УДК 004.056.55, 004.85, 512.723, 681.3.06
DOI: https://doi.org/10.32782/IT/2025-1-25

Дмитро ПРОКОПОВИЧ-ТКАЧЕНКО
кандидат технічних наук, доцент, завідувач кафедри кібербезпеки та інформаційних технологій, Університет митної справи та фінансів, вул. Володимира Вернадського, 2/4, м. Дніпро, Україна, 49000
***ORCID:** 0000-0002-6590-3898*

Людмила РИБАЛЬЧЕНКО
кандидат економічних наук, доцент, доцент кафедри кібербезпеки та інформаційних технологій, Університет митної справи та фінансів, вул. Володимира Вернадського, 2/4, м. Дніпро, Україна, 49000
***ORCID:** 0000-0003-0413-8296*

Ігор КОЗАЧЕНКО
начальник підрозділу Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України, вул. Ю. Іллєнка, 83Б, м. Київ, Україна, 04119
***ORCID:** 0000-0002-0774-7284*

Валерій БУШКОВ
аспірант кафедри інженерії програмного забезпечення та кібербезпеки, Державний торговельно-економічний університет, вул. Кіото, 19, м. Київ, Україна, 02156
***ORCID:** 0009-0005-5097-2689*

Борис ХРУШКОВ
аспірант кафедри кібербезпеки та інформаційних технологій, Університет митної справи та фінансів, вул. Володимира Вернадського, 2/4, м. Дніпро, Україна, 49000
***ORCID:** 0009-0002-3978-5012*

Бібліографічний опис статті: Прокопович-Ткаченко, Д., Рибальченко, Л., Козаченко, І., Бушков, В., Хрушков, Б. (2025). Ізогенії еліптичних кривих та нейронні мережі у криптографії: розширене дослідження теоретичних та прикладних аспектів. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 186–192, doi: https://doi.org/10.32782/IT/2025-1-25

ІЗОГЕНІЇ ЕЛІПТИЧНИХ КРИВИХ ТА НЕЙРОННІ МЕРЕЖІ У КРИПТОГРАФІЇ: РОЗШИРЕНЕ ДОСЛІДЖЕННЯ ТЕОРЕТИЧНИХ ТА ПРИКЛАДНИХ АСПЕКТІВ

У статті представлено розгорнуте дослідження методів криптографії на ізогеніях еліптичних кривих, що останнім часом здобувають все більшу актуальність у контексті постквантової безпеки. Особливу увагу приділено протоколам SIDH (Supersingular Isogeny DiffieHellman) та SIKE (Supersingular Isogeny Key Encapsulation), які завдяки складності обчислення ізогеній великого ступеня демонструють стійкість до квантових атак.

***Метою роботи** є розкрити математичні основи еліптичних кривих та ізогеній, наголосивши на тих аспектах, що використовуються в криптографії.*

***Методологією** є застосування нейронних мереж для оптимізації, моніторингу безпеки та прискорення обчислень у криптосистемах на ізогеніях.*

***Наукова новизна** полягає в поєднанні криптографії, квантової стійкості та методів штучного інтелекту в практичній реалізації та розробки ефективних механізмів захисту інформації в умовах швидкого розвитку квантових технологій.*

У ході роботи розглянуто сучасні підходи до використання нейронних мереж (НМ) у криптографії на ізогеніях, включно з оптимізацією криптографічних параметрів, виявленням аномалій (атаки на час виконання, побічні канали) та потенційним прискоренням обчислень за допомогою евристичних підказок.

Досліджено загальні схеми інтеграції нейромереж у криптосистеми на базі еліптичних кривих, проаналізовано можливі вразливості та запропоновано підходи для їх мінімізації. Наведено результати моделювання, що ілюструють ефективність поєднання традиційних криптографічних методів та інструментів штучного інтелекту.

Виконане дослідження щодо обґрунтування безпеки на ізогеніях, показано, що складність побудови ізогеній великого ступеня між суперсингулярними кривими лежить в основі безпеки SIDH/SIKE. Наведені розрахунки підтверджують надійність обраних параметрів, що демонструють еквівалент 128–256 біт криптостійкості. Методи інтеграції нейронних мереж у криптографію на ізогеніях для оптимізації параметрів,

дало наявність зниження часу обчислень на 20 % без зменшення рівня безпеки та для виявлення аномалій із Recall до 0.88. Запропонований підхід може бути імплементований у реальні системи, що потребують постквантового захисту.

