Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas

Eureka Journal of Computing Science & Digital Innovation (EJCSDI)

ISSN 2760-4993 (Online) Volume 2, Issue 3, March 2026

https://eurekaoa.com/index.php/10

ELLIPTICAL CURVE CRYPTOGRAPHY AND POST-QUANTUM CRYPTOGRAPHIC MODEL BASED ON ISOGENY IN A QUANTUM COMPUTING ENVIRONMENT

Muhamediyeva D. T.
Tagayev F. A.
Tashkent Institute of Irrigation and Agricultural
Mechanization Engineers National Research University

Abstract

This paper studies the modeling of elliptic curve cryptography and isogeny-based algorithms in a quantum computing environment, which play an important role in the post-quantum cryptography paradigm. In the study, the operations of adding and doubling points on an elliptic curve are mathematically analyzed and implemented using the Python programming language. In addition, a quantum scheme based on the Qiskit platform was developed to simulate the quantum computing environment. The model describes a simplified view of the isogeny mapping process using quantum superposition and nonlinear transformations. The proposed model was tested on a local quantum simulator and the results were analyzed using a probability distribution. The results obtained demonstrate the possibility of modeling elliptic curve-based cryptographic algorithms in a quantum environment and provide an important theoretical basis for post-quantum cryptography research.

Keywords: Post-quantum cryptography, elliptic curve cryptography, SIKE, quantum computing, Qiskit, isogeny maps, quantum simulation, quantum schemes.

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Computing Science & Digital Innovation (EJCSDI)
ISSN 2760-4993 (Online) Volume 2, Issue 3, March 2026

https://eurekaoa.com/index.php/10

Introduction

Cryptographic algorithms play an important role in modern information security systems. Most traditional cryptographic systems are based on complex mathematical problems, among which the prime factorization and discrete logarithm problems occupy a central place. However, the rapid development of quantum computing technologies poses a serious threat to the stability of these algorithms. In particular, it has been theoretically proven that many classical cryptographic systems can be effectively broken using quantum algorithms. Therefore, in recent years, a new direction has been formed, called post-quantum cryptography. This direction is aimed at creating cryptographic algorithms that are resistant to attacks by quantum computers. Among such algorithms are lattice-based, code-based, multivariable polynomial-based, and isogeny-based cryptographic systems. In particular, algorithms based on the elliptic curve isogeny problem have a high level of mathematical complexity and are considered one of the promising directions in the field of post-quantum cryptography. Elliptic curve cryptography (ECC) is characterized by providing a high level of security with smaller key sizes compared to traditional cryptographic systems. In ECC systems, the main mathematical operations are the addition and multiplication of points on the elliptic curve, which are implemented based on modular arithmetic. In cryptographic systems based on isogenies, special morphisms between elliptic curves are used [1-4].

In this study, the operation of adding points on the elliptic curve was mathematically modeled and implemented algorithmically using the Python programming language. In addition, a quantum scheme was developed based on the Qiskit platform to simulate the quantum computing environment. This scheme represents a simplified model of the isogeny mapping process using quantum superposition and quantum gates. The scientific novelty of this study is as follows: The main mathematical operations of elliptic curve cryptography were modeled algorithmically using the Python programming environment. A

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Computing Science & Digital Innovation (EJCSDI)
ISSN 2760-4993 (Online) Volume 2, Issue 3, March 2026

https://eurekaoa.com/index.php/10

simplified model representing post-quantum cryptographic mechanisms based on isogeny through quantum schemes was proposed. A method for modeling cryptographic processes based on quantum superposition and entanglement properties was developed using the Qiskit platform. The proposed model was tested in a quantum simulator and its performance was analyzed using probability distributions. The research results offer a new experimental approach for studying post-quantum cryptographic algorithms in a quantum computing environment [5-9]. The proposed approach allows modeling cryptographic systems based on elliptic curves in a quantum computing environment and creates an important experimental platform for studying post-quantum cryptographic algorithms. The research results are analyzed using probability distributions obtained using a quantum simulator [10-12].

