КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА

Кваліфікаційна наукова
праця на правах рукопису

АБРАМОВ СЕРГІЙ ВАДИМОВИЧ

УДК 004.056.55+003.26

ДИСЕРТАЦІЯ

МОДЕЛІ ТА МЕТОДИ ПІДВИЩЕННЯ ШВИДКОДІЇ АЛГОРИТМУ CSIDH НА ОСНОВІ СУПЕРСИНГУЛЯРНИХ СКРУЧЕНИХ КРИВИХ ЕДВАРДСА

Спеціальність 125 Кібербезпека
Галузь знань 12 Інформаційні технології

Подається на здобуття ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

_____ С. В. Абрамов

Науковий керівник:
Соколов Володимир Юрійович
кандидат технічних наук, доцент

Київ – 2025

АНОТАЦІЯ

Абрамов С. В. Моделі та методи підвищення швидкодії алгоритму CSIDH на основі суперсингулярних скручених кривих Едвардса. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії за спеціальністю 125 Кібербезпека. – Київський столичний університет імені Бориса Грінченка, Київ, 2025.

Дисертаційна робота присвячена вирішенню актуального наукового завдання, сутність якого полягає в підвищенні у постквантових умовах захищеності і швидкодії криптосистем на основі комутативної суперсингулярної ізогенії Діффі-Геллмана (від англ. Commutative Supersingular Isogeny Diffie–Hellman, CSIDH), який є одним з лідерів асиметричних постквантових криптосистем. Алгоритм пропонується будувати на ґрунті ізогеній нециклічних суперсингулярних кривих Едвардса як пар квадратичного кручення. Використання еліптичних кривих Едвардса значно підвищує захищеність криптоалгоритму, але при цьому збільшується складність обчислення алгоритму і відповідно зменшується його швидкодія. Тому є актуальною проблема підвищення швидкодії за рахунок модифікації цього алгоритму.

Методологія криптографії є потужним інструментом, який має значний вплив на безпеку держави та роботу комерційних організацій через високий ступінь захисту конфіденціальної інформації від пошкодження та перехоплення під час передавання, роботи у реальному часі і збереження. Сучасні криптосистеми працюють в умовах, які змушують звернути увагу на актуальність їх удосконалення, а саме:

1. Незабаром очікується створення потужного квантового суперкомп’ютера. Останнім часом дослідження в галузі квантових обчислень є одним з пріоритетів фінансування науки у світі. Теоретично такий комп’ютер здатний розв’язувати певні задачі набагато швидше, ніж звичайні комп’ютери, наприклад, задачу

факторизації цілих чисел або дискретного логарифмування у кінцевому полі. Це призведе до того, що деякі складні завдання можуть бути вирішені за дуже короткий час. Наприклад завдання криптоаналізу.

2. Відомо, що для роботи будь-якого комп’ютера потрібен відповідний алгоритм, який забезпечує успішну атаку на криптосистему. Наприклад, для такої атаки створено алгоритм Шора, але він не може атакувати симетричні системи і досить складні асиметричні, наприклад, системами на основі ізогеній еліптичних кривих.

3. Серед сучасних криптосистем є технології, які залишаються стійкими до атак з боку квантових комп’ютерів. Наприклад, деякі симетричні технології, серед асиметричних це такі найбільш популярні і розвинуті , як алгоритми на гратах і алгоритми на ізогеніях еліптичних кривих. Для них не існує алгоритму успішної атаки. Властивості симетричних і асиметричних систем вимушують їх працювати, як правило, спільно. Асиметричні системи добре керують ключами, чого бракує симетричним. Але продуктивність і швидкодія асиметричних систем значно нижча ніж симетричних.

4. Асиметричні системи з’явилися недавно, першими були криптосистеми Діффі-Геллмана, які мають багато модифікацій і наразі є модифікація, яка працює на ізогеніях еліптичних кривих, тобто вони є захищеними від атак з використанням квантових комп’ютерів. При цьому така система досить складна і має не дуже високу швидкодію. Крім того, слабким місцем криптосистеми Діффі-Геллмана є залежність від загрози атаки сторонніми каналами.

5. Таким чином, криптоалгоритм Діффі-Геллмана на ізогеніях еліптичних кривих є одним з найбільш перспективних для використання у постквантовий період. Дослідження щодо вдосконалення і модифікації криптоалгоритму Діффі-Геллмана на ізогеніях еліптичних кривих є актуальним завданням.

6. Для модифікації криптоалгоритму Діффі-Геллмана було обрано еліптичні криві у загальній формі Едвардса, які мають найкращі властивості серед інших кривих: найкоротший ключ і найбільшу швидкість. Запропоновано використовувати нециклічні криві з рандомізованим вибором, спростити метод

обчислення ізогеній, рандомізувати і оптимізувати вибір ізогеній, спростити метод обміну ключами за рахунок інкапсуляції ключа, використовувати паралельні обчислення.

7. Усі модернізації, що пропонуються, дозволяють посилити захист від атаки сторонніми каналами і пришвидшити обмін ключами, збільшення швидкості якого оцінюється у $3 \cdot 2^9$ разів.

Таким чином, дослідження щодо вдосконалення алгоритму CSIDH на основі скручених суперсингулярних кривих Едвардса є актуальним через його узгодження з поточними та майбутніми викликами кібербезпеки, вирішення проблем, пов'язаних із передаванням персональних, конфіденційних та секретних динних, а також еволюцією методів криптоаналізу. Воно забезпечує адаптивні підходи до безпеки, необхідної для забезпечення криптостійкості протоколів, які функціонують у локальних та глобальних інформаційно-комунікаційних системах.

Для досягнення мети в підвищенні швидкодії алгоритму CSIDH на основі скручених суперсингулярних кривих Едвардса було вирішено наступні задачі:

1. Вперше запропоновано і обґрунтовано метод підвищення швидкодії криптосистеми CSIDH шляхом використання замість одної циклічної повної кривої Едвардса двох нециклічних кривих з випадковим вибором однієї з кривих пари. Це у зрівнянні з CSIDH вдвічі розширює простір еліптичних кривих, спрощує обчислення параметра d кривих. Оцінка виграшу в швидкодії складає 2^5 рази. Використання додатково ізоморфних кривих породжує існування двох незалежних криптосистем з можливістю паралельних обчислень. Це додатково усуває загрозу атаки сторонніми каналами, подвоює швидкодію або довжину секретного ключа у два рази.

2. Вперше запропоновано модель інкапсуляції ключа CSIKE з рандомізацією з одним сеансом передачі і одним відкритим ключем замість двох у порівнянні з CSIDH. Модель ґрунтується на випадковому виборі однієї з нециклічних кривих Едвардса та випадковому виборі ступеня ізогенії на кожному кроці ланцюжка ізогеній. Такий випадковий вибір є альтернативою методам вирівнювання часу виконання групової операції постійного часу CSIDH, що не викликає штучного

збільшення часу виконання алгоритму і усуває загрозу атаки сторонніми каналами. Це дозволяє удвічі скоротити час на обмін ключами і підвищує загальну швидкодію у два рази.

3. Удосконалено метод обчислення і вибору структури ізогеній у криптоалгоритмах CSIDH на кривих Едвардса. Обчислення ізогенних функцій функції $\varphi(R)$ випадкової точки R замінюється на більш просте обчислення параметру d ізогенної кривої. При цьому виконуються менш затратні операції, пов'язані зі скалярними множеннями випадкових точок на число, що прискорює обчислення порядку точок і надає прискорення алгоритму більш ніж у 2^3 разів. Вибір структури ступенів ізогеній за рахунок скорочення їх діапазону дає лінійну оцінку прискорення алгоритму в 1,5 рази.

4. Набув подальшого розвитку метод CRS на несуперсингулярних (ординарних) кривих та поділу секретів Діффі-Геллмана на ізогеніях ординарних нециклічних кривих Едвардса. Замість двох ізоморфних криптосистем в алгоритмі CSIDH перехід до несуперсингулярних кривих породжує чотири незалежні криптосистеми з можливістю паралельних обчислень. Це дає оцінку виграшу швидкості обчислень у чотири рази. Оцінка загального виграшу швидкості обчислень досягає $3 \cdot 2^9$ разів.

У вступі обґрунтовується важливість й актуальність теми дисертаційного дослідження, сформульовано мету та задачі роботи, визначено основні положення, наукову та практичну цінність отриманих результатів роботи та наведено особистий внесок автора.

У першому розділі здійснено аналіз класичних асиметричних криптосистем. Показано їх важливість для систем шифрування. Показано розвиток асиметричних криптосистем з використанням еліптичних кривих. Аналізовані виклики майбутніх квантових комп'ютерів, а також стійкість і можливості асиметричних криптосистем при використанні постквантових обчислювальних машин. Обґрунтовано вибір криптосистеми Діффі-Геллмана як одну з найбільш перспективних, яка адаптована на використання ізогеній еліптичних кривих.

У другому розділі у якості еліптичних кривих обґрунтовано і обрано криві Едвардса, які мають переваги перед іншими еліптичними кривими. Розглянуті властивості і класифікацію кривих Едвардса та їх ізогеній. Розглянуто питання складності обчислення ізогенних функцій і параметрів ізогенних кривих та обґрунтована відмова від обчислення складних ізогенних функцій. Обрано використовувати нециклічні суперсингулярні криві Едвардса, що створюють пари квадратичного кручення, що, в свою чергу, збільшує простір еліптичних кривих і пришвидшує перехід між кривими, тобто збільшується криптостійкість і швидкодію алгоритму.

У третьому розділі розглядається шляхи модернізації алгоритму CSIDH на ізогеніях суперсингулярних еліптичних кривих Едвардса, що підвищує швидкість шифрування. Запропоновано метод інкапсуляції ключа CSIKE, що використовує один публічний ключ замість двох, методи рандомізації та оптимізації структури ізогеній алгоритму, які також збільшують криптостійкість і швидкодію алгоритму. Розглядається модель системи комбінованого шифрування.

У четвертому розділі показано, що додаткового збільшення швидкодії алгоритму можна отримати при використанні ізогеній несуперсингулярних нециклічних кривих Едвардса. З врахуванням усіх модифікацій швидкодія алгоритму CSIDH збільшується у $3 \cdot 2^9$ разів. Створено багатофункціональну модель шифрування на ізогеніях несуперсингулярних кривих Едвардса. Зроблено порівняння цієї системи з оригінальною системою Діффі-Геллмана на еліптичних кривих.

Дисертація виконувалась в Київському столичному університеті імені Бориса Грінченка.

Результати наукових досліджень були використані на кафедрі інформаційної та кібернетичної безпеки імені професора Володимира Бурячка факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка в рамках науково-дослідної роботи: «Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та

функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури» (№ 0122U200483, КСУБГ, м. Київ).

Також результати наукових досліджень прийняті до впровадження в діяльність Київського столичного університету імені Бориса Грінченка (акт від 12.09.2024 року) та Інституту програмних систем Національної академії наук України (акт від 02.09.2024 року).

Ключові слова: кібербезпека, інформаційна безпека, захист інформації, шифрування, асиметрична криптосистема, постквантова криптографія, криптосистема Діффі-Геллмана, еліптична крива, крива Едвардса, суперсингулярна крива Едвардса, ізогенія, скручена крива Едвардса, CRS, CSIDH, CSIKE, модифікація криптосистеми, швидкодія криптоалгоритму, ізоморфізм, рандомізація, оптимізація, атака сторонніми каналами, рівень безпеки, криптостійкість.

ANNOTATION

Abramov S. V. Models and Methods for Improving the Performance of the CSIDH Algorithm based on Supersingular Twisted Edwards Curves. – Qualification of scientific work on the rights of a manuscript.

Dissertation for the degree of Doctor of Philosophy in specialty 125 Cybersecurity. – Borys Grinchenko Kyiv Metropolitan University, Kyiv, 2025.

The dissertation is devoted to solving an urgent scientific problem, the essence of which is to increase the security and performance of cryptosystems based on the Commutative Supersingular Isogeny Diffie-Hellman, which is one of the leaders in asymmetric post-quantum cryptosystems, in post-quantum conditions. The algorithm is proposed to be built based on isogenies of noncyclic supersingular Edwards curves as pairs of quadratic torsion. The use of elliptic Edwards curves significantly increases the security of the cryptoalgorithm, but it increases the complexity of the algorithm's computation and, accordingly, reduces its performance. Therefore, the problem of improving performance by modifying this algorithm is relevant.

The cryptography methodology is a powerful tool that has a significant impact on the security of the state and the work of commercial organizations due to the high degree of protection of confidential information from damage and interception during transmission, real-time operation, and storage. Modern cryptosystems operate in conditions that make it necessary to pay attention to the relevance of their improvement, namely:

1. A powerful quantum supercomputer is expected to be created soon. Recently, research in the field of quantum computing has been one of the priorities of science funding in the world. Theoretically, such a computer is capable of solving certain problems much faster than conventional computers, such as the problem of factorizing integers or discrete logarithmization in a finite field. This will lead to the fact that some complex tasks can be solved in a very short time. For example, the task of cryptanalysis.

2. It is known that any computer requires an appropriate algorithm that ensures a successful attack on the cryptosystem. For example, Shor's algorithm was created for such an attack, but it cannot attack symmetric systems and rather complex asymmetric systems, for example, systems based on isogenies of elliptic curves.

3. Among modern cryptosystems, some technologies remain resistant to attacks by quantum computers. For example, some symmetric technologies, among the asymmetric ones, such as lattice algorithms and algorithms based on isogenies of elliptic curves, are the most popular and developed. There is no successful attack algorithm for them. The properties of symmetric and asymmetric systems make them work together, as a rule. Asymmetric systems are good at managing keys, which is something symmetric systems lack. However, the performance and speed of asymmetric systems are much lower than symmetric ones.

4. Asymmetric systems have appeared recently, the first was Diffie-Hellman cryptosystems, which have many modifications and now there is a modification that works on isogenies of elliptic curves, that is, they are protected from attacks using quantum computers. At the same time, such a system is quite complex and does not have very high performance. In addition, the weakness of the Diffie-Hellman cryptosystem is its dependence on the threat of the side channel attack.

5. Thus, the Diffie-Hellman cryptoalgorithm on the isogenies of elliptic curves is one of the most promising for use in the post-quantum period. Research on the improvement and modification of the Diffie-Hellman cryptoalgorithm on isogenies of elliptic curves is an urgent task.

6. To modify the Diffie-Hellman cryptoalgorithm, elliptic curves in the general Edwards form were chosen, which have the best properties among other curves: the shortest key and the fastest speed. It is proposed to use non-cyclic curves with randomized selection, simplify the method of calculating isogenies, randomize and optimize the choice of isogenies, simplify the method of key exchange by encapsulating the key, and use parallel computing.

7. All the proposed upgrades allow to strengthen protection against side channel attacks and speed up key exchange, which is estimated to increase the speed by $3 \cdot 2^9$ times.

Thus, the study on improving the CSIDH algorithm based on twisted supersingular Edwards curves is relevant due to its alignment with current and future cybersecurity challenges, solving problems related to the transmission of personal, confidential, and secret melon data, as well as the evolution of cryptanalysis methods. It provides adaptive approaches to the security required to ensure the cryptographic stability of protocols operating in local and global information and communication systems.

To achieve the goal of improving the performance of the CSIDH algorithm based on twisted supersingular Edwards curves, the following tasks were solved:

1. For the first time, a method of improving the performance of the CSIDH cryptosystem is proposed and substantiated by using two non-cyclic curves instead of one cyclic full Edwards curve with a random selection of one of the curves of the pair. Compared to CSIDH, this doubles the space of elliptic curves and simplifies the calculation of the parameter d of the curves. The estimated performance gain is 2^5 times. The use of additional isomorphic curves gives rise to the existence of two independent cryptosystems with the possibility of parallel computing. This additionally eliminates the threat of the side channel attack and doubles the speed or length of the secret key.

2. For the first time, a randomized key encapsulation model CSIKE with one transmission session and one public key instead of two is proposed in comparison with CSIDH. The model is based on a random selection of one of the noncyclic Edwards curves and a random selection of the degree of isogeny at each step of the isogeny chain. This random selection is an alternative to the CSIDH constant time group operation time equalization methods, which does not artificially increase the algorithm execution time and eliminates the threat of the side channel attack. This reduces the time for key exchange by half and doubles the overall performance.

3. Improved method for calculating and selecting the structure of isogenies in CSIDH cryptoalgorithms on Edwards curves. The calculation of the isogenic functions of the function $\varphi(R)$ of a random point R is replaced by a simpler calculation of the parameter d of the isogenic curve. At the same time, less costly operations related to scalar multiplications of random points by a number are performed, which speeds up the calculation of the point order and speeds up the algorithm by more than 2^3 times. The

choice of the structure of the isogeny degrees by reducing their range gives a linear estimate of the algorithm speedup by 1.5 times.

4. The CRS method on non-supersingular (ordinary) curves and the Diffie-Hellman secret partitioning on isogenies of ordinary non-cyclic Edwards curves were further developed. Instead of two isomorphic cryptosystems in the CSIDH algorithm, the transition to non-supersingular curves gives rise to four independent cryptosystems with the possibility of parallel computation. This gives an estimate of a fourfold increase in computing speed. The estimate of the total computation speed gain reaches $3 \cdot 2^9$ times.

The introduction substantiates the importance and relevance of the topic of the dissertation research, formulates the purpose and objectives of the work, defines the main provisions, and scientific and practical value of the obtained results, and presents the author's contribution.

Section 1 analyzes classical asymmetric cryptosystems. Their importance for encryption systems is shown. The development of asymmetric cryptosystems using elliptic curves is shown. The challenges of future quantum computers, as well as the stability and capabilities of asymmetric cryptosystems when using post-quantum computers, are analyzed. The choice of the Diffie-Hellman cryptosystem as one of the most promising, which is adapted to the use of isogenies of elliptic curves, is substantiated.

In Section 2, the elliptic curves are substantiated and selected as Edwards curves, which have advantages over other elliptic curves. The properties and classification of Edwards curves and their isogenies are considered. The complexity of the calculation of isogenic functions and parameters of isogenic curves is considered, and the refusal to calculate complex isogenic functions is substantiated. It is chosen to use noncyclic supersingular Edwards curves that create pairs of quadratic torsion, which, in turn, increases the space of elliptic curves and speeds up the transition between curves, i.e., increases the cryptographic strength and speed of the algorithm.

Section 3 discusses ways to modernize the CSIDH algorithm on the isogenies of supersingular elliptic Edwards curves, which increases the encryption speed. A method of key encapsulation CSIKE, which uses one public key instead of two, methods of

randomization and optimization of the structure of the algorithm's isogenies, which also increase the cryptographic strength and speed of the algorithm, are proposed. A model of a combined encryption system is considered.

Section 4 shows that an additional increase in algorithm performance can be obtained by using isogenies of non-supersingular noncyclic Edwards curves. Taking into account all modifications, the performance of the CSIDH algorithm increases by a factor of $3 \cdot 2^9$. A multifunctional model of encryption on the isogenies of non-supersingular Edwards curves is created. A comparison of this system with the original Diffie-Hellman system on elliptic curves is made.

The dissertation was carried out at the Borys Grinchenko Kyiv Metropolitan University.

The results of scientific research were used at the Department of Information and Cybersecurity named after Professor Volodymyr Buriachok of the Faculty of Information Technologies and Mathematics of Borys Metropolitan Grinchenko Kyiv University within the framework of research work: "Methods and Models for Ensuring Cybersecurity of Information Systems, Information Processing and Functional Security of Software and Hardware Complexes for Critical Infrastructure Management" (No. 0122U200483, BGKMU, Kyiv).

Also, the results of scientific research have been accepted for implementation in the activities of Borys Grinchenko Kyiv Metropolitan University and the Institute of Software Systems of the National Academy of Sciences of Ukraine.

Keywords: cybersecurity, information security, information protection, encryption, asymmetric cryptosystem, post-quantum cryptography, Diffie-Hellman cryptosystem, elliptic curve, Edwards curve, supersingular Edwards curve, isogeny, twisted Edwards curve, CRS, CSIDH, CSIKE, cryptosystem modification, cryptoalgorithm performance, isomorphism, randomization, optimization, side channel attack, security level, crypto resistance.

Наукові статті, опубліковані у наукових виданнях, включених на дату опублікування до переліку наукових фахових видань України:

1. Bessalov, A., Kovalchuk, L., & **Abramov, S.** (2022). Randomization of CSIDH Algorithm on Quadratic and Twisted Edwards Curves. *Electronic Professional Scientific Journal "Cybersecurity: Education, Science, Technique"*, *1*(17), 128–144. https://doi.org/10.28925/2663-4023.2022.17.128144.

Наукові статті, опубліковані у періодичних наукових виданнях, проіндексованих у базах даних Scopus і Web of Science Core Collection:

1. Bessalov, A., & **Abramov, S.** (2022). Special Properties of the Point Addition Law for Non-Cyclic Edwards Curves. *Cybernetics and Systems Analysis*, *58*(683), 851–861. https://doi.org/10.1007/s10559-023-00518-w (Scopus Q3).
2. Bessalov, V., & **Abramov, S.** (2023). PQC CSIKE Algorithm on Non-Cyclic Edwards Curves. *Cybernetics and Systems Analysis*, *59*(6), 867–879. https://doi.org/10.1007/s10559-023-00622-x (Scopus Q3).
3. Bessalov, A., Sokolov, V., & **Abramov, S.** (2024). Efficient Commutative PQC Algorithms on Isogenies of Edwards Curves. *Cryptography*, *8*(3), 1–17. https://doi.org/10.3390/cryptography8030038 (Scopus Q2, WoS Q2).

Наукові публікації, у яких додатково висвітлено результати дисертації:

1. Bessalov, A., Sokolov, V., Skladannyi, P., **Abramov, S.**, & Zhyltsov, O. (2022). Modeling CSIKE Algorithm on Non-Cyclic Edwards Curves. In *Cybersecurity Providing in Information and Telecommunication Systems (CPITS)*, *3288*, 1–10. (Scopus).
2. Bessalov, A., **Abramov, S.**, Sokolov, V., & Mazur, N. (2023). CSIKE-ENC Combined Encryption Scheme with Optimized Degrees of Isogeny Distribution. In *Cybersecurity Providing in Information and Telecommunication Systems (CPITS)*, *3421*, 36–45. (Scopus).

3. Bessalov, A., **Abramov, S.**, Sokolov, V., Skladannyi, P., & Zhyltsov, O. (2023). Multifunctional CRS Encryption Scheme on Isogenies of Non-Supersingular Edwards Curves. In *Classic, Quantum, and Post-Quantum Cryptography (CQPC)*, *3504*, 12–25. (Scopus).

4. **Abramov, S.**, Bessalov, A., & Sokolov, V. (2023). Properties of Isogeny Graph of Non-Cyclic Edwards Curves. In *Cybersecurity Providing in Information and Telecommunication Systems II (CPITS-II)*, *3550*, 234–239. (Scopus).

5. **Abramov, S.**, Sokolov, V., & Abramov, V. (2024). Research of the Graphic Model of the Points of the Elliptic Curve in the Edward Form. In *Cybersecurity Providing in Information and Telecommunication Systems II (CPITS-II)*, *3826*, 174–181. (Scopus).

6. **Абрамов, С.** (2024). Алгоритм інкапсуляції ключа на кривих Едвардса. На *IV Міжнародній науково-практичній інтернет-конференції «Цифрова трансформація фінансової системи України та країн V-4 в умовах євроінтеграції»*, *II*, 98–104.

7. **Абрамов, С.** (2024). Дослідження структури графа ізогеній еліптичної кривої Едвардса. На *Міжнародній науково-технічній конференції «Інформаційно-комунікаційні технології та кібербезпека» (ІКТК)*, 200–201.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

НКЕ – несуперсингулярна крива Едвардса

СКЕ – суперсингулярна крива Едвардса

CGA – Commutativ Group Action ‘комутативна групова дія’

CRS – Couveignes-Rostovtsev-Stolbunov ‘Кувенес-Ростовцев-Столбунов’

CSIDH – Commutative Supersingular Isogeny Diffie-Hellman ‘комутативна суперсингулярна ізогенія Діффі-Геллмана’

CSIKE – Commutative Supersingular Isogeny Key Encapsulation ‘комутативна інкапсуляція ключа суперсингулярної ізогенії’

CT CSIDH – Constant Time Commutative Supersingular Isogeny Diffie-Hellman ‘комутативна суперсингулярна ізогенія Діффі-Геллмана з постійним часом виконання’

DLP – Discrete Logarithm Problem ‘проблема дискретного логарифмування’

ECC – Elliptic-Curve Cryptography ‘еліптична криптографія’

ECDH – Elliptic-Curve Diffie-Hellman ‘алгоритм Діффі-Геллмана на еліптичних кривих’

PQC – Postquantum Cryptography ‘постквантова криптографія’

RCNIE – Randomized Commutative No-supersingular Isogeny Encryption ‘рандомізоване комутативне безсуперсингулярне шифрування ізогенії’

SIDH – Supersingular Isogeny Diffie-Hellman ‘суперсингулярна ізогенія Діффі-Геллмана’

SIKE – Supersingular Isogeny Key Encapsulation ‘інкапсуляція ключа суперсингулярної ізогенії’

ВСТУП

Обґрунтування вибору теми дослідження. Держава створює умови, що гарантують захист державних і особистих інформаційних ресурсів, безпечну обробку, зберігання та передачу інформації. Одним з найбільш надійних засобів захисту цих інформаційних ресурсів є криптографічне перетворення (шифрування) інформації. Розвиток криптографічних методів, які використовуються для захисту державних та особистих цінних інформаційних ресурсів, істотно впливає на інформаційну безпеку держави в цілому.

Для шифрування століттями використовувались, так звані, симетричні методи, які забезпечують високу ступінь захисту, є дуже простими і швидкими, але мають значні недоліки. Для шифрування і дешифрування потрібний один спільній секретний ключ. Цей ключ потрібно передавати і узгоджувати між двома сторонами по закритих каналах, але навіть якщо такий канал є, він збільшує час передавання і не гарантує безпечний захист. Тому для узгодження секретних ключів ідеальними умовами є можливість використовувати відкриті канали. І така можливість з’явилась з винаходом асиметричних алгоритмів.

У 1976 році Вітфілд Діффі та Мартін Геллман зі Стенфордського університету США опублікували статтю «New Directions in Cryptography ‘Нові напрямки у криптографії’». У ній була запропонована ідея асиметричної криптографії або криптографії з відкритим ключем. Алгоритм Діффі-Геллмана (від англ. Diffie-Hellman) дозволяє двом і більше сторонам створити спільний секретний ключ, використовуючи незахищений від прослуховування канал зв’язку. Це було новим революційним принципом побудови криптосистем, що не вимагає передачі секретного ключа. Як правило, цій ключ використовується для симетричного шифрування, яке є більш надійним для швидкої передачі великих обсягів інформації. Таким чином використовуються, як правило, комбінації методів симетричного та асиметричного шифрування.

Винахід Діффі і Геллмана здійснив переворот у криптографії. Почався розвиток асиметричних криптосистем і, у першу чергу, на ґрунті різних удосконалень алгоритму Діффі-Геллмана. У 1977 році Рональд Рівест, Аді Шамір і

Леонард Адлеман створили асиметричний алгоритм RSA (Rivest-Shamir-Adleman). У 1985 році Ель-Гамаль створив свій алгоритм. В 1985 году в незалежних роботах Віктора Міллера і Ніда Кобліца було запропоновано використати у криптографії різновид алгоритму Діффі-Геллмана на еліптичних кривих. Це у десятки разів прискорило та здешевило функціонування криптопротоколів.

В той же час нова небезпека для криптографії виникає у зв'язку з прогнозованою появою потужних квантових комп'ютерів, які становитимуть небезпеку для деяких систем шифрування. Виникла нова галузь науки – постквантова криптографія (від англ. Postquantum Cryptography, PQC), яка розробляє криптосистеми, що протистоять атакам з використанням квантових комп'ютерів.

Серед асиметричних криптосистем існують такі, для яких немає відповідного алгоритму злому і які не може зламати навить квантовий комп'ютер. До таких відноситься алгоритм Діффі-Геллмана на ізогеніях еліптичних кривих. Серед еліптичних кривих останній час з'явились криві Едвардса, які є дуже перспективними для використання в алгоритмах Діффі-Геллмана.

Тому, існує необхідність вирішення актуального наукового завдання, сутність якого полягає в подальшому дослідженню і розвитку найбільш перспективного криптоалгоритму на основі кривих Едвардса з метою підвищення його швидкодії, захищеності від атаки сторонніми каналами, застосування у сучасних постквантових криптосистемах та їх стандартизації.

Дослідженням даного питання займається досить велика кількість вчених, серед яких: Harold Edwards, Daniel Bernstein, Whitfield Diffie, Martin Hellman, Ronald Rivest, Adi Shamir, Leonard Adleman ,Taher Elgamal, Neal Koblitz, Peter Shor, Alexander Rostovtsev, Anton Stolbunov, Jean-Marc Couveignes, Wouter Castryck, Kourosch Hosseini, Reza Farashahi, Анатолій Бессалов, Людмила Ковальчук та інші. Переважна більшість робіт присвячена розробці принципів роботи криптосистем на різних еліптичних кривих.

Таким чином, з приведеного аналізу можна зробити висновок, що в практиці застосування найбільш перспективні і ефективні еліптичні криві Едвардса

використовуються у криптосистемах із комутативними суперсингулярними ізогеніями Діффі-Геллмана (від англ. Commutative Supersingular Isogeny Diffie-Hellman, CSIDH) не дуже часто.

У зв'язку з цим, існує необхідність вирішення актуального наукового завдання, сутність якого полягає в подальшому дослідженню і розвитку найбільш перспективного криптоалгоритму CSIDH на основі кривих Едвардса з метою підвищення його швидкодії, захищеності від атаки сторонніми каналами, застосування у сучасних постквантових криптосистемах та їх стандартизації.

Зв'язок роботи з науковими програмами, планами, темами. Напрям дисертаційного дослідження безпосередньо пов'язаний з реалізацією доктрини інформаційної безпеки України, Стратегії інформаційної безпеки та Стратегії кібербезпеки України. Дисертаційна робота виконана відповідно до планів наукової і науково-технічної діяльності Київського столичного університету імені Бориса Грінченка в рамках науково-дослідної роботи: «Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури» (№0122U200483, КСУБГ, м. Київ).

Мета і завдання дослідження. *Мета* дисертаційного дослідження полягає в підвищенні швидкодії і безпеки постквантового асиметричного криптоалгоритму CSIDH шляхом його моделювання і модернізації з використанням властивостей еліптичних кривих у формі Едвардса.

У відповідності до поставленої мети для вирішення наукового завдання в роботі визначено та розв'язано такі *часткові завдання*:

– проаналізувано поточний стан і властивості класичних криптоалгоритмів Діффі-Геллмана, які працюють на еліптичних кривих і мають відмінні криптографічні параметри;

– визначено можливості покращення роботи криптоалгоритмів Діффі-Геллмана на ізогеніях еліптичних кривих, які здатні працювати у постквантових умовах при здійсненні атак з боку потужних квантових комп'ютерів;

– визначено властивості кривих Едвардса як оптимальних кандидатів для використання у постквантових алгоритмах;

– обґрунтувано клас і досліджено властивості еліптичних кривих Едвардса, які мають найкращі характеристики для використання у постквантових алгоритмах;

– визначено властивості алгоритму CSIDH на кривих Едвардса і обґрунтувано застосування алгоритмів CSIDH на нециклічних кривих;

– пришвидшено обчислення ізогенії для збільшення швидкодії криптоалгоритму та захисту від атаки сторонніми каналами;

– розроблено модифікації алгоритму CSIDH і створено комбінований криптоалгоритм із застосуванням його модифікацій;

– оцінено величину парціального зростання швидкості від кожної модифікації криптоалгоритму CSIDH на ізогеніях суперсінгулярних еліптичних кривих Едвардса;

– розроблено модель алгоритму з використанням несуперсингулярних кривих Едвардса (НКЕ) і оцінено приріст швидкодії і криптографічної стійкості паралельних обчислень;

– оцінено інтегральний виграш у швидкодії модернізованих алгоритмів CSIDH і комутативної інкапсуляції ключа суперсингулярної ізогенії (від. англ. Commutative Supersingular Isogeny Key Encapsulation, CSIKE).

Об'єктом дослідження є процес перетворення інформації за допомогою асиметричної криптосистеми, що базується на складності пошуку графа ізогенного ланцюга між еліптичними кривими у формі Едвардса.

Предметом дослідження є моделі і методи підвищення швидкодії на основі скручених суперсингулярних кривих Едвардса (СКЕ) над простими полями F_p для створення паралельних криптосистем.

Методи дослідження. Для проведення досліджень в дисертаційній роботі використовувалися методи теорії чисел; теорії поля; теорія графів; теорія функцій; теорія алгоритмів; теорія односторонніх функцій; теорія складності алгоритмів; теорії ймовірностей та математичної статистики; абстрактної алгебри; алгебраїчної геометрії; математичне і комп'ютерне моделювання.

Наукова новизна одержаних результатів полягає в подальшому розвитку і обґрунтуванні методів підвищення ефективності постквантових криптоалгоритмів на ізогеніях еліптичних кривих Едвардса:

1. Вперше запропоновано і обґрунтовано метод підвищення швидкодії криптосистеми CSIDH шляхом використання замість одної циклічної повної кривої Едвардса двох нециклічних кривих з випадковим вибором однієї з кривих пари. Це у зрівнянні з CSIDH вдвічі розширює простір еліптичних кривих, спрощує обчислення параметра d кривих. Оцінка виграшу в швидкодії складає 2^5 рази. Використання додатково ізоморфних кривих породжує існування двох незалежних криптосистем з можливістю паралельних обчислень. Це додатково усуває загрозу атаки сторонніми каналами, подвоює швидкодію або довжину секретного ключа у два рази.

2. Вперше запропоновано модель інкапсуляції ключа CSIKE з рандомізацією з одним сеансом передачі і одним відкритим ключем замість двох у порівнянні з CSIDH. Модель ґрунтується на випадковому виборі однієї з нециклічних кривих Едвардса та випадковому виборі ступеня ізогенії на кожному кроці ланцюжка ізогеній. Такий випадковий вибір є альтернативою методам вирівнювання часу виконання групової операції постійного часу CSIDH, що не викликає штучного збільшення часу виконання алгоритму і усуває загрозу атаки сторонніми каналами. Це дозволяє удвічі скоротити час на обмін ключами і підвищує загальну швидкодію у два рази.

3. Удосконалено метод обчислення і вибору структури ізогеній у криптоалгоритмах CSIDH на кривих Едвардса. Обчислення ізогенних функцій функції $\varphi(R)$ випадкової точки R замінюється на більш просте обчислення параметру d ізогенної кривої. При цьому виконуються менш затратні операції, пов’язані зі скалярними множеннями випадкових точок на число, що прискорює обчислення порядку точок і надає прискорення алгоритму більш ніж у 2^3 разів. Вибір структури ступенів ізогеній за рахунок скорочення їх діапазону дає лінійну оцінку прискорення алгоритму в 1,5 рази.

4. Набув подальшого розвитку метод CRS на несуперсингулярних (ординарних) кривих та поділу секретів Діффі-Геллмана на ізогеніях ординарних нециклічних кривих Едвардса. Замість двох ізоморфних криптосистем в алгоритмі CSIDH перехід до НКЕ породжує чотири незалежні криптосистеми з можливістю паралельних обчислень. Це дає оцінку виграшу швидкості обчислень у чотири рази. Оцінка загального виграшу швидкості обчислень досягає $3 \cdot 2^9$ разів.

Практичне значення одержаних результатів полягає в наступному: динамічний розвиток технологій дешифрування призводить до появи потенційних можливостей злому існуючих алгоритмів шифрування за допомогою методів PQC, що, в той самий час, призводить до появи нових потенційних загроз для підприємств критичної інфраструктури, державних органів, приватного сектору та окремих громадян.

Саме ці тренди обумовлюють практичну значущість запропонованих в дослідженні методів вдосконалення систем шифрування на основі еліптичних кривих Едвардса. Розвинуто для практичного використання ланцюжків ізогеній еліптичних кривих Едвардса над простими полями в PQC криптоалгоритмах схеми Діффі-Геллмана для підвищення швидкодії та безпеки в умовах атак сторонніми каналами. Розроблено нові науково обґрунтовані методи і алгоритми функціонування криптосистеми на основі арифметики ланцюжків ізогеній еліптичних кривих Едвардса, що зменшує складність розрахунків до $3 \cdot 2^9$ разів у порівнянні з алгоритмами, які використовуються у попередніх алгоритмах. Запропоновано новий метод і створено відповідну комп'ютерну програму розрахунку ізогеній, у якої обчислюється тільки один параметр d кривої Едвардса без складного розрахунку ізогенної функції $\varphi(R)$, що значно підвищує швидкість роботи алгоритму. А з урахуванням сучасних вимог щодо стійкості і швидкості асиметричних криптосистем пропонується застосування суперсінгулярних квадратичних і скручених еліптичних кривих Едвардса для використання в сучасних асиметричних криптосистемах. Також отримано моделі алгоритмів на ізогеніях нециклічних СКЕ, які можна використовувати на практиці з врахуванням пропонованих модернізацій. Для практичного застосування потриманих наукових

результатів розроблено програмне забезпечення, яке дозволяє виконати моделювання та тестування запропонованих криптосистем.

Апробація результатів дисертації. Основні теоретичні та практичні результати були представлені та обговорені в ході ряду наукових конференцій:

1. Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS), 2022, 2023 (двічі) і 2024 (м. Київ).

2. Workshop on Classic, Quantum, and Post-Quantum Cryptography (CQPC), 2023 (м. Київ).

3. Цифрова трансформація фінансової системи України та країн V-4 в умовах євроінтеграції, 2024 (м. Дубляни).

4. Інформаційно-комунікаційні технології та кібербезпека (ІКТК), 2024 (м. Харків).

Публікації. Основні результати дисертації висвітлено у 11 наукових публікаціях, із них усі у співавторстві: 1 статті (з них усі у співавторстві) у наукових виданнях, включених на дату опублікування до переліку наукових фахових видань України; 3 статті (з них усі у співавторстві) у періодичних наукових виданнях, проіндексованих в наукометричних базах даних Scopus і Web of Science Core Collection; 7 публікацій (з них 5 у співавторстві) у яких додатково відображено результати дисертації. Наукові результати дисертації повною мірою висвітлено у наукових публікаціях.

Особистий внесок здобувача. Дисертація є самостійною науковою працею, в якій висвітлено власні ідеї і розробки автора, що дозволили вирішити поставлені завдання. Робота містить теоретичні та методичні положення і висновки, сформульовані здобувачкою особисто. Використані в дисертації ідеї, положення чи гіпотези інших авторів мають відповідні посилання і використані лише для підкріплення ідей здобувача.

У статті «Randomization of CSIDH Algorithm on Quadratic and Twisted Edwards Curves» опублікованій у співавторстві, внесок Абрамова С.В. полягає в огляді існуючих підходів до вирішення проблеми і обговорення шляхів її вирішення, що загалом складає 35% тексту статті.

У статті «Special Properties of the Point Addition Law for Non-Cyclic Edwards Curves» опублікованій у співавторстві, внесок Абрамова С.В. полягає в аналізі особливих властивостей двох класів квадратичних і скручених кривих Едвардса над простим полем, пов'язаних з їхньою нециклічною структурою і неповнотою закону додавання точок, у створенні моделі точок кривої Едвардса, що загалом складає 40% тексту статті.

У статті «PQC CSIKE Algorithm on Non-Cyclic Edwards Curves» опублікованій у співавторстві, внесок Абрамова С.В. полягає у обговоренні та реалізації ідеї відмови від обчислення ізогенної функції $\varphi(R)$ випадкової точки R, що загалом складає 40% тексту статті.

У статті «Efficient Commutative PQC Algorithms on Isogenies of Edwards Curves» опублікованій у співавторстві, внесок Абрамова С.В. полягає у створенні програмного забезпечення розрахунків і дослідження властивостей системи, що загалом складає 30% тексту статті.

У статті «Modeling CSIKE Algorithm on Non-Cyclic Edwards Curves» опублікованій у співавторстві, внесок Абрамова С.В. полягає у розробці ідеї використання в алгоритмі CSIKE нециклічних кривих Едвардса, створенні програм та розрахунків параметрів моделі алгоритму CSIKE на нециклічних кривих Едвардса, що загалом складає 40% тексту статті.

У статті «CSIKE-ENC Combined Encryption Scheme with Optimized Degrees of Isogeny Distribution» опублікованій у співавторстві, внесок Абрамова С.В. полягає у створенні загальної схеми комбінування модернізованого асиметричного алгоритму на кривих Едвардса із симетричними алгоритмами з автентифікацією, а також створення комп'ютерної моделі комбінованої системи та її програмування, що загалом складає 35% тексту статті.

У статті «Multifunctional CRS Encryption Scheme on Isogenies of Non-Supersingular Edwards Curves» опублікованій у співавторстві, внесок Абрамова С.В. полягає у тому, що зроблено оцінки властивостей для порівняння криптоалгоритмів CSIDH і RCNSE, виконано розрахунки для створення моделі криптосистеми на 4-х степенях ізогеній {3,5,7,37} над полем F_{863} для пари

квадратичного кручення з порядками 840 і 888, що загалом складає 30% тексту статті.

У статті «Properties of Isogeny Graph of Non-Cyclic Edwards Curves» опублікованій у співавторстві, внесок Абрамова С.В. полягає у обчислення графу і виявлення закономірностей його ізогеній, що загалом складає 85% тексту статті.

У статті «Research of the Graphic Model of the Points of the Elliptic Curve in the Edward Form» опублікованій у співавторстві, внесок Абрамова С.В. полягає у розрахунку моделі експоненціювання еліптичної кривої, створенні шаблону для обчислення порядку точок і правил реконструкції точок у шаблоні, що загалом складає 70% тексту статті.

Структура та обсяг дисертаційної роботи. Дисертація складається зі вступу, чотирьох розділів, висновків, списку використаних джерел із 76 найменувань на 9 сторінках і 3 додатків. Загальний обсяг роботи становить 166 сторінок, серед яких 149 сторінок – основного тексту, 18 рисунків і 16 таблиць.

РОЗДІЛ 1
АНАЛІЗ ЗАДАЧ І АЛГОРИТМІВ АСИММЕТРИЧНОЇ ПОСТКВАНТОВОЇ КРИПТОГРАФІЇ

1.1. Історичні засади до розвитку еліптичної криптографії

У 1976 році Вітфілд Діффі та Мартін Геллман зі Стенфордського університету США опублікували статтю «New Directions in Cryptography ‘Нові напрямки у криптографії’» [1], в якій була запропонована ідея асиметричної криптографії або криптографії з відкритим ключем (від англ. public-key cryptography). Алгоритм Діффі-Геллмана дозволяє двом і більше сторонам створити спільний секретний ключ, використовуючи незахищений від прослуховування канал зв’язку. Це було новим революційним принципом побудови криптосистем, що не вимагає передачі секретного ключа. Як правило, цій ключ використовується для симетричного шифрування, яке є більш надійним для швидкої передачі великих обсягів інформації, тому використовуються комбінації методів симетричного та асиметричного шифрування.

Винахід Діффі та Геллмана здійснив переворот у криптографії. Почався розвиток асиметричних криптосистем і, у першу чергу, різних алгоритмів Діффі-Геллмана.

У 1977 році Рональд Рівест, Ади Шамір і Леонард Адлеман створили свій асиметричний алгоритм шифрування, який заснований на проблемі розкладення на множники RSA [2]. У 1985 році Ель-Гамаль створив алгоритм на основі алгоритму Діффі-Геллмана [3, 4]. Ці алгоритми стали найпопулярнішими у світі. Однак алгоритми RSA і Ель-Гамаля з арифметикою в кінцевому кільці та кінцевому полі мають субекспоненціальну складність і потребують використання значних ресурсів.

