НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ПОЛІТЕХНІКА»

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ПОЛІТЕХНІКА»

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова

праця на правах рукопису

ХАМІТОВ ВІТАЛІЙ МИКОЛАЙОВИЧ

УДК 004.93

ДИСЕРТАЦІЯ

МОДЕЛІ ТА МЕТОДИ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ТА ЦІЛІСНОСТІ ОБМІНУ ЗОБРАЖЕННЯМИ ДЛЯ ГРУПИ ДОВІРЕНИХ КОРИСТУВАЧІВ

Спеціальність: 122 – «Комп’ютерні науки»

Галузь знань: 12 – «Інформаційні технології»

Подається на здобуття наукового ступеня доктора філософії

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

_____ В. М. Хамітов

Науковий керівник:

Антощук Світлана Григорівна, доктор технічних наук, професор

Одеса – 2026

АНОТАЦІЯ

Хамітов В. М. Моделі та методи підвищення конфіденційності та цілісності обміну зображеннями для групи довірених користувачів. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки» (12 – Інформаційні технології). – Національний університет «Одеська політехніка», МОН України, Одеса, 2026.

У вступі обґрунтовано актуальність роботи, що пов’язана з розробкою моделі та методів підвищення конфіденційності та цілісності обміну зображеннями для групи довірених користувачів. Визначено об'єкт, предмет, мету, задачі та методи дослідження; наведено наукову новизну та практичне значення отриманих результатів; висвітлено особистий внесок здобувача, наведено основні дані щодо апробації роботи, публікацій, відомості про структуру та загальну характеристику дисертаційної роботи.

В першому розділі дисертаційної роботи проведено аналіз проблеми підвищення конфіденційності та цілісності обміну зображеннями для групи довірених користувачів.

Проаналізовано основні підходи до підвищення конфіденційності та цілісності обміну зображеннями для групи довірених користувачів. Визначено, що однією з перспективних тем досліджень для підвищення конфіденційності та цілісності є захисне перетворення зображень на основі хаотичних відображень. За результатами проведеного аналізу сформульовано мету та завдання досліджень.

У другому розділі дисертаційної роботи розроблено метод генерації псевдовипадкових послідовностей на основі відображення Тент.

Для порівняння якості захисних перетвореннь зображень різними методами на підставі відомих метрик якості та можливості проводити обґрунтований вибір потокових та блочних шифрів запропоновано сформувати

інтегральний критерій якості шифрування, який поєднує кореляційні, ентропійні метрики та метрику резистентності.

Сформульовано перший пункт наукової новизни: удосконалено інтегральний критерій якості шифрування, який поєднує різні метрики якості шифрування (кореляційні, ентропійні та метрики резистентності), побудований методом ідеальної точки, що дозволило проводити комплексне оцінювання якості шифрування та проводити обґрунтований вибір потокових та блочних шифрів.

У розділі пропонується нова динамічна система, а саме узагальнене відображення Тент з управлінням, яке стабілізує цикли заданої довжини. Ці цикли залежать від параметрів системи та початкового значення; ці величини є коротким ключем для генерації довгої псевдовипадкової послідовності.

Математичною основою для побудови нових методів генерації псевдовипадкових криптосистем є одновимірне відображення Тент із додатково введеним у це відображення предикативним управлінням.

Запропоновано метод генерації псевдовипадкових послідовностей на основі відображення Тент. Проведено аналіз основних статистичних характеристик розроблених псевдовипадкових послідовностей для заданого ключа, який свідчить про їх псевдовипадковий характер, про відсутність закономірностей між окремими частинами послідовності, що дозволяє рекомендувати їх для використання в криптографічних методах. Перевагою наведеного рішення є коротка довжина ключа та незалежність алгоритму від застосовуваної апаратно-програмної платформи.

На основі запропонованого методу генерації псевдовипадкової послідовності розроблено наступний метод шифрування зображення.