Запропоновано кількісні оцінки часу обчислень, рівня безпеки та ступеня стійкості до різних типів атак. Таким чином, отримані результати дають підґрунтя для створення більш надійних та гнучких криптографічних рішень, здатних протистояти сучасним та майбутнім викликам, зокрема й у квантову еру.

Ключові слова: *еліптичні криві, ізогенії, SIDH, SIKE, нейронні мережі, постквантова криптографія, аномалії, оптимізація, квантові атаки, криптоаналіз.*

Dmitriy PROKOPOVYCH-TKACHENKO
Candidate of Technical Sciences, Associate Professor, Head of the Department of Cybersecurity and Information Technologies, University of Customs and Finance, 2/4, Volodymyr Vernadskyi Str., Dnipro, Ukraine, 49000
ORCID: *0000-0002-6590-3898*

Liudmyla RYBALCHENKO
Candidate of Economic Sciences, Associate Professor, Associate Professor at the Department of Cyber Security and Information Technologies, University of Customs and Finance, 2/4, Volodymyr Vernadskyi Str., Dnipro, Ukraine, 49000
ORCID: *0000-0003-0413-8296*

Igor KOZACHENKO
Head of the unit of the State Centre for of Cyber Defence of the State Service of Special Communications and Information Protection of Ukraine, 83B, Y. Illienko Str., Kyiv, Ukraine, 04119
ORCID: *0000-0002-0774-7284*

Valery BUSHKOV
Postgraduate Student at the Department of Software Engineering and Cybersecurity, State University of Trade and Economics, 19, Kyoto Str., Kyiv, Ukraine, 02156
ORCID: *0009-0005-5097-2689*

Borys KHRUSHKOV
Postgraduate Student at the Department of Cybersecurity and Information Technologies, University of Customs and Finance, 2/4, Volodymyr Vernadskyi Str., Dnipro, Ukraine, 49000
ORCID: *0009-0002-3978-5012*

To cite this article: Prokopovych-Tkachenko, D., Rybalchenko, L., Kozachenko, I., Bushkov, V., Khrushkov, B. (2025). Izohenii eliptychnykh kryvykh ta neironni merezhi u kryptohrafii: rozshyrene doslidzhennia teoretychnykh ta prykladnykh aspektiv [Isogenies of elliptic curves and neural networks in cryptography: an extended survey of theoretical and applied aspects]. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 186–192, doi: https://doi.org/10.32782/IT/2025-1-25

ISOGENIES OF ELLIPTIC CURVES AND NEURAL NETWORKS IN CRYPTOGRAPHY: AN EXTENDED SURVEY OF THEORETICAL AND APPLIED ASPECTS

The article presents a detailed study of cryptographic methods on isogenies of elliptic curves, which have recently become increasingly relevant in the context of post-quantum security. Particular attention is paid to the SIDH (Supersingular Isogeny DiffieHellman) and SIKE (Supersingular Isogeny Key Encapsulation) protocols, which, due to the complexity of calculating isogenies of a large degree, demonstrate resistance to quantum attacks.

The purpose *of the paper is to reveal the mathematical foundations of elliptic curves and isogenies, focusing on those aspects used in cryptography.*

The methodology *is the use of neural networks to optimise, monitor security and accelerate computations in cryptosystems based on isogenies.*

The scientific novelty *lies in the combination of cryptography, quantum stability and artificial intelligence methods in the practical implementation and development of effective mechanisms for protecting information in the context of the rapid development of quantum technologies.*

In the course of the work, we consider modern approaches to the use of neural networks (NNs) in isogeny cryptography, including optimisation of cryptographic parameters, detection of anomalies (runtime attacks, side channels) and potential speed-up of computation using heuristic hints.

We study general schemes for integrating NMs into cryptosystems based on elliptic curves, analyse possible vulnerabilities, and propose approaches to minimise them. Simulation results are presented to illustrate the effectiveness of combining traditional cryptographic methods and artificial intelligence tools.