В 1985 году в незалежних роботах В. Міллера [5] і Н. Кобліца [6] було запропоновано використати у криптографії алгебраїчні властивості еліптичних

кривих. Розпочався розвиток «криптографії на еліптичних кривих». В цих системах основною груповою операцією є скалярне множення точки кривої на ціле число, відповідно зворотна складна операція це дискретне логарифмування в кінцевому полі. Застосування еліптичних кривих забезпечує високу швидкодію та невелику довжину ключа криптоалгоритму. Так з'явився алгоритм Діффі-Геллмана на еліптичних кривих (від англ. Elliptic-curve Diffie–Hellman, ECDH).

Перехід на еліптичні криві у десятки разів прискорило та здешевило функціонування криптопротоколів. З XXI сторіччя розпочався активний процес стандартизації алгоритмів та протоколів асиметричних криптосистем на еліптичних кривих (від англ. Elliptic Curve Cryptosystems, ECC). Поширюється використання алгоритму Діффі-Геллмана на ґрунті множення в групах точок еліптичних кривих (криптосистема ECDH), а нові алгоритми поступово замінюють системи RSA і Ель-Гамаля.

В той же час нова небезпека для криптографії виникає у зв'язку з прогнозованою появою квантових комп'ютерів, які становитимуть небезпеку для деяких систем шифрування. Виникла нова галузь науки – PQC. Загрозою для існуючих криптосистем є поява квантових комп'ютерів достатньої потужності для їх розкриття [7]. Тому у 1994 році Шор створює квантовий алгоритм поліноміального часу для дискретного логарифмування в групі, якій може зламати деякі алгоритми на еліптичних кривих [8]. «Справді серйозний удар квантовий комп'ютер може завдати тільки асиметричної криптографії з публічним ключем. Симетричні алгоритми залишаться стійкими» (Брюс Шнаєр) [9].

Криптографія з відкритим ключем заснована на суворій теорії чисел і потенційно вразлива. Симетрична ж криптографія має ключі, що легко подовжуються, а її криптостійкість залежить лише від довжини ключа. Симетричні системи, як було показано раніше, є неприйнятними для вирішення проблем управління ключами. Тому найбільш перспективним є розвинення постквантових асиметричних алгоритмів і комбінування їх з симетричними методами.

Серед асиметричних криптосистем існують такі, для яких немає відповідного алгоритму злому і які не може зламати навить квантовий комп'ютер. До таких

відноситься алгоритм Діффі-Геллмана на ізогеніях еліптичних кривих, але цій алгоритм має проблеми зі швидкодією [10]. Тому виникає проблема збільшити швидкодію цього алгоритму і отримати дуже ефективну комбіновану криптосистему.

У 2011 році Девід Джао і Лука Де Фео [11] створюють алгоритм обміну ключами за схемою Діффі-Геллмана для графа ізогеній СКЕ. Так званий постквантовий алгоритм SIDH (Supersingular isogeny Diffie-Hellman) над розширеному кінцевому полі F_q, $q = p^n$, де p, n – примітиви. SIDH має невелику довжину ключа і не має алгоритму квантового злому (алгоритм Шора не працює на ізогеніях еліптичних кривих), тому він є стійким до атаки квантового комп'ютера. Алгоритм має добрі характеристики, але він був зламаний у 2022 р. на звичайному комп'ютері і наразі не рекомендується для використання [12].

Але у 2018 р. до ідей алгоритму SIDH було додано ідеї Кувенема, який запропонував у 1997 р. обмін ключами за схемою Діффі-Геллмана з використанням комутативності групової дії. Схема Кувенема на той час не було опубліковано, але у 2004 р. Ростовцев і Столбунов [13] незалежно перевідкрили схему Кувенема. В результаті схема отримала назву CRS (від англ. Couveignes-Rostovtsev-Stolbunov). На ґрунті ідей, закладених в SIDH і CRS, у 2018 р. запропоновано алгоритм CSIDH на ізогеніях суперсингулярних кривих у формі Монтгомері над простим кінцевим полем F_p. Множина ізогеній складає комутативну групу, алгоритм має рекордно малу довжину ключа і, крім того, алгоритм CSIDH не підпадає під дію алгоритму Шора. Недолік алгоритму у тому, що внаслідок вразливості до атаки сторонніми каналами, невдалого вибору еліптичної кривої і ступенів ізогеній, складності обчислення ізогенної функції та деяких інших недоліків, швидкість роботи алгоритму не достатньо висока. На перший недолік вказували також самі автори алгоритму [10].

У 2007 р. Гарольд Едвардс в роботі [14] доповів про дослідження ECC. Як з'ясувалось, ці криві мають найбільшу швидкість операцій скалярного множення точки, а відповідні криптосистеми мають меншу вразливість до атак сторонніми каналами. З тих пір популярні на той час криві у формі Монтгомері і Вейєрштрасса

в деяких стандартах криптографії замінюються більш стійкими та швидкими кривими у формі Едвардса. Однак в США досі існує стандарт цифрового підпису 2000 р., а в Україні – 2002 р., які давно застарілі і потребують заміни, в тому числі, через широке використання хмарних технологій [15] та систем із штучним інтерелектом [16]. Бурхливий розвиток процесорної техніки та систем із самонавчанням призводить до автортизації процесу взлому, що створює додаткові виклики для інформаційно-комунікаційних систем критичної інфраструктури [17].

1.2. Задачі і основні принципи криптографії

У загальному вигляді шифрування-дешифрування можна представити наступним чином: є початковий текст M. Використовуючи операцію шифрування CD, відкритий текст M перетворюється у шифрований текст

$$C = CD(M, K_c), \tag{1.1}$$

де K_c – секретний ключ шифрування [7].

Ключ K це де-який текст, який впливає на процес шифрування-дешифрування. Шифртекст вільно передається відкритими каналами зв'язку і не може бути дешифрованим сторонніми особами, які не мають ключа дешифрування K_c.

Дешифрування (знаходження початкового тексту M) здійснює тільки отримувач інформації, якому вона призначена і який має ключ дешифрування K_d. Дешифрування здійснюється за допомогою функції DC і ключа K_d:

$$M = DC(C, K_d), \tag{1.2}$$

де K_d – секретний ключ дешифрування.

Захист секретного тексту M від (атаки) несанкціонованого перехоплення і злому залежить від шифрування або дешифрування, довжини ключа K_d і захисту ключа від перехоплення.

Історично першою виникла симетрична система шифрування. У симетричній системі ключі шифрування і дешифрування однакові і є секретними $K_d = K_c$.

Сторони мають обмінюватись секретними ключами, а це є небезпечним і є головним недоліком симетричної системи [7].

Властивості симетричної криптографії:

– простота процесу;
– значно швидше, ніж асиметричні;
– легко збільшувати криптостійкість шляхом збільшення довжини ключа;
– потрібно менше обчислювальної потужності;
– не знижується швидкість передачі в мережах.

Існує багато алгоритмів симетричного шифрування, серед яких найбільш поширеними є AES, RC4, DES, 3DES, RC5, RC6 тощо [7]. На сьогодні AES є найпопулярнішим і найшвидшим симетричним алгоритмом, який широко застосовується в різних програмах. Багато урядових установ США використовують AES для захисту конфіденційної інформації.

Слабке місце симетричного шифрування це обмін ключами. Однаковий ключ має бути і у відправника, і в одержувача повідомлення. Тому ключ необхідно передати одержувачу; однак при передачі його можуть перехопити та використовувати сторонні особи. На практиці проблема отримання спільного ключа вирішується за допомогою асиметричного алгоритму і використання отриманого ключа в симетричної криптосистемі [7].

Таке спільне використання симетричного і асиметричного шифрування складає комбіноване (гібридне) шифрування.

1.2.1. Гібридне шифрування

Кожен із алгоритмів шифрування має свої недоліки. Метод симетричного шифрування чудово підходить для швидкого шифрування великих обсягів даних. Безпека, що забезпечується симетричним шифруванням, може бути покращена простим збільшенням довжини ключа. Для кожного окремого біта, що додається

до довжини симетричного ключа, складність злому шифрування за допомогою атаки методом перебору експоненційно збільшується.

Але симетричний метод не забезпечує управління ключами та перевірку особистості, що є необхідним, коли йдеться про безпеку в інтернеті. З іншого боку, асиметричне шифрування дозволяє здійснювати обмін ключами з одержувачем та перевірку особи. Однак виконання цих функцій робить процес шифрування досить повільним.

Гібридний метод шифрування застосовується в SSL/TLS сертифікатах для захищеного з'єднання між серверами та клієнтами (веб-браузерами) у процесі, відомому як «TLS handshake». Спочатку автентифікуються обидві сторони за допомогою відкритого та закритого ключів. Після успішного підтвердження особистості передача даних здійснюється за допомогою симетричного шифрування з використанням сеансового ключа. Це дозволяє швидко передавати великі обсяги даних, що постійно обмінюються в інтернеті.

З точки зору безпеки, асиметричне шифрування, безперечно, забезпечує автентифікацію та обмін ключами. Однак продуктивність є аспектом, який не можна ігнорувати, тому симетричне шифрування завжди буде необхідним. При цьому невелика швидкодія асиметричного шифрування є недоліком всього процесу шифрування. Тому дуже важливими є дослідження щодо підвищення швидкодії асиметричних алгоритмів.

1.2.2. Класична асиметрична криптографія

Реалізація ідеї несиметричного шифрування полягає в понятті односторонньої взаємно однозначної функції $Y = f(X)$, такий, що з відомому X порівняно просто обчислити Y, проте зворотну функцію $X = f^{-1}(Y)$ обчислити практично неможливо. Цю властивість називають практичною незворотністю. Наведене визначення дуже умовно, оскільки складність обчислення зворотної функції може знижуватися з допомогою залучення дедалі досконаліших алгоритмів, а час

обчислення знижується зі зростанням продуктивності електронно-обчислювальних машин. У теорії обчислювальної складності прийняті поняття поліноміальної та експоненційної складності залежно від того, в якій пропорції (лінійній чи експоненційної) зростає кількість операцій із зростанням довжини вхідного блоку даних. Зазвичай обчислення прямої функції має поліноміальну складність, а зворотній – у кращому разі експоненційну. Сьогодні немає відомої односторонньої функції, для якої математично була б доведена її практична незворотність або експоненційна складність (з залученням більш строгих визначень). Важке (зворотне) завдання має вирішуватися складно: не повинно бути алгоритму, за допомогою якого можна було знайти рішення за поліноміальний час щодо розміру завдання. Правильніше сказати: не повинно бути відомого поліноміального алгоритму, що вирішує дану задачу – оскільки для жодного завдання ще поки не доведено, що для нього відповідного алгоритму немає в принципі [8].

Криптосистема організована так, що алгоритми розшифрування для легального користувача та криптоаналітика суттєво різні. У той час як другий вирішує важке завдання, перший використовує секретну лазівку.

В асиметричних криптосистемах ключі K_c. і K_d – це два різних ключі. Кожен учасник обміну повідомленнями в асиметричній системі створює два ключа. При шифруванні тексту K_c. відкритий (публічний або public key) ключ, а K_d закритий (секретний або private key). Для шифрування досить відкритого ключа, але для дешифрування треба знати секретний. Для електронного підпису навпаки закритий ключ використовується для створення підпису, а відкритий для ідентифікації цього підпису.

Можна опублікувати свій відкритий ключ і безпечно отримувати повідомлення від будь-кого. Розшифрувати повідомлення може тільки той, чий відкритий ключ був використаний для шифрування.

Першим асиметричним алгоритмом є алгоритм Діффі-Геллмана. Він використовується в багатьох криптографічних протоколах і стандартах, наприклад:

1. TLS/SSL – протоколи передачі даних, що забезпечують захищене з’єднання між клієнтом та сервером.

2. IPSec – протокол безпеки для захисту даних, що передаються через мережі, у тому числі у VPN-з'єднаннях.

3. SSH – протокол безпечної оболонки, який використовується для безпечного віддаленого доступу до серверів та обміну даними між ними.

Асиметричний метод використовується для [18] безпечного створення спільного ключа і автентифікації співрозмовників. Дані, зашифровані за допомогою відкритого ключа, можуть бути розшифровані лише за допомогою закритого ключа, пов'язаного з ним. Отже, він гарантує, що дані бачить та дешифрує лише той об'єкт, який має їх отримати. Це підтверджує, що ви розмовляєте чи обмінюєтеся інформацією з реальним об'єктом.

1.2.3. Алгоритм розділення секретів Діффі-Геллмана

Ідея алгоритму Діффі-Геллмана полягає у наступному [1]. Аліса та Боб спочатку вибирають параметри криптосистеми: мультиплікативну групу, якій належать усі її $(p-1)$ елементів, кінцевого поля F_p та g – генератор її підгрупи максимального порядку $(p-1)/2 = q$, де q – просте. Таким чином, обом абонентам відомі деякі два елемента g і p, які не є секретними і можуть бути відомі також іншим заінтересованим особам. Для того, щоб створити невідомий нікому секретний ключ в інтерактивному протоколі, обидва абоненти генерують великі випадкові числа: Аліса – число $a < p$, Боб – число $b < p$. Потім вони відповідно обчислюють і пересилають один одному

$$A = g^a \bmod p, B = g^b \bmod p, \tag{1.3}$$

де p – модуль простого поля F_p.

Передбачається, що криптоаналітик (зловмисник) може перехопити обидва ці значення, але не модифікувати їх (тобто, не може втручатися в процес передачі). На другому етапі Аліса на основі наявного у неї a та отриманого по мережі значення B обчислює

$$b^a \bmod p = g^{ba} \bmod p = K. \tag{1.4}$$

Аналогічні обчислення Боба дають результат

$$a^b \bmod p = g^{ab} \bmod p = K, \qquad (1.5)$$

який співпадає з першим в силу комутативності операції піднесення в степінь [19].

Цей секретний ключ K може далі використовуватися для шифрування за допомогою алгоритмів симетричного шифрування.

Криптоаналітик має значення A і B, але він стикається з практично нерозв'язною (за розумний час) проблемою обчислення (1.4) або (1.5) за перехопленими $A = g^a$ та $B = g^b$. Якщо числа p, a, b вибрано досить великими, він має проблему дискретного логарифмування (від англ. Discrete Logarithm Problem, DLP). Алгоритм показано на рис. 1.1.

Криптографічна стійкість алгоритму Діффі-Геллмана (тобто складність обчислення $K = g^{ab} \bmod p$ за відомими p, g, $A = g^a \bmod p$ та $B = g^b \bmod p$) заснована на передбачуваній складності DLP. Тобто треба знайти $a = \log_g A$ і $b = \log_g B$ за відомими публічними ключами A та B. Інтуїтивно ясно, що складність вирішення цих завдань залежить як від розміру поля F_p, так і від вибору параметрів (відкритого параметра g та секретних чисел a та b). Число p, зване модулем, має бути простим; число $(p-1)/2 = q$ теж має бути простим, а p і g мають бути досить великими – не менше 512 біт у двійковому поданні [1].

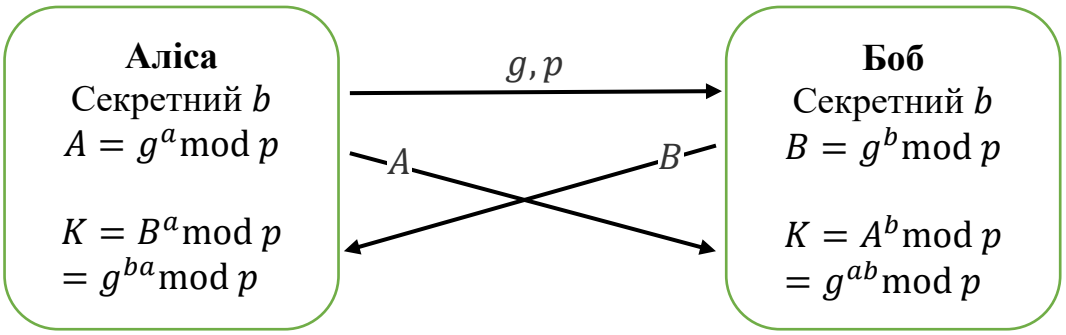

Рис. 1.1. Двостороння (інтерактивна) схема Діффі-Геллмана

Розглянутий варіант протоколу розділення секретів анонімний, тут відсутня можливість автентифікації абонентів. Таким чином, цей протокол вразливий для атаки «людина посередині». Крім того система Діффі-Геллмана вразлива до інших

атак, наприклад, атаки сторонніми каналами. Їхня суть полягає в тому, що зловмисник, аналізуючи непрямі ознаки, наприклад, час виконання обчислень у процесі шифрування та дешифрування, може отримати необхідні дані для криптоаналізу.

Є варіант, коли користувачі не потребують *спілкування* для узгодження секретного ключа. Одразу по прочитанні відкритого профілю користувача, з ним можна починати безпечний зв'язок. Цю властивість називають властивістю не інтерактивності протоколу Діффі-Геллмана.

Криптостійкість алгоритмів залежить від довжини ключа і складності перетворення об'єктів. В основі лежать складні завдання, які постійно змінюються і вдосконалюються по мері розвинення і модифікації алгоритму (рис. 1.2). Спочатку це була DLP в мультиплікативної групі кінцевого поля, потім з початку XXI сторіччя прийшов час еліптичних кривих. Трудним завданням стала задача дискретного логарифмування на еліптичній кривій.

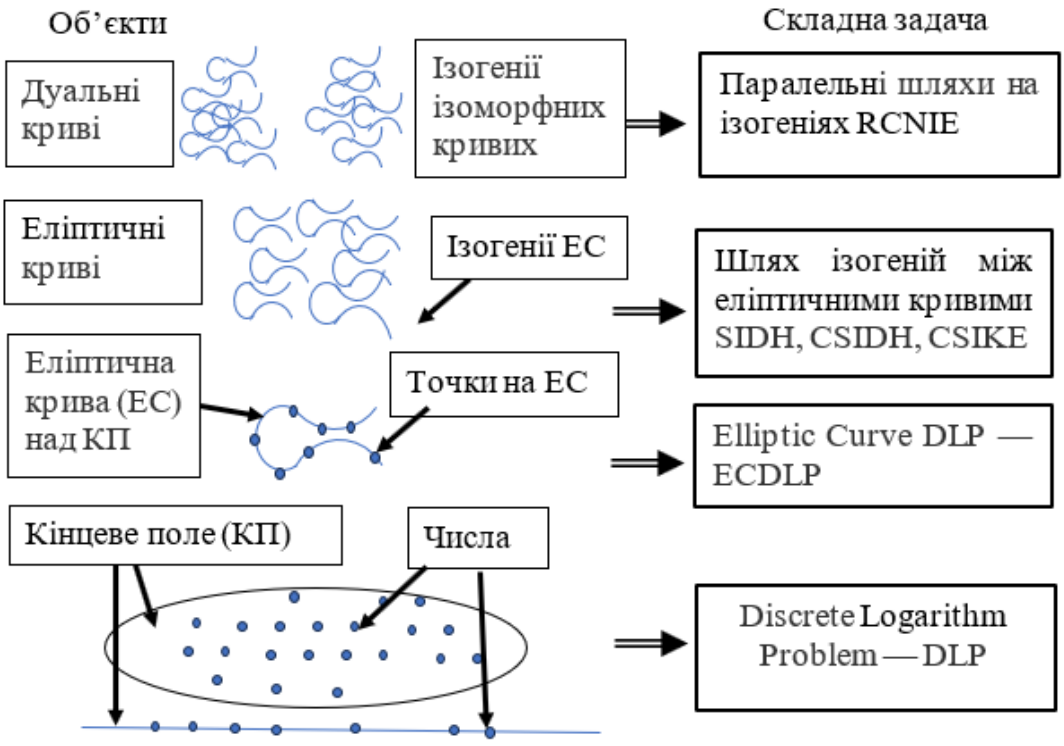

Рис. 1.2. Розвинення криптосистем лінійки Діффі-Геллмана

Останнє десятиріччя головна увага світу криптографії концентрується на PQC. Дуже перспективним сьогодні є використання ланцюжків ізогеній між еліптичними кривими. В розділі 4 розглядаються криптосистеми з паралельними обчисленнями на дуальних ізогенних кривих. Алгоритми лінійки CSIDH продовжують розвиватися.

1.3. Розвиток еліптичної криптографії

1.3.1. Особливості еліптичної криптографії

Криптосистеми на еліптичних кривих ECC запропоновано незалежно В. Міллером [5] і Н. Коблицем [6] у 1986 р. Було запропоновано використовувати групу точок еліптичної кривої з груповою операцією складання точок. Стійкість ECC базується на проблеми дискретного логарифмування на еліптичній кривій, яка експоненційно залежить від довжини ключа і наростає дуже швидко. ECC при однаковій стійкості з попередніми криптосистемами має розмір модуля поля p на порядок менше. ECC з розміром поля 160 біт забезпечує ту ж стійкість що традиційна криптосистеми з розміром модуля в 1024 біта [20].

Підвищений рівень захисту порівняно з класичними асиметричними алгоритмами пояснюється тим, що задача дискретного логарифмування в групі точок еліптичної кривої є значно складнішою, ніж у стандартних випадках [3, 4]. Головна перевага еліптичної криптографії полягає в тому, що наразі не існує субекспоненційних алгоритмів для розв'язання цієї задачі в таких групах.

Еліптична крива над простим полем F_p представляє набір точок (x, y), які задовольняють канонічному рівнянню

$$y^2 = (x^3 + ax + b) \bmod p, \tag{1.6}$$

разом з нейтральним елементом групи $O = (\infty)$ – точкою на нескінченності.

Для оперування точками еліптичних кривих розроблено спеціальну математику і метод дискретного логарифмування на еліптичній кривій.

Вважається, що для досягнення такого ж рівня крипостійкості, як і в RSA, потрібні групи менших порядків, що зменшує витрати на зберігання та передачу інформації. Алгоритми з відкритим ключем, які ґрунтувалися на основі модулярної арифметики (RSA, DSA та Діффі-Геллмана) сталі замінюватися на алгоритми на ґрунті еліптичних кривих ЕС. ЕС дозволила скоротити розмір ключа при такому ж рівні стійкості або підвищити стійкість при тому ж розмірі ключа.

Групова операція над точками еліптичної кривої це багаторазове складання точки із собою, тобто множення на постійну скалярну величину. Тобто операція скалярного множення точки еліптичній кривій на ціле число. Реалізується групова операція через операції складання та подвоєння точок еліптичної кривої, які, у свою чергу, виконуються на основі операцій складання, множення та інвертування в кінцевому полі, над якими розглядається крива [21].

Переваги шифрування на основі еліптичних кривих:

– ECC вимагає менше обчислювальних ресурсів і менше смуги пропускання для генерації ключів, шифрування та дешифрування;

– завдяки меншому розміру ключа, операції ECC, такі як генерація ключа, шифрування та дешифрування можуть виконуватися швидше в порівнянні з RSA, що означає меншу затримку для кінцевого користувача.

Ці переваги роблять ECC особливо корисним у середовищах з обмеженими ресурсами, таких як безпроводові і мобільні пристрої, а також пристрої інтернету речей [22].

Хоча ECC використовує коротші ключі порівняно з RSA, вона забезпечує вищий рівень захисту від сучасних методів злому. Асиметричні криптосистеми на основі еліптичних кривих гарантують високий рівень безпеки навіть при малій довжині ключа, що дає їм перевагу над RSA та іншими алгоритмами. Крім того, ECC є лідером у сфері PQC, готуючи систему до потенційних загроз, пов’язаних із появою квантових комп’ютерів.

Ще однією перевагою використання коротших ключів є підвищена продуктивність. Вони зменшують навантаження на мережу та споживання обчислювальних ресурсів, що особливо важливо для пристроїв із обмеженими

можливостями зберігання та обробки даних. Використання ECC у SSL/TLS сертифікатах значно скорочує час шифрування та дешифрування, що сприяє швидшому завантаженню веб-сайтів.

ECC має визнання і розвиток в усьому світі. Наприклад, на конференції RSA 2005 Агентство національної безпеки оголосило про створення «Suite B», в якому використовуються виключно алгоритми еліптичної криптографії, причому для захисту інформації, що класифікується до «Top Secret», використовуються лише 384-бітові ключі [21].

Сучасна криптографія з відкритим ключем ґрунтується на математиці еліптичних кривих. Вона забезпечує безпеку та високу продуктивність, високу швидкодію та невелику довжину ключа, а також безпечний спосіб виконання криптографічних операцій, таких як обмін ключами, цифрові підписи та шифрування.

Криптографія на еліптичних кривих ECC реалізована у вигляді алгоритмів ECDH та використовуються в TLS, PGP, SSH та інших найважливіших технологіях, на яких базуються сучасний веб та світ інформаційних технологій.

1.3.2. Властивості еліптичних кривих

Еліптичною кривою над полем K в узагальненій формі Вейєрштрасса вважається множина точок (x, y), що задовольняють рівнянню 3-го ступеня:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, a_i \in K. \quad (1.7)$$

Розрізняють еліптичні криві у формі Лежандра, Монтґомері, Гесс, Едвардса та інші. Всі форми мають свої властивості, які визначають їх використання. Використання тієї чи іншої форми може збільшити ефективність операцій над точками еліптичної кривої.

Якщо характеристика поля F не дорівнює 2 і 3 то криву (1.7) можна привести аморфним перетворенням до більш простої форми яка називається короткою (або канонічною, спрощеною або нормальною) формою Вейєрштрасса [21]:

$$W: y^2 = x^3 + Ax + B \ (\mathrm{mod}\, p). \tag{1.8}$$

Важливою характеристикою еліптичної кривої є її дискримінант, який для форми Вейєрштрасса обчислюється як:

$$\Delta = 4a^3 + 27b^2 \tag{1.9}$$

і постійна характеристика J-інваріант, яка залежить від параметрів кривої:

$$J = 1728\,\frac{4a^3}{4a^3 + 27b^2} \tag{1.10}$$

У додатках та алгоритмах часто використовується еліптична крива Монтґомері, ізоморфна кривої Вейєрштрасса, яка має вигляд:

$$\text{M: } v^2 = u^3 + Au^2 + Gu, \{A, G\} \in K. \tag{1.11}$$

Точки еліптичної кривої у купі з абстрактною нескінченно віддаленою точкою утворюють адитивну абелеву групу. Як відомо з [23], група має наступні властивості:

– *замкнутість* означає, що результат складання елементів групи також є елементом групи. Перекладемо в терміни еліптичної кривої: при складанні точок еліптичної кривої виходить точка, що належить цій же кривій;

– *асоціативність* означає незалежність результату додавання від зміни порядку дії. У групі має існувати нейтральний елемент. Результат складання будь-якого елемента групи та нейтрального дорівнюватиме тому ж елементу. У еліптичних кривих роль нейтрального елемента часто грає нескінченно віддалена точка. До кожного елемента має існувати зворотний (щодо основної операції). При складанні елемента групи та зворотного отримуємо нейтральний елемент;

– властивість *комутативності* робить групу абелевою.

Множина точок еліптичної кривої є групою тому, що має всі властивості групи. Зокрема:

– є нейтральний елемент – це нескінченно віддалена точка 0;

– є зворотна точка P – це точка, симетрична щодо осі x;

– існує групова операція – додавання.

Операція додавання задається наступним правилом: на кривій сума будь-яких трьох ненульових точок P, Q, R, що лежать на одній прямій, дорівнює нулю $P + Q + R = 0$. Звідси легко визначити правило складання чисел та подвоєння

«Циклічна підгрупа кривої» має елементи, які створюються скалярним множенням цілого числа на точку, яка зветься генератором або базовою точкою циклічної підгрупи G. Циклічні підгрупи є фундаментом для криптосистем ECC.

Перехід на «еліптичну» криптографію дозволяє зберегти прийнятну довжину ключа при різкому (на порядки) збільшенні стійкості криптосистем. Поява «еліптичної» криптографії і була обумовлена саме цією причиною.

1.3.3. Криптосистеми на еліптичних кривих

ECC, як і інші асиметричні системи, мають два ключі:

1. Закритий ключ – випадкове ціле число d, обране з $\{1, \dots, n-1\}$, де n – порядок підгрупи [24].

2. Відкритий ключ – це точка $H = dG$, де G – базова точка підгрупи. Якщо відомі d і G, то знайти H «просто». Але якщо відомі H і G, то пошук закритого ключа d є «складним» завданням, тому що вимагає розв'язання задачі дискретного логарифмування.

У криптографії на еліптичних кривих роль групової операції виконує скалярне множення точки еліптичної кривої на ціле число. Це адитивний аналог зведення у ступінь у мультиплікативній групі, тому теж зветься експоненціонуванням. Реалізується операція на основі операцій складання та подвоєння точок еліптичної кривої. Останні, у свою чергу, описуються та виконуються на основі операцій множення, зведення в ступінь та інвертування в кінцевому полі [21].

$$kP = P + \cdots + P, \tag{1.12}$$

де операція додавання виконується k разів.

Особливий інтерес до еліптичної криптографії обумовлений тими перевагами, які дає її застосування в безпроводових і мобільних комунікаціях – швидкодія та невелика довжина ключа [20].

Тоді можна використовувати менші за величиною прості числа, ніж у класичних системах з відкритим ключем.

У NIST для порівняння RSA та ECC, розроблено табл. 1.1 порівняння розмірів ключів RSA та ECC, необхідних для отримання однакового рівня захисту.

Таблиця 1.1

Порівняння розмірів ключів

Ключ RSA, біт	Ключ ECC, біт	Симетричний ключ, біт
1024	160	80
2048	224	112
3072	256	128
7680	384	192
15360	521	256

Стійкість асиметричної криптографії базується на складності розв’язання певних математичних задач, які вимагають значних обчислювальних ресурсів. Ранні криптосистеми з відкритим ключем, такі як RSA, забезпечували захист завдяки складності факторизації великих чисел. Натомість криптостійкість алгоритмів на основі еліптичних кривих зумовлена труднощами розв’язання задачі дискретного логарифмування в групах точок кривої. Вважається, що наразі не існує субекспоненційних алгоритмів, здатних ефективно вирішувати цю задачу.

Тобто асиметричні криптографічні алгоритми у ECC конструюються на основі обчислювальних складнощів: складання точок з раціональними координатами еліптичної кривої над кінцевому полі. Відповідну групову операцію для прийомності термінології звуть експоненціонуванням точки, а зворотна операція дискретне логарифмування.

Крипостійкість системи це стійкість до злому та перехоплення інформації (несанкціонованого доступу) третіми особами. Стійкість визначається ресурсами необхідними перехоплення. Чим більше потрібно ресурсів, тим вище стійкість (або

захист) тобто. складніше завдання злому шифру. Ресурси – це час і обчислювальні потужності (пам’ять і швидкодія).

1.3.4. Алгоритм Діффі-Геллмана на еліптичних кривих

Алгоритм ECDH полягає в наступному:

1. Аліса і Боб використовують однакові параметри відкритої області визначення: базову точку G на одній еліптичній кривій E_o в кінцевому полі F_q, $q = p^n$.

2. Спочатку Аліса та Боб генерують випадкові власні закриті та відкриті ключі. Аліса має закритий ключ d_a і відкритий ключ $H_A = D_A G$, у Боба є ключі d_b і $H_B = D_B G$. Звернемо увагу, що закриті ключі є елементами поля, а відкриті ключі – точки кривої (елементи групи точок).

3. Аліса та Боб обмінюються відкритими ключами H_A і H_B по незахищеному каналу. Якщо посередник при атаці «людина посередині» перехоплює H_A і H_B, то не може визначити ні d_A, ні d_B, не вирішивши задачі дискретного логарифмування.

4. Аліса обчислює $S = d_A H_B$ (за допомогою власного закритого ключа та відкритого ключа Боба), а Боб обчислює $S = d_B H_A$ (за допомогою власного закритого ключа та відкритого ключа Аліси). S однакові й у Аліси, й у Боба. В силу комутативності скалярного множення точки

$$S = d_A H_B = d_A(d_B G) = d_B(d_A G) = d_B H_A. \quad (1.13)$$

Посереднику відомі лише H_A і H_B (разом з іншими параметрами області визначення) і він не зможе знайти загальний секретний ключ S. Це відомо як завдання Діффі-Геллмана на еліптичних кривих [25].

Зворотне завдання Діффі-Геллмана для еліптичних кривих вважається так само «складним», як завдання дискретного логарифмування. Схему алгоритму ECDH зображено на рис. 1.3.

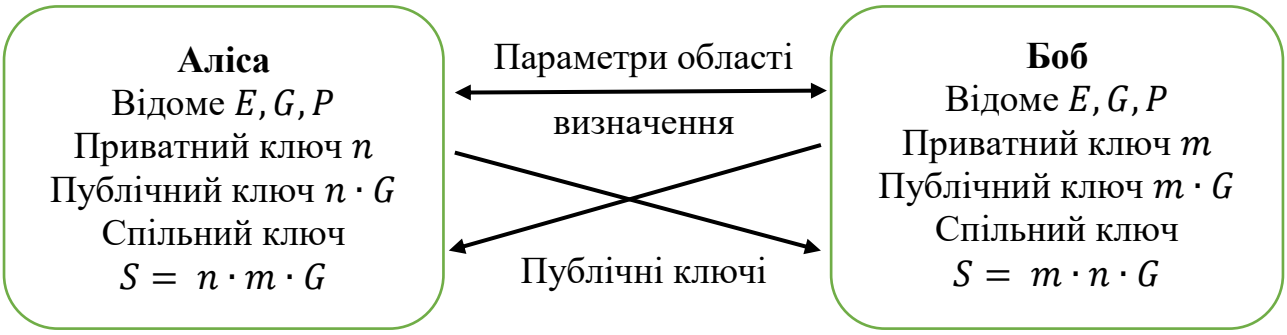

Рис. 1.3. Схема алгоритму Діффі-Геллмана на еліптичних кривих ECDH

Але складність дискретного логарифмування легко долається квантовим комп'ютером, тому алгоритм ECDH не є квантово резистентним. Тому у наступний постквантовий період використовується наступна модифікація алгоритму Діффі-Геллмана, це алгоритм CSIDH – комутований алгоритм Діффі-Геллмана на ізогеніях суперсінгулярних еліптичних кривих.

1.4. Постквантова криптографія

1.4.1. Основні методи постквантової криптографії

Незважаючи на те, що квантовий комп'ютер має ще багато конструктивних проблем, і невідомо, коли він з'явиться, фахівці в сфері PQC ведуть дослідження у багатьох можливих напрямках. Найбільш важливими є наступні основні підходи до синтезу постквантової моделі [26].

1. Криптографія, основана на хеш-функціях.
2. Симетричне шифрування с секретним ключом (наприклад, AEC).
3. Використання теорії цілих решіток.
4. Криптографія, основана на багатовимірних квадратичних системах.
5. Використання кодів, які виправляють помилки.
6. Використання багаточленів від багатьох змінних.
7. Використання ізогеній СКЕ.

8. Використання ізогеній НКЕ.

9. Проблеми сполученого пошуку (search problem) або операції у групах кіс (braid groups), алгебра октоніонів, багаточлени Чебишева тощо.

Протягом кількох років повністю небезпечними стають багато традиційних алгоритмів криптографії, наприклад:

– розподіл ключів (ECDH, Діффі-Геллмана);

– асиметричне шифрування (RSA);

– електронний підпис (ECDSA, DSA, ГОСТ Р 34.10-2018).

Розглянемо найбільш відомі алгоритми, що знаходяться у розробці:

1. Симетричні алгоритми-дуже швидкі і легко збільшувати стійкість збільшенням довжини ключа. При цьому складність процесу шифрування-дешифрування на багато простішій ніж асиметричних систем. Але симетричні алгоритми мають проблеми з керуванням ключами.

2. Асиметричні алгоритми на еліптичних кривих. Криптостійкість систем, основу яких складають операції над еліптичними кривими, спирається на складність обчислення дискретного логарифма. Такі системи мають меншу довжину ключа, для такого ж рівня безпеки. Також існують рекомендації деяких організацій, наприклад NIST: поточний стандарт ставить у відповідність 2048-бітному ключу для RSA 224-бітний ключ для криптосистем, заснованих на еліптичних кривих. Підраховано, що для підбору такого ключа знадобиться квантова машина, що має 1 600 кубітів.

3. Коди, що виправляють помилки. Такі криптосистеми засновані на теорії кодування, а самі алгоритми базуються на складності декодування повних лінійних кодів. Головними недоліками систем є великий розмір відкритого ключа та значне збільшення довжини зашифрованого повідомлення порівняно з вихідним. Однак такий підхід у PQC вважається одним з найбільш перспективних через відсутність серйозних недоліків (на кшталт обмеженої кількості підписів.

4. Ізогенії еліптичних кривих. Допустимість застосування ізогеній для розробки криптосистем була запропонована відносно недавно. Саме завдання, на складності якої можна вибудовувати криптосистему, можна сформулювати так: є

дві криві, про які відомо, що вони ізогенні (за теоремою Тейта), але невідомо, за допомогою якої підгрупи можна отримати цю ізогенію. Число підгруп має бути настільки великим, щоб неможливо було знайти ізогенію простим перебором, підставляючи підгрупи в алгоритм Велю (алгоритм пошуку можливих ізогеній для кожної кривої) [27].

Переваги ізогеній: система дозволяє шифрування з відкритим ключем, та здійснювати обмін ключами; невеликий розмір ключа. Недоліки: відносно повільний алгоритм, малопридатний для використання на невеликих, обмежених у ресурсах пристроях; це відносно нова та невивчена область.

У 2016 р. Національний інститут стандартів та технологій США опублікував звіт «NISTIR 8105: Report on Post-Quantum Cryptography», у якому проаналізовано основні підходи до побудови постквантових криптосистем [28]. Інформація з цього звіту і нова інформація після 2016 р. представлено в табл. 1.2.

Таблиця 1.2

Основні підходи до побудови постквантових криптосистем

Система	Тип	Властивості	Можливості
AES	Симетрична	Шифрування	Збільшення ключа
SHA-2, SHA-3	Хеш-функція	Хешування	Збільшення вихідної послідовності
RSA	Асиметрична	Формування загального ключа, підпис	Не стійкий
ECDSA, ECDH. Криптографія на еліптичних кривих	Асиметрична	Формування загального ключа, підпис	Не стійкий
DSA. Криптографія над кінцевими полями	Асиметрична	Формування загального ключа, підпис	Не стійкий
NTRU. Криптографія на решітках	Асиметрична	Більші розміри відкритих ключів ніж у RSA, ECC	Стійкий
Схема Ель-Гамаля	Асиметрична	Великі розміри відкритого ключа та шифротексту	Стійкий
Ізогенії SIDH	Асиметрична	Схильний до атак	Стійкий
Ізогенії CSIDH	Асиметрична	Схильний до атак сторонніми каналами	Стійкий

Лінійка алгоритмів CSIDH є досить конкурентоспроможною для використання у постквантовий період.

1.4.2. Ефективність квантових атак

Існують класичні криптосистеми, які спираються на обчислювально-складні завдання, які складно вирішити за доступний для огляду час. Ці системи незалежні від квантових атак і вважаються квантово-стійкими або «постквантовими» криптосистемами.

Криптографи всього світу нині ведуть розробку алгоритмів, стійких до квантових атак. PQC – це створення нових криптографічних алгоритмів, стійких до кібератаки із застосуванням квантових комп'ютерів, а також дослідження та посилення технологій з використанням вже перевірених квантово-стійких алгоритмів.

У 2017 р. Національним інститутом стандартів та технологій США було розпочато конкурс NIST, покликаний стандартизувати набір квантово-стійких криптографічних схем. Через кардинальні відмінності підходів у постквантової криптографії пряме порівняння алгоритмів часто неможливе, тому діяльність NIST спрямована на збільшення продуктивності представлених алгоритмів та отримання більшої впевненості у їхній захищеності.

Для асиметричної криптографії квантовий комп'ютер становить небезпеку лише за наявності відповідних алгоритмів. Таким алгоритмом є алгоритм Шора [8] запропонований 1994 року. Справа в тому, що одне із завдань, які досить легко вирішує квантовий комп'ютер це швидко знаходити період функції. Пітер Шор запропонував спочатку на квантовому комп'ютері визначати період деякої пов'язаної з криптосистемою функції, а потім на звичайному комп'ютері легко перебуває розкладання числа на множники або дискретний логарифм за досить найближчий час. Таким чином, завдання факторизації та дискретного

логарифмування зводяться до завдання знаходження періоду деякої функції, тому квантовий комп'ютер у цьому випадку прискорює криптоаналіз.

Однак завдання на ізогеніях еліптичних кривих не зводяться до знаходження періоду відповідної функції і відсутній відповідний алгоритм, який дозволяє вирішувати на квантовому комп'ютері важкі завдання на ізогеніях еліптичних кривих. Тому ці завдання не піддаються швидкому вирішенню на квантовому комп'ютері і використання ізогеній еліптичних кривих залишається актуальним у постквантовий період.

Таким чином небезпеки піддаються методи засновані на труднощі розбиття чисел на множники та дискретного логарифмування. Тому криптоаналіз прискорюється лише алгоритмів заснованих на складності цих операцій. Зокрема до них відносяться RSA, алгоритм Діффі-Геллмана засновані на польових операціях. При цьому алгоритми, засновані на ізогенії (наприклад, CSIDH) стійкі до аналізу квантового комп'ютера.

Таким чином, PQC має на увазі розвиток саме класичної криптографії, при цьому стійкості постквантові криптосистеми повинні мати стійкість до квантового криптоаналізу.

1.4.3. Суперсингулярні еліптичні криві

У постквантових системах використовуються, як правило, СКЕ. Еліптична крива E задана над кінцевим полем F_q, де $q = p^n$ ступінь простого числа називається суперсингулярною якщо $|E(F_q)| \equiv 1 \pmod p$.

СКЕ зручні для побудови ECC-криптосистем, оскільки їхній порядок легко обчислити, на відміну від НКЕ, для яких це завдання є значно складнішим.

Порядок N_E еліптичної кривої над простим полем F_p визначається на основі сліду t характеристичного рівняння Фробеніуса $\phi^2 + t\varphi + p = 0$ як $N_E = p + 1 - t$. Еліптична крива є суперсингулярною тоді і лише тоді, коли над будь-яким розширенням простого поля F_p слід рівняння Фробеніуса $t \equiv 0 \bmod p$ [23]. В

алгебраїчному замиканні $\bar{F}_p$ СКЕ не містить точок порядку p. Над простим полем F_p така крива завжди має порядок $N_E = p + 1$.

СКЕ мають правильний граф ізогеній фіксованого ступеня (тобто у кожної вершини є однакове число ребер). Для будь-якого простого числа l, яке ділить порядок групи точок кривої, існує $l + 1$ ізогеній з ядром порядку l (тобто існує $l + 1$ підгрупа порядку l, за допомогою якої можна обчислити ізогенію).

СКЕ дозволяють будувати криптографічні схеми, в основі стійкості яких лежить припущення про складність задачі пошуку шляху між двома вершинами в графі ізогеній. Ці властивості використовувалися в роботах [11], [29] і [30], коли вперше вдалося запропонувати стійкий та ефективний протокол вироблення загального ключа на СКЕ.

1.4.4. Криптографія на основі ізогенії еліптичних кривих

Однією з головних переваг є те, що квантові комп'ютери не суттєво полегшують завдання пошуку ізогенії на відміну від точок звичайної еліптичної кривої, яка заснована на задачі дискретного логарифму в групі. Тому алгоритм Діффі-Геллмана піддається аналізу на квантовому комп'ютеру на основі алгоритму Шора, а алгоритми на ізогеніях не піддається.