2. Methods

Elliptic curve cryptography (ECC) is a cryptographic system based on the complexity of the discrete logarithm problem over an elliptic curve. The elliptic curve is defined by the following general equation [13-15]:

$y^2 = x^3 + ax + b$,

here

a and b – curve parameters,

x and y – the coordinates of a point on the curve.

For the curve to be correctly defined, the discriminant must not be zero:

$4a^3 + 27b^2 \neq 0$.

In cryptographic applications, elliptic curves are often defined over a finite field F_p. For example, for a field of prime numbers, the curve is written as:

$y^2 \equiv x^3 + ax + b \pmod{p}$,

here p – is a prime number.

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Computing Science & Digital Innovation (EJCSDI)
ISSN 2760-4993 (Online) Volume 2, Issue 3, March 2026

https://eurekaoa.com/index.php/10

The basic operation in the ECC system is to add these points. If there are two points on the curve:

$P(x_1, y_1), \quad Q(x_2, y_2)a$,

then their sum $R = P + Q$ is determined by the following formulas.

If $P \neq Q$:

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \pmod p,$$

$$x_3 = \lambda^2 - x_1 - x_2 \pmod p,$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \pmod p.$$

The result is a new point $R(x_3, y_3)$.

If $P = Q$ so, that is, the point is added to itself, the following formula is used:

$$\lambda = \frac{3x_1^2 + a}{2y_1} \pmod p,$$

$$x_3 = \lambda^2 - 2x_1 \pmod p,$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \pmod p.$$

As a result,

$R = 2P$

it will be produced.

For example, parameters

$a = 2, \quad p = 17$

and starting point

$P = (5,1)$

the algorithm calculates twice the point.

The SIKE (Supersingular Isogeny Key Encapsulation) algorithm works on isogenies between supersingular elliptic curves. An isogeny is an algebraic morphism between two elliptic curves that preserves the structure of a point group.

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Computing Science & Digital Innovation (EJCSDI)
ISSN 2760-4993 (Online) Volume 2, Issue 3, March 2026

https://eurekaoa.com/index.php/10

If
E_1 and E_2
are elliptic curves, the isogeny is determined by the following map:
$\phi : E_1 \to E_2$.
This map has the following properties:
1. Preserves the group operation
2. Is represented by an algebraic function
3. Has a set of points called the kernel
In the SIKE algorithm, the initial curve is obtained in the following form:
$E_0 : y^2 = x^3 + Ax + B$
and the area is defined on
F_{p^2}
where a prime number of the form
$p = 2^a 3^b - 1$
is used.
Two users—Alice and Bob—follow these steps.

Alice
1.Chooses a private key
1. $m_A \in [1,2^a]$.
2.Isogeny builds
$\phi_A : E_0 \to E_A$.
3.Sends the following as a public key
$\left(E_A, \phi_A(P_B), \phi_A(Q_B)\right)$.

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Computing Science & Digital Innovation (EJCSDI)
ISSN 2760-4993 (Online) Volume 2, Issue 3, March 2026

https://eurekaoa.com/index.php/10

Bob

1.Selects a secret key

$m_B \in [1,3^b]$.

2. Isogeny builds

$\phi_B : E_0 \to E_B$.

3.Sends as a public key

$\left(E_B, \phi_B(P_A), \phi_B(Q_A)\right)$.

The parties will use the isogeny results sent to each other to generate the following general curve:

$E_{AB} = \phi_A\left(\phi_B(E_0)\right)$.

As a result

$j(E_{AB})$,

used as an invariant public secret $j-$key.

