication system.

References

[1] 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.

[2] B. Jankowski, K. Szydłowski, M. Niemiec, and P. Chołda, "An Internet messenger using post-quantum cryptography algorithms based on isogenies of elliptic curves," *Electronics*, vol. 14, no. 14, Art. no. 2905 (2025), doi: 10.3390/electronics14142905.

[3] S.Y. Chang and Q. Khan, "Post-quantum cryptography in networking protocols: Challenges, solutions, and future directions," *Cryptography*, vol. 10, no. 1, Art. no. 12 (2026), doi: 10.3390/cryptography10010012.

[4] J.-A. Septien-Hernandez, M. Arellano-Vazquez, M. A. Contreras-Cruz, and J.-P. Ramirez-Paredes, "A comparative study of post-quantum cryptosystems for Internet-of-Things applications," *Sensors*, vol. 22, no. 2, Art. no. 489 (2022), doi: 10.3390/s22020489.

[5] A. Havasi and M. H. Dehkordi, "Enhancing secret sharing security: A verifiable hierarchical threshold model and cheating detection based on integer factorization," *J. Discrete Math. Sci. Cryptogr.*, vol. 29, no. 1, pp. 77–86 (2026), doi: 10.47974/JDMSC-2217.

[6] I. Martinez-Diaz, R. Ali, and M. K. Jamil, "On the search for supersingular elliptic curves and their applications," *Mathematics*, vol. 13, no. 2, Art. no. 188 (2025), doi: 10.3390/math13020188.

[7] S. Li, Y. Chen, L. Chen, J. Liao, C. Kuang, K. Li, W. Liang, and N. Xiong, "Post-quantum security: Opportunities and challenges," *Sensors*, vol. 23, no. 21, Art. no. 8744 (2023), doi: 10.3390/s23218744.

[8] A. U. Abubakar and E. Chandrasekaran, "A new variable step-size hybrid block method for the numerical solution of ordinary differential equations," *J. Interdiscip. Math.*, vol. 29, no. 4, pp. 987–1000 (2026), doi: 10.47974/JIM-2412.

[9] Y. Wen, T. Jin, and W. Li, "Reusable fuzzy extractor from isogeny-based assumptions," *Symmetry*, vol. 17, no. 7, Art. no. 1065 (2025), doi: 10.3390/sym17071065.

[10] R. C. Poonia, T. Singh, C. K. Rajashri, D. Mondal, and S. M. Patil, "Optimizing communication system security through comprehensive testing and intelligent network configurations," *J. Inf. Optim. Sci.*, vol. 47, no. 5-A, pp. 1709–1717 (2026), doi: 10.47974/JIOS-2261.

Received April, 2026