Ізогенія – це раціональне відображення між двома еліптичними кривими, що є гомоморфізмом. Якщо існує такого роду відображення між двома кривими, то вони називаються ізогенними. Ізогенія двох еліптичних кривих E_1 і E_2 над одним і тим же полем F це не нульовий гомоморфізм еліптичних кривих заданих раціональними відображеннями, які в явному вигляді задаються раціональними функціями. По теоремі Тейта еліптичні криві E_1 і E_2 ізогенні над тим самим полем F_q якщо їх порядки однакові $N_1(F_q) = N_2(F_q)$.

Завдання PQC сьогодні успішно вирішуються різними алгоритмами, серед яких досить перспективними, зарекомендували себе алгоритми на ізогеніях СКЕ [10, 31].

Криптографія на основі ізогенії еліптичних кривих це відносно новий вид криптографії з еліптичними кривими, безпека якого заснована на проблемі пошуку явного відображення ізогенії між двома заданими ізогенними еліптичними кривими над кінцевим полем F_q.

Перша пропозиція криптосистеми, заснованої на ізогенії, була зроблена Кувенем у 1997 р. Він описував неінтерактивний протокол обміну ключами, на основі ізоморфізму звичайних еліптичних кривих над полем F_q.

Після забуття метод був незалежно перевідкритий Ростовцевим та Столбуновим на звичайних НКЕ у 2004 р. Схему назвали CRS, вона реалізована на ізогенії НКЕ [18]. Нестача методу є в тому, що схема дуже повільна: для одного обміну ключами потрібно кілька хвилин при передбачуваному класичному рівні безпеки 128 біт. Проте схема дуже проста, компактна та гнучка. Схема CRS стала історичною передумовою алгоритму SIDH, який був першою модифікацією на ізогеніях на основі алгоритму Діффі-Геллмана.

Криптосистема SIDH «Суперсингулярна ізогенія Діффі-Геллмана» була перша розроблена інтерактивна схема узгодження ключів на СКЕ, яка пропонована авторами Девідом Джао і Лукою Де Фео [11] для вирішення задачі обміну ключами на основі ізогенних відображень еліптичних кривих в цілому як адитивних абелевих груп, на ґрунті кривих Монтґомері. Ця схема за останні роки привернула майже всю увагу криптографії, що ґрунтується на ізогенії. Вона є протоколом обміну ключами аналогічний алгоритм Діффі-Геллмана, де використовується множина СКЕ над кінцевим полем.

На основі протоколу SIDH була створена схема інкапсуляції ключа суперсингулярної ізогенії (від англ. Supersingular Isogeny Key Encapsulation, SIKE), що дійшла до четвертого етапу конкурсу NIST. Схема SIDH дуже ефективна, однак у цій схемі виявлено уразливості [12]. Виявлено, що ключі SIDH піддаються активним атакам. Таким чином, в даний час ефективні криптографічні алгоритми SIDH, засновані на ізогенії, вважаються нестійкими і тому застосування SIDH не рекомендується.

Проте ця технологія отримала розвинення і продовження у вигляді комутованих технології CSIDH та CSIKE, які не мають вразливостей властивих SIDH і знайшли широкий розвиток та застосування.

1.4.5. Криптосистема CSIDH

Класична криптосистема CSIDH використовують операції у простому полі F_p на відміну від розширеного поля F_{p^2}, яке використовується у SIDH. Що для даного p вдвічі знижує довжину елементів поля та розміри ключів. Алгоритм CSIDH став ефективною альтернативою протоколу SIDH і має мінімальну з відомих довжину ключа.

Алгоритм CSIDH – це продовження лінійки протоколів (алгоритмів) обміну ключами, безпека якого заснована на складності знаходження ізогенії між двома СКЕ. Дана схема є стійкою до атаки Кастріка і Декру. Конструкція схеми ґрунтується на криптосистемі Ростовцева-Столбунова, де замість звичайних еліптичних кривих застосовуються СКЕ. На відміну від SIDH у схемі CSIDH використовується дія комутативної групи. Вперше протокол CSIDH описано у 2018 р. В. Кастріком, Т. Ланге та ін. [10]. Згодом він став основою численних технічних модернізацій.

В алгоритмі CSIDH використовується технологія СКЕ, що обґрунтовується порівняно швидкою імплементацією алгоритму. Спочатку використовувалися криві Монтґомері, але наразі значне місце займають криві Едвардса. Замість зведення у ступінь як у класичних алгоритмах в алгоритмі CSIDH використовується групова операція на ґрунті ізогенного відображення кривих [10].

Криптографія на ізогенії істотно відрізняється від попередніх типів, оскільки заснована на задачі, обчислення ізогеній між еліптичними кривими. А зворотне обчислення – це пошук шляху у графі ізогеній між СКЕ над $GF(p^2)$ це є дуже складне завдання. Класична складність – $O(p^{1/2})$; квантова складність – $O(p^{1/3})$.

Криптосистеми на ізогенії складають один з небагатьох алгоритмів, на даний момент стійких до атак з використанням квантового комп’ютера. У певному сенсі задачу знаходження ізогенії можна розглядати як аналог задачі дискретного логарифмування, в рамках якого замість абелевої групи точок кривої використовують граф ізогеній.

Складність алгоритму визначається тим що квантовий комп’ютер вирішує задачу дискретного логарифму в групі точок еліптичної кривої за поліноміальний час, для обчислення ізогенії існуючими алгоритмами потрібен субекспоненційний час при використанні звичайних еліптичних кривих та експоненційний час при використанні СКЕ.

Таким чином до основних властивостей криптосистем на ізогенії варто віднести невеликі розміри ключів і відносно повільну швидкість роботи. Також досить складною є процедура обчислення ізогеній. Незважаючи на це, криптографічні системи даного типу виглядають багатообіцяюче, але потребують ще дослідження для підвищення швидкодії і захисту.

Криптосистеми на ізогеніях є найперспективнішими системами PQC. Вони мають малий розмір ключа, але основною проблемою є повільна швидкість роботи. Тому найбільш важливим напрямом у галузі ізогеній є дослідження питань оптимізації з метою підвищення швидкодії наявних схем.

Відомою проблемою алгоритму CSIDH є вразливість до атаки сторонніми каналами, побудованої на вимірі часу обчислення ланцюжка ізогеній кожного ступеня, пропорційного секретній експоненті ключа.

1.4.6. Алгоритм CSIDH на ізогеніях

Алгоритм PQC CSIDH, побудованого за оригінальною схемою на ізогеніях еліптичних кривих CRS. Кастрік та ін. заявили, що він має найменшу з відомих довжину ключа 512 біт при рівні безпеки 128 біт. Водночас були відзначені проблеми з уразливістю до атак сторонніми каналами та швидкодією, як наслідок

схеми CRS. Для подолання повільності реалізації схеми CRS автори обґрунтували свій вибір суперсингулярних еліптичних кривих у формі Монтґомері замість несуперсингулярних у CRS, що прискорює імплементацію в 2 000 разів.

CSIDH – це новий криптографічний алгоритм, який може бути повною заміною протоколу обміну ключами ECDH, набуваючи при цьому стійкості до атак квантових комп'ютерів. Він забезпечує неінтерактивний (статичний) обмін ключами із повною перевіркою відкритого ключа. Розмір відкритого ключа є найменшим серед протоколів PQC. Це робить CSIDH особливо привабливим для подальшого розвитку та збільшення пропускної спроможності.

Імплементація оригінального алгоритму CSIDH переважно використовує швидку арифметику еліптичних кривих Монтґомері

$$y^2 = x^3 + Cx^2 + x,\ C \neq \pm 2, \tag{1.14}$$

які мають дві точки 4-го порядку і, відповідно, мають порядок $N_E = 4n$ (n – не парне, $n = \prod_{k=1}^{K} l_k$) [10].

У роботі [32] алгоритм будується на повних кривих Едвардса того ж порядку. Ідея CSIDH полягає у наступному: нехай крива E порядку $N_E = p + 1 \equiv 0 \bmod 8$ містить точки малих непарних порядків $l_k, k = 1,2, \dots, K$. Тоді існує ізогенна крива E' того ж порядку N_E як відображення ступеня l_k: $E \to E' = [l_k] * E$. Повторення цієї операції e_k раз будемо позначати $[{l_k}^{e_k}] * E$. Значення експонент $e_k \in Z$ визначають довжину ланцюжка ізогеній ступеня l_k. У роботі [10] прийнято інтервал значень експонент $[-m \leq e_k \leq m], m = 5, K = 74$, що забезпечує рівень безпеки 128 бітів при атаках квантового комп'ютера. Негативні значення експоненти e_i означають перехід до СКЕ квадратичного кручення.

Пропонується використовувати в алгоритмі CSIDH квадратичні та скручені СКЕ, що мають ті ж рекордні показники швидкодії, що й повні криві Едвардса. Така можливість виникає на основі теорем, доведених у [33]. При мінімальному кофакторі 8 порядок квадратичних та скручених СКЕ $N_E = 8n = p + 1$ модуль поля в алгоритмі CSIDH слід вибирати як $p \equiv 7 \bmod 8$ або $p = 8 \prod_{k=1}^{K} l_k - 1$.

Підкреслимо, що заміна одного класу повних СКЕ двома класами квадратичних і скручених СКЕ подвоює число кривих, що використовуються в

алгоритмі CSIDH, і, як наслідок, його безпеку [34]. Це подвоєння пояснюється тим, що параметр d всіх повних кривих Едвардса пробігає всі $\frac{p-1}{2}$ значень квадратичних не лишків, тоді як для двох інших класів використовуються всі значення $d \neq 0,1$.

Важливою перевагою CSIDH є також те, що можна ефективно перевіряти відкриті ключі, що дає змогу повторно використовувати ключ без необхідності перетворень для підтвердження того, що ключ іншої сторони був згенерований чесно. Таким чином, CSIDH має найменший розмір відкритого ключа, забезпечує неінтерактивний (статичний) обмін ключами з повною перевіркою відкритого ключа. Це робить CSIDH особливо привабливим.

Не інтерактивна схема алгоритму Діффі-Геллмана поділу секретів як пропонують автори [10] включає три етапи:

1. Вибір параметрів. Для непарних простих l_kобчислюється $n = \prod_{k=1}^{K} l_k$, обирається відповідний модуль поля $p = 2^m \prod_{k=1}^{K} l_k - 1, m \geq 3$ та стартова еліптична крива E_0.

2. Обчислення відкритих ключів. Аліса і Боб за допомогою секретних ключів у формі векторів $\Omega_{A,B} = (e_1, e_2, \dots, e_K)$ будують ізогенні відображення $\Theta_{A,B} = [{l_1}^{e_1}, {l_2}^{e_2}, .., {l_K}^{e_K}]$ і обчислюють ізогенні криві $E_{A,B} = \Theta_{A,B} * E_0$ як свої відкриті ключі. Ці криві визначаються їх параметрами з точністю до ізоморфізму.

3. Обмін ключами. Тут протокол подібний до п. 2 із заміною $E_0 \to E_B$ для Аліси та $E_0 \to E_A$ для Боба. Знаючи відкритий ключ Боба, Аліса обчислює $E_{BA} = \Theta_A * E_B = \Theta_A \Theta_B * E_0$. Аналогічні дії Боба дають результат $E_{AB} = \Theta_B * E_A = \Theta_B * \Theta_A * E_0$, збігається з першим з комутативності груповий операції. Як розділений секрет береться J-інваріант кривої E_{AB} (E_{BA}). Схема алгоритму зображена на рис. 1.4.

Дуже важливо, що для кожної функції Θ існує мультиплікативно зворотна $\overline{\Theta}$, така що $\Theta * \overline{\Theta} = I$, де $I = [1,1,1, \dots,1]^K$ – нейтральний елемент комутативної групової дії (від англ. Commutativ Group Action, CGA), K – мірний вектор з одиниць. Відображення $\overline{\Theta}$ будується шляхом інверсії знаків усіх експонентів e_k

відображення Θ. Ця властивість використовується у розділі 3 в алгоритмі інкапсуляції ключа CSIKE.

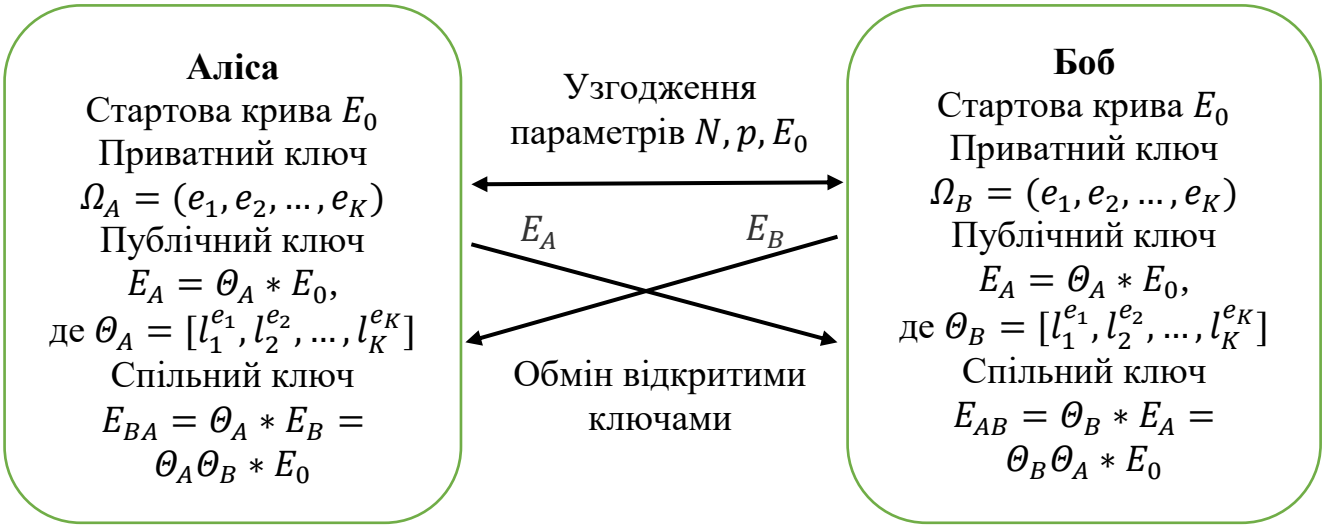

Рис. 1.4. Схема оригінального алгоритму CSIDH

Складним завданням для системи Діффі-Геллмана було: знайти k^{xy}, якщо відомі три цілих числа k, k^x і k^y.

У той час як у алгоритмі Діффі-Геллмана, заснованому на модулярній арифметиці, це завдання має вигляд: знати abP для відомих трьох точок P, aP і bP. В алгоритмі CSIDH складним є знайти $\Theta_A\Theta_B * E_0$ для відомих P, $\Theta_A * E_0$, $\Theta_B * E_0$.

1.5. Постановка наукового завдання дослідження

Таким чином алгоритм CSIDH, який є першим асиметричним алгоритмом і тому є основою для багатьох модифікацій, що значно покращили його властивості. На початку бурхливого розвитку постквантових криптосистем модернізація алгоритму CSIDH досягла рівня, коли у ньому використовувались ізогенії еліптичних кривих і алгоритм став вже квантово резистивним. Для вирішення подібних задач в основному використовуються еліптичні криві Монтгомері. При цьому основні властивості алгоритму зберігаються: він досить простий, гнучкий,

має малий розмір ключа, але також збереглися і основні недоліки, до яких належать відносно невелика швидкість і вразливість до атаки сторонніми каналами.

Незабаром почали використовуватись еліптичні криві Едвардса, які мають рекордно малу довжину ключа і тому спростилися групові операції на ізогеніях цих кривих, але основні недоліки збереглися, тому треба продовжувати модернізацію криптосистеми CSIDH.

Шляхів модернізації досить багато. У першу чергу, це вибір параметрів і властивостей еліптичної кривої, а також способи вибору, які дозволяють збільшити швидкодію і захист криптосистеми. Слід розглянути метод реалізації групової операції і знати такий, що може виконуватися швидше. Оскільки зазвичай для виконання алгоритмів використовується множина з великою кількістю ізогеній, то вибір цієї множини впливає на параметри криптосистеми.

У зв’язку з цим, існує необхідність вирішення актуального наукового завдання, сутність якого полягає в подальшому розвитку методів вдосконалення використання криптосистеми CSIDH на еліптичних кривих Едвардса шляхом підвищення швидкодії і захисту від атаки сторонніми каналами для забезпечення безпечного розподілу секретних ключів користувачів.

Метою дисертаційного дослідження є в підвищенні швидкодії і безпеки постквантового асиметричного криптоалгоритму CSIDH шляхом його моделювання і модернізації з використанням властивостей еліптичних кривих у формі Едвардса.

У відповідності до поставленої мети для вирішення наукового завдання в роботі мають бути розв’язані такі *часткові завдання*:

– проаналізувати поточний стан і властивості класичних криптоалгоритмів Діффі-Геллмана, які працюють на еліптичних кривих і мають відмінні криптографічні параметри;

– визначити можливості покращення роботи криптоалгоритмів Діффі-Геллмана на ізогеніях еліптичних кривих, які здатні працювати у постквантових умовах при здійсненні атак з боку потужних квантових комп’ютерів;

– визначити властивості кривих Едвардса як оптимальних кандидатів для використання у постквантових алгоритмах;

– обґрунтувати клас і дослідити властивості еліптичних кривих Едвардса, які мають найкращі характеристики для використання у постквантових алгоритмах;

– визначити властивості алгоритму CSIDH на кривих Едвардса і обґрунтувати застосування алгоритмів CSIDH на нециклічних кривих;

– пришвидшити обчислення ізогенії для збільшення швидкодії криптоалгоритму та захисту від атаки сторонніми каналами;

– розробити модифікації алгоритму CSIDH і створити комбінований криптоалгоритм із застосуванням його модифікацій;

– оцінити величину парціального зростання швидкості від кожної модифікації криптоалгоритму CSIDH на ізогеніях суперсінгулярних еліптичних кривих Едвардса;

– розробити модель алгоритму з використанням НКЕ і оцінити приріст швидкодії і криптографічної стійкості паралельних обчислень;

– оцінити інтегральний виграш у швидкодії модернізованих алгоритмів CSIDH і CSIKE.

Висновки до розділу 1

1. Визначено роль та проаналізований поточний стан і властивості класичних криптоалгоритмів Діффі-Геллмана, які працюють на еліптичних кривих і мають відмінні криптографічні параметри.

2. Встановлено, що квантову резистентність мають алгоритми CSIDH на ізогеніях еліптичних кривих, які є розвитком алгоритмів Діффі-Геллмана і які здатні працювати у постквантових умовах при здійсненні атак з боку потужних квантових комп’ютерів.

3. Встановлено, що найменшу довжину ключа, достатню швидкість і достатній захист мають алгоритми CSIDH на ізогеніях еліптичних кривих Едвардса. Цій метод є досить новим і потребує досліджень.

4. Сформульовано актуальне наукове завдання, яке полягає в подальшому розвитку методів та засобів забезпечення безпечного підвищенні швидкодії і безпеки постквантового асиметричного криптоалгоритму CSIDH на еліптичних кривих Едвардса шляхом його моделювання і модернізації з використанням властивостей СКЕ.

РОЗДІЛ 2
МЕТОД ПІДВИЩЕННЯ ШВИДКОДІЇ КРИПТОСИСТЕМИ CSIDH НА ДВОХ НЕЦИКЛІЧНИХ КРИВИХ

Одним із найбільш перспективних алгоритмів PQC, що визвав широкий потік наукових статей, є алгоритм CSIDH [10]. Він вирішує задачу не інтерактивного розподілу секретів Діффі-Геллмана на основі побудови ланцюжків ізогенних СКЕ з множиною $\{l_k\}^K$ із K найменших непарних простих ступенів l_k ізогеній над простим полем F_p. Двійкова довжина модуля поля $\log p$ визначає довжину ключа в алгоритмі та рівні безпеки $\log p/2$ при атаках звичайного комп'ютера та $\log p/4$ – квантового комп'ютера. Алгоритм CSIDH має найменшу серед відомих алгоритмів PQC довжину ключа.

Перші впровадження CSIDH були побудовані на швидких суперсингулярних кривих у формі Монтгомері [10], однак в роботах [35, 36] за допомогою $(W:Z)$-координати кривих у формі Едвардса вдалося отримати виграш 20% у порівнянні з [10] у швидкості обчислення. Далі, узагальнивши формули обчислення ізогенії для кривої Едвардса [37] на скручені криві Едвардса в роботі [38], проілюстровано впровадження моделі CSIDH на квадратичних і скручених кривих Едвардса [38–40]. З 2007 р. швидко почали розвиватися криптосистеми на кривих Едвадса, які серед відомих кривих, є рекордно продуктивними, у проєктивних координатах. Групові операції складання та подвоєння точок виконуються мінімальним числом польових операцій.

2.1. Криві Едвардса

Еліптичні криві, вивчені професором математики університету Нью-Йорка Гарольдом Едвардсом в 2007 р., отримали на его честь назву криві Едвардса. Він перший [14] розглядав властивості еліптичної кривої у формі:

$$x^2 + y^2 = e^2(1 + x^2y^2), d(1 - de^4) \neq 0, \left(\frac{d}{p}\right) = -1, \qquad (2.1)$$

де $\left(\frac{d}{p}\right)$ – символ Лежандра, d – квадратичний нелишок [33].

Едвардс довів, що рівняння (2.1) описує криву, ізоморфну еліптичній кривий у формі Вейєрштраса, і отримав закон складання її точок.

Перший асиметричний алгоритм було створено на основі кривих Монтгомері [10]. Пізніше було запропоновано використовувати криві Едвадса [41], які теж є ізоморфними кривим Вейєрштраса, а криптосистеми на їх основі мають рекордно малу довжину ключа.

Уперше значних успіхів у дослідженні кривих Едвадса у криптографії досягли Д. Бернстейн і Т. Ланґе [42–44] та їхні співавтори. Вони проаналізували властивості кривих, запровадили новий параметр кривої d як квадратичний нелишок поля, модифікували оригінальну криву Едвардса та отримали закон складання точок для модифікованої кривої. Досліджено властивості скручених кривих Едвардса [43], бінарних кривих [45], запропоновано арифметику проєктивних інвертованих координат для повних кривих Едвардса [44]. Автори показали, що ці криві мають рекордно мінімальну складність групової операції.

2.1.1. Класифікація кривих у формі Едвардса

У роботі [43] автори розширили клас кривих Едвардса з модифікацією Бернстейна-Ланге [42]. Вони додали новий параметр a у рівняння кривої (2.1) і зняли обмеження на неквадратичність параметра d. В результаті рівняння кривих Едвардса отримали вигляд:

$$E_{a,d}: ax^2 + y^2 = 1 + dx^2y^2, a, d \in F_p^*, a \neq d, d \neq 1. \quad (2.2)$$

У роботі [21] для повернення до горизонтальної симетрії точок еліптичної кривої, як це заведено в класичних роботах, зроблено ще одну модернізацію (змінено положення параметра a):

$$E_{a,d}: x^2 + ay^2 = 1 + dx^2y^2, a, d \in F_p^*, a \neq d, d \neq 1. \quad (2.3)$$

Це рівняння названо кривою в узагальненій формі Едвардса [46], які мають закони складання та подвоєння точок у вигляді

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1x_2 - ay_1y_2}{1 - dx_1x_2y_1y_2}, \frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}\right), \quad (2.4)$$

$$2(x_1, y_1) = \left(\frac{x_1^2 - ay_1^2}{1 - dx_1^2y_1^2}, \frac{2x_1y_1}{1 + dx_1^2y_1^2}\right). \quad (2.5)$$

У [21] доведено теорему про повноту закону складання точок цієї кривої. Якщо d не є квадратичним лишком у полі K крива не має особливих точок то для знаменників справедливо: $1 - dx_1x_2y_1y_2 \neq 0$ і $1 + dx_1x_2y_1y_2 \neq 0$.

Таким чином, вирази для суми двох точок (2.4) справедливі для будь-якої пари точок кривої Едвардса над полем K.

Для використання у криптосистемах пропонуються криві у формі Едвардса, які мають кращі криптографічні властивості. За оцінками [21], перехід від канонічних еліптичних кривих у формі Вейєрштрасса на нову технологію кривих у формі Едвардса дає виграш у швидкості експоненціювання точки кривої не менш ніж у 1,5–1,6 разів.

В Україні найбільший внесок у дослідження властивостей еліптичних кривих у формі Едвардса зробили А. В. Бессалов [38, 39, 47–57] і Л. В. Ковальчук [55–57]. Наприклад, в [21] модифіковано криву Едвардса, розроблено класифікацію, досліджено властивості повних і скручених кривих над простим полем і розроблено оригінальні протоколи криптосистем на кривих Едвардса, а також методи рандомізації [58], оптимізації, інкапсуляції та інші [47].

Серед кривих Едвардса є екземпляри з властивостями, що сильно відрізняються. Так в [21] запропоновано, на відміну від попередньої, нову коректну і зрозумілу класифікацію. Запропоновано залежно від квадратичних властивостей параметрів a, d розділити всі криві в узагальненій формі Едвардса на три класи, що не перекриваються [21]:

1. Повні криві Едвардса:

$$\chi(a) = \pm 1, \chi(d) = 1. \quad (2.6)$$

2. Квадратичні криві Едвардса:

$$\chi(a) = \chi(d) = 1. \quad (2.7)$$

3. Скручені криві Едвардса:

$$\chi(a) = \chi(d) = -1. \quad (2.8)$$

Основні властивості кривих цих класів наступні:

1. Щодо точок 2-го порядку клас повних кривих Едвардса над простим полем є класом циклічних кривих (з однією точкою 2-го порядку), скручені і квадратичні криві Едвардса утворюють класи нециклічних кривих (по три точки 2-го порядку). Максимальний порядок точок кривих останніх класів дорівнює $N_E/2$.

2. Клас повних кривих Едвардса не містить особливих точок.

3. Скручені СКЕ містять дві особливі точки 2-го порядку $D_{1,2} = \left(\pm\sqrt{\frac{a}{d}}, \infty\right)$, а квадратичні криві Едвардса, крім них – ще дві особливі точки 4-го порядку $\pm F_1 = \left(\infty, \pm\frac{1}{\sqrt{d}}\right)$.

4. Скручені та квадратичні криві Едвардса утворюють пари квадратичного кручення на основі перетворення параметрів: $\tilde{a} = ca, \tilde{d} = cd, \chi(\mathrm{c}) = -1$.

5. В класах скручених та квадратичних кривих Едвардса заміна $a \leftrightarrow d$ дає ізоморфізм $E_{a,d} \sim E_{d,a}$.

6. Повні та квадратичні криві Едвардса ізоморфні кривим с параметром $a = 1$: $E_{a,d} \sim E_{1,d/a} = E_d$. Введення нового параметра a в рівняння кривої (2.1) необхідне лише для класу скручених кривих Едвардса [21].

Ці класи кривих над простим полем F_p мають однакову кількість $\frac{p-3}{2}$ кривих кожного класу (параметр a фіксований) [33, 38, 51]. Для класів A і B прийнято брати $a = 1$. Структура і властивості кривих кожного класу істотно відрізняються.

Повні криві Едвардса класу A є циклічними і не містять особливих точок, тоді як класи кривих B і C є нециклічними. Вони, поряд з нейтральним елементом $O = (1,0)$ і точками $D = (-1,0)$ 2-го порядку і точками $\pm F = (0, \pm 1)$ 4-го порядку завжди містять, крім перерахованих, дві особливі точки $D_{1,2} = \left(\pm\sqrt{\frac{a}{d}}, \infty\right)$ 2-го порядку та (виключно в класі B) дві особливі точки $\pm F_1 = \left(\infty, \pm\frac{1}{\sqrt{d}}\right)$ 4-го порядку. Останні мають одну з координат на нескінченності ∞, яка не є елементом поля F_p.

Особливі точки створюють певні проблеми в класах B і C нециклічних кривих Едвардса, але вони легко усуваються [43]. Усунення пов'язане з тим, що в криптоалгоритмах CSIDH та подібних використовуються лише точки непарних порядків. Повні криві Едвардса (клас A) використовуються у відомій реалізації алгоритму CSIDH [10], яка побудована на координатній системі $W:Z$ (Фарашахи-Хоссейні), що прискорило його роботу на 20% порівняно з кривими Монтгомері у проєктивних координатах $X:Z$.

2.1.2. Нециклічні криві Едвардса

Повні криві Едвардса з одним параметром (d), визначені у роботі [21], мають добре відомі властивості: висока швидкість експоненціонування точки, універсальність закону складання точок, афінні координати нейтрального елемента групи точок. Згідно з прийнятою в [21] класифікації, два нових класи: скручені та квадратичні криві Едвардса, утворюють пари квадратичного кручення і дуже зручні для будування криптосистеми CSIDH.

Розглянемо деякі специфічні властивості СКЕ [21], які визначається рівнянням:

$$E_{a,d}: x^2 + ay^2 = 1 + dx^2y^2, a, d \in F_p^*, a \neq d, d \neq 1. \quad (2.9)$$

При квадратичному характері $\chi(ad) = -1$, крива (2.9) ізоморфна повній кривій Едвардса [21] з одним параметром d

$$E_d: x^2 + y^2 = 1 + dx^2y^2, \chi(d) = -1. \quad (2.10)$$

Таки криві є циклічними, а їх порядок $N_E \equiv 0 \bmod 4$.

У випадку $\chi(ad) = 1, \chi(a) = \chi(d) = 1$ має місце ізоморфізм кривої (2.9) з квадратичною кривою Едвардса [21]

$$E_d: x^2 + y^2 = 1 + dx^2y^2, \chi(d) = 1, d \neq 1. \quad (2.11)$$

Ці криві є нециклічними з порядком $N_E \equiv 0 \bmod 8$.

На відміну від (2.10), параметр d кривої (2.11) визначено як квадрат. Для обох кривих зазвичай приймають $a = 1$ [34].

Скручена крива Едвардса визначена в роботі [21] як окремий випадок кривої (2.9) при $\chi(ad) = 1, \chi(a) = \chi(d) = -1$. Пара квадратичної і скрученої кривої Едвардса [21] складають пару квадратичного кручення з параметрами $\chi(ad) = 1, a' = ca, d' = cd, \chi(c) = -1$.

Таким чином, перехід від квадратичної до скрученої кривої і назад має вигляд $E_d = E_{1,d} \leftrightarrow E_{-1,-d}$. Відповідно, рівняння скрученої криві при $p \equiv 3 \bmod 4$ можна записати як

$$E_{-1,-d}: x^2 - y^2 = 1 - dx^2y^2, d \in F_p^*, d \neq 1, \chi(d) = 1. \quad (2.12)$$

Порядок еліптичної кривої N_E над простим полем F_p визначається на основі сліду t характеристичного рівняння ендоморфізму Фробеніусу $\pi^2 - t\pi + p = 0$, як $N_E = p + 1 - t$. Для кривої квадратичного кручення E^t відповідний порядок дорівнює ${N_E}^t = p + 1 + t$. Еліптична крива є суперсингулярною тоді і лише тоді, якщо над будь яким розширенням простого поля F_p слід рівняння Фробеніусу $t \equiv 0 \, mod \, p$, при цьому $\pi^2 = -p, \pi = \pm\sqrt{-p}$. [6, 56, 57]. В алгебраїчному замиканні $\bar{F}_p$ СКЕ не містить точок порядку p. Над простим полем F_p така крива завжди має порядок $N_E = p + 1$. Важливо, що точки парних порядків у обчисленнях алгоритму CSIDH не беруть участь (після першого множення на чотири випадкові точки R).

2.1.3. Властивості нециклічних суперсингулярних кривих Едвардса

Для будови алгоритму CSIDH у роботах [37, 38, 40, 51, 59] обґрунтовано використання двох класів нециклічних СКЕ, класів B і C як пари квадратичного кручення, що обумовлено їх перевагами перед повними кривими Едвардса типу A [42], а саме:

1. Кількість усіх квадратичних і кручених кривих Едвардса $(p - 3)$ вдвічі більше числа $\frac{p-3}{2}$ усіх повних кривих Едвардса, відповідна пропорція справедлива і для числа ізогенних СКЕ і безпеки CSIDH.

2. Перехід до кривої квадратичного кручення $E_d \leftrightarrow E_{-1,-d}$ не вимагає трудомісткої інверсії параметра $d \leftrightarrow d^{-1}$, яка потрібна для повної СКЕ.

3. Порядок нециклічних СКЕ $p + 1 \equiv 0 \bmod 8$ дорівнює цілому числу n байт, при цьому елементи і арифметика простого поля F_p найбільш економно пакетується, що відповідає сучасним стандартам еліптичної криптографії.

4. Продуктивність експоненціальної операції точки такої кривої в середньому більш ніж в 1,5 рази вище, ніж для кривої Вейєрштрасса [21].

5. Програмування арифметики цих кривих значно спрощується за рахунок наявності афінного нейтрального елемента групи $O(1,0)$.

6. Універсальність закону додавання точок робить їх більш безпечними від атак сторонніми каналами [21].

7. Для аналізованих класів СКЕ заміна $d \to d^{-1}$ дає ізоморфізм, а для повних кривих Едвардса – квадратичне кручення.

Квадратичні та скручені СКЕ, мають ті ж самі рекордні показники швидкодії, що і повні криві Едвардса [40]. Можливість їх використання у алгоритмі CSIDH виникає з урахуванням доведених в [51] теорем. При мінімальному кофакторі 8 порядок квадратичних та скручених СКЕ $N_E = 8n$. Таким чином, для цих класів СКЕ с порядком $N_E = 8n = p + 1$, $n = \prod_{k=1}^{K} l_k$. модуль поля в алгоритмі CSIDH обирається як $p \equiv -1 \bmod 8$.

У скрученій кривий (2.12) обидва параметри кривої (2.11) помножуються на (-1) і стають квадратичними лишками. Порядки усіх СКЕ дорівнюють $N_E = p + 1 = 8n$, для алгоритму CSIDH $n = \prod_{i=1}^{K} l_i$, де l_i – ступень простих непарних ізогеній. Максимальний порядок точки нециклічної кривої дорівнює $4n$, тому для отримання точок непарних порядків достатньо будь-яку випадкову точку помножити на 4.

З (2.11) і (2.12) слідує, що перехід до квадратичного кручення для класів B і C практично безкоштовний, тоді як усередині класу A такий перехід досягається інверсією параметра d, яка за відомою оцінкою [53] вимагає $(10..50)M$, де M – складність множення групи F_p^*. Приймаючи умовно складність переходу між

кривими B і C за $1M$, отримуємо умовну середню оцінку виграшу $\gamma_2 \approx 2^5$ у швидкості обчислень у порівнянні з повними кривими A. Оскільки в алгоритмі CSIDH перехід к квадратичному крученню необхідний приблизно для половини ізогенних кривих, можна використовувати умовну нижню оцінку виграшу $\gamma_2 \approx 2^4$ [47].

Квадратичні і скручені криві Едвардса над простим полем мають особливі властивості, пов'язані з їхньою нециклічною структурою і неповнотою закону додавання точок. Обидва класи кривих містять нециклічну підгрупу 4-го порядку, що включає три точки 2-го порядку. Дві з цих точок особливі і мають нескінченні координати. Квадратичні криві Едвардса, крім того, містять дві особливі точки 4-го порядку. Неповнота закону додавання точок, як показав аналіз, породжує також точки з невизначеністю $\frac{0}{0}$ в одній з координат суми, названі в роботі [48] нечіткими.

В роботі [43] зроблено аналіз, що спирається на властивості квадратичних і скручених кривих Едвардса, пов'язаних як пари квадратичного кручення [49, 50]. СКЕ цих класів з однаковим порядком існують лише при $p \equiv 3 \bmod 4$. Мінімальний парний кофактор порядку таких кривих дорівнює 8, тоді для алгоритму CSIDH с непарним $n = \prod_{i=1}^{K} l_i$ модуль поля F_p слід обирати як $p = 8n - 1$. З метою адаптації визначень для арифметики ізогеній кривих Едвардса і кривих у формі Вейерштрасса будемо використовувати модифікований закон складання точок [21].

Обчислення ізогеній непарних ступенів для повних та квадратичних кривих Едвардса E_d здійснюється за формулами, визначеними теоремами 2–4 роботи [27]. У роботі [51] теореми узагальнені на криві у формі Едвардса з двома параметрами a, d що дозволяє застосувати квадратичні та скручені криві Едвардса над простим полем F_p для імплементації моделі CSIDH.

Важливо, що в розрахунках алгоритму CSIDH не беруть участь точки парних порядків (після першого множення на чотири випадкові точки) [47].

2.2. Властивості точок кривих Едвардса

2.2.1. Визначення точок кривих Едвардса

Операції з точками виконуються в алгоритмах CSIDH для обчислення порядку точок, знаходження координат точок ядра ізогенії і тому вивчення властивостей точок є важливим.

Точне число раціональних точок еліптичної кривої E над кінцевим полем F_p достатньо важко обчислити, але оцінку дає теорема Хассе, яка про еліптичні криві стверджує, що кількість точок N на еліптичній кривій над кінцевим полем F_q задовольняє нерівності:

$$|N - (q + 1)| < 2\sqrt{q}, \tag{2.13}$$

де q – модуль поля.

Тоді згідно з теоремою Хассе кількість точок на еліптичній кривій близька до розміру кінцевого поля. А число точок на даній кривій може бути обчислено за допомогою алгоритму Шуфа [60].

У роботі [43] показано, що введення нового параметра a в узагальнену форму (2.3) кривої Едвардса в 1,5 рази розширює множину кривих у формі Едвардса з мінімальним кофактором 4. При $\mathrm{p} \equiv 1 \bmod 4$ всі вони мають порядок $4n$, що спрощує пошук корисних кривих. Максимальний порядок точки такої кривої дорівнює $2n$, що дозволяє знайти генератор криптосистеми G одним подвоєнням випадкової точки кривої.

Нейтральний елемент групи має афінні координати $O(1,0)$. Використання модифікованих законів складання [21] дозволяє зберегти загальноприйняту горизонтальну симетрію (щодо осі x) зворотних точок. Зворотна точка $-P = -(x_1, y_1) = (x_1, -y_1)$ згідно з має властивість $(x_1, y_1) + (x_1, -y_1) = (1,0) = O$. Крім нейтрального елемента O на осі x також лежить точка $D_0 = (-1,0)$ другого порядку, для якої $2D_0 = (1,0) = O$.

Залежно від властивостей параметрів a та d маємо ще дві особливі точки другого порядку та двох, чотирьох або шести точок 4-го порядку. На осі y можуть лежати точки $\pm F_0 = (0, \pm 1/\sqrt{a})$ 4-го порядку, для яких $\pm 2F_0 = D_0 = (-1,0)$. Ці точки існують над полем F_p, якщо параметр a є квадратичним лишком [21].Кручені криві Едвардса містять дві особливі точки 2-го порядку $D_{1,2}$ а квадратичні криві Едвардса, крім них є ще дві особливі точки 4-го порядку $\pm F_1$ [48].

З цих формул випливає, що над простим полем F_p особливі точки $D_{1,2}$ існують в обох класах квадратичних і скручених кривих Едвардса, а точки 4-го порядку $\pm F_1$ – тільки в класі квадратичних кривих Едвардса.

Отже, всі нециклічні криві Едвардса містять три циклічні підгрупи 2-го порядку $G_2^{(0)} = \{O, D_0\}, G_2^{(1)} = \{O, D_1\}, G_2^{(2)} = \{O, D_2\}$, одну циклічну підгрупу точок непарного порядку n, G_n, а квадратичні криві Едвардса, крім того, дві циклічні підгрупи 4-го порядку $G_4^{(0)} = \{O, F_0, D_0, -F_0\}, G_4^{(1)} = \{O, F_1, 2F_1 = D_0, 3F_1 = -F_1\}$

Відповідно до (2.4) сума довільної точки (x_1, y_1) з однією з точок 2-го або 4-го порядків має координати [21]:

$$(x_1, y_1) + (-1,0) = (-x_1, -y_1), \tag{2.14}$$

$$(x_1, y_1) + (0, \pm 1) = (-(\pm) a y_1 \pm x_1), \tag{2.15}$$

$$(x_1, y_1) + \left(\pm\sqrt{\frac{a}{d}},\ \infty\right) = \left(\pm\sqrt{\frac{a}{d}} \cdot {x_1}^{-1}, \frac{\pm 1}{\sqrt{ad}} \cdot {y_1}^{-1}\right), \tag{2.16}$$

$$(x_1, y_1) + \left(\infty, \pm\frac{1}{\sqrt{d}}\right) = \left(\pm\frac{-1}{\sqrt{d}} \cdot {x_1}^{-1}, \pm\frac{1}{\sqrt{d}} \cdot {y_1}^{-1}\right). \tag{2.17}$$

Зокрема, якщо (x_1, y_1) – точка непарного порядку, то суми (2.14) та (2.17) дають точку парного порядку $2n_1$, а суми (2.15) та (2.17) – точку парного порядку $4n_1$. Неповнота закону додавання точок є лише для точок (2.16) і (2.17), утворених за допомогою особливих точок з однією з нескінченних координат.

Неповнота закону додавання точок, як показав аналіз, породжує також точки з невизначеністю $\frac{0}{0}$ в одній з координат суми, названі нечіткими. У [48] сформульовані і доведені п’ять теорем, що дозволяють вирішити ці невизначеності і довести умови, в яких закон додавання точок у даних класах кривих є повним.

2.2.2. Графічна модель точок кривих Едвардса

При обчисленнях точок в оригінальному алгоритмі Діффі-Геллмана використовується мультиплікативна операція піднесення до ступеня числа (експоненціонування).

При реалізації криптоалгоритмів часто використовуються операції обчислення скалярного добутку kP ($k = 1, \dots, KP$) точок P (при обчисленнях відкритого ключа, порядку точок і інших). Для спрощення цього процесу використовується графічна модель «колесо точок» [21].

Побудова групи $GK(P) = \{P, 2P, 3P, \dots, kP, \dots, KP\}$, де K – порядок точки, таке що $KP = O(1,0)$, а числа $P, 2P, \dots, KP$ утворюють групу точок кривої $GK = \{kP | k = 1, \dots, KP\}$ теж називається експоненціювання.

Експоненціювання точок кривої проводиться з використанням виразів (2.4, 2.5), які досить складні і тому створення методів спрощення та прискорення експоненціювання є актуальним для дослідження [40]. В роботі [50] на основі взаємозв'язку сімейств точок великого порядку здійснюється реконструкція точок kP кривої Едвардса без застосування групових операцій, скоротивши кількість розрахунків точок до 1/8 порядку групи [21].

Додаткові дослідження метода реконструкції точок цих кривих дозволяють ще більше спростити і прискорити знаходження координат цих точок і їх порядків.

Розглянемо приклад з роботи [48], у якій використовується квадратична крива Едвардса з параметрами $a = 1$, $d = 5^2 \bmod 23 = 2$. При $p = 23$ вона є суперсингулярною і має порядок $N_E = 24$, $n = 3$. Крива має базові точки $+F1 = (0, +1)$, $D_0 = (-1,0)$, $O = (1,0)$, особливі точки $(9, \infty)$, $(-9, \infty)$, $(\infty, 9)$, $(\infty, -9)$ і чотири сімейства по чотири циклічних групи точок порядку 3, 6, 12, з генераторами $(\pm 5, \pm 10)$, $(\pm 10, \pm 5)$, $(\pm 6, \pm 11)$, $(\pm 11, \pm 6)$ рядки табл. 2.1.