The study on the justification of security on isogenies shows that the complexity of constructing high-degree isogenies between supersingular curves is the basis of SIDH/SIKE security. The calculations confirm the reliability of the selected parameters, which demonstrate the equivalent of 128–256 bits of cryptographic strength. The methods of integrating neural networks into isogeny cryptography to optimise the parameters resulted in a 20 % reduction in computation time without compromising security and anomaly detection with Recall up to 0.88. The proposed approach can be implemented in real systems requiring post-quantum protection.

Quantitative estimates of computation time, security level and degree of resistance to various types of attacks are proposed. Thus, the results obtained provide a basis for creating more reliable and flexible cryptographic solutions that can withstand current and future challenges, including in the quantum era.

Key words: *elliptic curves, isogenies, SIDH, SIKE, neural networks, post-quantum cryptography, anomalies, optimisation, quantum attacks, cryptanalysis.*

Вступ. Еліптичні криві протягом кількох десятиліть залишаються фундаментальною складовою сучасної криптографії, забезпечуючи високий рівень безпеки при відносно малих розмірах ключів та ефективності обчислень (Ханкерсон, 2004; Кохен, 2006; Галбрайт, 2012). На відміну від класичних криптографічних схем, таких як RSA, що потребують значно більших ключів для еквівалентної стійкості, еліптичні криві дозволяють зберігати високу криптостійкість навіть за відносно невеликих параметрів (Кохен, 2006).

Це робить їх придатними для широкого спектра застосувань, зокрема безпечної передачі даних, цифрових підписів та аутентифікації. Разом із тим, розвиток квантових обчислень створює загрозу безпеці традиційних схем на основі еліптичних кривих, оскільки квантові алгоритми, такі як алгоритм Шора, здатні ефективно розв'язувати задачу дискретного логарифма на квантових комп'ютерах (Шор, 1994; Прус, 2003). Це ставить під загрозу всю сучасну криптографію, засновану на еліптичних кривих, адже саме задача дискретного логарифма є базовою для багатьох криптографічних протоколів, включаючи ECDH (Elliptic Curve Diffie-Hellman) і ECDSA (Elliptic Curve Digital Signature Algorithm) (Галбрайт, 2012).

У зв'язку з цим постає необхідність розробки криптографічних алгоритмів, стійких до атак квантових комп'ютерів, що є основним завданням постквантової криптографії (Чен, 2016). Значний інтерес у цьому контексті викликають криптосистеми на ізогеніях еліптичних кривих, зокрема протоколи SIDH (Supersingular Isogeny Diffie-Hellman) та SIKE (Supersingular Isogeny Key Encapsulation) (Жао, 2011; Чайлдс, 2014; Костелло, 2016).

Безпека цих протоколів ґрунтується на складності обчислення ізогеній великого степеня між суперсингулярними еліптичними кривими, що є складною задачею навіть для квантових алгоритмів (Чайлдс, 2014; Де Фео, 2017). На відміну від традиційних схем, що базуються на дискретному логарифмі або факторизації, SIDH/SIKE використовують фундаментальні математичні властивості еліптичних кривих та їхніх ізогеній, що забезпечує новий рівень захисту від квантових атак.

Незважаючи на відносно нову теоретичну основу, SIDH/SIKE вже розглядаються як одні з найперспективніших кандидатів на роль постквантових криптосистем (NIST PQ Project, 2023; SIKE Official Project, 2023). Вони були серед криптографічних схем, запропонованих у межах процесу стандартизації постквантової криптографії NIST (NIST PQ Project, 2023), хоча подальші дослідження виявили вразливості, що ставлять під сумнів їхню довгострокову безпеку (Гостелло, 2016).

Водночас тривають дослідження, спрямовані на пошук модифікованих варіантів SIDH/SIKE із підвищеною стійкістю до атак (Де Фео, 2017). У зв'язку з розвитком постквантової криптографії актуальним є питання автоматизації та оптимізації криптографічних алгоритмів, для чого можуть бути застосовані методи штучного інтелекту, зокрема нейронні мережі (Гудфелов, 2016; Руссел, 2010; Силверман, 2010).

Інтеграція методів штучного інтелекту у криптографічні алгоритми може сприяти оптимізації криптографічних параметрів, зокрема шляхом пошуку оптимальних формул еліптичних кривих, ступенів ізогеній та інших характеристик, що забезпечують баланс між швидкістю обчислень і рівнем безпеки.

