УДК 004.75

ДОСЛІДЖЕННЯ МЕТОДІВ ТА АЛГОРИТМІВ ДЛЯ РІШЕННЯ ПРОБЛЕМИ ДИСКРЕТНОГО ЛОГАРИФМУВАННЯ В КОНТЕКСТІ КРИПТОГРАФІЇ БІТКОЇНУ

Щербак Н.О.
e-mail: nazarii.shcherbak@nure.ua
Науковий керівник – к.т.н., доц. Мельнікова Р.В.
Харківський національний університет радіоелектроніки, каф. ПІ
м. Харків, Україна

This work investigates methods and algorithms for solving the discrete logarithm problem in the context of the cryptographic security of Bitcoin. Bitcoin cryptographic security depends on the difficulty of recovering a private key from a public key. The work analyzes classical approaches such as the Baby-step Giant-step and Pollard Rho algorithms, with attention to the Bernstein-Lange optimizations. The work also examines the use of GPU acceleration to increase the performance of cryptanalytic algorithms through large-scale parallelism. The results indicate that, despite algorithmic improvements and hardware acceleration, solving the discrete logarithm problem for Bitcoin parameters remains computationally infeasible with current technologies.

Система Bitcoin є однією з найбільш відомих реалізацій децентралізованих криптографічних протоколів, безпека яких базується на технології блокчейн та складності певних математичних задач. Однією з ключових задач, що забезпечує криптографічну стійкість цієї системи, є проблема дискретного логарифмування в групі точок еліптичної кривої. У протоколі Bitcoin використовується алгоритм цифрового підпису ECDSA, який працює над еліптичною кривою secp256k1 [1]. Надійність цієї криптографічної схеми визначається тим, що відновлення приватного ключа на основі відомого публічного ключа еквівалентне розв'язанню задачі дискретного логарифмування, яка на сучасному рівні розвитку техніки вважається обчислювально складною.

Проблема дискретного логарифмування у групі точок еліптичної кривої формулюється як задача знаходження такого числа k, для якого виконується співвідношення $Q = kG$, де G є фіксованою базовою точкою кривої, а Q – відома точка, що відповідає публічному ключу користувача. У випадку кривої secp256k1 порядок групи точок становить приблизно 2^{256}, що робить повний перебір можливих значень приватного ключа обчислювально неможливим. Саме ця властивість лежить в основі криптографічної стійкості Bitcoin та забезпечує захист цифрових активів користувачів від несанкціонованого доступу.

Для дослідження практичної складності задачі дискретного логарифмування розглядаються різні алгоритмічні підходи. Класичні алгоритми, такі як Baby-step Giant-step, дозволяють зменшити часову

складність задачі до порядку квадратного кореня від розміру групи. Проте такі методи потребують значних обсягів пам’яті для зберігання проміжних результатів, що робить їх малопридатними для застосування у випадку великих криптографічних параметрів. Більш практичним підходом вважається алгоритм Pollard Rho [2], який має аналогічну асимптотичну складність, але не потребує великих обсягів пам’яті та добре масштабується у паралельних обчислювальних середовищах.

Особливу увагу у сучасних дослідженнях приділяють оптимізаціям алгоритмів пошуку дискретного логарифма, спрямованим на зменшення кількості необхідних групових операцій. Одним із важливих напрямів таких досліджень є підхід, запропонований Деніелом Бернштейном та Танею Ланге, відомий як метод Bernstein-Lange [3]. У своїх роботах дослідники запропонували низку оптимізацій для реалізації алгоритмів пошуку дискретного логарифма в групах еліптичних кривих, зокрема оптимізовані представлення точок, ефективні методи виконання групових операцій та удосконалені техніки організації пошуку у просторі точок кривої.

Останніми роками значного розвитку набули дослідження, спрямовані на прискорення обчислень у задачах дискретного логарифмування за допомогою графічних процесорів. Архітектура GPU передбачає наявність великої кількості обчислювальних ядер, що дозволяє одночасно виконувати тисячі незалежних потоків обчислень. Така структура добре підходить для реалізації алгоритмів, заснованих на пошуку у групі точок еліптичної кривої, оскільки кожен обчислювальний потік може виконувати власну незалежну траєкторію пошуку.