Таблиця 2.1

Сімейства точок високого порядку кривої

з параметрами $a = 1$, $d = 5^2 \bmod 23 = 2$ при $p = 23$

Група	Порядок	$1P$	$2P$	$3P$	$4P$	$5P$	$6P$
1	6	(5,10)	(–5,10)	(–1,0)	(–5,–10)	(5,–10)	(1,0)
2	6	(5,–10)	(–5,–10)	(–1,0)	(–5,10)	(5,10)	(1,0)
пункт	6	6	3	2	3	6	—
		$1P$	$2P$	$3P$	$4P$	$5P$	$6P$
3	3	(–5,10)	(–5,–10)	(1,0)	—	—	—
4	3	(–5,–10)	(–5,10)	(1,0)	—	—	—
пункт	3	3	3	—	—	—	—
		$1P$	$2P$	$3P$	$4P$	$5P$	$6P$
5	12	(10,5)	(5,10)	(0,1)	(–5,10)	(–10,5)	(–1,0)
6	12	(10,–5)	(5,–10)	(0,–1)	(–5,–10)	(–10,–5)	(–1,0)
7	12	(–10,5)	(5,–10)	(0,1)	(–5,–10)	(10,5)	(–1,0)
8	12	(–10,–5)	(5,10)	(0,–1)	(–5,10)	(10,–5)	(–1,0)
9	12	(6,11)	(5,–10)	(∞,9)	(–5,–10)	(–6,11)	(–1,0)
10	12	(6,–11)	(5,10)	(∞,–9)	(–5,10)	(–6,–11)	(–1,0)
11	12	(–6,11)	(5,10)	(∞,9)	(–5,10)	(6,11)	(–1,0)
12	12	(–6,–11)	(5,–10)	(∞,–9)	(–5,–10)	(6,–11)	(–1,0)
пункт	12	12	6	4	3	12	2
		$7P$	$8P$	$9P$	$10P$	$11P$	$12P$
5	12	(–10,–5)	(–5,–10)	(0,–1)	(5,–10)	(10,–5)	(1,0)
6	12	(–10,5)	(–5,10)	(0,1)	(5,10)	(10,5)	(1,0)
7	12	(10,–5)	(–5,10)	(0,–1)	(5,10)	(–10,–5)	(1,0)
8	12	(10,5)	(–5,–10)	(0,1)	(5,–10)	(–10,5)	(1,0)
9	12	(–6,–11)	(–5,10)	(∞,–9)	(5,10)	(6,–11)	(1,0)
10	12	(–6,11)	(–5,–10)	(∞,9)	(5,–10)	(6,11)	(1,0)
11	12	(6,–11)	(–5,–10)	(∞,–9)	(5,–10)	(–6,–11)	(1,0)
12	12	(6,11)	(–5,10)	(∞,9)	(5,10)	(–6,11)	(1,0)
пункт	12	12	3	4	6	12	—
		$1P$	$2P$	$3P$	$4P$	$5P$	$6P$
13	6	(11,6)	(–5,–10)	(–9,∞)	(–5,10)	(11,–6)	(1,0)
14	6	(11,–6)	(–5,10)	(–9,∞)	(–5,–10)	(11,6)	(1,0)
15	6	(–11,6)	(–5,10)	(9,∞)	(–5,–10)	(–11,–6)	(1,0)
16	6	(–11,–6)	(–5,–10)	(9,∞)	(–5,10)	(–11,6)	(1,0)
пункт	6	6	3	2	3	6	—

У табл. 2.1 можна спостерігати цікаві особливості. Наприклад, усі точки подвоєння всіх груп (колонка $2P$) є виключно точками сімейства (5,10) і далі точки

цього сімейства також повністю займають колонки $4P$, $8P$ і $10P$. Сімейством будемо називати усі точки, у яких однакові абсолютні значення координат $(|x|, |y|)$. У табл. 2.1 також однакове розташування порядків точок у всіх групах одного порядку [61].

2.2.3. Колесо експоненціювання

Кожний рядок табл. 2.1 це циклічна група, створена експоненціюванням генератора у першому стовпчику $(1P)$. Для наочності та кращого розуміння усі точки циклічної групи розташовуються по колу і створюють «колесо експоненціювання» (рис. 2.1) [21].

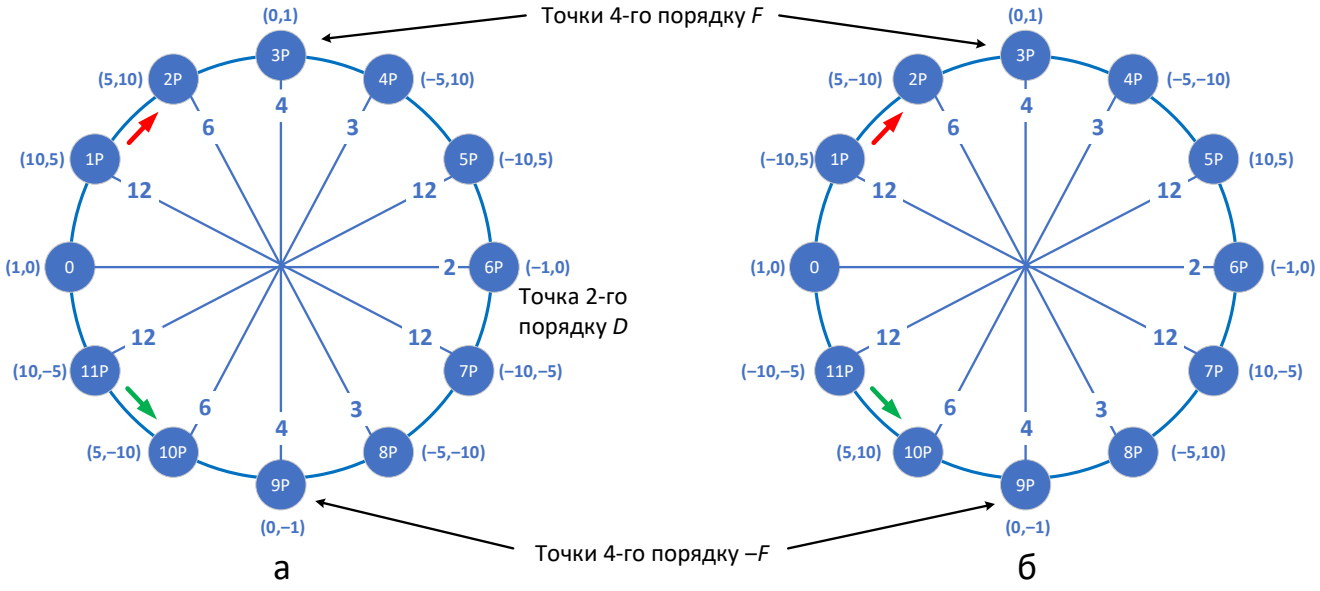

Рис. 2.1. Модель 12-го порядку циклічних груп точок груп (а) 5,6 і (б) 7,8

Для спрощення описання у тексті будемо називати точки і групи, у яких, координати x і y помінялися місцями, свап-точками (x, y) і (y, x); також є зворотні точки (x, y) і $(x, -y)$, де координата y має різні знаки; дзеркальні (x, y) і $(-x, y)$, де різні знаки мають координати x; діаметральні, у яких обидві координати мають різні знаки.

В точках колеса показано скалярні коефіцієнти на які множиться начальна точка $1P$ – генератор групи $< P >$. На зовнішній стороні колеса розташовуються координати точок групи, а на внутрішній стороні порядок відповідних точок.

Усі точки пов'язані між собою (рис. 2.1) базовими точками $D, \pm F$ і утворюють симетричну структуру

$$P \pm F = (x_1, y_1) + (0, \pm 1) = (\pm(-y_1), \pm x_1). \quad (2.18)$$

Центральну симетрію відносно повороту колеса на 180^o мають інверсні точки P і P^* розташовані на кінцях діаметра колеса:

$$P + D = (x_1, y_1) + (-1,0) = (-x_1, -y_1) = P^*. \quad (2.19)$$

Вертикальну (дзеркальну) симетрію утворюють симетричні точки щодо вертикальної осі. Ці точки з одного сімейства з однаковою координатою y, а координата x змінює знак: це точки (x, y) і $(-x, y)$. Точки нижнього півкола визначаються аналогічно за допомогою зворотної точки, у якої змінює знак координати y: $-P = (x_1, -y_1)$.

Перши дві групи $(10,5)$ і $(10, -5)$ не мають особливих точок, а колесо експоненціонування представлено на рис. 2.1.

Координати точок розташовані біля відповідного скалярного коефіцієнта при обході колеса за часовою стрілкою від точки – генератора $1P = (10,5)$. Група інверсної точки – генератора групи $(10, -5)$ починається при обході проти годинникової стрілки від точки $11P$.

2.2.4. Шаблон колеса циклічної групи

Симетрично відносно горизонтальної осі розташовуються інверсні точки з різними знаками координати y, симетрично відносно вертикальної осі розташовуються точки з одного сімейства але різних груп тобто у них координата y збігається а координата x має інший знак. На кінцях діагоналі розташовуються протилежні точки, у яких всі координати мають різні знаки.

У цього сімейства є ще групи з генераторами $(-10, 5)$ і $(-10, -5)$ мають вигляд трансформованого колеса (рис. 2.1б). Трансформація полягає в тому, що в непарних точках $(1P, 3P, \dots)$ інвертуємо знак координати X, а у парних точках $(2P, 4P, \dots)$ – координати Y (рис. 2.2б, 2.3б).

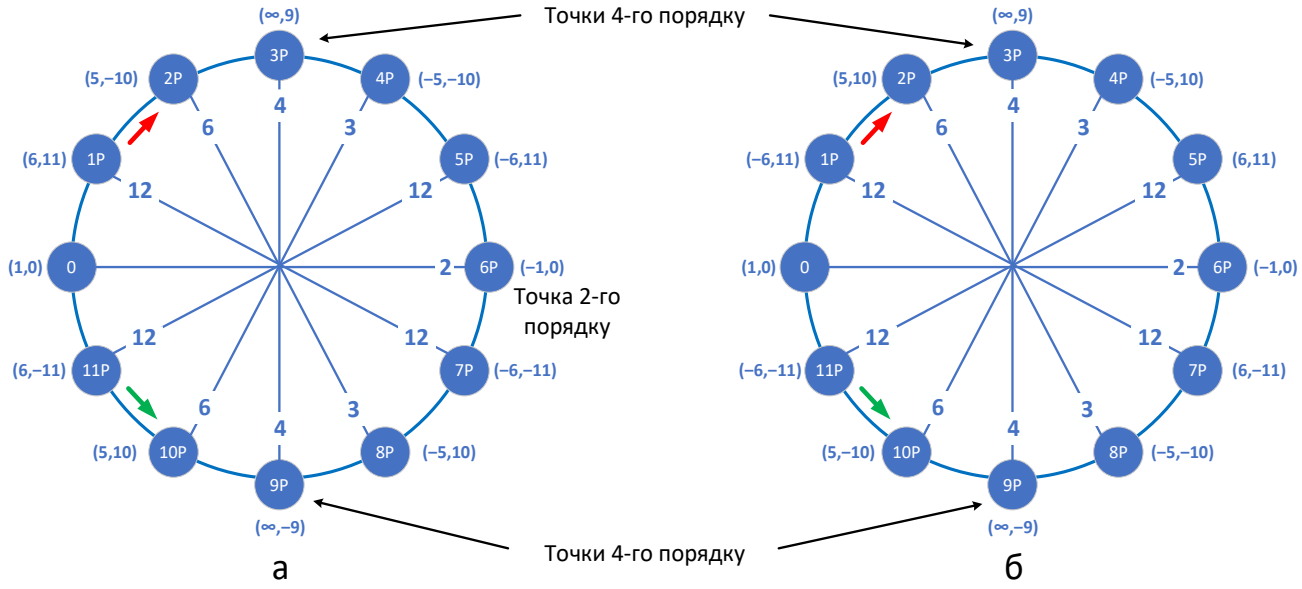

Рис. 2.2. Модель 12-го порядку циклічних груп (а) 9,10 і (б) 11,12

У розглянутих колесах спостерігаються деякі закономірності: кожна з чотирьох точок будь-якого сімейства (початкового або свап) розташовується у різних секторах. У кожному секторі точки з різних сімейств, по одній із кожного і самі сімейства не повторюються. Колесо всіх циклічних груп одного порядку мають однакове розташування точок. Це зручно використовувати для створення шаблону колеса заданого порядку. При цьому треба знати порядок групи експоненціювання. На рис. 2.3 представлено шаблон колеса 12-го порядку. Всередині колеса показано порядок точок, справедливий для будь-якої групи цього порядку. Колесо великого порядку зручніше представляти у вигляді шаблона (табл. 2.2).

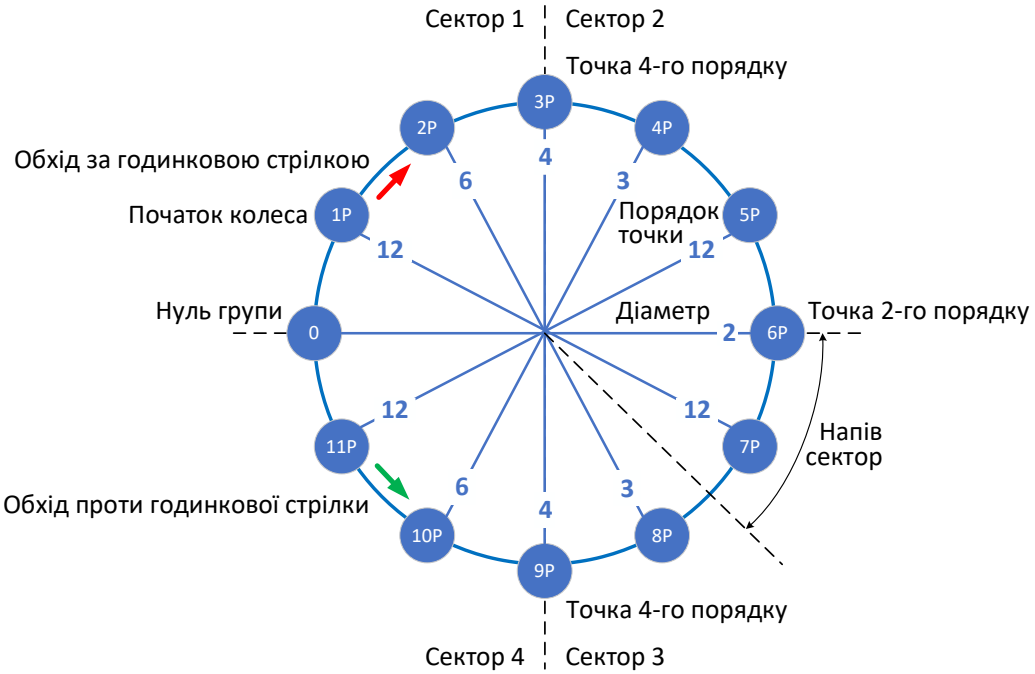

Рис. 2.3. Шаблон колеса експоненціювання для групи 12-го порядку

Як і у колесі в табл. 2.2 представлені точки кривої, коефіцієнт експоненціювання k і порядок точок N_T. Для побудови всієї групи, як було сказано в [21], достатньо знайти точки першого пів сектора (1/8 частина всіх точок колеса). Далі слід заповнити шаблон за певними правилами.

Таблиця 2.2

Побудова коліс циклічних груп кривої Едвардса $N_e = 28, d = 8, p = 19$

kP	P	$2P$	$3P$	$4P$	$5P$	$6P$	$7P$	$8P$	$9P$	$10P$	$11P$	$12P$	$13P$	$14P$
X	2	–8	–3	–5	–4	–9	0	9	4	5	3	8	–2	–1
Y	9	4	5	3	8	–2	1	–2	8	3	5	4	9	0
N_T	28	14	28	7	28	14	4	7	28	14	28	7	28	2
kP	$15P$	$16P$	$17P$	$18P$	$19P$	$20P$	$21P$	$22P$	$23P$	$24P$	$25P$	$26P$	$27P$	$28P$
X	–2	8	3	5	4	9	0	–9	–4	–5	–3	–8	2	1
Y	9	–4	–5	3	8	–2	–1	2	–8	–3	–5	–4	–9	0
N_T	28	7	28	14	28	7	4	14	28	7	28	14	28	1

Підгрупа має 28 порядок і до неї входять усі точки кривої. У табл. 2.2 є базові точки з відомим порядком: точки $7P$ та $21P$ порядок 4, $14P$ порядок 2 та нейтральна точка (1,0). Не базові точки можуть мати порядок 28, 14, 7, знайти їх порядки можна використовуючи мінімальну кількість обчислень. У табл. 2.2 28 точок і закінчується вона точкою (1,0), отже порядок точки-генератора буде 28. Подвоєна

точка $2P$ має порядок 14, тобто точку $2P$ треба помножити на 14 щоб отримати точку $O(1,0) = 28P$, тому що 2 є дільник 28, а $s = 28/k = 14$. Точка $4P$ перетворюється на точку $28P$ множенням на 7 (сім кроків), тобто незалежно від порядку точки P точка $4P$ має порядок 7, оскільки $28 = 4 \cdot 7$. З точок в яких k є дільником 28 можна досягти нуля за s кроків пройшовши r циклів підгрупи $28r = ks$, тобто коли ціле число $s = 28r/k$. Тут K дільник $28r$. У цьому рівнянні при заданому і мінімальному деякому r маємо ціле число s.

Наприклад, для третьої точки $3P$ маємо $K = 3$ тоді $s = N \cdot r/k = 28 \cdot r/3 = 2 \cdot 2 \cdot 7 \cdot r/3$. Загальних множників немає і ціле s може бути при $r = k = 3$ тоді порядок цієї точки $s = 28$. Для точки $6P$ маємо $K = 6 = 2 \cdot 3$, тоді $s = 2 \cdot 2 \cdot 7 \cdot r/2 \cdot 3$, скорочуємо на загальний множник 2 і отримуємо $s = 14$.

Розглянемо, наприклад, наступний шаблон для точки порядку 28. На рис. 2.4 зображено колесо, комірки якої, зручніші для заповнення даними.

кР	1P	2P	3P	4P	5P	6P	7P	8P	9P	10P	11P	12P	13P
X													
У													
N	28	14	28	7	28	14	4	7	28	14	28	7	28
28P													14P
1													-1
0													0
1													2
кР	27P	26P	25P	24P	23P	22P	21P	20P	19P	18P	17P	16P	15P
X													
У													
N	28	14	28	7	28	14	4	7	28	14	28	7	28

Рис. 2.4. Шаблон колеса експоненціювання для точок кривої 28-го порядку

Застосовуючи далі це правило, отримаємо для кожного порядку групи відповідний шаблон.

2.2.5. Правила реставрації точок одного сімейства

Тепер у цьому шаблоні треба розмістити точки, які залежать від першої точки $1P$. Правила та формули для спрощення цього процесу розроблені у [50].

Для кривої порядку N може бути підгрупи порядку $R_i|N$, а перша точка 4-го порядку $F1$, якщо вона є, з'явиться на кроці $(R_i/4) \cdot P$.

Послідовність побудови колеса циклічної підгрупи точки P кривої N-го порядку:

1. Входом є точка P кривої.

2. За виразами (3,4) знаходимо точки $2P$, $4P$, $8P$, …, 2^k тощо.

3. Якщо остання точка з'явилася з сімейства, яке вже було значить, ми перейшли в другий сектор колеса. А точка $F1$ знаходиться між останньою k та передостанньою $(k-1)$ точками $k < (R_i|N) < k-1$.

4. Звідси визначається порядок R_i точки P.

5. Обираємо відповідний шаблон колеса та заповнюємо його точками відповідно [21].

Закономірності зберігаються й у кривих більш високого порядку. Наприклад, крива $N_e = 80, a = 1, d = 2, p = 79$ її шаблон експоненціювання точки має вигляд, представлений на рис. 2.5, де початкова точка припадає на значення P, а кінцева – на $39P$.

На зеленому тлі показані координати точок, на жовтому – скалярний коефіцієнт експоненціювання, на сірому – порядки точок P_k. Усі описані вище властивості мають місце. Є нейтральна точка $O(1,0)$, дві спеціальні точки 4-го порядку $(\infty, \pm 35)$ та точка 2-го порядку. Є можливість по ⅛ частини всіх точок реконструювати інші точки. За отриманими даними можна реконструювати решту всіх груп цього сімейства вже навіть без знання ⅛ частини його точок.

X У	2, 24	-34 -14	23 12	-13 18	6 19	-20 -27	-30 29	37, -8	-15 -22	∞, 35	15, -22	-37 -8	30, 29	20, -27	-6, 19,	13, 18	-23 12	34, -14	-2, 24	
kP	P	2P	3P	4P	5P	6P	7P	8P	9P	10P	11P	12P	13P	14P	15P	16P	17P	18P	19P	
Ni	**40**	**20**	**40**	**10**	**8**	**20**	**40**	**5**	**40**	4	**40**	**10**	**40**	**20**	**8**	**5**	**40**	**20**	**40**	
(1,0) 40P 1	Перший сектор										Другий сектор									(-1,0) 20P 2
	Четвертий сектор										Третій сектор									
X У	2, -24	-34 14	23 -12	-13 -18	6 -19	-20 27	-30 -29	37, 8	-15 22	∞, -35	15, 22	-37 8	30, -29	20, 27	-6, -19	13, -18	-23 -12	34, 14	-2, -24	
kP	39P	38P	37P	36P	35P	34P	33P	32P	31P	30P	29P	28P	27P	26P	25P	24P	23P	22P	21P	
	40	**20**	**40**	**10**	**8**	**20**	**40**	**5**	**40**	**4**	**40**	**10**	**40**	**20**	**8**	**5**	**40**	**20**	**40**	

Рис. 2.5. Шаблон експоненціювання точок 40-го порядку кривої $N_e = 80$

Для будь-якої групи $P \cdot k_i$ порядку $\#G(x, y)$ незалежно від координат точок порядки розставляються однаково. З множників порядку групи $\#G(x, y) = g_1 \cdot g_2 \cdot \ldots \cdot g_s$ видаляють елементи, що збігаються з множниками скаляра $k_i = k_{i1} \cdot k_{i2} \cdot \ldots$, а множники, що залишилися, дають значення порядку точки. Наприклад, у нашому прикладі при $\#G(x, y) = 40 = 2 \cdot 2 \cdot 2 \cdot 5$ для точки $8P = 2 \cdot 2 \cdot 2$ видаляємо однакові множники $N(8P) = \cancel{2 \cdot 2 \cdot 2} \cdot 5 = 5$. Порядок дорівнює 5. А для симетричної точки $12P = 2 \cdot 2 \cdot 3$ маємо $\cancel{2 \cdot 2} \cdot 2 \cdot 5 = 10$. Порядок дорівнює 10. Порядки решти симетричних точок співпадають.

Розглянемо одну з груп максимального порядку, нехай її генератором є точка $P(x_1, y_1)$. Сюди входять точки з половини всіх точок кривої, по одній точці з кожного сімейства і точки з нього не повторюються. Інші точки колеса належать тільки цим сімействам.

Друга половина точок кривої включає свап-точки, що залишилися. Групу максимального порядку утворює свап-точка генератор $P(x_1, y_1)$, це перша точка групи (та колеса). Інші точки беруться з колеса і змінюються за такими правилами:

1. Парні точки беруться з початкових сімейств, а непарні – з свап-сімейств.

2. Знаки координат розставляються так: у другій точці інвертується знак координати x, у 3-й точці інвертуються обидві координати, у 4-й – інвертується у координата, у 5-й – знаки не змінюються, так процес повторюється до заповнення сектора.

2.2.6. Особливості арифметики нециклічних суперсингулярних кривих Едвардса

Важливою особливістю двох класів нециклічних кривих Едвардса (з трьома точками 2-го порядку) на відміну від повних є втрата властивості повноти закону додавання точок [21]. Це означає, що існують пари точок, сума яких породжує особливі точки з нескінченністю в одній із координат (нуль у знаменнику формул додавання), а також, як було виявлено, пари доданків, що утворюють невизначеності $\frac{0}{0}$ в цих формулах. У певному сенсі ці точки можна вважати небезпечними, що призводять до збою програм обчислень групових операцій.

В роботі [48] проведений аналіз особливих властивостей квадратичних і скручених кривих Едвардса, пов’язаних з неповнотою закону додавання точок. Це дозволило сформувати умови [21] для безпечного виконання скалярних добутків у даних класах кривих Едвардса.

Неповнота закону додавання точок, як показав аналіз, породжує також точки з невизначеністю $\frac{0}{0}$ в одній з координат суми, названі у нечіткими. Сформульовані і доведені п’ять теорем, що дозволяють вирішити ці невизначеності і довести умови, в яких закон додавання точок у даних класах кривих є повним. Перехід до підгрупи G_n точок непарного порядку знімає проблему (теореми 3 і 5). Досягається це дворазовим подвоєнням будь-якої точки максимального порядку $4n$ [48].

2.3. Криптосистеми на ізогеніях кривих Едвардса

2.3.1. Обчислення ізогенної функції

Для алгоритмів Діффі-Геллмана на ізогеніях груповою операцією є обчислення ланцюжка ізогеній, в результаті якої знаходяться відкритий і спільний ключі. В роботі [37], є теорема:

Для кривої $E_{a,d}$ в загальній формі Едвардса $x^2 + ay^2 = 1 + dx^2y^2$, заданій над простим полем F_p, є єдина ізогенна крива квадратичного кручення $E^t_{\vec{a},\vec{d}}$ с параметрами $\bar{a} = ca, \bar{d} = cd, c \in F_p{}^*$.

Звідки слідує, що в класі повних кривих Едвардса крива квадратичного кручення $E^t_d = E_{d^{-1}}$ лежить усередині цього класу, тоді як для квадратичної кривої квадратичне кручення дає скручену криву $E^t_{a,d} = E_{ca,cd}$, $\chi(c) = -1$. Кожен із трьох класів містить рівносильні множини $\frac{p-3}{2}$ кривих ($d \neq 0, \pm 1$). Тому заміна класу повних кривих Едвардса на два класи нециклічних кривих Едвардса вдвічі розширює простір пар кривих квадратичного кручення.

Ізогенне відображення еліптичної кривої $E(K)$ над полем K у криву $E'(K)$ є гомоморфізм $\phi: E(\bar{K}) \to E'(\bar{K})$, що задається раціональними функціями. Це означає, що існує раціональна функція [37]

$$\phi(x, y) = \left(\frac{p(x)}{q(x)}, y\frac{f(x)}{g(x)}\right) = (x', y'), \tag{2.20}$$

яка відображає точки кривої E в точки кривої E' для усіх точок $P, Q \in E(K)$, при збережені властивостей $\phi(P + Q) = \phi(P) + \phi(Q)$.

У основі побудови ізогеній непарних простих ступенів для квадратичних кривих Едвардса лежить теорема 2 з роботи [27], а для скручених кривих Едвардса – теорема 1 [51]. В останній роботі наведено формули відображень для кривої (2.3), що залежать від двох параметрів. Обчислення ізогеній кривих Едвардса класів A та B непарних ступенів виконується згідно з теоремою 2 [52]. В роботі [53] узагально цю теорему на криві класу C у наступній теоремі:

Нехай $G = \{(1,0), \pm Q_1, \pm Q_2, \dots, \pm Q_s\}$ – підгрупа непарного порядку $l = 2s + 1$ точок $\pm Q_i = (\alpha_i, \pm\beta_i)$ кривої E_d над полем F_p.

Визначимо, що

$$\phi(P) = (x', y') = \left(\prod_{Q \in G} \frac{x_{P+Q_i}}{x_{Q_i}} \frac{x_{P-Q_i}}{x_{-Q_i}},\ \prod_{Q \in G} \frac{y_{P+Q_i}}{x_{Q_i}} \frac{y_{P-Q_i}}{x_{-Q_i}}\right). \tag{2.21}$$

Тоді $\phi(x, y)$ є l-ізогенія з ядром G із кривої $E_{a,d}$ у криву $E'_{a',d'}$ з параметрами

$$a' = a^l;\ d' = A^8 d^l, \text{ де } A = \prod_{i=1}^{s} \alpha_i, \tag{2.22}$$

де α_i – координата x точки ядра ізогенії Q_i.

При цьому відображаюча функція

$$\phi(x,y)=\left(\frac{x}{A^2}\prod_{i=1}^{s}\frac{(\alpha_i x)^2-a^2(\beta_i y)^2}{1-(d\alpha_i\beta_i xy)^2},\frac{y}{A^2}\prod_{i=1}^{s}\frac{(\alpha_i y)^2-(\beta_i x)^2}{1-(d\alpha_i\beta_i xy)^2}\right) \tag{2.23}$$

або

$$\phi(x,y)=\left(\frac{x}{A^2}\prod_{i=1}^{s}\frac{x^2-a{\beta_i}^2}{1-d\beta_i x^2},\frac{-y}{A^2}\prod_{i=1}^{s}\frac{x^2-{a_i}^2}{a-d\alpha_i x^2}\right). \tag{2.24}$$

Здійснені розрахунки дозволяють зробити порівняння оцінки складності обчислення ізогенної функції $\phi(x,y)$ та параметра d' ізогенної кривої $E'_{a',d'}$. Це дозволить оцінити виграш у швидкості обчислення в алгоритмі CSIDH у разі відмови від складної функції $\phi(x,y)$.

Нехай M – складність множення у полі F_p, S – складність зведення у квадрат. Скористаємося результатами роботи [53]. З урахуванням складності обчислення координат точок ядра складність обчислення функції $\phi(x,y)$ дорівнює

$$C_\phi = s(8M+2S)+S-2M. \tag{2.25}$$

Вартість обчислення параметра d' ізогенної кривої E', відповідно,

$$C_d = s(6M+2S)+5S-4M. \tag{2.26}$$

Приймемо відому оцінку $S=\frac{2}{3}M$ [43]. Тоді маємо

$$C_\phi=\frac{28}{3}sM-\frac{4}{3}M,\ C_d=\frac{22}{3}sM-\frac{2}{3}M. \tag{2.27}$$

Виграш у швидкості обчислень без урахування C_ϕ дорівнює

$$\gamma_3=\frac{C_d+C_\phi}{C_d}=1+\frac{C_\phi}{C_d}=1+\frac{14s-2}{11s-1}. \tag{2.28}$$

Тоді якщо $\phi(x,y)$ є l-ізогенія з ядром G із кривої $E_{a,d}$ у криву $E'_{a',d'}$ і максимальна $l\approx 600$ маємо максимальну $s=(l+1)/2$ або $s\approx 300$, а мінімальну $s=1$ цей виграш дорівнює 2,27 та 2,20 відповідно. Обчислення ізогенної функції досить складна і трудомістка операція, у часі обчислення алгоритму вона займає біля 90%. Тому можна знехтувати часом виконання іншої частини алгоритму.

Таким чином при відмові від обчислення ізогенної функції $\phi(x,y)$ у середньому отримаємо виграш часу в обчисленні алгоритму $\gamma_3=2{,}235$ [47, 53].

2.3.2. Класичний алгоритм CSIDH

В роботі [10] представлений класичний постквантовий алгоритм PQC CSIDH на ізогеніях еліптичних кривих Монтгомері. CSIDH побудовано на основі ізогенних відображень еліптичних кривих в цілому як адитивних абелевих груп. Таке відображення над простим полем F_p визначено як клас групової дії і є комутативним. У ньому використані ідеї схеми CRS на НКЕ. У порівнянні з ними використання ізогеній СКЕ дозволило кардинально прискорити алгоритм і отримати найменший з відомих розмір ключа (512 біт) при рівні квантової безпеки 128 біт [10].

Алгоритм CSIDH базувався на швидкій арифметиці ізогеній кривих у формі Монтгомері $y^2 = x^3 + Cx^2 + x,\ C \neq \pm 2$. В роботі [36] алгоритм будується на повних кривих Едвардса того же порядку. У роботі [60] запропоновано новий ефективний метод обчислення ізогеній непарних ступенів на повних кривих Едвардса на основі координат Фарашахи-Хоссейні. В роботах [38, 40, 47] замість повних кривих Едвардса обґрунтовано і проілюстровано на прикладі імплементацію алгоритму CSIDH на квадратичних і скручених кривих Едвардса.

Особливості CSIDH на ізогеніях полягають у наступному, Нехай крива E порядка N_E містить точки малих непарних порядків $l_k, k = 1,2, \dots, K$. Тоді існує ізогенна крива E' того же порядку N_E як відображення ступені l_k: $E \to E' = [l_k] * E$. Це є групова функція. Позначка $[l_k]$ означає один ізогенний перехід по ізогенії l_k Повторювання цієї операції e_k раз будем записувати як $[{l_k}^{e_k}] * E$. В результаті отримаємо ланцюжок ізогенних переходів від кривої E до кривої E'.

Значення експонент $e_k \in Z$ визначають довжину ланцюжка ізогеній ступені l_k. В роботі [10] довжина ланцюжків обмежується обранням інтервалу значень експонент $[-m \leq e_k \leq m], m = 5,\ K = 74$, що забезпечує рівень безпеки 128 біт при атаках квантового комп'ютера. Величина К це кількість ступенів ізогеній. Негативні значення e_i визначають перехід до СКЕ квадратичного кручення [34].

Функція CGA має вигляд $\Theta = [{l_1}^{e_1}, {l_2}^{e_2}, .., {l_K}^{e_K}]$, де l_i – непарні прості степені ізогеній..Функція CGA здійснює ізогенне відображення Θ СКЕ E порядку $N_E =$

$p+1$ у криву $E' = E * \Theta$ того ж порядку. Значення експонент ізогеній $e_k \in Z$ визначають довжину ланцюжка ізогеній ступеню l_k. Відображення Θ є комутативним. Таким чином усі ізогенні перетворення створюють ланцюжки (шляхи), які складаються у граф ізогеній.

Обчислення ізогенних ланцюжків в оригінальному алгоритмі CSIDH здійснюється у два етапи: спочатку формується множина S з експонентами ключа e_k одного знаку, потім після обнуління всіх e_k іншого знаку (множина $S1$). На кожної кривої послідовно обчислюються ядра та параметри рівно $|e_k|$ ізогенних кривих ступенів l_k побудованих на кривих одного класу (E_d або $E_{-1,-d}$).

Цей алгоритм схильний до атак сторонніми каналами на основі непрямого вимірювання часу обчислень, який пропорційний абсолютної величині $|e_k|$ і ступеня l_k кожного ланцюжка $\left[l_k^{e_k}\right]$. У зв'язку з цим у [62] розглядаються різні варіанти алгоритму CSIDH з постійним часом виконання (від. англ. Constant Time CSIDH, CT CSIDH), у яких секретні експоненти e_k нарощуються до верхній межи m фіктивними ланцюжками ізогеній. Такий захист дає значну надмірність і уповільнює роботу алгоритму.

Неінтерактивний обмін ключами за класичною схемою Діффі-Геллмана включає етапи [10]:

1. Вибір параметрів. Для малих простих непарних l_k обчислюється $n = \prod_{k=1}^{K} l_k$, де значення K визначається рівнем безпеки, і обирається модуль поля $p = 2^m \prod_{k=1}^{K} l_k - 1, m \geq 3$ і стартова еліптична крива E_0.

2. Обчислення відкритих ключів. Аліса за допомогою свого секретного ключа $\Omega_A = (e_1, e_2, .., e_K)$ будує ізогенне відображення $\Theta_A = [{l_1}^{e_1}, {l_2}^{e_2}, .., {l_K}^{e_K}]$ і обчислює ізогенну криву $E_A = \Theta_A * E_0$ як свій відкритий ключ. Боб на основі секретного ключа Ω_B і функції Θ_A виконує те же обчислення і отримає свій відкритий ключ $E_B = \Theta_B * E_0$. Ці криві визначаються їх параметрами с точністю до ізоморфізму.

3. Обмін ключами. Далі виконується протокол подібний п. 2 зі заміною $E_0 \rightarrow E_B$ для Аліси і $E_0 \rightarrow E_A$ для Боба. Знаючи відкритий ключ Боба, Аліса обчислює $E_{BA} = \Theta_A * E_B = \Theta_A \Theta_B * E_0$ Аналогичні дії Боба дають результат $E_{AB} = \Theta_B * E_A =$

$\Theta_B\Theta_A * E_0$, співпадаючій с першим в силу комутативності групової операції. В якості розділеного секрету обирається J-інваріант кривої E_{AB} (E_{BA}).

Натомість повних кривих А. В. Бессалов запропонував [38] і обґрунтував використовувати квадратичні та скручені СКЕ, а у роботах [40, 48, 57] разом із учнями та послідовниками досліджували як найбільш ефективні технології, алгоритми на основі класів квадратичних та скручених СКЕ, пов'язані як пари квадратичного кручення.

2.3.3. Ланцюжки ізогеній кривої порядку 840

У роботі [40] розглянуто імплементацію алгоритму CSIDH на квадратичних і скручених СКЕ, що утворюють пари квадратичного кручення з однаковим порядком. Такі криві існують лише за $p \equiv -1 \bmod 8$ і мають порядок $N_E = N_E^t = p + 1 = cn \rightleftarrows (n - odd), c \equiv 0 \bmod 8$. Нехай така пара кривих містить ядра 3-го, 5-го та 7-го порядків, тоді $n = 105$, а мінімальне просте $p = 8n - 1 = 839$ і порядок цих кривих $N_E = 8n = 840$. Параметр d всього сімейства 418 квадратичних кривих Едвардса можна прийняти як квадрати $d = r^2 \bmod p$, $r = 2{,}419$. З них у роботі [37] знайдено 66 пар квадратичних та скручених СКЕ з параметрами $a = \pm 1$ та $\chi(ad) = 1$. Квадратичну СКЕ (3) позначаємо E_d, а скрученну СКЕ (4) – як $E_{-1,-d}$.

Аналіз усіх кривих, які мають модуль $p = 839$ та параметри а $= 1$, $d = r^2$, де $r = 2 \ldots 419$ показав, що ці криві мають 15 різних порядків N_e, зображених у табл. 2.3 , де кількість кривих C_N з порядком N_e.

Таблиця 2.3

Кількість кривих C_N з порядком N_e

№	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
N_e	784	792	800	808	816	824	832	840	848	856	864	872	880	888	896
C_N	8	26	30	16	48	30	18	66	18	30	48	16	30	26	8

Серед них є 66 СКЕ порядку 840 у яких слід Фробеніуса $t = 0$. Ці криві мають два сегменти по 33 кривих 840 порядку, які складають два ланцюжки ізогеній 3-го

ступеня (рис. 2.16). Послідовність, у якої перелічені криві згідно з (2.11) будемо вважати позитивною, зворотна послідовність – негативною.

Перший сегмент 33 кривих 840 порядку (1-й ланцюжок ізогеній 3-го ступеня):

144, 414, 405, 2, 28, 259, 752, 773, 15, 243, 21, 433, 180, 514, 578, 293, 666, 38, 112, 172, 683, 258, 772, 488, 636, 286, 508, 76, 236, 43, 788, 61, 289

Другий сегмент 33 кривих 840 порядку (2-й ланцюжок ізогеній 3-го ступеня):

705, 610, 810, 420, 30, 230, 135, 750, 56, 511, 40, 808, 564, 475, 45, 63, 742, 552, 427, 200, 640, 423, 288, 98, 777, 795, 365, 276, 32, 800, 329, 784, 90

Криві 1 і 2 сегменту у вигляді ланцюжка ізогеній 3-го ступеня складають дві групи ізогеній 3-го ступеня з періодом 33, зображених відповідно у табл. 2.4 та 2.5 і на рис. 2.6. Криві кожного сегменту також входять у три групи ізогеній 5-го і 7-го порядку с періодом 11, які розташовані в окремих рядках табл. 2.4 і 2.5.

Таблиця 2.4

Ізогенії п’ятого порядку

Підгрупа	1	2	3	4	5	6	7	8	9	10	11
1	144	2	752	243	180	293	112	258	636	76	788
2	414	28	773	21	514	666	172	772	286	236	61
3	405	259	15	433	578	38	683	488	508	43	289

Перший ланцюжок 5-ізогеній має вигляд: 144-76-258-293-243-2-788-636-112-180-752.

Таблиця 2.5

Ізогеній сьомого порядку

Підгрупа	1	2	3	4	5	6	7	8	9	10	11
1	705	420	135	511	564	63	427	413	777	276	329
2	90	810	230	56	808	45	552	640	98	365	800
3	784	610	30	750	40	475	742	200	288	795	32

Друга група ізогеній 3-го ступеня з періодом 33.

Для кривої з параметром d розрахунок параметра d' ізогенії виконувався за формулою (2.21).

Якщо вибрати початкову випадкову криву, яка відсутня у табл. 2.4 та 2.5, наприклад, криву з параметром $d = 467$, отримаємо ланцюжок НКЕ порядку 816 з періодом 24. З табл. 2.3 видно, що цій порядок (816) мають 48 кривих, тобто два ланцюжки з періодом 24 кожен.

Пари кривих з першого та другого ланцюгів пов'язані між собою виразом $d' = d^{-1}$ тобто їх параметри d є зворотними величинами. Тому ці пари створюють суперсингулярні пари квадратичного кручення.

Ще циклічний вигляд мають ланцюжки 864 порядку 2×24, ланцюжки 792 та 888 порядків з періодом 2×13. Інші криві циклічних ланцюжків не утворюють.

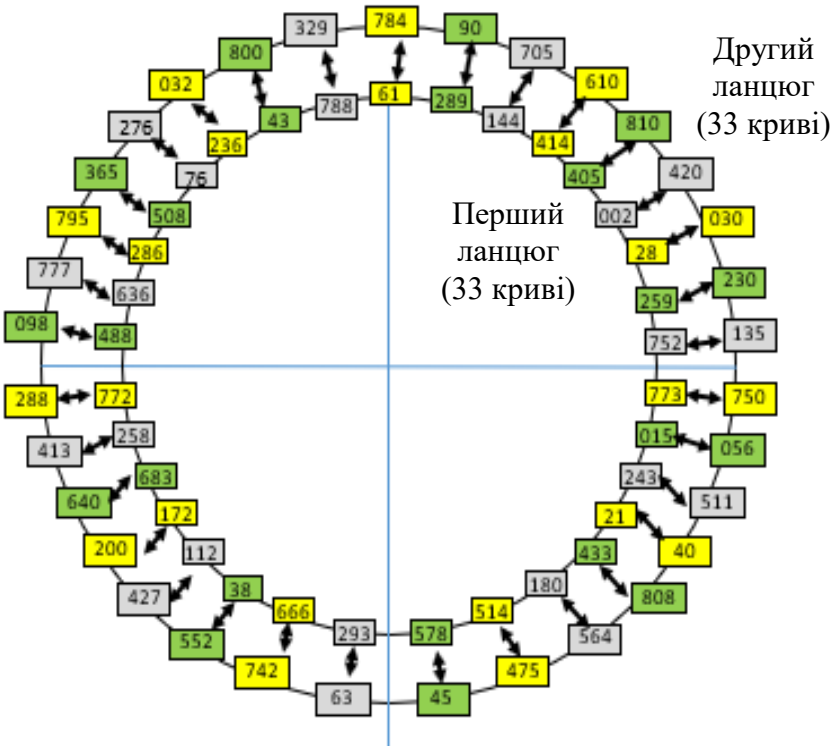

Рис. 2.6. Суперсингулярні пари квадратичного кручення ізогеній третього ступеня кривої 840 порядку

Інші криві є несуперсингулярними парами квадратичного кручення порядку $840 \pm t$, де t-слід рівняння Фробеніуса. Найбільш численні криві порядку 816 та 864 (по 48 кривих), які становлять пари квадратичного кручення порядку 840 ± 24 ($t = \pm 24$). Загальна кількість таких кривих $48 + 48 = 96$. Майже в 1,5 рази більше, ніж кількість СКЕ.