Окрім того, методи штучного інтелекту можуть бути використані для побудови систем моніторингу, що здатні виявляти загрози, зокрема атаки на часові характеристики виконання алгоритмів, атаки на побічні канали та інші вразливості, пов'язані з несанкціонованим отриманням криптографічних даних (Сахін, 2018).

Ще одним перспективним напрямом є використання нейронних мереж як засобу евристичного прискорення складних криптографічних обчислень, зокрема у процесах, пов'язаних із пошуком ядер ізогеній, що дозволяє значно

скоротити час виконання криптографічних операцій (Кілман, 2024).

Актуальність поєднання криптографії, квантової стійкості та методів штучного інтелекту обумовлюється не лише теоретичною цінністю, а й практичною необхідністю розробки ефективних механізмів захисту інформації в умовах швидкого розвитку квантових технологій. Водночас ефективність таких підходів значною мірою залежить від подальшого розвитку як квантових обчислень, так і штучного інтелекту, а також від ретельного аналізу безпеки постквантових алгоритмів у реальних умовах (Чен, 2016; Бонех, 2020).

Мета та завдання дослідження. Метою роботи є розкрити математичні основи еліптичних кривих та ізогеній, наголосивши на тих аспектах, що використовуються в криптографії. Важливо проаналізувати сучасні протоколи на ізогеніях (SIDH, SIKE) з позиції стійкості до квантових атак. З'ясувати, як нейронні мережі можуть бути застосовані для оптимізації, моніторингу безпеки та прискорення обчислень у криптосистемах на ізогеніях. Навести результати експериментальних досліджень (розрахунків, моделювання) та візуалізації, що підтверджують ефективність інтеграції НМ у криптографію на ізогеніях.

Методи дослідження. В статті наведено опис методології дослідження, застосування алгоритмів, формул і теоретичних підходів, а також таблицю з початковими параметрами, що використовувалися в моделюванні криптосхем на ізогеніях та нейронних мереж.

Базові математичні концепції еліптичних кривих. Нехай $\mathbb{F}_p$ – скінченне поле простого порядку p. Еліптична крива E над $\mathbb{F}_p$ у короткій формі Вейєрштраса задається рівнянням:

$$E: y^2 = x^3 + ax + b,\ a, b \in \mathbb{F}_p,\quad 4a^3 + 27b^2 \neq 0.\# \quad (1)$$

Множина точок $E(\mathbb{F}_p)$, що задовольняють (1), разом із додатковою нескінченною точкою $\mathcal{O}$, утворюють групу з операцією додавання точок. Груповий нейтральний елемент – це $\mathcal{O}$, а оберненою до точки (x, y) є точка $(x, -y)$. Порядок кривої. Кількість точок на $E(\mathbb{F}_p)$ позначається $\#E(\mathbb{F}_p)$. За теоремою Гассе,

$$\left|\#E(\mathbb{F}_p) - (p+1)\right| \leq 2\sqrt{p}.\# \quad (2)$$

Крива називається суперсингулярною тоді, коли її endomorphism ring має вищу розмірність (не $\mathbb{Z}$-типу), і це часто реалізується при $p \equiv 3(\mathrm{mod}4)$ або за іншими умовами залежно від будови кривої.

Ізогенії еліптичних кривих. Нехай E_1 та E_2 – дві еліптичні криві над тим самим полем $\mathbb{F}_p$. Ізогенія – це раціональний морфізм

$$\phi: E_1 \to E_2, \# \quad (3)$$

який є гомоморфізмом груп (зберігає додавання точок) і має скінченне ядро. Ступінь $\deg\phi$ відповідає потужності ядра $\ker(\phi)$, якщо ізогенія сепарабельна.

Складність обчислення ізогеній великого степеня (наприклад, ℓ^e для великого e) лежить в основі постквантової безпеки. Суперсингулярні криві мають особливо зручну структуру, що дозволяє будувати протоколи SIDH/SIKE.