1. Генерується короткий ключ. Ключ зберігається на стороні, що передає, і передається на приймальну сторону.

2. Зображення розглядається як масив елементів, кожному з яких приписаний тривимірний вектор десяткових чисел. Стандартними методами десяткові

послідовності переводяться в бітові. Для шифрування зображення на підставі короткого ключа треба згенерувати псевдовипадкову десяткову послідовність та перевести її в бітову. Далі поелементно скласти по модулю 2 з елементами тривимірного вектору зображення. Це є відомий шифр Вернама (або XOR cipher).

3. Зашифроване зображення передається на приймальну сторону. На приймальній стороні на підставі короткого ключа генерується така сама псевдовипадкова послідовність (десяткова, яка переводиться в бітову) і зашифроване зображення відновлюється також операцією XOR.

Показано, що розроблений метод шифрування зображень працює значно швидше традиційних методів, що дуже важливо для оперативності систем професійного обміну зашифрованими зображеннями. Це пояснюється такими факторами: по-перше, шифр Вернама ґрунтується на простих математичних операціях; по-друге, у цьому шифрі операції розсіювання та перемішування поєднані, тоді як у стандартних шифрах вони виконуються послідовно.

Розроблений метод шифрування зображень за інтегральним показником якості майже не поступається сучасним стандартам потокового та блокового шифрування, що дозволяє його рекомендувати для широкого кола завдань, які пов’язані з підвищенням конфіденційності обміну зображеннями.

Сформульовано другий пункт наукової новизни: запропоновано метод шифрування зображень на основі хаотичного відображення Тент з управлінням, що дозволило на підставі короткого ключа (насіння) генерувати довгу псевдовипадкову послідовність, що значно підвищило швидкодію шифрування та розшифрування при збереженні стійкості шифрування за інтегральним критерієм якості.

В третьому розділі дисертаційної роботи запропонована модель побудови псевдовипадкових послідовностей на основі згорнутих чисел *k*-перетину послідовності Фібоначчі.

Показано, що серед рекурентних цілочисельних послідовностей, які використовуються для аналізу інформації та підвищення її криптозахищеності, найбільш популярною є послідовність Фібоначчі та її узагальнення. У роботі набуло подальше узагальнення чисел Фібоначчі, а саме, запропоновані згорнуті числа *k*-перетину послідовності Фібоначчі. Проведено визначення властивостей отриманих послідовностей, знаходження нових зв'язків між їх елементами. Запропоновано подальший розвиток послідовностей типу Фібоначчі, який заснований на зв'язку між похідними поліномів Чебишева другого роду та власне поліномами Чебишева, а також на зв'язку згорнутих чисел *k*-перетину послідовності Фібоначчі з похідними поліномів Чебишева другого роду через числа Люка. Отримано ряд тотожностей, що пов'язують числа Фібоначчі та числа Люка. Показано, що похідні поліномів Чебишева вищого порядку виявилися ефективним базисом для розв’язку деяких завдань теорії чисел, а саме, побудови нових цілочисельних послідовностей. Таким чином, в результаті дослідження отримано сімейство узагальнених послідовностей зі зростанням вищого порядку і складнішими коефіцієнтами зв'язку, ніж у відомих послідовностей Фібоначчі. Це робить отримані узагальнені послідовності доречними для стиснення розріджених даних, розв’язку низки завдань у сфері забезпечення цілісності інформації. Доведено, що отримані послідовності є оригінальними і згідно з поданою заявою були представлені в онлайн-енциклопедії цілочисельних послідовностей (OEIS) під номерами A395431, A393329, A395902, A396356, що підтверджує потенціал запропонованого підходу до формування різних послідовностей, які можуть бути використані для підвищення надійності інформаційних систем. Запропонована методика дослідження послідовності згорнутих чисел *k*-перетину послідовності Фібоначчі, заснована на принципі відкидання, яка показала потенціал запропонованого підходу до формування

різних послідовностей, що можуть бути використані для підвищення надійності інформаційних систем.