Усі криві як суперсингулярні, так і несуперсингулярні можна використовувати для будови паралельних криптосистем, як показано, наприклад, в роботах [56] і [63]. Або ланцюги ізогеній кривих порядку 816 та 864.

Ланцюг 3-ізогеній порядку $P = 816$. Криві з параметрами d [4, 196, 729, 347, 626, 244, 527, 177, 748, 411, 265, 378, 381, 634, 318, 751, 377, 715, 296, 106, 75, 179, 128, 221, 690, 283, 162, 59, 207, 746, 19, 608, 467, 227, 674, 454, 499, 343, 143, 602, 424, 516, 450, 366, 320, 300, 252, 210] 48 кривих.

Ланцюг 3-ізогеній порядку $P = 864$:

Криві з параметрами d [9, 225, 324, 361, 576, 386, 530, 619, 125, 613, 429, 150, 193, 575, 774, 188, 443, 644, 313, 341, 224, 633, 111, 661, 540, 622, 228, 593, 806, 257, 94, 607, 371, 588, 509, 697, 373, 781, 271, 281, 491, 663, 512, 92, 493, 241, 630, 342] число кривих 48.

У табл. 2.6 показано які ще є пари кручення серед кривих з модулем 839.

Таблиця 2.6

Пари квадратичного кручення серед кривих з модулем 839

№	1	2	3	4	5	6	7	8
Крива $+t$	840	848	856	864	872	880	888	896
Крива $-t$	840	832	824	816	808	800	792	784
t	0	8	16	24	32	40	48	56
Кількість кривих	66	2·18	2·30	2·48	28·16	2·30	2·26	2·8

Для першої кривої ${E_d}^{(0)} = E_{144}$ у роботі [37] побудовані 3-, 5- та 7-ізогенії та знайдено параметри $d^{(i)}$ ланцюжки ізогенних кривих ${E_d}^{(i)}, i = 0,1,2, \dots, T$. Крива E_{144} дає початок ланцюжку ізогеній 3-го ступеня із періодом 33 тобто. до неї входить половина всіх кривих порядку 840 назвемо їх першим сегментом кривих. З цих же кривих складаються і ланцюжки 5- та 7-ізогеній.

Інші 33 кривих утворюють другий сегмент, всі криві якого мають параметр d зворотний до параметрів першого сегмента. Так наприклад, $144^{-1} = 705$.

На рис 2.10 показані графи цих ізогеній першого і другого сегментів. На графі показано ланцюжки 3-ізогеній, де всередині прямокутників показано значення

параметра d ізогенної кривої. Ланцюжок починається від параметра $d = 144$ а чергова обчислена ізогенія розташовується за годинниковою стрілкою.

Ізогенії 5-го та 7-го ступеня утворюють по три ланцюжки кожного ступеня з періодом 11. На рис 2.12 параметри ланцюжка ізогеній 5 ступеня позначені суцільними стрілками, а 7-го ступеня пунктирними. Приклади ізогеній 5 і 7 порядку другого сегменту показано на рис. 2.8.

На рис. 2.7 і 2.8 показані тільки 1 і 2 ланцюги 5- і 7-ізогенії (жовтий і зелений). Треті ланцюги (сірого кольору) не показано, вони мають аналогічний вигляд. Структура всіх ізогеній СКЕ порядку 840 представлена на рис. 2.9. Всі криві складають два сегменти по 33 криві, що не перетинаються. Криві кожного сегмента утворюють один ланцюжок ізогеній 3-го ступеня (період 33) та по три ланцюжка 5-го та 7-го ступенів.

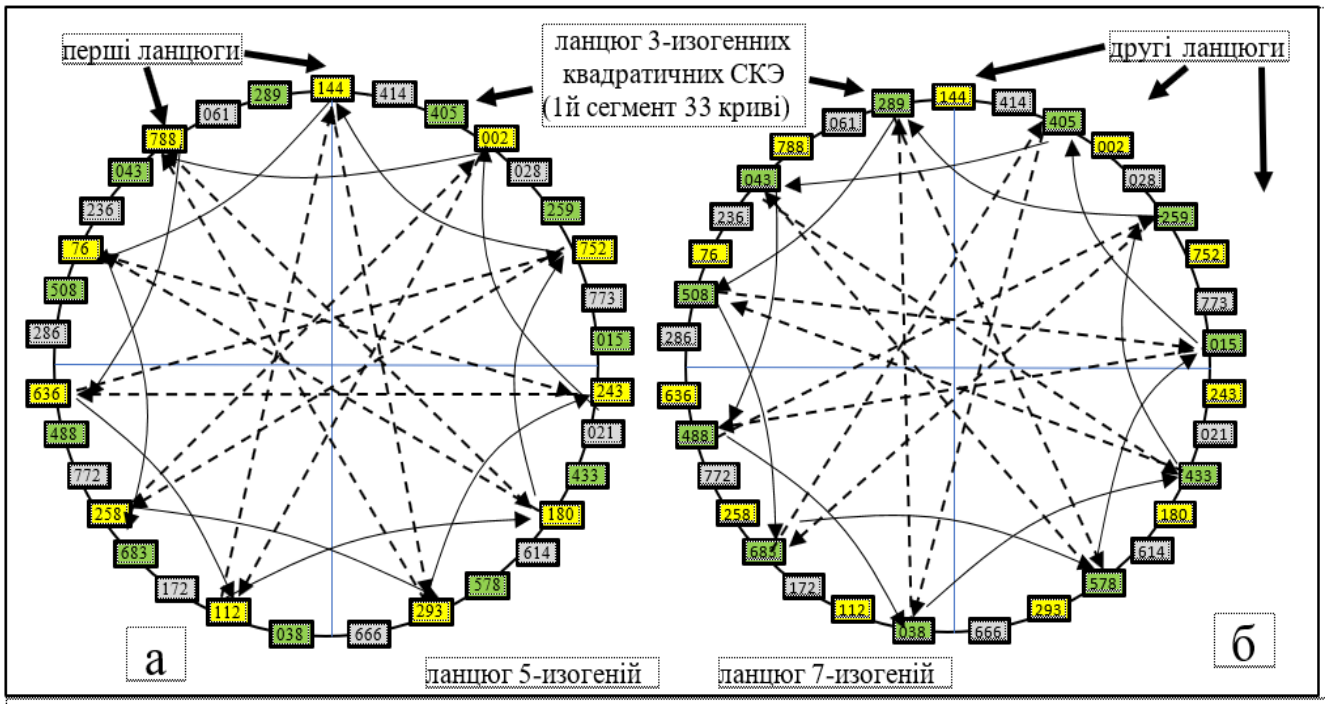

Рис. 2.7. Граф ізогеній першого сегменту

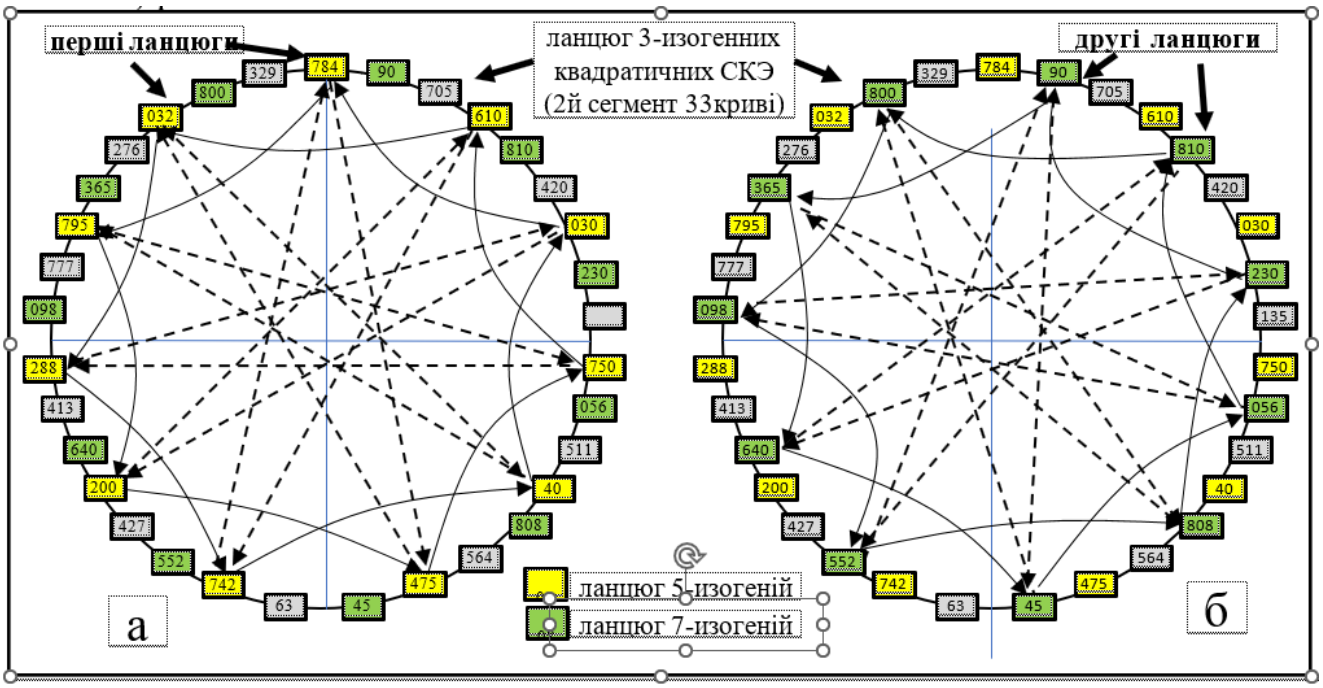

Рис. 2.8. Граф ізогеній другого сегменту

На рисунках показані лише перший (рис. 2.7а і 2.8а) і другий (рис. 2.7б і 2.8б) ланцюги 5-го і 7-го ступеня. Треті ланцюги не показані.

На рис. 2.9 показано, що перехід між ланцюгами ізогеній 3 ступеню здійснюється шляхом мультиплікативної інверсії параметра $d' = d^{-1}$, який є досить складний для обчислення.

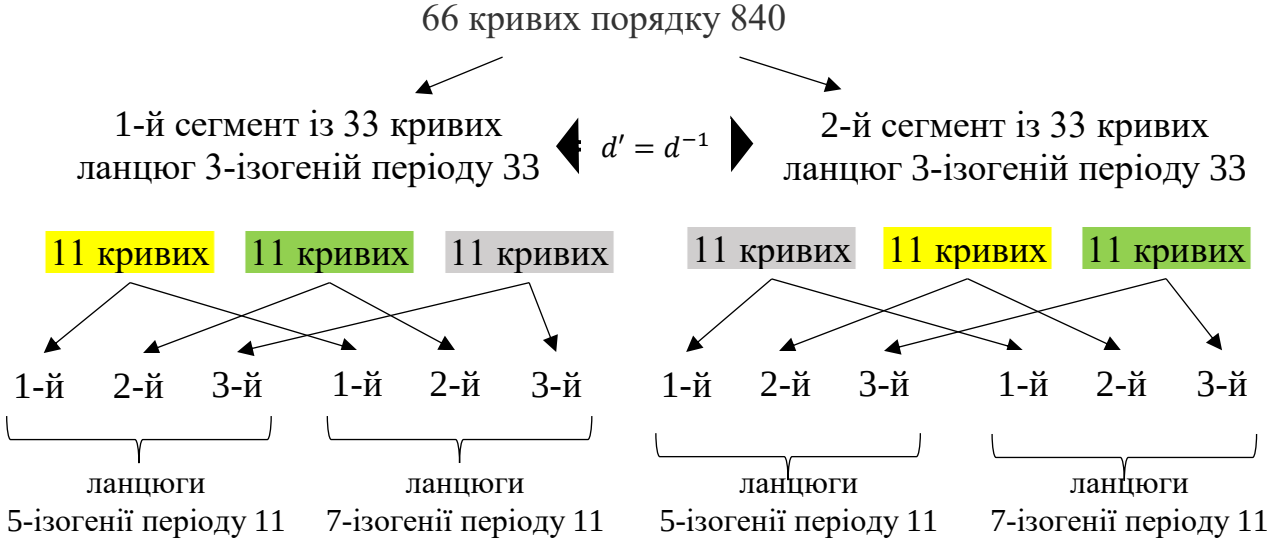

Рис. 2.9. Структура ізогенії СКЕ 840 порядку

На рис. 2.10 показані шляхи – переходи на графі між ізогенними кривими з параметрами $d = 144 \to 243$ та $d = 144 \to 433$. Стрілками червоного кольору

показано ланцюги 3-ізогеній, зеленим ланцюги 5-ізогеній, синим – ланцюги 7-ізогеній.

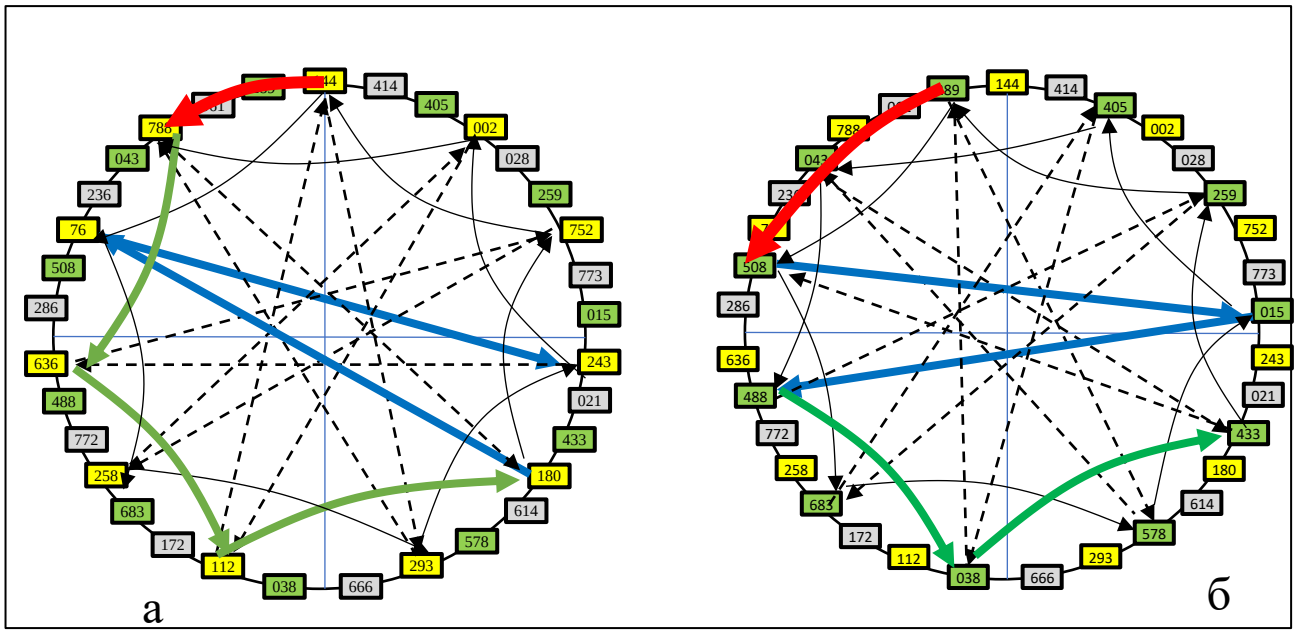

Рис. 2.10 Приклади переходів за графом ізогеній (а) $E_{144} * [l_3^3 \cdot l_5^3 \cdot l_7^2] = E_{243}$ і (б) $E_{289} * [l_3^6 \cdot l_5^2 \cdot l_7^2] = E_{433}$

Ще пари квадратичного кручення можна отримати на ґрунті модуля $p = 863 \pm t$ де $t = 24$. Це НКЕ порядку 840 і 888. Вони розглядаються у розділі 4.

З графа видно, що показники ступеня у векторі $\Omega K = (e_1, e_2, \dots, e_K)$ можуть бути будь якими, але маємо тільки один ланцюжок ізогенії l_3 3-го ступеню і по три варіанти ланцюжків 5-го або 7-го ступеню $\{l_5^1, l_5^2, l_5^3\}$ і $\{l_7^1, l_7^2, l_7^3\}$. Тому при виборі 5- і 7-ізогеній ми можемо рухатись по різним варіантам. Такі властивості графа ізогеній дещо обмежує свободу блукань по графу, а кількість шляхів між кривими зменшується, але це зменшення не має суттєвого впливу на крипостійкість алгоритму.

2.3.4. Алгоритм CSIDH на нециклічних суперсингулярних кривих

В роботі [37] узагальнюються теореми на криві в формі Едвардса с двома параметрами a, d, що дозволяє застосувати квадратичні та скручені криві Едвардса над полем F_p для імплементації моделі CSIDH.

Нижче наведено модифікацію алгоритму обчислень Аліси згідно з п. 2 з [64] з використанням ізогеній квадратичних та скручених СКЕ алгоритм CSIDH TQSEC.

Алгоритм 2.1. Реалізація групової операції на квадратичних та скручених суперсингулярних кривих Едвардса [47]

Input: $d_A \in E_A, \chi(d) = 1$ *and a list of integers* $\Omega_A = (e_1, e_2, \dots e_K)$.

Output: d_B *such that* $[{l_1}^{e_1}, {l_2}^{e_2}, \dots {l_K}^{e_K}] * E_A = E_B$, *where* $E_{A,B}$: $x^2 + y^2 = 1 + d_{A,B}x^2y^2$,

1. While *some* $e_i \neq 0$ **do**

2. *Sample a random* $x \in F_p$,

3. Set $a \leftarrow 1$, E_A: $x^2 + y^2 = 1 + d_A x^2 y^2$ **if** $(1 - x^2)/(1 - dy^2)$ *is a square in* F_p,

4. Else $a \leftarrow -1$, E_A: $x^2 - y^2 = 1 - d_A x^2 y^2$,

5. *Let* $S = \{i | ae_i > 0\}$. **If** $G = \emptyset$ *then start over to line 2 while* $a \leftarrow -a$,

6. *Let* $n = \prod_{i \in S} l_i$, *and compute* $R \leftarrow [(p+1)/2n]P, P \leftarrow P(x, y)$,

7. For e*ach* $i \in S$ **do**

8. *Compute* $Q \leftarrow [k/l_i]R$

9. If $Q \neq (1,0)$ *Compute an isogeny* $\varphi: E_A \rightarrow E_B$ *with* $\ker \varphi = Q$,

10. ***Set*** $d_A \leftarrow d_B, R \leftarrow \varphi(R), e_i \leftarrow e_i - a$ **,**

11. *Skip* i *in* ѕ*and* $n \leftarrow n/l_i$ **if** $e_i = 0$,

12. Return d_A**.**

У порівнянні з алгоритмом 2 з [64] в Алгоритмі 3.1, адаптованому до квадратичних і скручених СКЕ:

1. Перевірка квадратичного характеру у правій частині п. 3 виконується для рівняння квадратичної кривої Едвардса (2.11).

2. При порядку скрученої кривої Едвардса $N_E = 8n = p + 1$ з максимальним порядком точки $N_E/2 = 4n$ для отримання точки порядку n досить дворазового подвоєння випадкової точки P. У п.6 цю властивість враховано зменшенням одного подвоєння в скалярному добутку точки R.

3. В п. 9 скориговано: скидання i після обнуління e_i в п. 10.

4. В п. 11 оновлення числа $n \leftarrow n/l_i$ разом зі скиданням i зроблено після обнуління e_i.

Згідно з п. 10 для кожного l_i обчислюється рівно e_i ізогеній до обнуління експоненти e_i. В залежності від знаку ізогенії обчислюються в класі квадратичних ($e_i > 0$) або кручених СКЕ ($e_i < 0$).

У основі побудови ізогеній непарних простих ступенів для квадратичних кривих Едвардса лежить теорема 2 [27], а скручених кривих Едвардса – теорема 1 [51]. В останній роботі вперше наведено формули відображень $\phi(P)$ для кривої (2.7), яке залежить від двох параметрів a і d [47].

2.3.5. Модель алгоритму на нециклічних кривих Едвардса

Розглянемо попередню (п. 2.3.3) модель алгоритму CSIDH на квадратичних та скручених СКЕ, що утворюють суперсингулярні пари квадратичного кручення з однаковим порядком 840. В табл. 2.7 наведені значення параметра d для пар квадратичних і скручених СКЕ в виде квадратів $d = r^2 \bmod p, r = 2, \dots, 419$ у порядку зростання r.

У цьому прикладі відносна частка СКЕ становить близько 16%. Зауважимо, що для кожної кривої табл. 2.7 існує щонайменше одна ізоморфна крива з параметром $d^{(-1)}$ та однаковим J-інваріантом.

Таблиця 2.7

Значення 66 параметрів d квадратичних і скручених СКЕ ($a = \pm 1$)

при $p = 839$ і $N_E = 840$

144*	289*	784	2*	61*	258*	508*	365	488*	30	705
742	56	259*	180*	329	135	640	32	38*	28*	90
564	772*	286*	40	610	98	475	63	511	43*	795
414*	76*	752*	800	405*	666*	112*	413	200	236*	433*
15*	683*	293*	750	808	578*	288	636*	514*	276	773*
243*	45	788*	172*	777	427	21*	810	552	420	230

Така пара кривих містить ядра 3-го, 5-го та 7-го порядків при значенні $n = 105$, $p = 8n - 1 = 839$ і порядок $N_E = 8n = 840$ [34].

Усі 66 криві, які складають два сегмента по 33 криві у кожному. Точки першого сегменту позначені зірочкою. Точки кожного сегменту складають циклічну підгрупу, які зображені на рис. 2.7 і 2.8. Для першої квадратичної кривої ${E_d}^{(0)} = E_{144}$ можна побудувати ланцюги 3-, 5- і 7-ізогенії і знайти параметри $d^{(i)}$ ланцюжків ізогенних кривих ${E_d}^{(i)}, i = 0,1,2,\dots,T$, таких що $d^{(T)} = d^{(0)}$. Період T ланцюжки ізогеній ділить число $66 = 2 \cdot 3 \cdot 11$ усіх СКЕ.

В табл. 2.8–2.10 наведені результати розрахунків параметрів $d^{(i)}$ ланцюжків відповідно 3-, 5- і 7-ізогений квадратичних СКЕ. На кожному кроці $i = 0,1,2,\dots,$ T ізогенії ступеню $l = 2s + 1$ нециклічних кривих обчислюються координати $\alpha_1, \alpha_s, s = (l-1)/2$ точок ядра, після чого за формулою (2.21) розраховується параметр $d^{(i+1)}$ ізогенної кривої ${E_d}^{(i+1)}$. В усіх таблицях в першому рядку вказані номера i, в наступних s строках – координати точок ядра, потім – рядок с параметрами $d^{(i)}$. В табл. 2.8–2.10 зображені тільки криві 1-го сегменту. У кожному сегменті є по три ланцюжка 5- і 7-ізогеній, кожний ланцюжок позначений своїм кольором жовтий, зелений, сірий. Криві обох сегментів представлено на рис. 2.6. Комутативність функції $\Theta_A = [l_1^{e_1}, l_2^{e_2}, \dots, l_K^{e_K}]$ спрощує отримання результату кількома шляхами.

Таблиця 2.8

Значення параметрів ланцюжка 3-ізогенних квадратичних СКЕ ($a = 1$) при $p = 839$ (період $T = 33$)

i	0	1	2	3	4	5	6	7	8	9	10
$\alpha^{(i)}$	518	558	768	178	502	44	372	136	258	75	487
$d^{(i)}$	**144**	**414**	**405**	**2**	**28**	**259**	**752**	**773**	**15**	**243**	**21**
i	11	12	13	14	15	16	17	18	19	20	21
$\alpha^{(i)}$	697	481	333	248	613	378	663	404	20	377	99
$d^{(i)}$	**433**	**180**	**514**	**578**	**293**	**666**	**38**	**112**	**172**	**683**	**258**
i	22	23	24	25	26	27	28	29	30	31	32
$\alpha^{(i)}$	718	379	327	139	781	41	601	344	561	230	477
$d^{(i)}$	**772**	**488**	**636**	**286**	**508**	**76**	**236**	**43**	**788**	**61**	**289**

Таблиця 2.9

Значення параметрів трьох ланцюжків 5-ізогенних квадратичних СКЕ ($a = 1$) при $p = 839$ (період $T = 11$)

i	0	1	2	3	4	5	6	7	8	9	10
$\alpha_1^{(i)}$	78	343	152	337	318	344	588	222	151	352	390
$\alpha_2^{(i)}$	537	655	632	720	545	837	790	832	748	372	790
$d^{(i)}$	**144**	**76**	**258**	**293**	**243**	**2**	**788**	**636**	**112**	**180**	**752**
$\alpha_1^{(i)}$	327	390	91	125	653	17	251	744	409	586	103
$\alpha_2^{(i)}$	726	552	609	583	655	682	393	764	577	692	531
$d^{(i)}$	**289**	**508**	**683**	**578**	**15**	**405**	**43**	**488**	**38**	**433**	**259**
$\alpha_1^{(i)}$	558	344	610	792	73	820	20	779	779	748	188
$\alpha_2^{(i)}$	445	443	342	113	546	71	463	651	635	304	252
$d^{(i)}$	**61**	**286**	**172**	**514**	**773**	**414**	**236**	**772**	**666**	**21**	**28**

Таблиця 2.10

Значення параметрів трьох ланцюжків 7-ізогенних квадратичних СКЕ ($a = 1$) при $p = 839$ (период $T = 11$)

i	0	1	2	3	4	5	6	7	8	9	10
$\alpha_1^{(i)}$	9	485	99	161	255	103	367	73	41	422	362
$\alpha_2^{(i)}$	718	700	319	248	705	131	828	258	731	582	820
$\alpha_3^{(i)}$	17	826	678	465	322	324	700	99	229	689	591
$d^{(i)}$	**144**	**293**	**788**	**180**	**76**	**243**	**636**	**752**	**258**	**2**	**112**
$\alpha_1^{(i)}$	314	204	30	86	86	74	324	37	281	284	251
$\alpha_2^{(i)}$	563	416	337	222	489	314	530	164	513	741	544
$\alpha_3^{(i)}$	678	207	313	720	571	430	595	496	418	828	342
$d^{(i)}$	**289**	**578**	**43**	**433**	**508**	**15**	**488**	**259**	**683**	**405**	**38**
$\alpha_1^{(i)}$	165	552	726	37	772	5	32	44	93	161	7
$\alpha_2^{(i)}$	653	485	278	219	748	78	663	165	655	275	127
$\alpha_3^{(i)}$	322	397	385	327	565	518	220	251	467	408	248
$d^{(i)}$	**61**	**514**	**236**	**21**	**286**	**773**	**772**	**28**	**172**	**414**	**666**

Ізогенії кручених СКЕ $E_{-1,-d}^{(i)}, i = 0,1,2, \dots, T-1$ мають просту властивість: послідовності параметрів $d^{(i)}$ ізогений $[l_i^{e_i}], e_i > 0$ і $[l_i^{e_i}], e_i < 0$ на періоді ізогеній

$i = 0,1,2,\dots,T-1$ мають реверсний (зустрічний) характер. Тобто, якщо для квадратичної СКЕ $(e_i > 0)$ послідовність параметрів має вигляд $d^{(0)}, d^{(1)}, \dots, d^{(T)}, d^{(0)} = d^{(T)}$, то для крученої СКЕ $(e_i < 0)$ має зворотний порядок $d^{(T)}, d^{(T-1)}, \dots, d^{(0)}, d^{(0)} = d^{(T)}$.

Нехай секретні ключи $\{e_i\}$ Аліси і Боба $\Omega_A = (7,-5,8), \Omega_B = (-8,\ 6,-5)$, їх функції класу групових операцій, відповідно, $\Theta_A = [3^7, 5^{-5}, 7^8]$, $\Theta_B = [3^{-8}, 5^6, 7^{-5}]$. Розрахуємо їх відкриті ключі d_A і d_B. В якості стартової кривої ланцюжки ізогеній приймемо криву ${E_d}^{(0)} = E_{144} \to d = 144$. Тоді $E_A = E_0 * \Theta_A$, $E_B = E_0 * \Theta_B$.

З метою спрощення записи в алгоритме обчислення ізогенної кривої $E_A = E_0 * \Theta_A$ ми будемо корисуватися лише параметрами $d^{(i)}$, які цілком визначають криві ${E_d}^{(i)}(e_k > 0)$ і ${E_{-1,-d}}^{(i)}(e_k < 0)$ як пари квадратичного кручення. Властивість комутативності функції Θ_{A} у нашому випадку означає, що є $3! = 6$ варіантів вибору порядку розташування ступенів ізогеній. При виборі початкової точки ${E_d}^{(0)} = E_{144} \to d = 144$, і функції $\Theta_A = [3^7, 5^{-5}, 7^8]$, тобто виборі порядку ступеней ізогеній 3-5-7 значення $d^{(i)}$ кінцевих очок ланцюжків ізогеній мають вигляд

$$\frac{d_0 = 144}{(3)} \xrightarrow{7} \frac{773}{(5)} \xrightarrow{-5} \frac{28}{(7)} \xrightarrow{8} 286. \tag{2.28}$$

Тут під значенням $d^{(i)}$ в дужках ми умовно ставимо ступень ізогенії, а над стрілкою – значення e_k експоненти секретного ключа Аліси (число кроків в послідовності $d^{(i)}$ вправо або вліво в залежності від от знаку e_k).

Можна навести приклад ще двох шляхів:

$$\frac{d_0 = 144}{(7)} \xrightarrow{8} \frac{258}{(5)} \xrightarrow{-5} \frac{112}{(3)} \xrightarrow{7} 286, \tag{2.29}$$

$$\frac{d_0 = 144}{(5)} \xrightarrow{-5} \frac{788}{(57)} \xrightarrow{8} \frac{112}{(3)} \xrightarrow{7} 286. \tag{2.30}$$

Таким чином, відкритий ключ Аліси $d_A = 286$. Аналогічно визначаємо відкритий ключ Боба на ґрунті ${E_d}^{(0)} = E_{144}$ і функції $\Theta_B = [3^{-8}, 5^6, 7^{-5}]$

$$\frac{d_0 = 144}{(5)} \xrightarrow{6} \frac{788}{(7)} \xrightarrow{-5} \frac{258}{(3)} \xrightarrow{-8} 514, \tag{2.31}$$

$$\frac{d_0 = 144}{(7)} \xrightarrow{-5} \frac{636}{(5)} \xrightarrow{6} \frac{258}{(3)} \xrightarrow{-8} 514. \quad (2.32)$$

Отримаємо відкритий ключ Боба $d_B = 514$. В не інтерактивному алгоритмі CSIDH ключи d_A, d_B відомі обом користувачам. варіантів вибору порядку розташування ступенів ізогеній $E_{BA} = E_B * \Theta_A$. Симетрично діє Боб і отримує $E_{AB} = E_A * \Theta_B$. В нашим прикладі обчислень Аліси $E_{AB} = E_{514} * \Theta_A$ при $\Theta_A = [3^7, 5^{-5}, 7^8]$ і виборі порядку ступенів ізогеній 3-5-7 дають результат

$$\frac{d_0 = 514}{(3)} \xrightarrow{7} \frac{683}{(5)} \xrightarrow{-5} \frac{38}{(7)} \xrightarrow{8} 259 \Rightarrow d_{BK} = 259, \quad (2.33)$$

$$\frac{d_0 = 514}{(7)} \xrightarrow{8} \frac{414}{(5)} \xrightarrow{-5} \frac{289}{(3)} \xrightarrow{7} 259. \quad (2.34)$$

Відповідно обчисленням Боба $E_{AB} = E_{286} * (\Theta_B = [3^{-8}, 5^6, 7^{-5}])$ можна записати

$$\frac{d_0 = 286}{(3)} \xrightarrow{-8} \frac{38}{(5)} \xrightarrow{6} \frac{578}{(7)} \xrightarrow{-5} 259 \Rightarrow d_{AB} = 259. \quad (2.35)$$

В силу комутативності CSIDH $d_{BA} = d_{AB}$. І відомих секреті ключи Аліси і Боба та їх суму $\Omega_A + \Omega_B = (-1,1,3)$, легко перевірити цей результат відповідно до алгоритму $E_d^{(0)} * \Theta_A * \Theta_B = E_{144} * [3^{-1}, 5,\ 7^3]$

$$\frac{d_0 = 144}{(7)} \xrightarrow{3} \frac{180}{(5)} \xrightarrow{1} \frac{752}{(3)} \xrightarrow{-1} 259 \Rightarrow d_{AB} = 259. \quad (2.36)$$

Щоб уникнути неоднозначності при отриманні ізоморфних кривих за розділений секрет, приймається J-інваріант (5) $J(d_{AB}) = 725$ кривої E_{259}. Так на рис. 2.11 і 2.12 зображено ланцюги ізогеній від кривої з $d = 144$ до $d = 286$, а на рис. 2.13 – з $d = 514$ до $d = 259$.

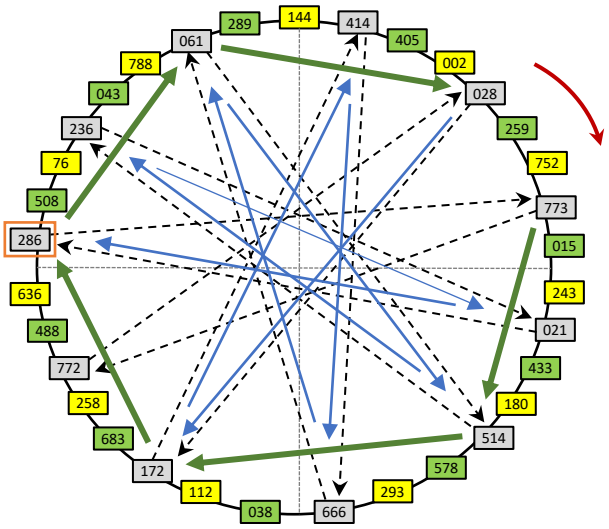

Рис. 2.11 Шлях за (2.28) від кривої $d = 144 \to d = 286$

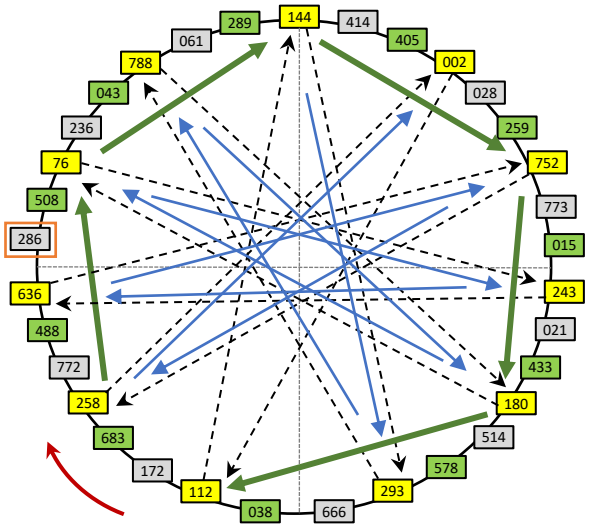

Рис. 2.12. Другій шлях за (2.29) від кривої $d = 144 \to d = 286$

На рис. 2.11 і 2.12 показано графічне уявлення на графі двох шляхів перетворення A кривих $d = 144 \to 286$ (перетворення сторони A). Перетворення сторони B легко знайти по таблицях, воно має вигляд $d = 144 \to 514$. Тепер якщо після перетворення до кривої 514 застосувати перетворення A отримаємо $d = 514 \to 259$.

На рис. 2.11–2.13 червоним кольором показані ціпочки 3-ізогеній, зеленим – 5-ізогеній та синім – 7-ізогеній.

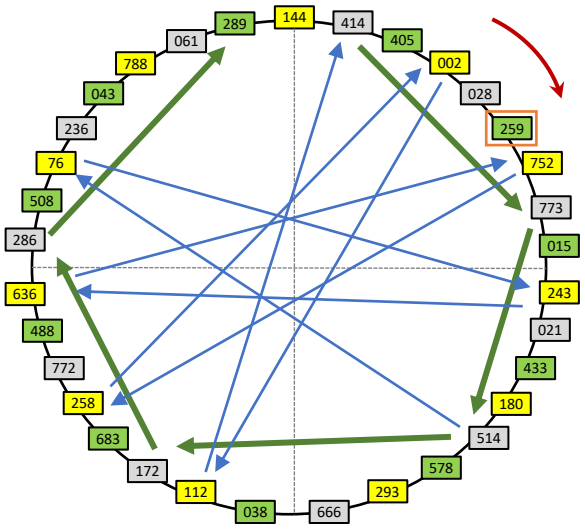

Рис. 2.13. Ланцюжок ізогеній за (2.34) від кривої $d = 514 \rightarrow d = 259$

Можна зробити висновок, що метод обчислення ізогеній непарних ступенів у координатах, запропонований в [35], з використанням повних і скручених СКЕ, дозволяє реалізувати найбільш швидкі на сьогодні обчислення при побудові PQC алгоритму CSIDH і подібних. Доведені у роботі [51] теореми відкривають їх імплементації класи скручених і квадратичних кривих Едвардса. Найбільші обчислювальні витрати в алгоритмі CSIDH пов'язані зі скалярним множенням SM випадкових точок, які потребують швидше експериментальної оцінки. Багато наукових праць сьогодні присвячено темі CT CSIDH [62, 65–67] та пропонують різні алгоритми захисту від атак сторонніми каналами.

Висновки до розділу 2

1. Нециклічні криві Едвардса, завдяки їх перевагами перед повними СКЕ, можна ефективно використовувати для створення алгоритмів лінійки CSIDH. Доопрацьовано метод реконструкції точок експоненціювання еліптичної кривої. Розглянуті властивості, які дозволяють знайти всі точки kP всіх груп кривої за значенням ⅛ частини точок лише однієї групи (колеса). При відомому порядку групи кожному коефіцієнту експоненціювання k відповідає свій порядок точки, який не залежить від координат точки а тільки від порядку групи і k. На ґрунті цих

властивостей створено метод побудови шаблону для швидкого експоненціювання точок. Шаблон можна використовувати для реконструювань і експоненціювання точки та обчислення їх порядку, наприклад при моделюванні алгоритмів.

2. Для ідентифікації кривої Едвардса зручно використовувати її параметр d. Якщо крива Едвардса має параметри a і d, то для знаходження ізогенії порядку l з параметрами a' і d' слід використовувати запропоновані співвідношення. Якщо загальний від функції Едвардса відомий, то більше нічого знати не потрібно і можна відмовитись від обчислення ізогенної функції.

3. У розділі наведено обґрунтування вибору нециклічних класів квадратичних та скручених СКЕ, визначених як пара квадратичного кручення над простим полем F_p. Їх перевагами перед класом повних СКЕ є розширення вдвічі множини всіх кривих, виключення трудомісткої операції мультиплікативної інверсії $d^1 = d^{-1}$ параметра d при переході до кривих квадратичного кручення. Парціальна оцінка виграшу складає $\gamma_1\gamma_2 = 2^5$ у швидкості обчислення в CSIDH на нециклічних СКЕ у порівнянні з повними СКЕ.

4. Обчислення ізогенних кривих з від'ємними показниками e_i, заданими секретним ключем Ω, в порівняно з відомими реалізаціями CSIDH на повних кривих Едвардса не вимагають ресурсномісткої інверсії параметра d при переході до квадратичного кручення.

5. Наведено модифікацію методу CSIDH, що використовує ізогенії нециклічних кривих замість повних кривих у формі Едвардса, тому наступні модернізації алгоритму CSIDH виконуються на нециклічних кривих Едвардса.

РОЗДІЛ 3
МОДЕЛЬ ІНКАПСУЛЯЦІЇ КЛЮЧА CSIKE З РАНДОМІЗАЦІЄЮ

У попередніх розділах показано позитивні якості нециклічних СКЕ. Ці якості роблять такі криві першими претендентами на використання в криптосистемах типу Діффі-Геллмана. Насамперед це рекордно малі розміри ключів. Швидкодія вже досить велика, але ще є резерви.

Дослідження таких систем постійно дає нові можливості для їх удосконалення. У даному розділі розглядаються такі варіанти вдосконалення як рандомізація алгоритму [55], оптимізація ступенів ізогеній [68], алгоритм інкапсуляції ключа [68, 69], використання ізогеній нециклічних НКЕ [48, 69].

Ці модернізації підвищують швидкодію алгоритму CSIDH і покращують інші його характеристики, роблячи його все більш конкурентоспроможним.

3.1. Рандомізація алгоритму CSIDH на нециклічних кривих Едвардса

Відомою проблемою [10] алгоритму CSIDH є вразливість до атаки сторонніми каналами, заснованої на непрямому вимірі часу виконання окремих операцій обчислення ізогеній кожного ступеня l_k, пропорційного секретній експоненті e_k ключа. Непряме вимірювання це, наприклад, вимірювання електроспоживання, електро-магнітного випромінювання і т. ін. У статтях [62] і [65] вирішення цієї проблеми пропонується шляхом нарощування експонент e_k фіктивними до відомого максимуму (метод CT CSIDH). Зрозуміло, що така надмірність обчислень знижує швидкість виконання алгоритму.

Для вирішення цієї проблеми пропонується метод рандомізації та відповідний рандомізований алгоритм CSIDH на нециклічних кривих Едвардса [55]. Як основа для модернізації пропонується найбільш ефективна технологія на квадратичних і скручених СКЕ, пов’язаних як пари квадратичного кручення.

В оригінальному алгоритмі шлях у графі ізогеній складається з ланцюжків на окремих ізогеніях. У наслідок комутативності групової операції при рандомізації

окремі ланцюжки перемішуються, виникає багато шляхів на графі, серед яких обирається випадковий шлях. Це створює керований хаос і значно ускладнює роботу криптоаналітика.

При складанні випадкового шляху здійснюється рівноймовірний відбір кривої з двох класів на кожному кроці ланцюжка ізогеній. У цьому методі також запропоновано відмовитися від обчислення ізогенної функції $\varphi(R)$ випадкової точки R, що суттєво прискорює алгоритм і призводить до неминучого зростання ймовірності помилки аналітика, єдина помилка, якого на довгому шляху аналізу, повністю зриває атаку.

3.1.1. Алгоритм CSIDH з рандомізацією

Ідея рандомізації полягає в тому [55], що будь-яка випадкова координата x еліптичної кривої завжди породжує випадкову точку $P = (x, y)$ однієї з двох кривих пари квадратичного кручення. Тоді замість спроб (безуспішних із ймовірністю 1/2) знайти точку кривої заданого класу та успіхом із ймовірністю 1 ми визначаємо клас кривої (у нашому випадку це крива E_d або $E_{-1,-d}$, однією з яких належить точка $P = (x, y)$. Далі в даному класі обчислюється перша ізогенна крива $E^{(1)} = [l_k] * E^{(0)}$ ступеня ізогенії l_k, що відповідає знаку експоненти e_k. Далі вибирається наступна l_k, а значення $|e_k|$ знижується на 1.

На наступному кроці з новим значенням параметра $d^{(1)}$ знову визначається випадкова точка $P = (x, y)$ однієї з кривих E_d або $E_{-1,-d}$, визначається ядро ізогенії випадково обраного ступеня l_k, і обчислюється параметр $d^{(2)}$ ланцюжка. Процес продовжується до обнуління всіх e_k.

Відповідний рандомізований алгоритм CSIDH на кривих пари квадратичного кручення наведено нижче [55].

Алгоритм 3.1. Реалізація групової операції на квадратичних та скручених суперсингулярних кривих Едвардса з рандомізацією [47]

Input: $d_A \in E_A, \chi(d) = 1$ *and a list of integers* $\Omega_A = (e_1, e_2, \dots e_K)$.