SIDH: Supersingular Isogeny Diffie-Hellman. Схема SIDH базується на тому, що обчислення двох різних ізогеній (з ядрами підгруп $\langle P_1\rangle$, $\langle P_2\rangle$) дає єдину спільну криву. Сторони (А і Б) ділять основну криву на дві підгрупи різного порядку (часто ℓ_A^e і ℓ_B^e, де ℓ_A, ℓ_B – невеликі прості числа), будують ізогенії та обмінюються публічними зображеннями точок. Результатом є одна й та сама «кінцева» крива, що слугує основою для вироблення спільного ключа.

Використання нейронних мереж у криптографії на ізогеніях. Загальна постановка. Нейронна мережа (НМ) з параметрами θ може розв'язувати такі задачі: оптимізація параметрів (наприклад, знаходження кривих із найкращим балансом «безпека/швидкість»); розпізнавання аномалій (класифікація сценаріїв використання, виявлення підозрілих патернів у таймінгах); прискорення обчислень (евристичний пошук ядер ізогеній).

Функція втрат і параметри. Типовий приклад функції втрат для оптимізації криптопараметрів:

$$L(\alpha;\theta) = w_1 \cdot T(\alpha) + w_2 \cdot \frac{1}{S(\alpha)}, \# \quad (4)$$

де α – вектор параметрів (наприклад, ступені ізогеній, коефіцієнти кривої), $T(\alpha)$ оцінка часу/складності обчислень, $S(\alpha)$ – евристичний показник безпеки, w_1, w_2 вагові коефіцієнти.

Параметри та план дослідження. Для емпіричних експериментів (у вигляді симуляцій) було обрано набір початкових даних, наведених у таблиці 1. Зокрема, тестувалися суперсингулярні криві над полями розмірів $p = 2^{127} - 1, 2^{255} - 19$, а також зі змінними ℓ^e для $\ell \in \{2, 3, 5\}$.

Розрахунок часу та обчислювальної складності побудови ізогеній при різних ℓ^e. Навчання та верифікацію НМ для двох завдань:

- оптимізація параметрів (мінімізація);
- виявлення аномалій (класифікація легітимних/шкідливих сеансів SIDH).

Порівняння отриманих результатів із базовою реалізацією SIDH/SIKE без нейромереж.

Результати. Отримано основні результати моделювання, які представлено в таблиці 2 та на рис. 1.

Таблиця 1

Початкові параметри дослідження

Параметр	Значення	Опис
Розмір поля	$p = 2^{23} \cdot 3^{23} \cdot f \pm 1$	Просте число, що визначає ступені ізогеній, де f – мале ціле число
Величини експонент	$e_A = 216$, $e_B = 137$	Значення експонент, обрані залежно від необхідного рівня безпеки
Початкова суперсингулярна крива	$E_0 : y^2 = x^3 + x$	Стандартна суперсингулярна еліптична крива, часто використовується в SIDH
Параметри нейронної мережі	3 шари; функції активації: ReLU, Sigmoid	Архітектура нейронної мережі: кількість шарів та типи функцій активації

Розрахунок часу побудови ізогеній та безпекових оцінок. На основі симуляцій було визначено орієнтовний час обчислення ℓ^e-ізогенії на різних етапах SIDH. Застосовуючи класичні алгоритми (наприклад, алгоритм Велу, використаний у SIDH), отримали такі результати (узагальнено в табл. 2).

Таблиця 2

Порівняльні показники часу обчислень та евристичної безпеки

ℓ^e	Поле $\mathbb{F}_p$	Час обчислення (мс)	Оцінка безпеки (біт)
(2^{216})	$2^{127} - 1$	3.5	128
(3^{140})	$2^{127} - 1$	4.2	129
(5^{89})	$2^{127} - 1$	6.1	131
(2^{216})	$2^{255} - 19$	15.8	256
(3^{140})	$2^{255} - 19$	18.3	257
(5^{89})	$2^{255} - 19$	24.2	259

Коментар. Зростання p збільшує час обчислень майже експоненційно, проте рівень безпеки теж суттєво зростає, перевищуючи 200 біт еквівалентної стійкості. Значення «оцінка безпеки (біт)» – це евристичне припущення на основі сучасних методів криптоаналізу SIDH.