У GPU-реалізаціях алгоритмів пошуку дискретного логарифма, що засновані на технології CUDA [4], велика кількість потоків виконує операції над точками еліптичної кривої, генеруючи послідовності точок та перевіряючи умови для так званих distinguished points. Ці точки використовуються для синхронізації результатів між різними обчислювальними потоками та дозволяють виявляти колізії між проміжними значеннями алгоритму.

Важливою складовою алгоритму Bernstein-Lange є підбір сталих значень, що використовуються під час розрахунків. Для цього було розроблено програмне забезпечення, що автоматично робить підбір констант для найменших часових параметрів. Задля пришвидшення тестувань розмір секрету було обрано таким, що дорівнює 64 біта. Емпіричним шляхом було визначено, що найбільше на часовий результат впливає константа N, що відповідає за кількість вже відомих distinguished points та використовуються під час розрахунків. Результат є очікуваним, так як кількість вже відомих точок, прямопропорційно впливає на шанс знаходження колізії. При тому, чим більше ця константа, тим менше часу алгоритм витрачає на знаходження одного дискретного логарифму.

На рисунку 1 зображено графік залежності часу від кількості distinguished points (константа N).

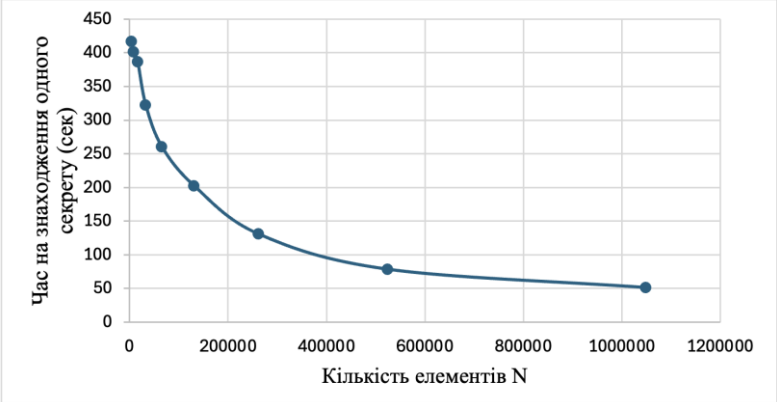

Рисунок 1 – Графік залежності часу у секундах,
що було витрачено на знаходження дискретного логарифму
розміром 64 біт від кількості distinguished points

Можна зробити висновок, що графік має обернену залежність і, відповідно, при збільшенні константи N прискорення алгоритму буде знижуватись. Окрім цього, очікується, що при збільшенні розміру дискретного логарифму буде також збільшуватись значення константи N.

Незважаючи на високу стійкість Bitcoin, використання алгоритму Bernstein-Lange у поєднанні з GPU-обчисленнями поступово знижує бар'єр для атак. Експериментально підтверджено обернену залежність між кількістю distinguished points (N) та часом пошуку логарифму: автоматизований підбір N суттєво пришвидшує розрахунки, хоча темп приросту ефективності поступово спадає. Паралелізація процесів на графічних процесорах у синергії з оптимізацією параметрів створює реальні передумови для успішного криптоаналізу сучасних схем у майбутньому.

Список використаних джерел:

1. Nakamoto S. Bitcoin – Open source P2P money. URL: https://bitcoin.org/bitcoin.pdf (дата звернення: 05.03.2026).

2. Anjan K. Koundinya, Harish G., Srinath N. K., Raghavendra G. E., Pramod Y. V., Sandeep R. and Punith Kumar G. - Performance Analysis of Parallel Pollard's Rho Factoring Algorithm. URL: https://arxiv.org/pdf/1305.4365 (дата звернення: 05.03.2026).

3. Bernstein D. J., Lange T – Computing small discrete logarithms faster. URL: https://cr.yp.to/dlog/cuberoot-20120919.pdf (дата звернення: 06.03.2026).

4. CUDA Programming Guide – CUDA Programming Guide. NVIDIA Documentation Hub – NVIDIA Docs. URL: https://docs.nvidia.com/cuda/cuda-programming-guide (дата звернення: 07.03.2026).