Output: d_B *such that* $\left[l_1^{e_1}, l_2^{e_2}, \dots, l_K^{e_K}\right] * E_A = E_B$, *where* $E_{A,B}: x^2 + y^2 = 1 + d_{\mathrm{A,B}} x^2 y^2$,

1. *Let* $S_0 = \{k | e_k > 0\}$, $S_1 = \{k | e_k < 0\}$, $n_0 = \prod_{k \in S_0} l_k$, $n_1 = \prod_{k \in S_1} l_k$

2. While *some* $e_k \neq 0$ **do**

3. *Sample a random* $x \in F_p$,

4. Set $a \leftarrow 1,\ s \leftarrow 0$, E_A: $x^2 + y^2 = 1 + d_A x^2 y^2$ **If** $\chi((x^2 - 1)/(dx^2 - 1) = 1$,

5. Else $a \leftarrow -1,\ s \leftarrow 1$ E_A: $x^2 - y^2 = 1 - d_A x^2 y^2$,

6. *Compute* y -coordinate of the point $P = (x, y) \in E_A$

7. *Compute* $R \leftarrow \left[\frac{p+1}{2n_s}\right] P$,

8. *Sample a random* $l_k | k \in S_s$,

9. *Compute* $Q \leftarrow \left[\frac{n_s}{l_k}\right] R$

10. If $Q \neq (1,0)$ *compute kernel* G *of* l_k*-isogeny* $\phi: E_A \rightarrow E_B$,

11. Else start over to line 3,

12. *Compute* d_B *of curve* E_B, $d_A \leftarrow d_B$,$e_k \leftarrow e_k - s$ **,**

13. *Skip* k *in* V_s *and* set $n_s \leftarrow \left(\frac{n_s}{l_k}\right)$ **If** $e_k = 0$,

14. Return d_{A}**.**

Цей алгоритм має дві важливі відмінності від оригінального алгоритму CSIDH.

По-перше, ми не розбиваємо обчислення ізогеній на два етапи з кривими одного класу, потім іншого ($a \leftarrow -a$), а будуємо випадкову послідовність $\{s\}$ з рівноймовірним вибором кривих E_d або $E_{-1,-d}$, на кожному кроці. Разом із прискоренням удвічі процедури відбору кривих це позбавляє аналітика можливості впорядкованої побудови підмножин V_0 і V_1 ступенів ізогеній. Крім того, для кожної складової $[l_k^{e_k}]$ функції Θ ланцюжок ізогеній завдовжки $|e_k|$ розбивається на фрагменти загального ланцюжка, що вставляються у випадковий час. Це неминуче ускладнює завдання вимірювання часу обчислень відповідно до функції $[l_k^{e_k}]$.

По-друге, в (п. 12) ми відмовляємося від обчислення ізогенної функції $\varphi(R)$, що також значно прискорює алгоритм. Кінцевою метою алгоритму поділу секретів

CSIDH є знаходження загального параметра d_{AB} кривой E_{AB}. Для кожного кроку в ланцюжку ізогеній $E \to E'$ необхідним є лише розрахунок параметра $d' = \psi(d, Q)$ на основі параметрів d і ядра $< Q >$ домену E. Цей розрахунок вимагає два скалярні множення SM випадкових точок R непарного порядку n_s і $(l_k - 1)/2$ рекурентних подвоєння точок з $< Q >$.

Таким чином, побудова та обчислення досить складної функції $\varphi(R)$ не є необхідним для реалізації алгоритму CSIDH. У той час як порядок точки R завжди містить помножувач l_k, порядок її образу $\varphi(R)$ такого помножувача не має, і точка $\varphi(R) \in \mathrm{E}'$ марна для знаходження ядра кривої E'. Вона використовується лише в кінці ланцюжка ізогеній при $R = Q, \varphi(Q) = (1,0)$, проте ця відома властивість не вимагає перевірки. Частина обчислень в оригінальному алгоритмі, пов'язаних з розрахунком функції $\varphi(R)$, можна заощадити.

У цьому алгоритмі по зрівнянню з оригіналом замість однієї множини S формується дві множини S_0 і S_1, які записуються номери ступенів ізогеній, що відповідають позиціям ключа Ω_A з позитивними і негативними експонентами e_k, відповідно. За будь-якого випадкового вибору x-координати отримуємо випадкову точку $P = (x, y)$, що належить перший чи другій кривій крученої пари. Множення на 4 у п.7 дає точку R непарного порядку. Скалярне множення у п. 9 обчислює точку Q ядра ізогенії, далі розраховуються координати всіх точок ядра G. Нарешті, в п. 12 згідно (2.19) обчислюється параметр d' ізогенної кривої E'.

Дві підмножини на початку алгоритму $S_\lambda, \lambda = 0,1$, с номерами ступенів l_k, разом з двома факторами n_0 і n_1 числа $n = n_0 n_1$ (індекс $\lambda = 0$ ($e_k > 0$) відповідає вибору квадратичного СКЕ, а $\lambda = 1$ – скрученої СКЕ ($e_k < 0$)). Так як порядок кривої $p + 1 = 8n$, то в п. 7 алгоритму для кривої E_d обчислюється точка $R = 4n_1 P$ непарного порядку n_0, а для кривої $E_{-1,-d}$ – точка $R = 4n_0 P$ непарного порядку n_1. Це мінімізує вартість наступного точкового добутку, який визначає точку Q ядра ізогенії степені l_k (п. 9). Далі, в пункті 10 алгоритму, методом подвоєння точок обчислюються: $s = (l_k - 1)/2$ x-координат точек ядра G. Оцінки вартості цих обчислень у $(W:Z)$ координатах дано у [53].

В п. 7 Алгоритму 3.1 подвоєння випадкової точки P відразу дозволяє позбутися від точок парного порядку (в їх числі – особливі точки 2-го і 4-го порядку) і далі йдуть розрахунки скалярних добутків у підгрупах точок непарного порядку кривої. Їх задача – знайти $\frac{(l_k-1)}{2}$ x-координат α_i точок ядра G простого порядку l_k. В результаті по формулі (2.21) розраховується параметр d' l_k-ізогенної квадратичної СКЕ. При цьому параметри скрученої СКЕ мають вигляд $\mathrm{a}' = -1, d' \to -d'$.

Принциповим є то, що в CSIDH NCE реалізується побудова ланцюгів ізогенних кривих як абелеві групи, а не ізогенні функції $\varphi(R)$ випадкової точки R. Трудомісткі розрахунки останніх [53] є зайві.

Це є додатковий захист до того, що у класичному CSIDH вже є гарантований рівень захисту від описаного вище типу атаки сторонніми каналами. Він визначається знаком секретної експоненти e_k ключа. Так як для кожної складової $[l_k]$ функції Θ час обчислення $[l_k^{+1}]$ і $[l_k^{-1}]$ однаково, Імовірність успіху аналітика навіть в умовах безпомилково знайдених значеннях l_k дорівнює $2^{-K} = 2^{-74}$ (для даних роботи [10]). А лише одна помилка аналітика руйнує всю його трудомістку роботу.

При середній довжині $\frac{m+1}{2} = 3$ ланцюжка ізогеній кожного ступеню l_k загальна довжина ізогенного ланцюга функції Θ складає $3 * 74 = 222$ кроку. Нехай p_1 імовірність безпомилкового визначення ступеня l_k аналітиком на одному кроці рандомізованого алгоритму CSIDH, то ймовірність його успіху може бути оцінена за значенням $2^{-74}{p_1}^{222}, p_1, < 1$. Наприклад, при $p_1 = \frac{1}{2}$ ймовірність успішності аналітика дорівнює 2^{-296}, а при $p_1 = \frac{3}{4}$ ця ймовірність близька к величині 2^{-165}. Це значно нижче рівня безпеки 2^{-128}

Можливі різні модифікації пропонованого методу рандомізації зі вставками одиночних фіктивних експонентів у вибіркові складові $[l_k]$ функції Θ, що не внесе надмірності у обчислення.

Алгоритм не включає обчислення ізогенної функції $\phi(x, y)$, що дає оцінку виграшу у швидкодії алгоритму 2 $\gamma_3 = 2{,}235$. Наступний виграш $\gamma_4 = 2$ метод Рандомізація забезпечує те, що з ймовірністю ½ в алгоритмі будь-який вибір попадає на одну з кривих. Приблизний виграш складає $\gamma_5 = 2$ у порівнянні з CT CSIDH, в якому близько половини ізогеній є фіктивними [55].

3.1.2. Модель шляхів на графі ізогеній

Повернімося до моделі, розглянутої у п. 2.3.5. табл. 2.7–2.10.

Комутативність групової функції $\Theta_A = [l_1^{e_1}, l_2^{e_2}, \dots, l_K^{e_K}]$ дозволяє досягати кінцевої кривої декількома шляхами. Це досягається перестановкою як ізогеній, та кроків по цих ізогеніях.

Приймемо секретні ключі експонент ізогеній $\{e_i\}$ Аліси та Боба $\Omega_A = (7, -5, 8)$, $\Omega_B = (-8,\ 6, -5)$, їх функції класу групових операцій, відповідно, $\Theta_A = [3^7, 5^{-5}, 7^8]$, $\Theta_B = [3^{-8}, 5^6, 7^{-5}]$. Обчислимо їх відкриті ключі d_A, d_B. Як стартову криву у ланцюжку ізогеній приймемо криву ${E_d}^{(0)} = E_{144}$. Тоді $E_A = E_0 * \Theta_A$, $E_B = E_0 * \Theta_B$. Тоді можемо побудувати декілька шляхів до відкритих ключів, три з яких показані у (2.28), (2.29) і (2.30) [70, 71].

3.1.3. Модель створення випадкових шляхів на графі ізогеній

Нагадаємо, що в алгоритмі крок по ізогенії K визначається як $[l_k]$, шлях визначається секретним ключом $\Omega_A = (e_1, e_2, \dots, e_K)$ і зберігається у вигляді $\theta = \left[l_1^{e_1}, l_2^{e_2}, l_i^{e_i}, \dots, l_K^{e_K}\right]$, тобто e_i кроків по кожної ізогенії l_i, де K – кількість ізогеній, e_K – кількість кроків у ланцюжку ізогенії l_i. В алгоритмі CSIDH може бути до сотні ізогеній і десятки значеній експонент e_K. Це впливає на кількість шляхів на графі ізогеній і важливим є контролювати щоб не повторювати ці шляхи.

Для ілюстрації методу рандомізації розглянемо модель з урахуванням даних табл. 2.8–2.10. Наведемо приклад обчислення Аліси свого відкритого ключа за допомогою секретного ключа $\Omega_A = (7, -5, 8)$. В послідовності ізогеній нехай символ $s = 0$ відповідає випадковому вибору кривої E_d, а символ $s = 1$ – вибору $E_{-1,-d}$. У досить довгій послідовності $\{s\}$ ці символи вважатимуться рівноймовірними. У нашому прикладі довжина ланцюжка ізогеній дорівнює $7 + 5 + 8 = 20$, тоді можна змоделювати псевдовипадкову послідовність $\Lambda = 00101001000101000000$ довжини 20 ізогенних кривих на шляху обчислення відкритого ключа Аліси. Виходячи, як і в попередньому розділі, із стартової кривої E_{144}, ми користуємося даними табл. 2.7–2.10 для серій символів 0 послідовності Λ, і даними таблиці 3 – для серій символів 1 У першому випадку рядками таблиць ми рухаємося вправо, у другому – вліво. Число кроків визначається довжиною серії однакових символів у Λ та записано зі знаками експонент над стрілками ізогенних переходів нижче. Таким чином, на шляху Λ за 20 кроків Аліса обчислює

$$\frac{d_0 = 144}{(3)} \xrightarrow{2} \frac{405}{(5)} \xrightarrow{-1} \frac{15}{(7)} \xrightarrow{1} \frac{488}{(5)} \xrightarrow{-1} \frac{43}{(7)} \xrightarrow{2} \frac{508}{(5)} \xrightarrow{-1} \frac{289}{(3)} \xrightarrow{2} \frac{43}{(7)} \xrightarrow{3} \frac{405}{(5)} \xrightarrow{-1} \frac{15}{(3)} \xrightarrow{1} \frac{243}{(5)} \xrightarrow{-1} \frac{293}{(7)} \xrightarrow{5} \frac{636}{(3)} \xrightarrow{1} 286 \Rightarrow d_A = 286. \quad (3.1)$$

Цей результат співпадає з результатом попереднього розділу. Рандомізація вибору кривих, по суті, випадково дробить експоненти ключа Ω_A і вносить значну невизначеність у завдання аналітика.

При використанні псевдовипадкової послідовності Λ виникають деякі питання. При виборі елемента 0 виникає невизначеність, яку таблицю (з табл. 2.7–2.10) використовувати. Замість послідовності Λ зручніше використовувати наступну послідовність S.

Склад послідовності S це однократні кроки з вказівкою конкретних ізогеній, які задаються секретним ключем θ. Шлях θ складається з ланцюжків $\left[l_i^{e_i}\right]$ довжино. e_i ізогеній порядку l_i:

$$\theta = [l_1^{e_1}] \, U \, [l_2^{e_2}] \, U \, [l_i^{e_i}] \, U \, \left[l_K^{e_K}\right]. \quad (3.2)$$

Кожний ланцюжок $l_i^{e_i}$ можна представити як кількість e_i однократних кроків по ізогенії l_i:

$$\left[l_K^{e_K}\right] = \left[l_K^1, l_K^i, \dots, l_K^{R_K}\right], \tag{3.3}$$

де i – номер кроку, всього кроків $R_K = |e_K|$.

Якщо $e_K < 0$ то усі $l_K^i < 0$ і крок виконується по відповідній скрученій кривій.

Для зручності обробки шляхів пропонується записувати шлях у вигляді множини S однократних кроків s_i по всім ізогеніям l_i: елементи множини $S = \{l_1, l_2, \dots, l_R\}$ розташовані у випадковому порядку, де R – кількість однократних кроків у шляху:

$$R = |e_1| + |e_2| + \cdots + |e_K|. \tag{3.4}$$

S представляє собою послідовність номерів ізогеній l_i по яким здійснюються однократні крокі. Розташування елементів в S є випадковим і визначається наступним образом:

Обираємо чергову ізогенію l_i і $|e_i|$ разів вставляємо число (i) зі знаком e_i в множину S на місця, які визначаються генератором випадкових чисел.

При виконанні операції θ однократні кроки виконуються у порядку який визначає множина S.

Одна з можливих випадкова послідовність для попереднього прикладу має вигляд:

$$S = \{3,3,-5,7,-5,7,7,-5,3,3,7,7,7,-5,3,-5,3,-5,7,7,7,7,7,3\}. \tag{3.5}$$

Елементи послідовності можна переставляти від цього результат не змінюється.

Головною перевагою класів B і C кривих Едвардса перед повними є подвоєння числа кривих в алгоритмі з приростом безпеки. Крім того, не потрібно трудомісткої інверсії параметра $d \to d^{-1}$, необхідної під час переходу до повної кривої квадратичного кручення. Це також прискорює виконання алгоритму.

Можна зробити висновок, що запропонований у цій роботі метод рандомізації алгоритму CSIDH на квадратичних та скручених СКЕ забезпечує ефективну та безпечну альтернативу різним варіантам СТ CSIDH [47].

3.2. Алгоритм CSIKE на нециклічних кривих Едвардса

Класичний не інтерактивний алгоритм Діффі-Геллмана базується на використанні двох відкритих ключів. Те ж завдання формування загального секрету може бути вирішено в протоколі з одним сеансом передачі та одним відкритим ключем одержувача, що безпечніше [34]. Ми пропонуємо оригінальну модифікацію алгоритму CSIDH – алгоритм CSIKE. Він досить далекий від відомого прототипу SIKE [68] і, у свою чергу, відкритий для модифікації. У статті наведено ілюстрацію його роботи на простій моделі. Найбільш важлива перевага CSIKE – використання одного відкритого ключа замість двох.

3.2.1. Схема інкапсуляції ключа

Пропонується [63, 68, 69] алгоритм CSIKE як модифікацію CSIDH, замінюючи секретний ключ Аліси секретним вектором Ω_K, за допомогою якого вона обчислює ключову криву $E_K = \Theta_K * E_0$ та загальний секретний ключ $d_K = K$. Далі Аліса шифрує його відкритим ключем Боба E_B і обчислює криву $E_{KB} = \Theta_K * E_B = \Theta_K * \Theta_B * E_0$. Боб при деінкапсуляції знімає свій шифр за допомогою мультиплікативної зворотної функції $\overline{\Theta_B}$ (такої що $\Theta_B * \overline{\Theta_B} = I$), тим самим він реставрує криву $E_K = \Theta_K * E_0$. Як ключ інкапсуляції обома сторонами можна взяти J-інваріант кривої E_K.

В [37] і [69] пропонується алгоритм як модифікація CSIDH на НКЕ є алгоритмом інкапсуляції ключа K як загального секрету Аліси та Боба, який складається з трьох частин:

1. Генерація секретного ключа K. Аліса за допомогою датчика випадкових чисел знаходить секретний вектор інкапсуляції $\Omega_K = (e_1, e_2, .., e_K)$, будує функцію класу групової дії $\Theta_K = \left[l_1^{e_1}, l_2^{e_2}, \dots, l_K^{e_K}\right]$ і обчислює ізогенну криву $E_K = \Theta_K * E_0$, параметр d_K якої приймає як секретний ключ $d_K = K$.

2. Інкапсуляція ключа. Це процедура шифрування Алісою ключа K відкритим ключем Боба E_B. Для цього Аліса обчислює ізогенну криву $\Theta_K * E_B = E_{KB}$. Параметр d_{KB} цією кривою вирушає Бобу.

3. Декапсуляція ключа. Дешифрування Бобом кривої E_{KB} своїм секретним ключем Ω_B зводиться до обчислення ним ізогенної кривої $\overline{\Theta_B} * E_{KB} = E_K$, де відображення $\overline{\Theta_B}$ (таке що $\Theta_\text{B} * \overline{\Theta_\text{B}} = I$) будується інверсією всіх знаків експонент секретного ключа Боба: $\Omega_B \to (-\Omega_B)$ [34].

Таким чином, Аліса та Боб мають спільний секрет K замість розділеного секрету d_{AB} в CSIDH. Зазвичай ці параметри замінюються J-інваріантом, однаковим для ізоморфних кривих. Секретний і відкритий ключі Аліси в цій версії CSIKE поки що не беруть участь.

На рис 3.1 зображено схему алгоритму CSIDH з інкапсуляцією ключа.

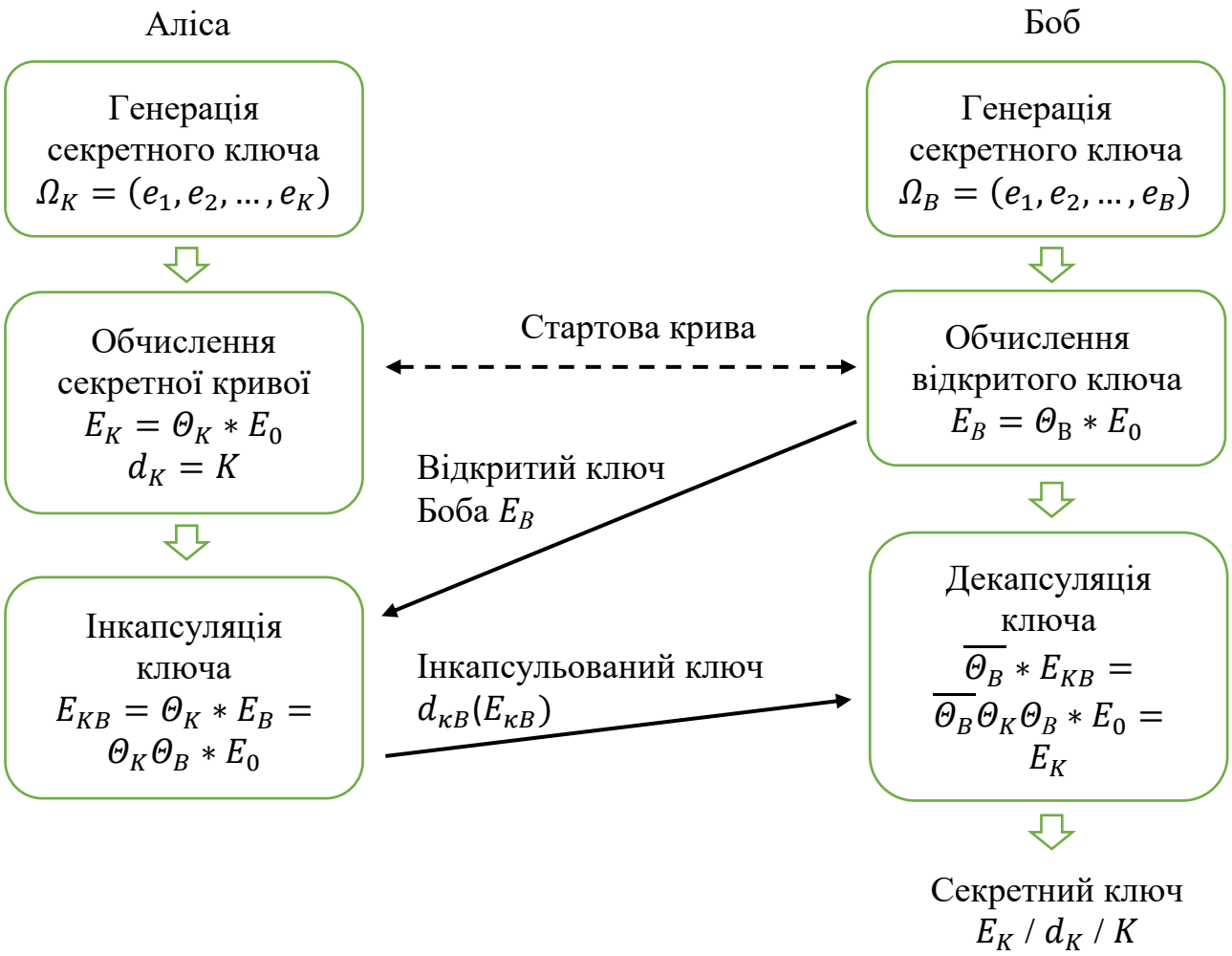

Рис. 3.1. Схема алгоритму інкапсуляції ключа

У аналітика відсутня будь-яка інформація про ключ κ для організації атаки, що неминуче підвищує безпеку алгоритму. У роботі [63] наведено два приклади роботи 4-х ізогенної моделі CSIKE при класичній та рандомізований імплементації. Також наведено приклад 2 обчислення Аліси та Боба з метою автентифікації Аліси.

Стартова крива E_0 може бути відкритою, або стати додатковим секретним параметром двох сторін, яку одноразово можна обирати з відомого масиву або обчислювати згідно секретної функції Θ_s. Це нарощує рівень безпеки алгоритму [34].

3.2.2. Моделювання алгоритму CSIKE

Продовжимо розгляд моделі (п. 2.3.5.) для імплементації алгоритму CSIKE на квадратичних і скручених СКЕ, що утворюють пари квадратичного кручення кривих з порядком 840 [69]. В табл. 2.7 наведено значення параметру d для пар квадратичних E_d і скручених $E_{-1,-d}$ СКЕ. В табл. 2.8–2.10 наведено результати розрахунків параметрів $d^{(i)}$ ланцюжків відповідно 3-, 5- і 7-ізогеній квадратичних СКЕ.

Нехай Аліса згенерувала секретний вектор $\Omega_K = (7, -5, 8)$, який ізогенним відображенням $\Theta_K = [3^7, 5^{-5}, 7^8]$ вона на першому етапі трансформує у загальний секретний ключ κ, тобто обчислює криву $E_K = \Theta_K * E_0$.

Далі на другому етапі вона шифрує цей ключ відкритим ключем Боба d_B. Приймемо секрет Боба $\Omega_B = (-8{,}6, -5)$, відповідно, його функція класу групової дії $\Theta_B = [3^{-8}, 5^6, 7^{-5}]$. Виконаємо їх обчислення ключів K, d_B. Як стартовий кривий ланцюжок ізогеній приймемо криву ${E_d}^{(0)} = E_{144}$. Тоді $E_K = E_0 * \Theta_K, E_B = E_0 * \Theta_B$.

З метою спрощення запису в алгоритмі обчислення ізогенної кривої $E_K = E_0 * \Theta_K$ ми користуватимемося параметрами $d^{(i)}$, які повністю визначають криві ${E_d}^{(i)}(e_K > 0)$ і ${E_{-1,-d}}^{(i)}(e_K < 0)$ як пари квадратичного кручення. У ланцюжку параметрів $d^{(i)}$ знизу ми записуємо в дужках ступінь ізогенії, над стрілкою число кроків зі знаком експоненти e_K. Наприклад, згідно з функцією $\Theta_K = [3^7, 5^{-5}, 7^8]$ і

кривой $E_d{}^{(0)} = E_{144}$, не вдаючись до методу рандомізації (розділ 3.1), Аліса обчислює ланцюжок (2.29).

Отже, загальний секретний ключ $K = 286$. Аналогічно Боб обчислює свій відкритий ключ на основі кривої E_{144} та функції $\Theta_B = [3^{-8}, 5^6, 7^{-5}]$ за (2.31) і (2.32).

Таким чином, відкритий ключ Боба $d_\text{B} = 514$. Далі на другому етапі інкапсуляції Аліса шифрує відкритим ключом Боба секретний ключ $K = 286$ та обчислює $E_{BK} = E_\text{B} * \Theta_K$ за (2.33). Нарешті, на третьому етапі декапсуляції Боб із кривою $d_{BK} = 259$ знімає свій секретний ключ за допомогою зворотної функції $\overline{\Theta_B} = [3^8, 5^{-6}, 7^5]$

$$\frac{d_0 = 259}{(7)} \xrightarrow{5} \frac{578}{(5)} \xrightarrow{-6} \frac{38}{(3)} \xrightarrow{8} 286 \Rightarrow d_K = 286. \tag{3.6}$$

У результаті він отримує загальний секретний ключ $K = 286$, розрахований йому Алісою. Щоб уникнути неоднозначності при отриманні ізоморфних кривих за ключ інкапсуляції, обома сторонами приймається J-інваріант (6) $J(d_K) = 525$ кривої E_{286}.

Наведений приклад дає лаконічну ілюстрацію роботи алгоритму CSIKE. Його ефективність значно зростає після використання методу рандомізації.

Наприклад, обчислення Алісою ключа інкапсуляції K на основі секретного вектора $\Omega_K = (7, -5, 8)$ можна реалізувати псевдовипадковим ланцюжком ізогенних кривих за 20 кроків

$$\begin{gathered}\frac{d_0 = 144}{(3)} \xrightarrow{2} \frac{405}{(5)} \xrightarrow{-1} \frac{15}{(7)} \xrightarrow{1} \frac{488}{(5)} \xrightarrow{-1} \frac{43}{(7)} \xrightarrow{2} \frac{508}{(5)} \xrightarrow{-1} \frac{289}{(3)} \xrightarrow{2} \frac{43}{(7)} \xrightarrow{3} \\ \frac{405}{(5)} \xrightarrow{-1} \frac{15}{(3)} \xrightarrow{1} \frac{243}{(5)} \xrightarrow{-1} \frac{293}{(7)} \xrightarrow{2} \frac{636}{(3)} \xrightarrow{1} 286 \Rightarrow d_K = K = 286.\end{gathered} \tag{3.7}$$

Цей результат, зрозуміло, збігається з першим результатом вище [34, 69].

3.2.3. Паралельні обчислення

У табл. 2.7 представлено параметри d 3-ізогеній, рівно половина параметрів d позначені зірочками. Ці 33 параметра входять у ланцюжок з періодом $T = 33$ та

утворюють множину параметрів d^* першої криптосистеми зі стартовою кривою E_{144} (або будь-якої іншої кривої цієї множини d^*). У нашому прикладі всі ізогенні криві належать цій множині. Не помічені в таблиці параметри утворюють другу множину 33-х параметрів ізоморфних кривих з параметром d^{-1}, на яких можна побудувати незалежну від першої другу криптосистему з можливістю паралельних обчислень.

Наприклад, від стартової кривої з $d^* = 144$ інверсією параметра приходимо до ізоморфної кривої E_{705} другої криптосистеми (див. табл. 2.7). Далі, задаючи різні секрети Ω_{K1} і Ω_{K2} у двох криптосистемах, можна вдвічі наростити довжину ключа (скажімо, 512 → 1024 біт). Паралельні обчислення, крім того, роблять безнадійною атаку сторонніми каналами. Зауважимо також, що така можливість виникає при використанні лише класів нециклічних кривих Едвардса.

Можна зробити висновок, що запропонований алгоритм CSIKE та модифікації алгоритму CSIDH на квадратичних та скручених СКЕ забезпечує ефективну та безпечну альтернативу різним варіантам СТ CSIDH з нижньою оцінкою виграшу у швидкості обчислень до $1{,}5 \cdot 2^9$ [37, 47].

3.3. Оптимізація структури ізогеній в CSIDH

У цьому розділі ми покращуємо структуру степенів ізогеній $\{l_k\}$ та оцінюємо виграш γ_7 від такого покращення у порівнянні з моделлю CSIDH [10].

У роботі [10] показано, що 74 степені l_k ізогеній зі значенням $l_{\max} = 587$ пробігають лише частина (74 числа) всіх мінімальних простих чисел від 3 до 587, повне число яких дорівнює 106. 32 значення простих чисел не входить до списку ступенів l_k в моделі, що означає що є розриви (перепустки) у множині $\{l_k\}$. На обробку ізогеній високих ступенів потрібно більше ресурсів ніж на обробку малих. Тому пропускати і не використовувати ізогенії малих ступенів не вигідно.

При середній ціні кожного ступеня 8 біт груба оцінка вартості віддалених ступенів становить $32 \cdot 8 = 256$ біт. Ці біти зайві і породжують уповільнення роботи алгоритму при надмірно високих ступенях ізогеній.

Тому є актуальним завдання проаналізувати можливі розподіли множин простих чисел множини $L = \{l_k\}^K$ розміру K і знайти варіанти оптимізації (ущільнення) цього розподілу для досягнення максимальної швидкодії алгоритму.

Множина простих чисел $L = \{l_k\}^N = \{3,5,7,\ldots,587\}$ містить $N = 106$ прості числа. В алгоритмі [10] використовуються 74 числа, решта 32 не найбільших числа не використовуються, що є недоліком.

Назвемо впорядковане за зростанням множину простих чисел $\{l_k\}^K$ *оптимальним*, якщо за відомих $l_{\min} = l_m$ і K добуток $\prod_{k=m}^{K+m-1} l_k = \max$. З визначення випливає, що оптимальна кількість простих чисел є щільною (без перепусток) з елементами $\{l_m, l_{m+1}, \ldots, l_{K+m-1}\} \in L$. Воно будується як сегмент довжини K упорядкованих простих чисел. Видалення із середини сегмента хоча б одного числа (крім крайніх) дає не оптимальну множину $\{l_k\}^K \notin L$. Видалення одного із крайніх чисел l_m, $l_{\max}$ сегмента дає дві різні оптимальні множини розміру $K - 1$. Будь-яке підмножина (сегмент довжини K) повної множини L є оптимальною множиною. Не оптимальна множина містить перепустки, що порушують умову $\prod_{k=m}^{K+m-1} l_k = \max$.

Повна множина $L = \{l_k\}^{106} = \{3,5,7, \ldots, 587\}^{106}$ за визначенням оптимальне. Видалення з нього 32 чисел дає множину $\{l_k\}^{K=74}$, далеке від оптимального, але воно використовується в алгоритмі [10]. Поняття оптимальності ми пов'язуємо виключно з максимізацією добутку елементів множини.

Розіб'ємо L на підмножини $Lh = \{l_k\}^{K_h}, h = 1 \ldots 6$, включають прості числа у яких сотня дорівнює h. Для першої сотні, наприклад, маємо підмножину $L1 = \{3,5,7, \ldots, 97\}^{K_1}$, где $K_1 = 24$. Для всіх 6 підмножин Lh ці числа K_h дано у другому рядку табл. 3.1.

Таблиця 3.1

Розподіл числа K_h простих чисел у підмножинах Lh та їх добутків B_h в межах сотень з номерами h

h	1	2	3	4	5	6
K_h	24	21	16	16	17	12
B_h	119,795	151,245	127,623	135,192	149,782	109,134

Кожна степінь l_k у двійковій формі має $\log l_k$ біт для всіх добутків чисел l_k у підмножинах Lh розрахуємо бітову довжину $B_h = \sum_{l_k \in Lh} \log l_k$ ступенів ізогеній. Значення B_h наведено у 3-му рядку табл. 3.1. Ці результати дозволяють зробити такі висновки.

По-перше, сума всіх біт третього рядка $\sum_{h=0}^{6} B_h = 792{,}772 = 793$ біт, визначальний добуток усіх 106 простих чисел $\{3, \dots, 587\}$, має надмірність на 283 біти в порівнянні з мінімальним нижнім порогом 510 біт ($4n > 2^{512}$, $n > 2^{510}$) [10] вимоги безпеки.

По-друге, прості числа в 5-й та 6-й сотні ($L5$ та $L6$) можна видалити, оскільки $\sum_{h=1}^{4} B_h = 533{,}855 = 534$ біт, що задовольняє із запасом у 24 біта на вимогу $4n > 2^{512}$. Ігноруючи два останні стовпці табл. 3.1, отримуємо 77 значень елементів оптимальної множини $\{l_k\}^{K=77} = \{3, \dots, 397\}$ простих чисел. Далі, ми пропонуємо видалити в першій сотні 3 молодших ступеня $\{3,5,7\}$ і побудувати оптимальну множину ступенів ізогеній $Lopt = \{11,13, \dots, 397\}^{74}$ того ж розміру 74, що й у роботі [10]. Це зберігає довжину $K = 74$ секретного ключа. З урахуванням рівності $\log(3 \cdot 5 \cdot 7) = 6{,}714$, добуток n усіх l_k оптимальної множини $Lopt$ оцінюється двійковим числом завдовжки 528 біт. Додаючи два біти, отримуємо оцінку $logp = 530$ біт.

Для розподілу $Lopt$ можна скоригувати табл. 3.5: у стовпці $h = 1$ таблиці слід поставити значення $K_1 = 21, B_1 = 113{,}081$, а останні два стовпці таблиці видалити. Тоді $\sum_{h=1}^{4} K_h = 74, \sum_{h=1}^{4} B_h$ =527.141=528 біт, $\log p = 530$ біт. Такий оптимальний розподіл ступенів $\{l_k\}$ ізогеній забезпечує перевищення мінімального порога безпеки 512 біт алгоритму на 18 біт.

Резерв 18 біт можна витратити, видаливши дві максимальні ступені ізогеній 397 і 389 загальною вартістю 18 біт і приймаючи $l_{\max} = 383$. Однак це вимагає зниження довжини $K \leftarrow K - 2$ секретного ключа на 2.

Головною перевагою запропонованої множини ступенів ізогеній $Lopt$ відносно множини [10] є значне (в 1,5 рази) зниження $l_{\max} = 587$ до $l_{\max} = 397$ з оптимальним розподілом простих чисел.

Отже, лінійна оцінка виграшу у швидкості обчислень за рахунок оптимізації розподілу ступенів ізогеній дорівнює $\gamma_7 = 1{,}5$. Разом із сумарним виграшом попередніх розділів отримуємо прискорення алгоритму CSIDH $1{,}5 \cdot 2^9 \cong 770$ разів.

На основі табл. 3.5 можна оцінити інші оптимальні розподіли $\{l_k\}^K$, видаляючи молодші ступені l_k і зберігаючи K. Зрозуміло, що це лише збільшує рівень безпеки алгоритму та значення $l_{\max}$. Наприклад, приймемо $l_{\min} = 101$, тоді 24 ступеня першої сотні чисел треба замінити 17-ма числами 5-ї сотні та мінімальними 7-ма простими числами 6-ї сотні ($l_{\max} = 557$).

Отримуємо оптимальну множину $\{l_k\}^{74} = \{101{,}107{,}..{,}557\}$. Загальна сума $\log l_k$ цієї множини дорівнює 627,161, що з додаванням 2 біт дає оцінку $\log p = 630$ біт. Порівняно з першим розподілом довжина ключа $\log p$ збільшилася на 100 біт. Можна обміняти ці 100 біт на зниження $l_{\max}$, але вже за рахунок зниження значення K.

Важливим висновком ймовірнісного аналізу вдалого вибору випадкової точки є рекомендація уникати використання наймолодших ступенів ізогенії. Вони дають найменший внесок у безпеку алгоритму та найбільший – у проблему пошуку ядер ізогеній [47].

3.4. Комбіноване шифрування CSIKE-ENC

Недоліком запропонованого CSIKE алгоритму є відсутність автентифікації відправника [69]. Водночас доступна Бобу інформація – відкритий ключ Аліси d_{A} – може бути використана для вирішення цього завдання за допомогою CSIDH. Крім

того, розширення та модифікація алгоритму дозволяє в одному пакеті виконати і цільову функцію – шифрування повідомлення M відправника. Такий розширений алгоритм можна назвати CSIKE-ENC. Він є комбінованим асиметрично-симетричним алгоритмом. Для протоколів класичних ECC він подібний до інтегрованої схеми шифрування еліптичної кривої [72–75].

Введемо позначення:

1. C_o – результат шифрування секретного ключа $\boldsymbol{к}$ відкритим ключем Боба ($C_o < p$).

2. M – повідомлення.

3. $C_K = ENC_K(M)$ – шифр повідомлення M ключем K симетричного шифрування.

4. $DEC_K(C_K)$ – результат дешифрування повідомлення M ключем K.

5. $Teg_{A,B}$ – імітівставки автентифікації Аліси та Боба.

6. $H(M)$ – хеш-код повідомлення M.

У цій роботі ми пропонуємо наступний алгоритм передачі повідомлення *M*:

0. Попереднє обчислення:

Аліса та Боб на основі їх відкритих ключів d_A, d_B та не інтерактивного алгоритму CSIDH обчислюють розділені секрети $d_{BA} = Teg_A$ та $d_{AB}= Teg_B$, призначені як імітівставки для автентифікації Аліси Бобом.

1. Шифрування (Аліса):

1.1. Генерує секретний вектор $\Omega_K = (e_1, e_2, \dots, e_K)$, будує функцію CGA $\Theta_K = [l_1^{e_1}, l_2^{e_2}, \dots, l_K^{e_K}]$ і обчислює ізогенну криву $E_K = \Theta_K * E_0$, параметр d_K якої використовується як ключ K.

1.2. У процесі інкапсуляції шифрує ключ K відкритим ключем Боба та обчислює зашифрований ключ $d_{KB} = C_o < p$.

1.3. Розширює повідомлення M у вигляді $\widetilde{M} = (Teg_A, M)$.

1.4. За допомогою відомого сторонам стандарту шифрує ключем K симетричної криптосистеми повідомлення $\widetilde{M}$: $C_K = ENC_K(\widetilde{M})$

1.5. Відправляє Бобу пакет із двома шифрами $DP = (C_o, C_K)$.

2. Дешифрування (Боб):

2.1. За допомогою свого адитивно зворотного ключа – Ω_B дешифрує перший шифр C_o ($C_o < p$) та обчислює ключ K (декапсуляція ключа).

2.2. Дешифрує другий шифр за допомогою ключа K: $\widetilde{M} = DEC_K(C_K) = (Teg_A, M)$.

2.3. Перевіряє рівність $Teg_A = Teg_B$. При їх розбіжності автентифікація не виконана та повідомлення відкидається.

У разі успішної тестової передачі шифрів доцільно обом сторонам ключа K зробити заміну $K \leftarrow H(K)$. Це може радикально підвищити рівень безпеки симетричної криптосистеми.

При використанні блочного симетричного шифрування будь-яка помилка або модифікація повідомлення є хаотичним дешифруванням. У такому разі наведений протокол без цифрового підпису виконує дві його функції – автентифікацію та перевірку цілісності повідомлення (у тому числі помилки під час передачі) [76].

У роботах [63] наведено приклади імплементації моделі CSIKE із вхідними параметрами $p = 9239$, $\{l_k\}^K = \{3,5,7,11\}$, $\Omega_K = (4,-3,-3,2), \Omega_B = (3,-2,2,-3)$, з використанням 2-х секретних ключів Ω_K, Ω_B, без ключа Аліси Ω_A. З метою автентифікації Аліси в наведеному вище протоколі комбінованого шифрування пропонується використовувати цей третій ключ для обчислення тегів Аліси та Боба згідно з алгоритмом поділу секретів CSIDH. Вони служать як імітівставка, достовірність якої перевіряє Боб. В прикладі 2 з [63] ми ілюструємо приклад обчислення рандомізованих ізогенних ланцюжків для визначення параметрів d_{BA}, d_{AB}.

Приклад. Нехай секретний ключ Аліси $\Omega_A = (2,-3,1,-4)$, а функція CGA, відповідно, $\Theta_A = [3^2, 5^{-3}, 7^1, 11^{-4}]$. Тоді вона обчислює свій відкритий ключ $E_A = \Theta_A * E_0$ однією з 2^{20} можливих ланцюжків ізогеній завдовжки 10:

$$\begin{gathered}\frac{d^{(0)} = 2}{(11)} \xrightarrow{-1} \frac{6661}{(11)} \xrightarrow{-1} \frac{5469}{(5)} \xrightarrow{-1} \frac{1548}{(7)} \xrightarrow{1} \frac{6482}{(3)} \xrightarrow{1} \frac{384}{(5)} \xrightarrow{-1} 7935 = d^{(6)}, \\ \frac{d^{(6)} = 7935}{(5)} \xrightarrow{-1} \frac{7971}{(11)} \xrightarrow{-1} \frac{5154}{(11)} \xrightarrow{-1} \frac{211}{(3)} \xrightarrow{1} 5308 = d^{(10)}.\end{gathered} \tag{3.8}$$

Отже, відкритий ключ Аліси $d_A = 5308$. У схемі Діффі-Геллмана Аліса шифрує функцією CGA $\Theta_A = [3^3, 5^{-2}, 7^2, 11^{-34}]$ відкритий ключ Боба $d_B = 2504$ та отримує $E_{BA} = \Theta_A * E_B$ за 10 кроків:

$$\begin{gathered}\frac{d^{(0)} = 2504}{(5)} \xrightarrow{-1} \frac{7430}{(5)} \xrightarrow{-1} \frac{5373}{(11)} \xrightarrow{-1} \frac{50}{(3)} \xrightarrow{1} \frac{8935}{(7)} \xrightarrow{1} \frac{4468}{(5)} \xrightarrow{-1} 8001 = d^{(6)}, \\ \frac{d^{(6)} = 8001}{(11)} \xrightarrow{-1} \frac{6813}{(11)} \xrightarrow{-1} \frac{1908}{(3)} \xrightarrow{1} \frac{7761}{(11)} \xrightarrow{-1} 2384 = d^{(10)}.\end{gathered} \tag{3.9}$$

У результаті $d_{BA} = 2384 = Teg_A$.

Шифрування Бобом відкритого ключа Аліси $d_A = 5308$ функцією CGA $\Theta_B = [3^3, 5^{-2}, 7^2, 11^{-3}]$ згідно $E_{AB} = \Theta_B * E_A$ можна визначити випадковим ланцюжком параметрів $d^{(i)}$ ізогенних кривих

$$\begin{gathered}\frac{d^{(0)} = 5308}{(7)} \xrightarrow{1} \frac{7805}{(5)} \xrightarrow{-1} \frac{4900}{(11)} \xrightarrow{-1} \frac{3466}{(3)} \xrightarrow{1} \frac{7327}{(5)} \xrightarrow{-1} \frac{6250}{(11)} \xrightarrow{-1} 2723 = d^{(6)}, \\ \frac{d^{(6)} = 2723}{(11)} \xrightarrow{-1} \frac{4550}{(3)} \xrightarrow{1} \frac{5881}{(7)} \xrightarrow{1} \frac{6562}{(3)} \xrightarrow{1} 2384 = d^{(10)}.\end{gathered} \tag{3.10}$$

Зрозуміло, що через комутативність CSIDH $Teg_B = d_{AB} = 2384 = Teg_A$. Ці результати Аліса і Боб отримують на етапі перед обчислення алгоритму CSIKE-ENC. Власне, цей етап означає вставку CSIDH в CSIKE-ENC.