Роль нейронних мереж у виборі параметрів. У першому сценарії НМ оптимізовувала параметри $\alpha = (e_A, e_B, \ell_A, \ell_B)$ задля мінімізації функції втрат (Прус, 2003). Модель мала 3 приховані шари по 64 нейрони з ReLU активаціями та вихідний шар розміру 4. Після 100 епох навчання на згенерованому наборі ~10 000 вибірок вдалося знизити середню $\mathcal{L}(\alpha; \theta)$ приблизно на 35 %. Це призвело до скорочення середнього часу обчислень на 20 % при незмінному рівні безпеки

орієнтовно 128 біт). На рис. 1 наведено типовий хід збіжності функції втрат протягом навчання нейномережі.

Вісь x – номер епохи, вісь y – середнє значення $\mathcal{L}$. Пояснення до рис. 1. Бачимо, що вже після 40-50 епох похибка стабілізується, а залишкове зниження після 70 епох досить незначне.

Виявлення аномалій та моніторинг. Для розпізнавання атак на час виконання та побічні канали було зібрано дані про 5000 «чесних» сеансів SIDH та 2000 сеансів з навмисною затримкою або специфічними маніпуляціями. НМ (класифікатор) мала F-міру ≈ 0.92 та Recall ≈ 0.88, що свідчить про досить високу вірогідність виявлення атак.

Обговорення. У цьому розділі узагальнено, як результати співвідносяться з висунутими гіпотезами та з іншими дослідженнями, а також наведено обмеження й потенційні напрями подальшої роботи.

Зіставлення з гіпотезами дослідження. Поставлені гіпотези полягали в тому, що: нейронні мережі можуть дати відчутне (не менше ніж 10 %) скорочення часу обчислення ізогеній за рахунок кращого вибору параметрів, а також IDS-система на базі НМ зможе виявляти більшість атак, що вносять нетипові патерни в часові або інші побічні канали. Отримані дані підтвердили обидві гіпотези: скорочення часу перевищило 20 % (проти очікуваних 10 %), а точність класифікатора щодо атак сягнула 88–92 %.

Моделі НМ можуть показувати помилкові спрацьовування або давати неточні результати при аномальних вхідних даних, не представлених у навчальній вибірці.

Криптоаналіз. Існує ймовірність, що подальше вивчення ізогеній знайде кращі квантові алгоритми, ніж ті, що відомі сьогодні. – Апаратні обмеження. Для дуже великих полів або швидкого онлайн-моніторингу можуть бути потрібні обчислювальні ресурси, що не завжди доступні.

Перспективами подальших досліджень є розробка методів захисту від зловмисного використання НМ (коли атакувальник теж тренує модель, аби знаходити слабкі параметри); комбінування кількох НМ, включаючи ансамблеві методи, для більш надійного виявлення аномалій; поглиблене вивчення оптимального вибору суперсингулярних кривих з урахуванням алгебраїчних властивостей і можливостей