In the created program, the SIKE process is modeled in a simplified way through a quantum scheme. The Hadamard gate creates a superposition state. The CNOT gate creates a quantum entanglement. This process leads to the following quantum state:

$$|\psi\rangle = \frac{|000\rangle + |110\rangle}{\sqrt{2}}.$$

This situation gives a quantum probability distribution and represents a quantum modeled view of the isogeny process. In the proposed model, the quantum computing process is modeled using the Qiskit platform. The quantum scheme is built on the basis of a quantum register consisting of three qubits. This scheme represents a simplified quantum model of the isogeny process based on an elliptic curve.

The quantum scheme consists of the following main steps:

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Computing Science & Digital Innovation (EJCSDI)
ISSN 2760-4993 (Online) Volume 2, Issue 3, March 2026

https://eurekaoa.com/index.php/10

1.Creating a quantum register

The quantum system consists of three qubits, which are defined as follows:

$|q_0\rangle,|q_1\rangle,|q_2\rangle$.

Initially, all qubits are in the ground state:

$|000\rangle$.

2.Creating a superposition

A Hadamard gate is applied to the first qubit. This operation puts the qubit into a superposition state:

$$H|0\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}.$$

As a result, the system state will be as follows:

$$|\psi_1\rangle = \frac{|000\rangle+|110\rangle}{\sqrt{2}}.$$

3.Quantum Entanglement

The next step is to use a CNOT (Controlled-NOT) gate. This gate uses the first qubit as the control qubit and the second qubit as the target qubit. If the control qubit is 1, the second qubit is changed.

As a result, the system enters the following entangled state:

$$|\psi_2\rangle = \frac{|000\rangle+|110\rangle}{\sqrt{2}}.$$

This creates a probability distribution in the quantum system.

4.Measurement process

In the final step, all qubits are measured to the classical register

$|q_0,q_1,q_2\rangle \rightarrow c_0,c_1,c_2$.

O‘lchash natijasida kvant tizimi ehtimollik asosida klassik bitlar ketma-ketligiga kollaps qiladi.

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Computing Science & Digital Innovation (EJCSDI)
ISSN 2760-4993 (Online) Volume 2, Issue 3, March 2026

https://eurekaoa.com/index.php/10

As a result of the measurement, the quantum system collapses into a classical bit sequence based on probability.

3. Experimental results

The proposed quantum model was tested on a local quantum simulator using Qiskit Aer qasm_simulator. During the simulation, the scheme was executed 1024 times. According to the expected theoretical result, the system can be in the following states: |000⟩| and |110⟩. Each state has approximately equal probability (Table 1).

Table 1

Simulation results table

Quantum state	Measurement	Probability
000	512	0.50
110	512	0.50

The results confirm the existence of superposition and entanglement in a quantum system. The simulation results show the following conclusions: Superposition property -

The Hadamard gate allows a qubit to exist in two states at the same time. Quantum entanglement - The CNOT gate creates quantum entanglement between qubits. Probability distribution - The measurement results are equally distributed between the two quantum states. These results confirm the theoretically correct operation of the proposed quantum model and demonstrate the possibility of modeling elliptic curve-based cryptographic processes in a quantum computing environment.

This study considers the issue of modeling elliptic curve cryptography and isogeny-based post-quantum cryptographic mechanisms in a quantum computing environment. In the proposed model, the operations of adding and doubling points on the elliptic curve were implemented in the Python programming language, and

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Computing Science & Digital Innovation (EJCSDI)
ISSN 2760-4993 (Online) Volume 2, Issue 3, March 2026

https://eurekaoa.com/index.php/10

the Qiskit platform was used to simulate quantum processes. The simulation results showed that the quantum scheme works in accordance with the theoretical model. As a result of the application of the Hadamard gate in the quantum system, the qubit entered a superposition state, which ensured the simultaneous existence of several possible states. At the next stage, quantum entanglement was created between the qubits using the CNOT gate. As a result of this process, the system acquired a probability distribution in the combinations of two main states - $|000\rangle$ and $|110\rangle$.