Може виникнути питання: якщо за допомогою CSIDH завдання поділу секретів вирішується простіше і швидше, яку мету переслідує CSIKE-ENC? Безперечна перевага останнього – у прирості безпеки. CSIDH включає три секретні ключі Ω_A, Ω_B, d_{BA} у той час як CSIKE-ENC – п’ять секретних ключів $\Omega_A, \Omega_B, d_{BA}, \Omega_K, K$. Головним аргументом нашого твердження є те, що атака на d_{BA} у CSIDH спирається на відомі відкриті ключі d_A та d_B Аліси та Боба, тоді як у CSIKE-ENC у аналітика для атаки на ключ K взагалі відсутня інформація. Ключем Ω_K, генеруючим K, має лише одна Аліса. Наведені аргументи ускладнюють завдання атаки на злам ключа K. Різні варіанти запропонованої вище заміни $K \leftarrow H(K)$ підвищують ентропію ключа та рівень безпеки.

Гарною модифікацією CSIDH та CSIKE-ENC є засекречування параметра d_0 початкової СКЕ E_0. Це вимагає заміни відкритих ключів Аліси та Боба, але додає

ще один секретний ключ і практично робить завдання аналітика безнадійним. При повторному сеансі передачі шифрованого повідомлення на базі CSIKE-ENC можна, наприклад, приймати $d_0 \leftarrow K$.

Слід зазначити, що рівень безпеки CSIDH оцінюється розміром множини всіх СКЕ, близьким $\sqrt{p}$. Тоді для модуля p довжиною 512 біт, як у роботі [10], він дорівнює 256 біт для звичайного комп'ютера і 128 біт – для квантового. Ми вважаємо, що хешування ключа $K \in F_p$ дозволить досягти максимального рівня безпеки.

Таким чином, схема CSIKE-ENC комбінованого шифрування ключа K та повідомлення $\widetilde{M}$ з автентифікацією відправника. Асиметричні алгоритми CSIKE та CSIDH вирішують завдання інкапсуляції ключа K та автентифікації Аліси за допомогою імітовставок, а симетричний алгоритм $ENC(\widetilde{M})_K$ з ключем K шифрує повідомлення разом із секретною імітовставкою. Запропонована схема відрізняється від відомих механізмів інкапсуляції ключів простотою та ефективністю. Рівень безпеки щодо квантового комп'ютера цієї схеми оцінюється як $\frac{\log p}{4}$. Обґрунтовано збільшення безпеки у схемі інкапсуляції ключа K у порівнянні з поділом секретів Діффі-Геллмана. Подальшого приросту безпеки схеми можна досягти:

1. Засекречуванням стартової кривої E_0.

2. Хешуванням ключа K.

Підвищена ефективність імплементації схеми досягається:

1. Використанням швидких квадратичних та скручених СКЕ та $(W:Z)$-координат.

2. Відмовою від надлишкових обчислень ізогенних функцій $\varphi(R)$ точки R.

3. Рандомізацією алгоритмів CSIKE та CSIDH.

4. Оптимізацією скалярних добутків точки R та $(W:Z)$-координатах.

5. Оптимізацією розподілу $Lopt$ ступенів ізогеній зі значним (в 1,5 рази) зниженням максимального ступеня $l_{\max} = 397$.

6. Видаленням малих значень ступенів із множини $\{l_k\}^K$ [68].

Висновки до розділу 3

1. Криві Едвардса однозначно ідентифікуються за двома параметрами. Параметр a інколи дорівнює 1, в цьому випадку ідентифікація здійснюється тільки за параметром d.

2. Обґрунтовано можливість відмовитися від обчислення ізогенної функції $\phi(R)$ випадкової точки R, що радикально прискорює виконання алгоритму. Знаходити складну для обчислення функцію ізогенії $\phi(x, y)$ немає необхідності, достатньо одного параметра d. Для кривої з параметром d обчислення ізогенії ступеня l з параметром d' зручно розраховувати за допомогою запропонованої формули. Прискорення роботи алгоритму CSIDH у разі відмови від обчислення функції $\phi(x, y)$ оцінюється коефіцієнтом 2,235.

3. Перехід від класу повних кривих Едвардса до класів квадратичних і скручених кривих Едвардса вдвічі розширює безліч кривих і вимагає інверсії параметра d кривих Едвардса, що оцінюється парціальною оцінкою виграшу в 2^5 разів.

4. У роботі представлено оригінальний алгоритм PQC CSIKE, що реалізує схему шифрування загального секрету K одним відкритим ключем одержувача. Метод рандомізації алгоритму CSIDH прискорює алгоритм більш ніж у 2^3 разів.

5. Оптимізація ступенів ізогеній алгоритму CSIDH знижує максимальний рівень ізогеній з лінійною оцінкою прискорення алгоритму в 1,5 рази.

6. Метод рандомізації алгоритму CSIDH на квадратичних та скручених СКЕ забезпечує ефективну та безпечну альтернативу різним варіантам методу CT CSIDH. Наведено модель рандомізації для простої моделі алгоритму CSIDH.

РОЗДІЛ 4
МЕТОД CRS НА НЕСУПЕРСИНГУЛЯРНИХ КРИВИХ ЕДВАРДСА

4.1. Схема CRS шифрування на ізогенії несуперсингулярних нециклічних кривих Едвардса

Першим алгоритмом на ізогенії НКЕ була схема CRS [13]. Чудовими її властивостями є комутативність ізогенних переходів, гнучкість та простота, пов'язані з використанням арифметики простого поля F_p. Але у роботі [10], зазначається, що шифрування за схемою CRS неприпустимо повільне і при безпеці 128 біт може зайняти кілька хвилин. Тому автори [10] на ґрунті CRS запропонували алгоритм CSIDH який використовує вже технологію СКЕ і обґрунтували це порівняно більш швидкою імплементацією алгоритмів.

Однак множина НКЕ приблизно в $\sqrt{p}$ разів ширше за множину СКЕ, крім того зростання числа ступенів ізогеній при заданому або близькому модулі p поля, а також наявність 4-х паралельних незалежних криптосистем, комутативність ізогенних переходів подвоює швидкість алгоритму і тому використання НКЕ ще має шанс.

Порядок еліптичної кривої E над простим полем F_p визначається як $\#E = p + 1 - t$, де t – слід рівняння ендоморфізму Фробеніуса ($|t| \leq 2\sqrt{p}$). Для кривої квадратичного кручення E^t цей порядок $\#E^t = p + 1 + t$. Порядки обох кривих симетричні щодо середнього значення $p + 1$. Для СКЕ $t = 0$ і порядки обох кривих $p + 1$ збігаються, а множина ступенів ізогеній однакові, але в алгоритмі CSIDH знаки експонент ступенів зворотні один одному. У разі НКЕ порядки пар квадратичного кручення відрізняються на $2t$, тоді існують різні ступені ізогенії на кривих двох класів, пов'язаних як пари квадратичного кручення з різними порядками. У цьому вся основна специфіка НКЕ.

4.2. Модель криптосистеми на несуперсингулярних кривих Едвардса

Ідея полягає в тому, що в класах B та C для будь-якої кривої Едвардса (2.9) та (2.10) з параметром d існує ізоморфна крива з параметром d^{-1}. Фіксуючи стартову криву E_0, ми будуємо ланцюжки ізогеній всіх ступенів першої криптосистеми із секретним ключем Ω_1. Другу криптосистему із секретним ключем Ω_2 легко побудувати на багатьох всіх кривих, ізоморфних першої. Для цього інша стартова крива вибирається шляхом інверсії параметра d будь-якої кривої першої криптосистеми. Ясно, що ці дві множини кривих не перетинаються, і можна одночасно вирішувати два завдання замість однієї, що подвоює продуктивність обчислень.

Експоненти ступенів нециклічних ізогеній, як і в CSIDH, мають протилежні знаки. Чергування ступенів ізогеній згідно з методом рандомізації випадкове, а простота переходів ланцюжка ізогеній з одного класу нециклічних кривих Едвардса B і C в інший досягається тим, що їх параметри адитивно зворотні: $(a, d) \leftrightarrow (-a, -d)$.

За аналогією з CSIDH неважко сформувати загальні параметри CRS – подібної криптосистеми на ізогенії НКЕ порядку $\#E \equiv 0 \bmod 8$ над полем з модулем $p \equiv 7 \bmod 8$. Нехай $n_0 = \prod_{k=1}^{K} l_k$ та $N = 8n_0 -$ порядок квадратичної СКЕ над полем із модулем $p_0 = N - 1$. Задаючи значення сліду Фробеніуса $t = \pm 8m, m = 1,2,3, \ldots$ визначаємо суму $p_0 \pm 8m = p$, рівну простому числу p. Тоді над полем F_p існують квадратична НКЕ (2.9) порядку $\#E_d = 8n_0$ та скручена крива (2.10) порядку $\#E_{-1,-d} = N \pm 16m = 8n_1$.

Наприклад, для багатьох ступенів ізогеній $\{l_k\} = \{3,5,7\}, n_0 = 105, N = 840, p_0 = 839$, тоді при $m = 3$ отримаємо просте число $p = 839 + 24 = 863$. При цьому порядки кривих пари квадратичного кручення дорівнюють $\#E_d = 840 = 8 \cdot 3 \cdot 5 \cdot 7$ і $\#E_{-1,-d} = N + 48 = 888 = 8 \cdot 3 \cdot 37, n_1 = 111 = 3 \cdot 37$.

Отже, ми маємо чотири ступеня ізогеній $\{l_k\} = \{3,5,7,37\}$, перші три з яких є співмножниками порядку 840 квадратичної кривої (4), а ступеня 3 і 37 ділять порядок 888 кривої скрученої (5) над полем F_{863} і слідом рівняння ендоморфізму

Фробеніуса є $t = -24$. Для першої кривої (2.9) знаки експонент ізогеній $e_k > 0$, а для кривої (5) $e_k < 0$. Тут ступень 3 є двонапрямленим (допускає обидва знаки), а ступеня 5 та 7 ($e_k > 0$) та 37 ($e_k < 0$) – односпрямовані. Ці особливості ізогеній НКЕ обговорюються в [63].

При порівняно невеликому модулі поля $p = 863$ не важко оцінити значення $\sqrt{p}$ параметрів d всіх кривих (2.9) з порядком 840. Оскільки вони є квадратами, то повний перебір за модулем p всіх $c = 2,3,\dots,431$, і $d = c^2$ дає безліч всіх 62 значень параметрів d НКЕ (2.9) та (2.10). Кількість всіх кривих становить 124. Тут число параметрів парне, тому що для кожної кривої існує ізоморфна крива з параметром $d \leftrightarrow d^{-1}$ і однаковим J-інваріантом. Наприклад, $169^{-1} = 623,\ J(169) = J(623) = 826$. Тоді неізоморфних кривих (2.9) залишається 31, стільки ж і кривих (2.10). Ізогенії всіх ступенів мають простий період $\pi = 31$.

Усі значення параметрів табл. 4.1 можна знайти, обчислюючи ланцюжки будь-якої ізогенії ступенів $\{3,5,7,37\}$ періоду $\pi = 31$.

Таблиця 4.1

Масив значень 62-х параметрів d квадратичних та скручених НКЕ ($a = \pm 1$) при $p = 863$, $\#E_d = 840$, $\#E_{-1,-d} = 888$ ($t = 24$) [47]

169*	400*	729	161*	818	210*	436*	309	43*	665*	840*
19	779	111	308	253*	116	705*	503*	32	573	472*
71	616*	618*	444*	302*	192	486	318*	852*	231	728*
300	113*	311*	858*	673*	725	589	75	684	551*	307
688	843	339	623	706	281	181*	27*	186*	652*	130
835*	409	345	283*	596	326*	236				

Наприклад, обчислимо ланцюжок 3-ізогенії квадратичної кривої (2.9) так само, як у роботі [68] для CSIDH на СКЕ порядку 840 над полем F_{839}. Вибираючи першу криву в табл. 4.1 як стартову, отримаємо за 31 крок весь ланцюжок кривих:

$$\frac{d^{(0)}=169}{(3)}\xrightarrow{1}\frac{503}{(3)}\xrightarrow{1}\frac{318}{(3)}\xrightarrow{1}\frac{652}{(3)}\xrightarrow{1}\frac{181}{(3)}\xrightarrow{1}\frac{551}{(3)}\xrightarrow{1}\frac{326}{(3)}\xrightarrow{1}\frac{161}{(3)}\xrightarrow{1}\frac{618}{(3)}\xrightarrow{1}$$
$$\frac{436}{(3)}\xrightarrow{1}\frac{302}{(3)}\xrightarrow{1}\frac{186}{(3)}\xrightarrow{1}\frac{665}{(3)}\xrightarrow{1}\frac{400}{(3)}\xrightarrow{1}\frac{43}{(3)}\xrightarrow{1}\frac{858}{(3)}\xrightarrow{1}\frac{835}{(3)}\xrightarrow{1}\frac{210}{(3)}\xrightarrow{1}\frac{705}{(3)}\xrightarrow{1}$$
$$\frac{311}{(3)}\xrightarrow{1}\frac{27}{(3)}\xrightarrow{1}\frac{728}{(3)}\xrightarrow{1}\frac{616}{(3)}\xrightarrow{1}\frac{840}{(3)}\xrightarrow{1}\frac{472}{(3)}\xrightarrow{1}\frac{283}{(3)}\xrightarrow{1}\frac{444}{(3)}\xrightarrow{1}\frac{113}{(3)}\xrightarrow{1}\frac{673}{(3)}\xrightarrow{1}$$
$$\frac{852}{(3)}\xrightarrow{1}\frac{253}{(3)}\xrightarrow{1}\frac{169}{(3)}=d^{(31)} \tag{4.1}$$

Цифра над стрілкою означає один крок ланцюжка 3-ізогенії квадратичної НКЕ з експонентою $e_k > 0$. Під значенням параметра $d^{(i)}$ у дужках ми пишемо ступінь ізогенії.

Для скрученої кривої (2.10) з $e_k < 0$ також існує 3-ізогенія того ж періоду $\pi = 31$

$$\frac{d^{(0)}=169}{(3)}\xrightarrow{-1}\frac{253}{(3)}\xrightarrow{-1}\frac{852}{(3)}\xrightarrow{-1}\frac{673}{(3)}\xrightarrow{-1}\frac{113}{(3)}\xrightarrow{-1}\frac{444}{(3)}\xrightarrow{-1}\frac{283}{(3)}\xrightarrow{-1}\frac{472}{(3)}\xrightarrow{-1}$$
$$\frac{840}{(3)}\xrightarrow{-1}\frac{616}{(3)}\xrightarrow{-1}\frac{728}{(3)}\xrightarrow{-1}\frac{27}{(3)}\xrightarrow{-1}\frac{311}{(3)}\xrightarrow{-1}\frac{705}{(3)}\xrightarrow{-1}\frac{210}{(3)}\xrightarrow{-1}\frac{835}{(3)}\xrightarrow{-1}\frac{858}{(3)}\xrightarrow{-1}\frac{43}{(3)}\xrightarrow{-1}$$
$$\frac{400}{(3)}\xrightarrow{-1}\frac{665}{(3)}\xrightarrow{-1}\frac{186}{(3)}\xrightarrow{-1}\frac{302}{(3)}\xrightarrow{-1}\frac{436}{(3)}\xrightarrow{-1}\frac{618}{(3)}\xrightarrow{-1}\frac{161}{(3)}\xrightarrow{-1}\frac{326}{(3)}\xrightarrow{-1}\frac{551}{(3)}\xrightarrow{-1}\frac{181}{(3)}\xrightarrow{-1}$$
$$\frac{652}{(3)}\xrightarrow{-1}\frac{318}{(3)}\xrightarrow{-1}\frac{503}{(3)}\xrightarrow{-1}\frac{169=d^{(31)}}{(3)} \tag{4.2}$$

має реверсний порядок чергування ізогенних кривих (останній ланцюжок (4.2) та (4.1) прочитуються у зворотному порядку). Цифра над стрілкою (–1) означає один крок ізогенії скрученої кривої з негативними параметрами.

Пара кривих кручення E_d та $E_{-1,-d}$ тут мають порядки 840 та 888 відповідно. Для будь-якого іншого ступеня ізогенії можна побудувати подібні (4.1) та (4.2) ланцюжки ізогенних кривих періоду $\pi = 31$ з тією ж безліччю параметрів $d^{(i)}$, але з різними порядками чергування. У табл. 4.1 цей 31 параметр d позначений зірочками. Це безліч параметрів d першої криптосистеми. Інвертуючи кожен параметр d^*, отримуємо у табл. 4.1 не помічений 31 параметр d другої

криптосистеми. Тут ми також маємо дві ізоморфні криптосистеми з можливістю паралельних обчислень.

Чудовою властивістю НКЕ у порівнянні з СКЕ є ще двох ізоморфних криптосистем. Ідея проста: можна поміняти місцями порядки квадратичної та скрученої НКЕ, відома також як дуальна криптосистема.

Порядки кривих над полем F_{863} $\#E_d = 888$, $\#E_{-1,-d} = 840$. Для дуальної криптосистеми можна обчислити масив значень параметрів d замість перебірного методу (табл. 4.1). Знайдемо лише одну скручену криву з порядком $\#E_d = 888$ та параметром $d = 6$. Обчислимо ланцюжок 37-ізогенії зі стартовим значенням $d = 6$, та її позначені зірочкою значення занесемо у перші три рядки табл. 4.2. У тій же послідовності в наступні три рядки масиву запишемо інвертовані значення d^{-1} ізоморфних кривих (не позначені зірочкою). Верхня та нижня частина таблиці утворюють рівновеликі множини параметрів d двох ізоморфних дуальних криптосистем.

Таблиця 4.2

Масив значень 62 параметрів d квадратичних та скручених НКЕ ($a = \pm 1$) при $p = 863$, $\#E_d = 888$, $\#E_{-1,-d} = 840$ ($t = 24$) [47]

6*	678*	703*	212*	611*	420*	248*	159*	821*	562*	538*
546*	12*	581*	136*	654*	464*	438*	313*	361*	191*	392*
837*	29*	199*	246*	683*	695*	751*	24*	553*	—	—
144	849	685	460	613	150	87	38	226	453	470
49	72	254	514	128	478	664	670	153	122	284
697	744	425	214	513	488	732	36	103	—	—

Отже, використовуючи НКЕ замість СКЕ, ми отримуємо чотири незалежні криптосистеми замість двох, що при паралельних обчисленнях забезпечує чотирьох кратний виграш у продуктивності криптосистеми в порівнянні з класичною CSIDH. Дуже важливо, що паралельні обчислення унеможливлюють реалізацію атаки сторонніми каналами та безглуздою надмірність у СТ CSIDH. Резервні криптосистеми можна використовувати як для чотирьох кратного

нарощування довжини ключа в алгоритмах інкапсуляції, так і для спрощення алгоритму (зниження числа ступенів ізогенії при фіксованій довжині ключа).

Розглянемо модель алгоритму поділу секретів Діффі-Геллмана на першій криптосистемі з 31 параметром d^* із табл. 4.1. У нашій моделі із ізогеніями ступенів $\{3,5,7,37\}$ з метою вирівнювання ймовірностей вибору кривих пари квадратичного кручення приймемо всі ступеня односпрямованими, тоді в секретних ключах ступеня $\{5,7\}$ віднесемо до квадратичної кривої $(e_k > 0)$, а степені $\{3,37\}^t$ – до скрученої $(e_k < 0)$.

Приймемо секретні ключі Аліси $\Omega_A = (-2,5,1,-4)$ і Боба $\Omega_B = (-1,3,3,-5)$. Обчислимо за 12 випадково обраних кроків ізогеній кожен із відкритих ключів. Відкритий ключ Аліси з випадковим вибором кривих та ступенів визначається як

$$\frac{d^{(0)} = 169}{(5)} \xrightarrow{1} \frac{840}{(3)} \xrightarrow{-1} \frac{616}{(5)} \xrightarrow{1} \frac{43}{(5)} \xrightarrow{1} \frac{326}{(5)} \xrightarrow{1} \frac{852}{(3)} \xrightarrow{-1} 673 = d^{(6)},$$

$$\frac{d^{(6)} = 673}{(37)} \xrightarrow{-1} \frac{472}{(7)} \xrightarrow{1} \frac{551}{(37)} \xrightarrow{-1} \frac{503}{(5)} \xrightarrow{1} \frac{472}{(37)} \xrightarrow{-1} \frac{27}{(37)} \xrightarrow{-1} 835 = d^{(12)} \Rightarrow \tag{4.3}$$

$$d_A = 835.$$

Аналогічні обчислення Боба дають

$$d^{(0)} = \frac{169}{(3)} \xrightarrow{-1} \frac{253}{(5)} \xrightarrow{1} \frac{616}{(5)} \xrightarrow{1} \frac{43}{(7)} \xrightarrow{1} \frac{444}{(7)} \xrightarrow{1} \frac{161}{(5)} \xrightarrow{1} 253 = d^{(6)},$$

$$\frac{d^{(6)} = 253}{(7)} \xrightarrow{1} \frac{186}{(37)} \xrightarrow{-1} \frac{161}{(37)} \xrightarrow{-1} \frac{652}{(37)} \xrightarrow{-1} \frac{253}{(37)} \xrightarrow{-1} \frac{444}{(37)} \xrightarrow{-1} 616 = d^{(12)} \Rightarrow \tag{4.4}$$

$$d_B = 616.$$

У результаті двом сторонам доступні відкриті ключі $d_A = 835$ і $d_B = 616$. Далі Аліса обчислює за допомогою свого секретного ключа $\Omega_A = (-2,5,1,-4)$ криву E_{BA}

$$\frac{d^{(0)} = 616}{(3)} \xrightarrow{-1} \frac{728}{(3)} \xrightarrow{-1} \frac{27}{(5)} \xrightarrow{1} \frac{665}{(5)} \xrightarrow{1} \frac{181}{(5)} \xrightarrow{1} \frac{113}{(5)} \xrightarrow{-1} 311 = d^{(6)},$$

$$\frac{d^{(6)} = 311}{(5)} \xrightarrow{-1} \frac{186}{(7)} \xrightarrow{1} \frac{840}{(37)} \xrightarrow{-1} \frac{311}{(37)} \xrightarrow{-1} \frac{858}{(37)} \xrightarrow{-1} \frac{186}{(37)} \xrightarrow{-1} 161 = d^{(12)} \Rightarrow \tag{4.5}$$

$$d_{BA} = 161.$$

Симетричні обчислення Боба:

$$\frac{d^{(0)}=835}{(5)} \xrightarrow{1} \frac{618}{(3)} \xrightarrow{-1} \frac{161}{(5)} \xrightarrow{1} \frac{253}{(5)} \xrightarrow{1} \frac{616}{(7)} \xrightarrow{1} \frac{652}{(7)} \xrightarrow{1} 858 = d^{(6)},$$

$$\frac{d^{(6)}=858}{(7)} \xrightarrow{1} \frac{113}{(37)} \xrightarrow{-1} \frac{840}{(37)} \xrightarrow{-1} \frac{311}{(37)} \xrightarrow{-1} \frac{858}{(37)} \xrightarrow{-1} \frac{186}{(37)} \xrightarrow{-1} d^{(12)} \Rightarrow \quad (4.6)$$

$$d_{AB} = 161.$$

дають той же результат через комутативність ізогеній $d_{AB} = d_{BA} = 161$, що визначає квадратичну криву E_{161} розділеного секрету. Як вище зазначалося, це значення унікальне (для заданої стартової кривої). Тут не потрібно в розділеному секреті $K = 161$ переходити до J-інваріанту. Подібні обчислення з іншими стартовими кривими та ключами можна паралельно виконувати і в інших трьох незалежних криптосистемах для вирішення різних завдань.

4.3. Багатофункціональна CRS схема шифрування на ізогенії несуперсингулярних кривих Едвардса

Пропонується схема PQC рандомізованого комутативного безсупер-сингулярного шифрування ізогенії (від англ. Randomized Commutative No-supersingular Isogeny Encryption, RCNIE). Від відомих її відрізняють існування 4-х паралельних криптосистем (з додаванням дуальної та 2-х ізоморфних) і, головне – багатофункціональність.

Запропоновано багатофункціональну криптосистему RCNIE на ізогеніях НКЕ, що вирішує завдання поділу секретів Діффі-Геллмана, цифрового підпису та шифрування з відкритим ключем. Розглянуто проблеми вибору параметрів НКЕ, що утворюють пари квадратичного кручення з порядками $p + 1 \pm t \equiv 0 \bmod 8$ над простим полем F_p. Наведено алгоритми шифрування із взаємною автентифікацією Аліси та Боба на основі поділу їх секретів, при цьому довжина ключа та розмір цифрового підпису мінімально короткі та не перевищують розміру елемента поля F_p.

Пропонується модель криптосистеми на 4-х ступенях ізогеній {3,5,7,37} над полем F_{863} для пари кривих квадратичного кручення з порядками 840 та 888. Показано, що для НКЕ існують основна та дуальна криптосистеми, кожна з яких має також ізоморфну криптосистему. Це дозволяє виконувати паралельні обчислення та прискорювати алгоритми. Дана порівняльна оцінка арифметики та властивостей CSIDH та RCNIE.

У цій роботі ми використовуємо НКЕ двох класів з тим самим обмеженням $p \equiv 3 \bmod 4$. Це дозволяє виразити рівняння кривих пари квадратичного кручення за допомогою адитивно зворотних параметрів.

Експоненти ступенів ізогенії цих двох кривих, як і в CSIDH, мають протилежні знаки. Чергування ступенів ізогеній згідно з методом рандомізації випадкове, а простота переходів ланцюжка ізогеній з одного класу кривих в інший досягається тим, що їх параметри адитивно зворотні: $(a, d) \leftrightarrow (-a, -d)$.

У даному розділі розглядаються НКЕ двох класів B та C, пов'язаних як пари квадратичного кручення з порядками $p + 1 \pm t \equiv 0 \bmod 8$. Ненульове значення t у $\sqrt{p}$ разів розширює множину кривих [21, 23]. Тобто множина НКЕ ширше відповідної множини СКЕ з грубою оцінкою в $\sqrt{p}$ раз, і, як наслідок, має чимало потенційних можливостей.

На відміну від схеми CRS на кривих у формі Вейєрштрасса з двома параметрами, що не використовує пари квадратичного кручення, ми будуємо алгоритми шифрування на найбільш швидких сьогодні парах крутіння крутих Едвардса з одним варіюється параметром d. Іншими важливими факторами прискорення наших алгоритмів є відмова від досить трудомісткого обчислення ізогенної функції $\varphi(R)$ випадкової точки R та рандомізація алгоритмів [47].

Пара НКЕ квадратичного кручення має різні порядки та різні множини ступенів $\{l_k\}$ та $\{l_k\}^t$, які можуть частково перетинатись. Для перетину $\{l_k\} \cap \{l_k\}^t$, як у CSIDH, кожна l-ізогенія має обидва знаки, і тоді $\left[l_k^{e_k}\right] * \left[l_k^{-e_k}\right] = 1$. Це означає, що ланцюжки l-ізогеній різного знаку будуються у зворотному порядку та гасять один одного. Тому ключі в CSIDH задають для кожного ступеня l_k

експонентуe_k лише одного знака. Для НКЕ будується об'єднання множин $\{l_k\} \cup \{l_k\}^t$, а знаки експонент e_k визначаються приналежністю ізогенії до однієї з кривих пари кручення. Слід прагнути рівноймовірного використання обох кривих, що виконується при рівносильних множинах $\{l_k\}$ і $\{l_k\}^t$.

Так як ізогенні криві відповідних ступенів існують у класах кривих B і C, пов'язаних як пари квадратичного кручення, для побудови комутативних ланцюжків ізогеній ми користуємося функцією шифрування CGA $\Theta = [l_1^{e_1}, l_2^{e_2}, \dots, l_K^{e_K}]$. Специфічною особливістю застосування цієї функції для НКЕ є кардинальне ускладнення операції мультиплікативного обігу для частини ступенів ізогеній, різних у множинах $\{l_k\}$ та $\{l_k\}^t$. Для наших завдань це не порушує працездатності алгоритмів шифрування, одночасно ускладнюючи завдання криптоаналізу.

У всіх алгоритмах функція шифрування CGA $\Theta(\Omega)$ шифрує секретний ключ $\Omega = (e_1, e_2, \dots, e_K)$ за допомогою відображення $\Theta = [l_1^{e_1}, l_2^{e_2}, \dots, l_K^{e_K}]$ та стартової кривої E_0 в ізогенну криву $E' = E_0 * \Theta$, параметр d якою приймається або як відповідний відкритий ключ або як новий короткий секретний ключ.

Рандомізований алгоритм обчислення Алісою свого відкритого ключа d_A за допомогою секретного ключа $\Omega_A = (e_1, e_2, \dots, e_K)$.

Алгоритм 4.1. Реалізація групової операції на квадратичних та скручених несуперсингулярних кривих Едвардса з рандомізацією [47]

Input: $d_A \in E_A, \chi(d) = 1$ *and a secret key* $\Omega_A = (e_1, e_2, \dots e_K)$.

Output: d_B *such that*$[l_1^{e_1}, l_2^{e_2}, \dots, l_K^{e_K}] * E_A = E_B$, *where* $E_{A,B}: x^2 + y^2 = 1 + d_{A,B}x^2y^2$,

1. *Let* $S_0 = \{k | e_k > 0\}, S_1 = \{k | e_k < 0\}, n_0 = \prod_{k \in S_0} l_k, n_1 = \prod_{k \in S_1} l_k$,

2. While *some* $e_k \neq 0$ **do**

3. *Sample a random* $x \in F_p$,

4. Set $a \leftarrow 1,\ \lambda \leftarrow 0, E_A:\ x^2 + y^2 = 1 + d_A x^2 y^2$ **If** $\chi(\frac{x^2-1}{dx^2-1}) = 1$,

5. Else $a \leftarrow -1,\ \lambda \leftarrow 1, E_A:\ x^2 - y^2 = 1 - d_A x^2 y^2$,

6. *Compute* y -coordinate of the point $P = (x, y) \in E_A$,

7. *Compute* $R \leftarrow [4]P$,

8. *Sample a random* $l_k|, k \in S_\lambda$,

9. *Compute* $Q \leftarrow [n_\lambda / l_k]R$,

10. If $Q \neq (1,0)$ c*ompute kernel* G *of* l_k*-isogeny* $\varphi: E_B \leftarrow E_A$,

11. Else start over to line 3,

12. *Compute* d_B *of curve* E_B, $d_A \leftarrow d_B$, $e_k \leftarrow e_k - a$,

13. *Skip* k *in* S_λ *and* set $n_\lambda \leftarrow (n_\lambda / l_k)$ **If** $e_k = 0$,

14. Return d_A.

Цей алгоритм має важливі відмінності від оригінального алгоритму 2 з [11], які обговорюються у роботі [47]. Крім модифікацій, пов'язаних з методом рандомізації алгоритму CSIDH, тут ми відмовляємося від надлишкової ізогенної функції $\varphi(R)$ випадкової точки R, що радикально прискорює алгоритм.

Ідея рандомізації полягає в тому, що для будь-якого випадкового значення змінної x ($xy \neq 0, \infty$) точка $P = (x, y)$ при відомому параметрі d завжди належить одній із двох кривих. Це дозволяє вдвічі прискорити відбір випадкової точки P та ускладнити атаку сторонніми каналами. Цьому сприяє випадковий вибір ступенів ізогеній (у міру їх вичерпання). Крім того, при невдалому виборі P перехід до нового ступеня часто усуває проблему швидше, ніж варіації x.

На початку Алгоритму 4.1 формуються два підмножини $S_\lambda, \lambda = 0,1, \ldots$ з номерами ступенів l_k, разом із двома співмножниками n_0 та n_1 числа $n = n_0 n_1$, індекс $\lambda = 0$ ($e_k > 0$) відповідає вибору квадратичної НКЕ, а $\lambda = 1$ – скрученої НКЕ ($e_k < 0$). Оскільки порядок кривої $\#E_d = 8n_0$, то в п. 7 алгоритму для кривої E_d обчислюється точка $R = 4n_1 P$ непарного порядку n_0, а для кривої $E_{-1,-d}$ – точка $R = 4n_0 P$ непарного порядку n_1. Це мінімізує витрати наступного скалярного твору, що визначає точку Q ядра ізогенії степені l_k (п. 9). Далі в п. 10 алгоритму методом подвоєння точок розраховуються $s = (l_k - 1)/2$ x-координат точок ядра $< Q >$.

В п. 7 Алгоритму 4.1 дворазове подвоєння випадкової точки P. Одночасно дозволяє позбутися точок парного порядку (у тому числі – особливі точки 2-го і 4-го порядку) і далі йдуть обчислення скалярних творів у підгрупах точок непарного порядку кривої. Їхнє завдання – знайти $\frac{(l_k-1)}{2}$ x-координат α_i точок ядра $< Q >$ простого порядку l_k. У результаті за формулою (2.19) розраховується параметр d' l_k-ізогенної квадратичної НКЕ. Параметри скрученої НКЕ (2.10) $a' = -1, d' \rightarrow -d'$.

Підкреслимо, що концепція RCNIE – побудова ланцюжків ізогенних кривих як абелевих груп, а не ізогенних функцій $\varphi(R)$ випадкової точки R. Трудомісткі обчислення останніх у [10] є надмірними.

4.4. Моделювання RCNIE

У роботі [47] наведено моделі як спосіб ілюстрації властивостей алгоритмів. Розуміння цих властивостей відкриває шляхи для дослідження нових властивостей.

У розділі 4.2. у табл. 4.1 наведено масив значень 62 параметрів d квадратичних та скручених НКЕ ($a = \pm 1$) при $p = 863$, $\#E = 840$, $\#E^t = 888$ ($t = 24$). Там же у розділі 4.2 розглядаються ланцюжки ізогеній НКЕ.

У цій моделі спостерігається чудова властивість подвійного знаходження мультиплікативного обігу елемента ізогенного ланцюжка. З одного боку, справедливо

$$E^{(0)} = E^{(1)} * E^{(2)} * \ldots * E^{(\pi)} * E^{(0)} \rightarrow \left[E^{(0)}\right] * \left[E^{(0)}\right]^{-1} = 1, \quad \left[E^{(0)}\right]^{-1} = E^{(1)} * E^{(2)} * \ldots * E^{(\pi)}. \tag{4.7}$$

З іншого боку, для двонаправлених l-ізогеній пари кривих кручення з експонентами ± 1 має місце

$$E^{(1)} * E^{(-1)} = 1 \Rightarrow \left[E^{(1)}\right]^{-1} = E^{(-1)}. \tag{4.8}$$

Іншими словами, щоб мультиплікативно звернути один крок ізогенного ланцюжка, потрібно в загальному випадку знайти ланцюжок періоду π (див. (4.7) і

(4.8)). Це ж завдання для двонаправлених ізогеній вирішується за один крок замість π кроків за (4.8). Зворотні знаки експонент таких ізогеній гасять один одного: $[l^{+1}] * [l^{-1}] = 1$.

Наведений випадок має місце у CSIDH, що вигідно відрізняє його від CRS. Але в CSIDH ізогенія кожного ступеня в ключах використовується як односпрямована експоненти, що зрозуміло, оскільки різні знаки експоненти лише нейтралізують один одного. Властивість (4.8) корисна лише захисту від атак сторонніми каналами [55], й у завдання CSIKE [69]. Разом з тим для НКЕ обіг елемента односпрямованої ізогенії згідно з (4.7) і (4.8) вимагає знання періоду ізогенії та нереалізованого для реальних криптосистем часу обчислень. У цих криптосистемах слід уникати завдань, пов'язаних із зверненням.

Характерно, що при стартовій кривій ${E_d}^{(0)} = E_{169}$ послідовність $d^{(i)}$ (4.1) не містить елемента $169^{-1} = 623$ з рівним J-інваріантом. Звідси випливає, що це справедливо і для всіх елементів цієї послідовності періоду 31, кожен з яких можна прийняти стартовим з відповідним циклічним зсувом (як у циклічному коді довжини 31). Все J-інваріанти різні. Ізогенні криві інших ступенів 5, 7 і 11 містять ті ж параметри і той же період, що і (4.1), що чергуються в іншому порядку. Далі ми побачимо, що самі робочі параметри містять усі обчислення в схемі поділу секретів. Якщо інвертувати стартову криву $169^{-1} \to 623$, не треба будувати нові ізогенні ланцюжки, достатньо інвертувати результати. У цьому випадку активними будуть інша половина параметрів табл. 4.2.

Таким чином, існують дві ізоморфні криптосистеми з різними взаємно зворотними параметрами d і збігаються множинами J-інваріантів. Якщо стартова крива задана і не змінюється, всі параметри $d^{(i)}$ ізогенних ланцюжків унікальні і немає необхідності переходити до J-інваріанту результуючої кривої. Ізоморфна перша криптосистема може паралельно вирішувати інші завдання, що подвоює продуктивність такої системи. Далі ми побачимо, що крім ізоморфної криптосистеми існують ще дуальна криптосистема, яка також має свою ізоморфну. Загалом з'являється потенційна можливість уточнити продуктивність схеми. RCNIE.

4.5. Імплементація алгоритму поділу секретів Діффі-Геллмана

Крім того, паралельні обчислення взагалі знімають загрозу атаки сторонніми каналами і роблять безглуздою надмірність СТ CSIDH.

У нашій моделі із ізогеніями ступенів {3,5,7,37} з метою вирівнювання ймовірностей вибору кривих пари квадратичного кручення приймемо всі ступеня односпрямованими, тоді в секретних ключах ступеня {5,7} віднесемо до квадратичної кривої ($e_k > 0$), а степені $\{3, 37\}^t$ – до скрученої ($e_k < 0$). Приймемо секретні ключі Аліси $\Omega_A = (-2,5,1,-4)$ та Боба $\Omega_B = (-1,3,3,-5)$. Обчислимо за 12 випадково обраних кроків ізогеній кожен із відкритих ключів.

Відкритий ключ Аліси з випадковим вибором кривих та ступенів визначається за (4.3), а аналогічні обчислення для Боба дають (4.4). В результаті двом сторонам доступні відкриті ключі $d_A = 835$ і $d_B = 616$. Далі Аліса обчислює за допомогою свого секретного ключа $\Omega_A = (-2,5,1,-4)$ криву E_{BA}, як показано у (4.5), а симетричні обчислення Боба, представлені у (4.6), дають той самий результат через комутативність ізогеній $d_{AB} = d_{BA} = 161$. Це значення унікальне (для заданої стартової кривої) і тут не потрібно в розділеному секреті $K = 161$ переходити до J-інваріанту.

4.6. Порівняльні оцінки CSIDH і RCNIE

У роботі [63] ми запропонували рандомізовану модель CSIDH с двонаправленими ізогеніями ступенів {3,5,7} на кривих B та C над полем F_{839}. Ці параметри близькі до прийнятих у цій роботі параметрів нециклічних НКЕ над полем F_{863} з різними порядками 840 і 888 і слідом рівняння Фробеніуса $t = 24$. Ці дві моделі найбільш зручно та коректно порівнювати.

Вже можна стверджувати, що з переходом від CSIDH до НКЕ завжди з’являються один або більше ступенів ізогенії (у нашому випадку $l = 37$). Незначним їх мінусом є односпрямованість, а для великих криптосистем –

практично неможливість обігу ізогенних ланцюжків, і таких завдань слід уникати алгоритмів. Тут ми бачимо взаємні переваги та недоліки.

Якщо тепер звернутися до проблем, пов'язаних із швидкодією, то ми не виявили жодних нових причин, що гальмують виконання алгоритму. Зазвичай при виборі випадкової точки P на початку кожного кроку обчислення ізогенної кривої, точка P може виявитися невдалою за певної міри l_k. Це означає, що порядок точки P не містить співмножника l_k. Імовірність такої події l_k^{-1} тим більше, чим менше ступінь, і досягає максимального значення ⅓.

Ми не рекомендуємо у криптосистемах відбирати надто малі ступені, вони найбільш проблематичні. В цьому випадку рандомізація дозволяє випадкові переходи на інші ступені ізогеній. З нашого досвіду, невдалі випадкові точки виникають з однаковою частотою незалежно від того, чи є крива суперсингулярною, чи ні. Як зазначено в попередньому розділі, повільність реалізації обчислень ізогеній, швидше за все, пов'язана з непомірною надмірністю характеристики простого поля. F_p та порядку кривої у використовуваних моделях. Причина такої надмірності залишається незрозумілою.

Для НКЕ існує унікальна у порівнянні з СКЕ можливість будувати не лише пари квадратичного кручення з порядками $p + 1 \pm t$, але і всередині кожного класу знаходити пари кривих з такими ж порядками, як у кривій квадратичного кручення. Відповідні криві назвемо *дуальними.* Їхнє існування дозволяє замінювати квадратичні криві скрученими і навпаки. Наприклад, ступінь ізогенії $l = 37$ у нашій моделі належить безлічі скручених кривих $E_{-1,-d}$ потужності 64 та порядку 888. Над полем F_{863} існує крива E_d порядку 888 з мінімальним параметром $d = 6$. Обчислимо для кривих E_d параметри $d^{(i)}$ ланцюжка 37-ізогенії на періоді $\pi = 31$:

$$\frac{d^{(0)}=6}{(37)} \xrightarrow{1} \frac{678}{(37)} \xrightarrow{1} \frac{703}{(37)} \xrightarrow{1} \frac{212}{(37)} \xrightarrow{1} \frac{611}{(37)} \xrightarrow{1} \frac{420}{(37)} \xrightarrow{1} \frac{248}{(37)} \xrightarrow{1} \frac{159}{(37)} \xrightarrow{1}$$
$$\frac{821}{(37)} \xrightarrow{1} \frac{562}{(37)} \xrightarrow{1} \frac{538}{(37)} \xrightarrow{1} \frac{546}{(37)} \xrightarrow{1} \frac{12}{(37)} \xrightarrow{1} \frac{581}{(37)} \xrightarrow{1} \frac{136}{(37)} \xrightarrow{1} \frac{654}{(37)} \xrightarrow{1}$$
$$\frac{464}{(37)} \xrightarrow{1} \frac{428}{(37)} \xrightarrow{-1} \frac{313}{(37)} \xrightarrow{1} \frac{361}{(37)} \xrightarrow{1} \frac{191}{(37)} \xrightarrow{1} \frac{392}{(37)} \xrightarrow{1} \frac{837}{(37)} \xrightarrow{1} \frac{29}{(37)} \xrightarrow{1}$$
$$\frac{199}{(37)} \xrightarrow{1} \frac{246}{(37)} \xrightarrow{1} \frac{683}{(37)} \xrightarrow{1} \frac{695}{(37)} \xrightarrow{1} \frac{751}{(37)} \xrightarrow{1} \frac{24}{(37)} \xrightarrow{1} \frac{553}{(37)} \xrightarrow{1} \frac{6}{(37)}. \quad (4.9)$$

Тут представлено половину параметрів дуальних кривих E_d з порядком 888. Як і (4.1), в цій послідовності жоден елемент d не має інверсного d^{-1}. Друга половина параметрів $d^{(i)}$ обчислюється інверсією (для ізоморфних кривих) наведених вище. Відповідні скручені криві мають порядок 840. Існування дуальних кривих дає можливість над тим самим полем F_{863} побудувати дві криптосистеми: основну та дуальну, знаки експонент ізогеній яких змінюються місцями. Ці криптосистеми можуть працювати незалежно, і, отже, подвоювати число розв’язуваних завдань.