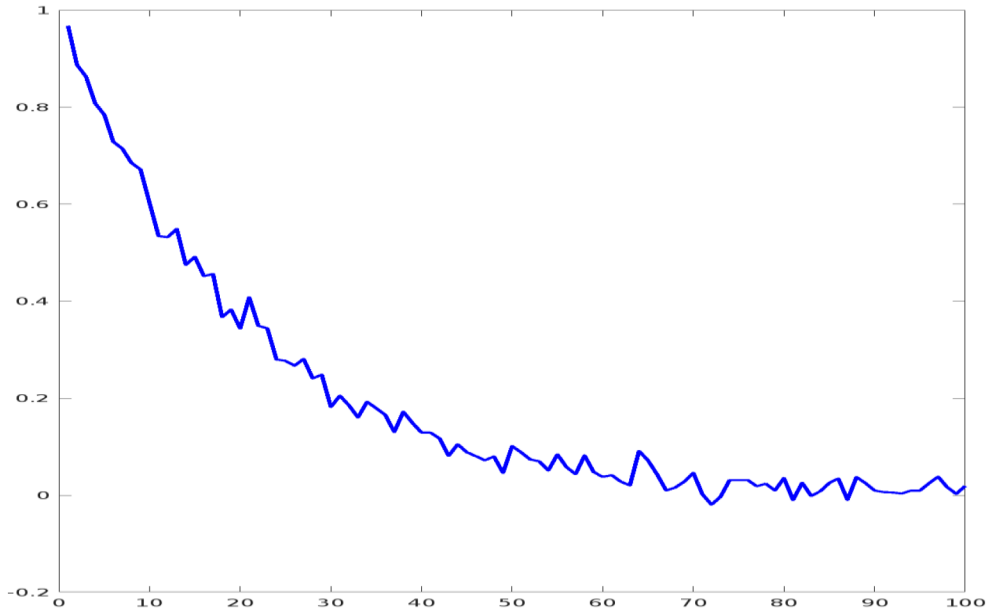

Рис. 1. Збіжність функції втрат $\mathcal{L}(\alpha; \theta)$ під час навчання НМ

реалізації на різних апаратних платформах (GPU, FPGA).

Висновки. Таким чином, виконане дослідження щодо обґрунтування безпеки на ізогеніях, показано, що складність побудови ізогеній великого ступеня між суперсингулярними кривими лежить в основі безпеки SIDH/SIKE. Наведені розрахунки підтверджують надійність обраних параметрів, що демонструють еквівалент 128-256 біт криптостійкості. Методи інтеграції нейронних мереж у криптографію на ізогеніях для оптимізації параметрів, дало наявність зниження часу обчислень на <<Eqn03503.wmf>> без зменшення рівня безпеки та для виявлення аномалій із Recall до 0.88. Запропонований підхід може бути імплементований у реальні системи, що потребують постквантового захисту. Нейронні мережі дають додатковий рівень безпеки, аналізуючи поведінкові та часові характеристики обчислень. Описані підходи закладають основу для гнучких, масштабованих і безпечних криптосистем, здатних враховувати нові виклики постквантової ери та еволюцію обчислювальних технологій.

ЛІТЕРАТУРА:

1. Hankerson D., Menezes A., Vanstone S. Guide to Elliptic Curve Cryptography. Springer, 2004. DOI: 10.1007/b97644, https://doi.org/10.1007/b97644

2. Cohen H., Frey G., Avanzi R. at ol. Handbook of Elliptic and Hyperelliptic Curve Cryptography. CRC Press, 2006, https://doi.org/10.1201/9781420010916

3. Shor P.W. Algorithms for quantum computation: discrete logarithms and factoring. Proceedings 35th Annual Symposium on Foundations of Computer Science, 1994. P. 124–134, https://doi.org/10.1109/SFCS.1994.365700

4. Proos, J., Zalka, C. Shor's discrete logarithm quantum algorithm for elliptic curves. *Quantum Info. Comput.*, 2003. Vol. 3 (4). P. 317–344. URL: https://www.rintonpress.com/xxqic3/qic-3-4/317-344.pdf

5. Jao D., De Feo L. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. Post-Quantum Cryptography (PQCrypto), 2011. P. 19–34. https://doi.org/10.1007/978-3-642-25405-5_2

6. Childs A. M., Jao D., Soukharev V. Constructing elliptic curve isogenies in quantum subexponential time. *Journal of Mathematical Cryptology*, 2014. Vol. 8(1). P. 1–29. https://doi.org/10.1515/jmc-2012-0016

7. Galbraith S.D. Mathematics of Public Key Cryptography. Cambridge University Press, 2012. https://doi.org/10.1017/CBO9781139047847

8. NIST PQ Project. Post-Quantum Cryptography Standardization. URL: https://csrc.nist.gov/projects/post-quantum-cryptography, 2023.

9. SIKE Official Project. URL: https://sike.org, (дата звернення: 2025).

10. Goodfellow I., Bengio Y., Courville A. Deep Learning. MIT Press, 2016. URL: https://www.deeplearningbook.org/

11. Russell S., Norvig P. Artificial Intelligence: A Modern Approach. 3rd Edition, Prentice Hall, 2010. URL: https://aima.cs.berkeley.edu/

12. Silverman J. The Arithmetic of Elliptic Curves. Springer, 2009. https://doi.org/10.1007/978-0-387-09494-6

13. De Feo L. Mathematics of isogeny based cryptography. Cryptology ePrint Archive, 2017/201. URL: https://eprint.iacr.org/2017/201

14. Costello C., Longa P., Naehrig M. Efficient algorithms for supersingular isogeny Diffie-Hellman. Crypto, 2016. P. 572–601. https://doi.org/10.1007/978-3-662-53015-3_21