The results obtained show that elliptic curve-based cryptographic processes can be modeled in a quantum computing environment. In particular, modeling cryptographic mechanisms based on isogeny through quantum schemes allows for a deeper study of the theoretical properties of post-quantum cryptographic algorithms. The results of the study also indicate the need to reconsider cryptographic systems based on new security paradigms with the development of quantum computing technologies. Post-quantum cryptographic algorithms, including mechanisms based on isogeny, are one of the promising directions for ensuring a high level of security even in the conditions of quantum computers.

4. Conclusion

This study investigated the modeling of elliptic curve cryptography and post-quantum cryptographic systems based on isogeny in a quantum computing environment. During the study, the operations of adding and doubling points on an elliptic curve were mathematically analyzed and implemented algorithmically in the Python programming language. A quantum scheme was developed based on the Qiskit platform, and a simplified model of the isogeny process was created using the properties of superposition and quantum dependence. The proposed quantum scheme was tested using a local quantum simulator, and the results were analyzed using a probability distribution. The results obtained confirmed the possibility of modeling elliptic curve-based cryptographic systems in a quantum

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Computing Science & Digital Innovation (EJCSDI)
ISSN 2760-4993 (Online) Volume 2, Issue 3, March 2026

https://eurekaoa.com/index.php/10

computing environment. The results of the study serve as an important theoretical basis for developing new algorithmic models in the field of post-quantum cryptography and studying cryptographic systems in a quantum environment. In the future, this research will involve creating more complex quantum schemes, conducting experiments on real quantum devices, and conducting a more in-depth analysis of the effectiveness of isogeny-based cryptographic algorithms in a quantum environment.

References

1. Shor, P.W., 1997. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 26(5), pp.1484–1509.
2. Bernstein, D.J., Lange, T., 2017. Post-quantum cryptography. Nature, 549(7671), pp.188–194.
3. Jao, D., De Feo, L., 2011. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. Post-Quantum Cryptography, pp.19–34.
4. De Feo, L., Jao, D., Plût, J., 2014. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. Journal of Mathematical Cryptology, 8(3), pp.209–247.
5. Childs, A.M., Van Dam, W., 2010. Quantum algorithms for algebraic problems. Reviews of Modern Physics, 82(1), pp.1–52.
6. Nielsen, M.A., Chuang, I.L., 2010. Quantum Computation and Quantum Information. Cambridge University Press.
7. Arute, F. et al., 2019. Quantum supremacy using a programmable superconducting processor. Nature, 574, pp.505–510.
8. Preskill, J., 2018. Quantum computing in the NISQ era and beyond. Quantum, 2, 79.

Eureka Open Access Journals
Open Access | Peer Reviewed | International Journals | Multidisciplinary Areas
Eureka Journal of Computing Science & Digital Innovation (EJCSDI)
ISSN 2760-4993 (Online) Volume 2, Issue 3, March 2026

https://eurekaoa.com/index.php/10

9. Chen, L., Jordan, S., Liu, Y.K., Moody, D., Peralta, R., Perlner, R., Smith-Tone, D., 2016. Report on post-quantum cryptography. NIST Interagency Report.
10. Galbraith, S.D., 2018. Mathematics of Public Key Cryptography. Cambridge University Press.
11. De Feo, L., 2017. Mathematics of isogeny based cryptography. arXiv preprint arXiv:1711.04062.
12. Aggarwal, D., Brennen, G.K., Lee, T., Santha, M., Tomamichel, M., 2017. Quantum attacks on Bitcoin, and how to protect against them. Ledger, 3, pp.68–90.
13. Wootters, W.K., Zurek, W.H., 1982. A single quantum cannot be cloned. Nature, 299, pp.802–803.
14. Gottesman, D., 1998. The Heisenberg representation of quantum computers. Group22: Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics.
15. Farhi, E., Goldstone, J., Gutmann, S., 2014. A quantum approximate optimization algorithm. arXiv preprint arXiv:1411.4028.