Якщо до кожної з двох згаданих криптосистем додати ізоморфну, утворюється чотири паралельні криптосистеми з різними множинами параметрів d, що допускають паралельні незалежні обчислення. Поки неясно, чи є простий (як пар квадратичного кручення), зв’язок між параметрами основних і дуальних кривих. Це питання залишається відкритим. У будь-якому разі існування дуальних криптосистем, унікальних для НКЕ, обіцяє чотирьох кратне розширення можливостей криптосистем на ізогенії еліптичних кривих. Ця перспектива потребує подальших досліджень, але незважаючи на це виклики, виграш запропонованих методів є значним, то підтверджується результатами, приведеними в табл. 4.3.

Таблиця 4.3

Інтегральні нижні оцінки виграшу у швидкодії для модифікацій алгоритму CSIDH

Джерело прискорення	Мінімальна парціальна оцінка прискорення γ
Перехід від класу повних кривих Едвардса до класів квадратичних і скручених кривих Едвардса вдвічі розширює множину кривих і не потребує інверсії параметра d	$\approx 2^5$
Метод рандомізації алгоритму CSIDH та відмова від обчислення ізогенної функції $\phi(x, y)$ у проєктивних координатах $(W:Z)$ Фарашахі-Хосейні	2^3
Оптимізація ступенів ізогеній алгоритму CSIDH знижує максимальний ступінь ізогеній з лінійною оцінкою прискорення алгоритму	1,5
Одночасне вирішення двох завдань, що подвоює продуктивність обчислень	2
Паралельні обчислення у чотирьох незалежних криптосистемах CRS на НКЕ	2
Підсумкова нижня оцінка прискорення	$3 \cdot 2^9$

Знижуючи для спрощення оцінку γ_3 і приймаючи $\gamma_3 = 2$, отримуємо парціальну оцінку виграшу у швидкості обчислень алгоритму CSIDH $\gamma_3\gamma_4\gamma_5\gamma_6 = 2^4$. Отже, підсумкову нижню оцінку прискорення модифікованого алгоритму CSIDH отримуємо не менше, ніж $\prod_{k=1}^{6}\gamma_k \geq 2^9$. У наступних розділах обговорюються подальші модифікації CSIDH та оцінюється їх ефективність [47, 63].

Висновки до розділу 4

1. Запропоновано багатофункціональну криптосистему RCNIE на ізогеніях НКЕ, що вирішує завдання поділу секретів Діффі-Геллмана, цифрового підпису та шифрування з відкритим ключем. Вона побудована на двох класах нециклічних кривих Едвардса, які утворюють пару квадратичного кручення. Базовим алгоритмом RCNIE є алгоритм поділу секретів, який також служить для взаємної автентифікації користувачів.

2. Побудовано модель виконання криптоалгоритмів на ізогенії чотирьох ступенів $\{3,5,7,37\}$ та надано аналіз її властивостей. Проілюстровано існування двох ізоморфних та двох дуальних криптосистем, що розширюють можливості алгоритмів на НКЕ порівняно з СКЕ. Наведено приклади обчислень параметрів кривих у алгоритмах з використанням методу рандомізації. Існування над одним простим полем F_p чотирьох ізоморфних та дуальних криптосистем може бути використане для їх резервування, оновлення, а також паралельних обчислень.

3. Дана порівняльна оцінка арифметики криптосистем на ізогенії СКЕ та НКЕ. Підстав вважати технологію останніх повільнішою за прийняти у CSIDH не знайдено. Оскільки число всіх НКЕ оцінено в $\sqrt{p}$ разів перевищує число СКЕ, у майбутніх додатках перспективно використовувати ряд згаданих вище переваг.

ВИСНОВКИ

У дисертації вирішено актуальне наукове завдання, яке полягає в обґрунтуванні і виборі еліптичних кривих для використання у постквантових криптоалгоритмах лінійки CSIDH, підвищенні їх швидкодії і захисту шляхом модернізації. Дане наукове завдання має важливе значення для теорії і практики захисту інформації, створення та забезпечення функціонування інформаційних систем і технологій на об’єктах інформаційної діяльності у сфери кібербезпеки та захисту інформації. Відсутність глибоких досліджень цих відносно нових областей науки робить результати досліджень важливими для розробки і використання існуючих і нових методів захисту інформації.

Отримані результати мають важливе значення для модернізації існуючих та в процесі розробки нових методів захисту інформації.

На підставі проведених досліджень зроблені наступні висновки:

1. Вперше запропоновано і обґрунтовано метод підвищення швидкодії криптосистеми CSIDH шляхом використання замість одної циклічної повної кривої Едвардса двох нециклічних кривих з випадковим вибором однієї з кривих пари. Це у зрівнянні з CSIDH вдвічі розширює простір еліптичних кривих, спрощує обчислення параметра d кривих. Оцінка виграшу в швидкодії складає 2^5 рази. Використання додатково ізоморфних кривих породжує існування двох незалежних криптосистем з можливістю паралельних обчислень. Це додатково усуває загрозу атаки сторонніми каналами, подвоює швидкодію або довжину секретного ключа у два рази. Для цього було проаналізувано поточний стан і властивості класичних криптоалгоритмів Діффі-Геллмана, а також визначено можливості покращення роботи цих криптоалгоритмів на ізогеніях еліптичних кривих, які здатні працювати у постквантових умовах при здійсненні атак квантових комп’ютерів. В результаті визначено властивості кривих Едвардса як оптимальних кандидатів для використання у постквантових алгоритмах.

2. Вперше запропоновано модель інкапсуляції ключа CSIKE з рандомізацією з одним сеансом передачі і одним відкритим ключем замість двох у порівнянні з CSIDH. Модель ґрунтується на випадковому виборі однієї з нециклічних кривих

Едвардса та випадковому виборі ступеня ізогенії на кожному кроці ланцюжка ізогеній. Такий випадковий вибір є альтернативою методам вирівнювання часу виконання групової операції постійного часу CSIDH, що не викликає штучного збільшення часу виконання алгоритму і усуває загрозу атаки сторонніми каналами. Це дозволяє удвічі скоротити час на обмін ключами і підвищує загальну швидкодію у два рази. Для цього обґрунтувано клас і досліджено властивості еліптичних кривих Едвардса, які мають найкращі характеристики для використання у постквантових алгоритмах, а також визначено властивості алгоритму CSIDH на кривих Едвардса і обґрунтувано застосування алгоритмів CSIDH на нециклічних кривих, що пришвидшено обчислення ізогенії для збільшення швидкодії криптоалгоритму та захисту від атаки сторонніми каналами.

3. Удосконалено метод обчислення і вибору структури ізогеній у криптоалгоритмах CSIDH на кривих Едвардса. Обчислення ізогенних функцій функції $\varphi(R)$ випадкової точки R замінюється на більш просте обчислення параметру d ізогенної кривої. При цьому виконуються менш затратні операції, пов'язані зі скалярними множеннями випадкових точок на число, що прискорює обчислення порядку точок і надає прискорення алгоритму більш ніж у 2^3 разів. Вибір структури ступенів ізогеній за рахунок скорочення їх діапазону дає лінійну оцінку прискорення алгоритму в 1,5 рази. Для цього були розроблені модифікації алгоритму CSIDH і створено комбінований криптоалгоритм із застосуванням цих модифікацій, а також оцінено величину парціального зростання швидкості від кожної модифікації криптоалгоритму CSIDH на ізогеніях суперсінгулярних еліптичних кривих Едвардса.

4. Набув подальшого розвитку метод CRS на НКЕ та поділу секретів Діффі-Геллмана на ізогеніях ординарних нециклічних кривих Едвардса. Замість двох ізоморфних криптосистем в алгоритмі CSIDH перехід до НКЕ породжує чотири незалежні криптосистеми з можливістю паралельних обчислень. Це дає оцінку виграшу швидкості обчислень у чотири рази. Оцінка загального виграшу швидкості обчислень досягає $3 \cdot 2^9$ разів. Для цього було розроблено модель алгоритму з використанням НКЕ і оцінено приріст швидкодії і криптографічної

стійкості паралельних обчислень, а також оцінено інтегральний виграш у швидкодії модернізованих алгоритмів CSIDH і CSIKE.

Мета дослідження щодо підвищення швидкодії і безпеки постквантового асиметричного криптоалгоритму CSIDH шляхом його моделювання і модернізації з використанням властивостей еліптичних кривих у формі Едвардса досягнута і всі часткові завдання вирішені повністю. Наукові результати можуть бути використані дослідно-конструкторськими організаціями та державними структурами при розробці та удосконаленні систем передавання інформації в режимі реального часу на об’єктах інформаційної діяльності критичної інфраструктури та державних органів. Перспективність запропонованих рішень для таких галузей як передача зашифрованих даних для державних організацій і підприємств, збройних сил, приватних підприємств та осіб тощо є очевидною.

В якості пріоритетних напрямів подальших досліджень планується експериментальна перевірка захищеності запропонованих модифікацій криптоалгоритмів і розробка паралельних систем шифрування даних, які передаються в державних та приватних системах.

Таким чином, поставлене актуальне наукове завдання розв’язане у повному обсязі. Усі визначені часткові завдання вирішено, мету досліджень досягнуто.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Diffie, W., & Hellman, M. E. (2022). New Directions in Cryptography. *Democratizing Cryptography*, 365–390. https://doi.org/10.1145/3549993.3550007
2. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, *21*(2), 120–126. https://doi.org/10.1145/359340.359342
3. Elgamal, T. (1985). A Public Key Cryptosystem and a Signature Scheme based on Discrete Logarithms. *IEEE Transactions on Information Theory, 31*(4), 469–472. https://doi.org/10.1109/tit.1985.1057074
4. ElGamal, T. (2000). A Public Key Cryptosystem and a Signature Scheme based on Discrete Logarithms. *Advances in Cryptology*, 10–18. https://doi.org/10.1007/3-540-39568-7_2
5. Miller, V. S. (1985). Use of Elliptic Curves in Cryptography. In *Advances in Cryptology (CRYPTO)*, 417–426. https://doi.org/10.1007/3-540-39799-x_31
6. Koblitz, N. (1987). Elliptic Curve Cryptosystems. *Mathematics of Computation, 48*(177), 203. https://doi.org/10.2307/2007884
7. Schneier, B. (2015). Applied Cryptography, *2nd Edition*. https://doi.org/10.1002/9781119183471
8. Shor, P. W. (1994). Algorithms for Quantum Computation: Discrete Logarithms and Factoring. In *35th Annual Symposium on Foundations of Computer Science,* 124–134. https://doi.org/10.1109/sfcs.1994.365700
9. Schneier, B. (2018). Cryptography after the Aliens Land. *IEEE Security & Privacy, 16*(5), 86–88. https://doi.org/10.1109/msp.2018.3761724
10. Castryck, W., Lange, T., Martindale, C., Panny, L., & Renes, J. (2018). CSIDH: An Efficient Post-Quantum Commutative Group Action. In *Advances in Cryptology (ASIACRYPT)*, 395–427. https://doi.org/10.1007/978-3-030-03332-3_15
11. Jao, D., & De Feo, L. (2011). Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies. *Post-Quantum Cryptography*, 19–34. https://doi.org/10.1007/978-3-642-25405-5_2

12. Castryck, W., & Decru, T. (2023). An Efficient Key Recovery Attack on SIDH. In *Advances in Cryptology (EUROCRYPT)*, 423–447. https://doi.org/10.1007/978-3-031-30589-4_15
13. Rostovtsev, A., & Stolbunov, A. (2006). Public-Key Cryptosystem based on Isogenies, *ePrint*, Paper 2006/145. https://ia.cr/2006/145
14. Edwards, H. (2007). A Normal Form for Elliptic Curves. *Bulletin of the American Mathematical Society, 44*(3), 393–422. https://doi.org/10.1090/s0273-0979-07-01153-6
15. Ilyenko, A., Ilyenko, S., Prokopenko, O., Hulak, H., & Melnyk, I. (2023). Practical Aspects of Using Fully Homomorphic Encryption Systems to Protect Cloud Computing. In *Cybersecurity Providing in Information and Telecommunication Systems II, 3550*, 226–233.
16. Virovets, D., Obushnyi, S., Zhurakovskyi, B., Skladannyi, P., & Sokolov, V. (2024). Integration of Smart Contracts and Artificial Intelligence using Cryptographic Oracles. In *Classic, Quantum, and Post-Quantum Cryptography (CQPC), 3829*, 39–46.
17. Hulak, H., Zhdanova, Y., Skladannyi, P., Hulak, Y., & Korniiets, V. (2022). Vulnerabilities of Short Message Encryption in Mobile Information and Communication Systems of Critical Infrastructure Objects. *Electronic Professional Scientific Journal "Cybersecurity: Education, Science, Technique," 1*(17), 145–158. https://doi.org/10.28925/2663-4023.2022.17.145158
18. Stolbunov, A. (2010). Constructing Public-Key Cryptographic Schemes based on Class Group Action on a Set of Isogenous Elliptic Curves. *Advances in Mathematics of Communications, 4*(2), 215–235. https://doi.org/10.3934/amc.2010.4.215
19. Циганкова, О. В. (2021). Методи підвищення швидкодії асиметричних криптосистем з використанням еліптичних кривих у формі Едвардса. *Дисертація к.т.н. за спеціальністю 05.13.21 «Системи захисту інформації»*. КПІ. https://ela.kpi.ua/bitstream/123456789/40610/1/Tsygankova_dys.pdf

20. National Institute of Standards and Technology (2006). Recommendation for Pair-Wise Key Establishment Schemes using Discrete Logarithm Cryptography. https://doi.org/10.6028/nist.sp.800-56a
21. Бессалов, А. В. (2017). Еліптичні криві у формі Едвардса та криптографія. Монографія. *Політехніка*.
22. Chernenko, R., Anosov, A., Kyrychok, R., Brzhevska, Z., & Spasiteleva, S. (2022). Encryption Method for Systems with Limited Computing Resources. In *Cybersecurity Providing in Information and Telecommunication Systems, 3288*, 142–148.
23. Washington, L. C. (2008). Elliptic Curvres. Number Theory and Cryptography. *2nd Edition. CRC Press*.
24. Zhurakovskyi, B., Otrokh, S., Poliakov, M., Poliakov, O., & Skladannyi, P. (2024). Enhancing Information Transmission Security with Stochastic Codes. In *Classic, Quantum, and Post-Quantum Cryptography (CQPC), 3829*, 62–69.
25. Станкевіч, А. О. (2021). Дослідження та реалізація протоколу Діффі-Геллмана на еліптичних кривих. Автореферат магістерської роботи за спеціальністю 122 «Комп'ютерні науки». Чорноморський нац. унів. ім. П. Могили. https://krs.chmnu.edu.ua/jspui/bitstream/123456789/1692/1/Автореферат%20601%20Станкевіч%20Андрій%20Олександрович.pdf
26. Bernstein, D. J. (2009). Introduction to Post-Quantum Cryptography. *Post-Quantum Cryptography,* 1–14. https://doi.org/10.1007/978-3-540-88702-7_1
27. Moody, D., & Shumow, D. (2015). Analogues of Vélu's formulas for isogenies on Alternate Models of Elliptic Curves. *Mathematics of Computation, 85*(300), 1929–1951. https://doi.org/10.1090/mcom/3036
28. Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). Report on Post-Quantum Cryptography. *National Institute of Standards and Technology*. https://doi.org/10.6028/nist.ir.8105
29. Couveignes, J.-M. (1997). Quelques revêtements définis sur Q. *Manuscripta Mathematica, 92*(1), 409–445. https://doi.org/10.1007/bf02678203

30. Charles, D., Goren, E., & Lauter, K. (2006). Cryptographic Hash Functions from Expander Graphs, *ePrint*, Paper 2006/021. https://ia.cr/2006/021
31. Yoneyama, K. (2019). Post-Quantum Variants of ISO/IEC Standards. In *5th ACM Workshop on Security Standardisation Research Workshop*. https://doi.org/10.1145/3338500.3360336
32. Kim, S., Yoon, K., Park, Y.-H., & Hong, S. (2019). Optimized Method for Computing Odd-Degree Isogenies on Edwards Curves. In *Advances in Cryptology (ASIACRYPT)*, 273–292. https://doi.org/10.1007/978-3-030-34621-8_10
33. Bessalov, A., Sokolov, V., & Skladannyi, P. (2020). Modeling of 3- and 5-Isogenies of Supersingular Edwards Curves. In *2nd International Workshop on Modern Machine Learning Technologies and Data Science, 2631*(I), 30–39.
34. Абрамов, С. (2024). Алгоритм інкапсуляції ключа на кривих Едвардса. На *IV Міжнародній науково-практичній інтернет-конференції «Цифрова трансформація фінансової системи України та країн V-4 в умовах євроінтеграції», II*, 98–105.
35. Farashahi, R. R., & Hosseini, S. G. (2017). Differential Addition on Twisted Edwards Curves. *Information Security and Privacy*, 366–378. https://doi.org/10.1007/978-3-319-59870-3_21
36. Kim, S., Yoon, K., Kwon, J., Hong, S., & Park, Y.-H. (2018). Efficient Isogeny Computations on Twisted Edwards Curves. *Security and Communication Networks*, 1–11. https://doi.org/10.1155/2018/5747642
37. Bessalov, A., & Abramov, S. (2023). PQC CSIKE Algorithm on Non-Cyclic Edwards Curves. *Cybernetics and Systems Analysis, 59*(6), 867–879. https://doi.org/10.1007/s10559-023-00622-x
38. Bessalov, A. (2022). How to Construct CSIDH on Quadratic and Twisted Edwards Curves. *Electronic Professional Scientific Journal "Cybersecurity: Education, Science, Technique," 3*(15), 148–163. https://doi.org/10.28925/2663-4023.2022.15.148163

39. Bessalov, A. (2022). On Correctness of Conditions for the CSIDH Algorithm Implementation on Edwards Curves. *Radiotekhnika, 208*, 16–27. https://doi.org/10.30837/rt.2022.1.208.02
40. Bessalov, A., Sokolov, V., Skladannyi, P., Mazur, N., & Ageyev, D. (2022). Implementation of the CSIDH Algorithm Model on Supersingular Twisted and Quadratic Edwards Curves. In *Cybersecurity Providing in Information and Telecommunication Systems, 3187*(1), 302–309.
41. Bernstein, D. J., & Lange, T. (2017). Montgomery Curves and the Montgomery Ladder. *Topics in Computational Number Theory Inspired by Peter L. Montgomery*, 82–115. https://doi.org/10.1017/9781316271575.005
42. Bernstein, D. J., & Lange, T. (2007). Faster Addition and Doubling on Elliptic Curves. In *Advances in Cryptology (ASIACRYPT)*, 29–50. https://doi.org/10.1007/978-3-540-76900-2_3
43. Bernstein, D. J., Birkner, P., Joye, M., Lange, T., & Peters, C. (2008). Twisted Edwards Curves. In *Progress in Cryptology (AFRICACRYPT)*, 389–405. https://doi.org/10.1007/978-3-540-68164-9_26
44. Bernstein, D. J., & Lange, T. (2007). Inverted Edwards Coordinates. *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, 20–27. https://doi.org/10.1007/978-3-540-77224-8_4
45. Bernstein, D. J. (2009). Batch Binary Edwards. In *Advances in Cryptology (CRYPTO)*, 317–336. https://doi.org/10.1007/978-3-642-03356-8_19
46. Бессалов, А. В., Циганкова, О. І. (2015). Взаємозв'язок родин точок великих порядків кривої Едвардса над простим полем. *Захист інформації, 17*(1), 73–80.
47. Bessalov, A., Sokolov, V., & Abramov, S. (2024). Efficient Commutative PQC Algorithms on Isogenies of Edwards Curves. *Cryptography, 8*(3), 1–17. https://doi.org/10.3390/cryptography8030038
48. Bessalov, A., & Abramov, S. (2022). Special Properties of the Point Addition Law for Non-Cyclic Edwards Curves. *Cybernetics and Systems Analysis, 58*(683), 851–861. https://doi.org/10.1007/s10559-023-00518-w

49. Bessalov, A. V., & Tsygankova, O. V. (2017). Number of Curves in the Generalized Edwards Form with Minimal Even Cofactor of the Curve Order. *Problems of Information Transmission, 53*(1), 92–101. https://doi.org/10.1134/s0032946017010082
50. Bessalov, A. V., & Tsygankova, O. V. (2015). Interrelation of Families of Points of High Order on the Edwards Curve over a Prime Field. *Problems of Information Transmission, 51*(4), 391–397. https://doi.org/10.1134/s0032946015040080
51. Bessalov, A., Sokolov, V., Skladannyi, P., & Zhyltsov, O. (2021). Computing of Odd Degree Isogenies on Supersingular Twisted Edwards Curves. In *Cybersecurity Providing in Information and Telecommunication Systems, 2923*, 1–11.
52. Bessalov, A., Kovalchuk, L., Sokolov, V., Skladannyi, P., & Radivilova, T. (2020). Analysis of 2-Isogeny Properties of Generalized Form Edwards Curves. In *Cybersecurity Providing in Information and Telecommunication Systems, 2746*, 1–13.
53. Бессалов, А., Циганкова, О., & Абрамов, С. (2021). Оцінка обчислювальної складності алгоритму CSIDH на суперсингулярних скручених і квадратичних кривих Едвардса. *Всеукраїнський міжвідомчий науково-технічний збірник «Радіотехніка», 4*(207), 40–51. https://doi.org/10.30837/rt.2021.4.207.03.
54. Bessalov, A., & Kovalchuk, L. (2015). Exact Number of Elliptic Curves in the Canonical Form, Which are Isomorphic to Edwards Curves over Prime Field. *Cybernetics and Systems Analysis, 51*(2), 165–172. https://doi.org/10.1007/s10559-015-9709-x
55. Bessalov, A., Kovalchuk, L., & Abramov, S. (2022). Randomization of CSIDH Algorithm on Quadratic and Twisted Edwards Curves. *Electronic Professional Scientific Journal "Cybersecurity: Education, Science, Technique," 1*(17), 128–144. https://doi.org/10.28925/2663-4023.2022.17.128144
56. Bessalov, A., & Kovalchuk, L. (2019). Supersingular Twisted Edwards Curves Over Prime Fields. I. Supersingular Twisted Edwards Curves with j-Invariants Equal to Zero and 123. Cybernetics and Systems Analysis, 55(3), 347–353. https://doi.org/10.1007/s10559-019-00140-9

57. Bessalov, A., & Kovalchuk, L. (2019). Supersingular Twisted Edwards Curves over Prime Fields. II. Supersingular Twisted Edwards Curves with the j-Invariant Equal to 663. *Cybernetics and Systems Analysis, 55*(5), 731–741. https://doi.org/10.1007/s10559-019-00183-y
58. Popereshnyak, S., Novikov, Y., & Zhdanova, Y. (2024). Cryptographic System Security Approaches by Monitoring the Random Numbers Generation. In *Cybersecurity Providing in Information and Telecommunication Systems II (CPITS-II), 3826*, 301–309.
59. Бессалов, А. В., Діхтенко, А. А., & Яценко, О. І. (2013). Параметри криптосистеми на кривій Едвардса над розширеннями малих простих полів. *Прикладна радіоелектроніка, 12*(2), 273–277.
60. Schoof, R. (1995). Counting Points on Elliptic Curves over Finite Fields. *Journal de Théorie Des Nombres de Bordeaux, 7*(1), 219–254. https://doi.org/10.5802/jtnb.142
61. Abramov, S., Sokolov, V., & Abramov, V. (2024). Research of the Graphic Model of the Points of the Elliptic Curve in the Edward Form. In *Workshop on Cybersecurity Providing in Information and Telecommunication Systems II (CPITS-II), 3826*, 174–181.
62. Jalali, A., Azarderakhsh, R., Kermani, M. M., & Jao, D. (2019). Towards Optimized and Constant-Time CSIDH on Embedded Devices. *Constructive Side-Channel Analysis and Secure Design*, 215–231. https://doi.org/10.1007/978-3-030-16350-1_12
63. Bessalov, A., Abramov, S., Sokolov, V., Skladannyi, P., & Zhyltsov, O. (2023). Multifunctional CRS Encryption Scheme on Isogenies of Non-Supersingular Edwards Curves. In *Workshop on Classic, Quantum, and Post-Quantum Cryptography (CQPC), 3504*, 12–25.
64. Diffie, W., & Hellman, M. (1976). New Directions in Cryptography. *IEEE Transactions on Information Theory, 22*(6), 644–654. https://doi.org/10.1109/tit.1976.1055638
65. Onuki, H., Aikawa, Y., Yamazaki, T., & Takagi, T. (2020). A Constant-Time Algorithm of CSIDH Keeping Two Points. *IEICE Transactions on Fundamentals of*

Electronics, Communications and Computer Sciences, E103.A(10), 1174–1182. https://doi.org/10.1587/transfun.2019dmp0008

66. Meyer, M., Campos, F., & Reith, S. (2019). On Lions and Elligators: An Efficient Constant-Time Implementation of CSIDH. *Post-Quantum Cryptography*, 307–325. https://doi.org/10.1007/978-3-030-25510-7_17
67. Barthe, G., Betarte, G., Campo, J., Luna, C., & Pichardie, D. (2014). System-Level Non-Interference for Constant-Time Cryptography. In *ACM SIGSAC Conference on Computer and Communications Security*. https://doi.org/10.1145/2660267.2660283
68. Bessalov, A., Abramov, S., Sokolov, V., & Mazur, N. (2023) CSIKE-ENC Combined Encryption Scheme with Optimized Degrees of Isogeny Distribution. In *Cybersecurity Providing in Information and Telecommunication Systems (CPITS), 3421*, 36–45.
69. Bessalov, A., Sokolov, V., Skladannyi, P., Abramov, S., & Zhyltsov, O. (2022). Modeling CSIKE Algorithm on Non-Cyclic Edwards Curves. In *Cybersecurity Providing in Information and Telecommunication Systems (CPITS), 3288*, 1–10.
70. Abramov, S., Bessalov, A., & Sokolov, V. (2023). Properties of Isogeny Graph of Non-Cyclic Edwards Curves. In *Cybersecurity Providing in Information and Telecommunication Systems II (CPITS-II), 3550*, 234–239.
71. Абрамов, С. (2024). Дослідження структури графа ізогеній еліптичної кривої Едвардса. На *Міжнародній науково-технічній конференції «Інформаційно-комунікаційні технології та кібербезпека» (ІКТК)*, 200–201.
72. American National Standards Institute (2011). ANSI X9.63-2011 (R2017). Public Key Cryptography for the Financial Services Industry. Key Agreement and Key Transport Using Elliptic Curve Cryptography.
73. Institute of Electrical and Electronics Engineers (2004). IEEE 1363a-2004. IEEE Standard Specifications for Public-Key Cryptography. Amendment 1: Additional Techniques. https://doi.org/10.1109/ieeestd.2004.94612
74. International Organization for Standardization (2006). ISO/IEC 18033-2:2006. Information technology. Security techniques. Encryption algorithms. Part 2: Asymmetric ciphers.

75. Brown, D. R. L. (2009). Standards for Efficient Cryptography. SEC 1: Elliptic Curve Cryptography. Version 2.0. *Certicom Corporation*. https://www.secg.org/sec1-v2.pdf

76. Sokolov, V., Skladannyi, P., & Hulak, H. (2022). Stability Verification of Self-Organized Wireless Networks with Block Encryption. In *5th International Workshop on Computer Modeling and Intelligent Systems, 3137*, 227–237.

Додаток А

ПРОГРАМНИЙ КОД ДЛЯ ОБЧИСЛЕННЯ

L-ІЗОГЕНІЇ КРИВОЇ ЕДВАРДСА

```
from tkinter import *
from array import *
from typing import Union, Any

# задання параметрів для полегшення вводу
a = 1
d = 76
m = 839
L = 5
# контроль параметрів
print("a= " + str(a) + " d= " + str(d) + " m= " + str(m))
# номери середини списку
m2 = int((m - 1) / 2)
bk = 88

# масив квадратів xq[]
xq = [0,1]
# квадрати до середини списку
for x in range(2, m2 + 1):
        xz=(xq[x - 1] + 2 * (x - 1) + 1) % m
        # массив квадратів до середини списку
        xq.append(xz)
# квадрати після середини списку
for k in range (m2):
        xz = xq[m2 - k]
        # квадрати повторюються після середини списку
        xq.append(xz)
```

```
# квадрат
def qud(x):
        # вибір із списку квадратів
        return (xq[x])

# квадратний корень
def kor(q:int):
        if q < 0: q = q + m
        for i in range(m):
                if xq[i] == q:
                        return i
                continue
        else:
                print ('q=', q, 'корня нет')
                # vn - корня немає
                return('vn')

# інвертування числа по модулю m
def inv(g: int, m: int):
        if g == 0:
                return ('∞')
        else:
                if g < 0: g = g + m
                f = pow(g, m - 2, m)
                if f > m2: f = f - m
        return f

# друк масиву
# p - масив, s - рядок назви масиву
```

```
def pema(p, s):
        i = 0
        pn = len(p)
        print(s, end = '')
        while (i < pn):
                print('%4s' % p[i], end=',')
                i = i + 1
        print('\n', end='')


# додавання точок
def sum(x1, y1, x2, y2, a, d, m):
        if (x1 == '∞' and x2 == '∞' and y1 == y2):
                x3 = -1
                y3 = 0
        elif (x1 == '∞' and x2 == '∞' and y1 == -y2):
                x3 = 1
                y3 = 0
        # додавання з особливими точками
        elif y2 == '∞':
                x3 = (x2 * x1i) % m
                y3 = (ai * x2 * y1i) % m
                if x3 > m2: x3 = x3 - m
                if y3 > m2: y3 = y3 - m
        elif x2 == '∞':
                x3 = (-y2 * y1i) % m
                y3 = (y2 * x1i) % m
                if x3 > m2: x3 = x3 - m
                if y3 > m2: y3 = y3 - m
                return (x3, y3)
        # додавання звичайних точок
```

```
else:
        # чисельник x3
        z12=((x1 * x2) % m - (a * y1 * y2) % m) % m
        # знаменник x3
        z5=(1 - d * x1 * x2 * y1 * y2) % m
        # особливі точки із нескінченними координатами
        if z5 == 0:
                if z12 == 0:
                        x3 = '00'
                        y3 = '00'
                else:
                        x3 = '∞'
        else:
                # інвертування числа
                z5i = int(inv(z5, m))
                # координата x суми
                x3=(z12 * z5i) % m
                # симетрування відносно вісі y
                if x3 > m2: x3 = x3 - m
        z34 = ((x1 * y2) % m + (x2 * y1) % m) % m
        # знаменник y3 суми
        z6 = (1 + d * x1 * x2 * y1 * y2) % m
        # отримання точки із нескінченними координатами
        if z6 == 0:
                if z34 == 0:
                        x3 = '00'
                        y3 = '00'
                else:
                        y3='∞'
        else:
```

```
                    z6i = int(inv(z6, m))
                    # координата y суми
                    y3 = (z34 * z6i) % m
                    # симметрування відносно вісі x
                    if y3 > m2: y3 = y3 - m
        return (x3), (y3)

# вивід списку X
w = 0
print("127 x=  ", end='')
while (w < m):
        print('%5d' % w, end='')
        w = w+1
print('\n', end='')

pema(xq, '133 xq= ')

# обчислення Y квадрат
# масив Y квадрат
Yquad = []
Y1a = []
Y2a = []
Y3a = []
# Zy особливі точки y = ∞
Zy = []
# Zx особливі точки x = ∞
Zx = []
for i in range(m2 + 1):
        # чисельник
        Y1 = (1 - (i) ** 2) % m
```

```
        # знаменник
        Y2 = (a - d * (i) ** 2) % m
        # особлива точка Y = ∞
        if Y2 == 0:
                # додаємо координату x особливої точки в масив Zx = []
                Zx.append(i)
                Zx.append(-i)
                # поточне значення Yq в масиві Yquad
                Yq = '∞'
        # особливих точок немає, обчислюємо Y квадрат
        else:
                # інвертування Y3, інверсія від Y2
                Y3 = inv(Y2, m)
                # обчислення Y квадрат
                Yq = (Y1 * Y3) % m
        Yquad.append(Yq)

# особливі точки x = ∞, y = 1 / √d = vdi
# d1 корень з d (√d)
d1 = "ні"
# d2 інверсія d1 (vdi)
d2 = 0
# перебір всіх q від 0 до m2 = (m - 1) / 2
for q in range(m2 + 1):
        # перевірка чи є d квадратом
        if d == (q ** 2) % m:
                # якщо d - квадрат, то d1 - корень із d
                d1 = q
                # якщо корень знайдений, то вихід з циклу
                break
```

```
# інвертування d1
for r in range(m):
        # якщо корня немає, то вихід із циклу
        if d1 == "ні":
                d2 = "ні"
                break
        # якщо корень є, то виконуємо інвертування
        if (1 + r * m) % d1 == 0:
                # d2 інверсія корня d1
                d2 = (1 + r * m) // d1
                if d2 > m2: d2 = d2 - m
                # додаємо d2 в масив особливих точок Zy
                Zy.append(d2)
                Zy.append(-d2)
                break

pema(Yquad, '178 Yquad')

# корень із Y квадрат
# масив координат точок
XY = []
Y = []
for i in range(m2 + 1):
        for j in range(m):
                n=((j) ** 2) % m
                if Yquad[i] == n:
                        Y.append(j)
                        XY.append(i)
                        XY.append(j)
                        break
```

```
        else:
                if Yquad[i] == '∞':
                        Y.append('∞')
        else:
                Y.append('-')

pema(Y, '236 Y = ')
Nx = len(Zx)
Ny = len(Zy)

# додавання знаку точок
# розгорнута множина точок
XYZ = []
# масив координат x
XXZ = []
# масив координат y
YYZ = []
l = int(len(XY) / 2)
# вибираємо 1 точку
for r in range (l):
        xx = XY[2 * r]
        rr = 2 * r + 1
        yy = XY[rr]
        if yy == 0:
                h2m = 1
                h1m = 2
        elif xx == 0:
                h2m = 2
                h1m = 1
        else: h1m = h2m = 2
```

```
        # робимо 4 точки
        for h1 in range (h1m):
                for h2 in range (h2m):
                        # розглядаємо 4 точки +x,+y +x,-y -x,+y -x,-y
                        z1 = (-1) ** h1
                        z2 = (-1) ** h2
                        xxx = xx * z1
                        yyy = yy * z2
                        # координати x y, додаємо x
                        XYZ.append(xxx)
                        # координати x y, додаємо y
                        XYZ.append(yyy)
                        # координати x
                        XXZ.append(xxx)
                        # координати y
                        YYZ.append(yyy)
Nxyz = int(len(XYZ) / 2)

print(' ')
pema(XXZ, '238 x=   ')
pema(YYZ, '239 y=   ')
print('y = ∞ особливі точки 2 порядку Zx = ', Zx, "кількість = ", Nx)
print('x = ∞ особливі точки 4 порядку Zy = ', Zy, "кількість = ", Ny)
print('порядок кривої = ', Nxyz + Nx + Ny)

# порядок точки
P = []
x3 = 0
y3 = 0
ai = inv(a,m)
```

```
print('Порядок точок:')
xr = 0
yr = 0
xn = 0
yn = 0
R = len(XXZ)
pt = 0
# номер точки кривої із масивів XXZ і YYZ
for r in range(0, R):
        xxr = XXZ[r]
        # поточна точка № r P(r)
        yyr = YYZ[r]
        # зберігаємо точку № r, для якої розраховуємо порядок
        xr = xxr
        yr = yyr
        x1i = inv(xxr, m)
        y1i = inv(yyr, m)
        xd = 0
        yd = 0
        # складаємо точки № r P(r) v разів
        for v in range(1, m + 1):
                if v == 2:
                        # зберігаємо подвійну точку
                        xd = xxr
                        yd = yyr
                # нейтральна точка
                if xxr == 1 and yyr == 0:
                        pt = v
                        P.append(pt)
                        break
```

```
                # sum помножуємо на v, v*P(r)
                (x3, y3) = sum(xr, yr, xxr, yyr, a, d, m)
                if x3 == '00':
                        # розраховуємо через попередню точку
                        (x3, y3) = sum(xd, yd, xn, yn, a, d, m)
                # зберігаємо попередню точку
                xn = xxr
                yn = yyr
                # готуємо нову точку
                xxr = x3
                yyr = y3
        else:
                P.append('-')
Jc = (16 * (a ** 2 + d ** 2 + 14 * a * d) ** 3) % m
Jz = ((a * d) * (a - d) ** 4) % m
Jzo = pow(Jz, m-2, m)
J = (Jc * Jz) % m
# J-інваріант
print('J = ', J)

# вивід списку X
i = 0
print(" ")
print("288 x= ", end='')
while (i < m):
        print('%5d' % i, end='')
        i = i+1
print('\n',end='')

pema(XXZ, '294 x= ')
```

```
pema(YYZ, '295 y= ')
pema(P, '296 p= ')

# пошук точки L-го порядку
# размір масиву порядків
lp = len(P)
S = []
NA = []
a = a ** L
z = 0
# переглядаємо список всіх порядків
for i in range(0, lp - 1):
        # ключ, щоб пропустити наступну точку, у якої той же альфа
        if z == 1:
                z = 0
        else:
                # знайти номер точки порядку l
                if P[i] == L:
                        # x координата точки порядку l
                        s = XXZ[i]
                        # масив координат x точок порядку l
                        S.append(s)
                        NA.append(i)
                        z = 1
# размір масиву координат x
ls = len(S)
A = 1
for i in range(0, ls):
        A = A * S[i] % m
A8 = A ** 8 % m
```

```
dL = d ** L % m
ds = A8 * dL % m
# N - число точок, всього (840)
print('a = ', a, 'd = ', d, 'N = ', Nxyz + Nx + Ny, 'L = ', L, 'A = ', A, 'ds = ', ds)
# alfa x координати ядра точок L-го порядку
print('alfa = ', S)
# NA номери x координат у списку
print('NA = ', NA)

# розраховуємо число точок кожного порядку
NP = []
NPM = set(P)
for m in NPM:
        NP.append(m)
NP.sort()
print('Порядки точок:')
pema(NP, 'NP = ')
# CP кількість порядків точок
CP = []
for i in range(0, len(NP)):
        # заготовка списку CP з нулями
        CP.append(0)
# переглядаємо список порядків точок P
for k in range(0, len(P) - 1, 2):
        # порядок поточної точки TP
        TPK = P[k]
        # номер поточної точки у списку порядків NP
        NPK = NP.index(TPK)
        # знаходимо елемент з числом точок поточного порядку
        CPT = CP[NPK]
```

```
        # точки завжди йдуть парами
        CPT = CPT + 2
        # збільшуємо число точок поточного порядку на 2
        CP[NPK] = CPT
# кількість точок порядку P
pema(CP, 'CP = ')
```

Додаток Б

АКТ ВПРОВАДЖЕННЯ В КИЇВСЬКОМУ СТОЛИЧНОМУ УНІВЕРСИТЕТІ ІМЕНІ БОРИСА ГРІНЧЕНКА

КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ БОРИСА ГРІНЧЕНКА

ФАКУЛЬТЕТ
ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
ТА МАТЕМАТИКИ
вул. Левка Лук'яненка, 13-Б, м. Київ, Україна, 04207
Тел.: +380 44 428-34-14
fitm.kubg.edu.ua, fitm@kubg.edu.ua

BORYS GRINCHENKO
KYIV METROPOLITAN UNIVERSITY

FACULTY
OF INFORMATION TECHNOLOGIES
AND MATHEMATICS
13-B Levka Lukianenka St, Kyiv, Ukraine, 04207
Tel.: +380 44 428-34-14
fitm.kubg.edu.ua, fitm@kubg.edu.ua

12.09.2024 № 18/1

АКТ
про впровадження результатів дисертаційного дослідження
Абрамова Сергія Вадимовича
на тему «Моделі і методи підвищення швидкодії алгоритму CSIDH на основі суперсингулярних скручених кривих Едвардса»,
поданої на здобуття наукового ступеня доктора філософії
зі спеціальності 125 Кібербезпека

Цим Актом, ґрунтуючись на рішенні кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка, засвідчуємо, що нижчеперелічені наукові положення, а саме:

- метод підвищення швидкодії криптосистеми CSIDH шляхом використання замість одної циклічної повної кривої Едвардса двох нециклічних кривих з випадковим вибором однієї з кривих пари;

- модель інкапсуляції ключа CSIKE з рандомізацією з одним сеансом передачі і одним відкритим ключем замість двох у порівнянні з CSIDH;

- метод обчислення і вибору структури ізогеній у криптоалгоритмах CSIDH на кривих Едвардса;

- метод CRS на несуперсингулярних (ординарних) кривих.

Розроблені особисто Абрамова Сергієм Вадимовичем у ході проведення ним дисертаційних досліджень та отримали високу оцінку при обговоренні на засіданнях кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики

Київського столичного університету імені Бориса Грінченка.

Зазначені наукові результати:

по-перше, впроваджені в освітній процес кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка у робочих програмах навчальних дисциплін спеціальності 125 Кібербезпека за захист інформації першого (бакалаврського), другого (магістерського) та третього (освітньо-наукового) рівнів вищої освіти;

по-друге, впроваджені в програмно-апаратне забезпечення лабораторій безпеки інформаційних активів, антивірусного захисту інформації, систем технічного та криптографічного захисту інформації.

Дослідження Абрамова Сергія Вадимовича відповідає всім вимогам до організації наукового пошуку та дає позитивний результат у практичному застосуванні.

Декан
Факультету інформаційних технологій та математики
кандидат фізико-математичних наук,
старший науковий співробітник Оксана ЛИТВИН

Додаток В

АКТ ВПРОВАДЖЕННЯ В ІНСТИТУТІ ПРОГРАМНИХ СИСТЕМ НАЦІОНАЛЬНОЇ АКАДЕМІЇ НАУК УКРАЇНИ

ЗАТВЕРДЖУЮ
Директор Інституту програмних систем
Національної академії наук України
_____ Ігор СІНІЦИН
02 вересня 2024 року

АКТ
впровадження матеріалів дисертаційних досліджень
Абрамова Сергія Вадимовича
на тему:
«Моделі і методи підвищення швидкодії алгоритму CSIDH на основі суперсингулярних скручених кривих Едвардса»

Комісія у складі:
голова комісії – заступник директора з наукової роботи Шевченко В.Л.;
члени комісії:
учений секретар Дергильова О.В.
заступник завідувача відділу Ігнатенко П.П.

Встановила та цим актом засвідчує, що нижчеперелічені матеріали дисертаційних досліджень Абрамова Сергія Вадимовича, а саме:
- метод підвищення швидкодії криптосистеми CSIDH шляхом використання замість одної циклічної повної кривої Едвардса двох нециклічних кривих з випадковим вибором однієї з кривих пари;
- модель інкапсуляції ключа CSIKE з рандомізацією з одним сеансом передачі і одним відкритим ключем замість двох у порівнянні з CSIDH;
- метод обчислення і вибору структури ізогеній у криптоалгоритмах CSIDH на кривих Едвардса;
- метод CRS на несуперсингулярних (ординарних) кривих.

Впроваджені в Інституті програмних систем Національної академії наук України. Надані матеріали були використані при формуванні плану перспективних досліджень. Даний акт не є підставою для фінансових зобов'язань.

Голова комісії Віктор ШЕВЧЕНКО
Члени комісії Олена ДЕРГИЛЬОВА
Петро ІГНАТЕНКО