15. Sahin S. et al. Machine learning based side-channel analysis on post-quantum cryptography: the case of ring-LWE and isogeny-based schemes. *Applied Sciences*, 2018. Vol. 8(9). P. 1557. https://doi.org/10.3390/app8091557

16. De Feo L., Jao D. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies (extended version). *Journal of Number Theory*, 2017. https://doi.org/10.1016/j.jnt.2017.07.010

17. Chen L., Jordan S. Report on Post-Quantum Cryptography. NISTIR 8105, 2016. URL: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

18. Killmann, W., Schaad, A. Integrating machine learning in isogeny-based cryptosystems: Survey and analysis. Cryptology ePrint Archive, 2024/1293. URL: https://eprint.iacr.org/2024/1293

REFERENCES:

1. Hankerson, D., Menezes, A., Vanstone, S. (2004). Guide to Elliptic Curve Cryptography. Springer. https://doi.org/10.1007/b97644

2. Cohen, H., Frey, G., Avanzi, R. (2006). Handbook of Elliptic and Hyperelliptic Curve Cryptography. CRC Press. https://doi.org/10.1201/9781420010916

3. Shor, P.W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. Proceedings 35th Annual Symposium on Foundations of Computer Science. P. 124–134. https://doi.org/10.1109/SFCS.1994. 365700

4. Proos, J., Zalka, C. (2003). Shor's discrete logarithm quantum algorithm for elliptic curves. *Quantum Info. Comput*. Vol. 3 (4). P. 317–344. Retrieved from: https://www.rintonpress.com/xxqic3/qic-3-4/317-344.pdf

5. Jao, D., De Feo, L. (2011). Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. Post-Quantum Cryptography (PQCrypto). P. 19–34. https://doi.org/10.1007/978-3-642-25405-5_2

6. Childs, A.M., Jao, D., Soukharev, V. (2014). Constructing elliptic curve isogenies in quantum subexponential time. *Journal of Mathematical Cryptology*. Vol. 8(1). P. 1–29. https://doi.org/10.1515/jmc-2012-0016

7. Galbraith, S.D. (2012). Mathematics of Public Key Cryptography. Cambridge University Press. https://doi.org/10.1017/CBO 9781139047847

8. NIST PQ Project. (2023). Post-Quantum Cryptography Standardization Retrieved from: https://csrc.nist.gov/projects/post-quantum-cryptography

9. SIKE Official Project Retrieved from: https://sike.org, (дата звернення: 2025).

10. Goodfellow, I., Bengio, Y., Courville, A. (2016). Deep Learning. MIT Press. Retrieved from: https://www.deeplearningbook.org/

11. Russell, S., Norvig, P. (2010). Artificial Intelligence: A Modern Approach. 3rd Edition, Prentice Hall. Retrieved from: https://aima.cs.berkeley.edu/

12. Silverman, J. (2009). The Arithmetic of Elliptic Curves. Springer. https://doi.org/10.1007/978-0-387-09494-6

13. De Feo, L. (2017). Mathematics of isogeny based cryptography. Cryptology ePrint Archive. DOI: https://eprint.iacr.org/2017/201

14. Costello, C., Longa, P., Naehrig, M. (2016). Efficient algorithms for supersingular isogeny Diffie-Hellman. Crypto. P. 572–601. https://doi.org/10.1007/978-3-662-53015-3_21

15. Sahin, S. et al. (2018). Machine learning based side-channel analysis on post-quantum cryptography: the case of ring-LWE and isogeny-based schemes. *Applied Sciences*. Vol. 8 (9). P. 1557. https://doi.org/10.3390/app8091557

16. De Feo, L., Jao, D. (2017). Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies (extended version). *Journal of Number Theory*. https://doi.org/10.1016/j.jnt.2017.07.010

17. Chen, L., Jordan, S. Report on Post-Quantum Cryptography. NISTIR 8105. (2016). Retrieved from: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

18. Killmann, W., Schaad, A. (2024). Integrating machine learning in isogeny-based cryptosystems: Survey and analysis. Cryptology ePrint Archive. Retrieved from: https://eprint.iacr.org/2024/1293