Сформульовано третій пункт наукової новизни: отримала подальший розвиток модель побудови псевдовипадкових послідовностей, яка заснована на зв'язку між похідними поліномів Чебишева другого роду та поліномами Чебишева, а також на зв'язку згорнутих чисел *k*-перетину послідовності Фібоначчі з похідними поліномів Чебишева другого роду через числа Люка, що дало можливість отримати сімейство узагальнених послідовностей Фібоначчі, які можуть бути використані для підвищення рівня забезпечення цілісності інформації при її обміні нею у групі довірених користувачів.

В четвертому розділі розроблено метод оперативного обміну конфіденційними зображеннями для групи довірених користувачів та проведено його дослідження.

Запропоновано методику дослідження ефективності протоколів групового узгодження ключів. Показано, що при формуванні груп довірених користувачів з невеликим числом користувачів та малою динамікою найбільш ефективним є поєднання протоколу Бурместера-Десмедта та еліптичної кривої Монтгомері.

Розроблено метод обміну конфіденційними зображеннями групи довірених користувачів. Конфіденційність зображень забезпечується шифруванням із застосуванням псевдовипадкових послідовностей на основі модифікованого хаотичного відображення Тент. Крім того, розроблено протокол формування групи довірених користувачів, яким дозволено доступ до зображень. Збереження зображень забезпечується шістьма рівнями захисту. Протокол ґрунтується на застосуванні операцій на еліптичних кривих Монтґомері.

Проведено імітаційне моделювання розробленого методу. Моделювання продемонструвало працездатність методу в масштабі часу, близькому до реального, та масштабування на основі швидкодіючого протоколу Бурместера-Десмедта.

Сформульовано четвертий пункт наукової новизни: розроблено метод обміну зображеннями групи довірених користувачів, який відрізняється багаторівневим захистом з застосуванням захисного перетворення на основі модифікованого хаотичного відображення Тент та швидкодіючого протоколу на основі еліптичних кривих Монтґомері, що дозволило підвищити швидкодію шифрування та розшифрування при збереженні стійкості.

Загалом, результати апробації свідчать про практичну придатність запропонованих методів до впровадження в системи реального часу. Висновки, отримані на основі експериментальних вимірювань та порівнянь із базовими підходами, підтверджують доцільність їх використання в інформаційних системах.

Результати дисертаційної роботи отримали впровадження у діяльності державного підприємства Український науково-дослідний інститут медицини транспорту Міністерства охорони здоров'я України» (акт ДПУКРНДІ МТ МОЗ України від 02 березня 2026 р.), у діяльності Військово-медичного клінічного центру Південного регіону (довідка від 05 березня 2026 р.) та знайшли відображення у навчальному та науково-дослідницькому процесі Національного університету «Одеська політехніка».

Ключові слова: інформаційні технології, перетворення зображень, шифрування, протоколи групового обміну інформацією, критерій якості перетворення зображень, детермінований хаос, хаотичне відображення Тент, *k*-перетини послідовності Фібоначчі.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Праці, які відображають основні наукові результати дисертації

1. *Dmitrishin D. V.; Khamitov V. M.; Antoshchuk S. G.; Boltenkov V. O.* A Modified Image Encryption Algorithm Based on the chaotic Tent Map. *Herald of*

Advanced Information Technology . 2026. 9(1). P. 9–19. https://doi.org/10.15276/hait.09.2026.01. *Видання включено до переліку наукових фахових видань України (категорія А). Видання включено до наукометричної бази SCOPUS*

https://hait.od.ua/index.php/journal/article/view/247

2. *Khamitov, V. M.* .; Dmitrishin, D. V. .; Stokolos, A. M. .; Gray, D. A. . Convolved Numbers of K-Section of the Fibonacci Sequence: Properties, Consequences. *Herald of Advanced Information Technology*. 2026. 9 (2). P. 129–139. https://doi.org/10.15276/hait.09.2026.09. *Видання включено до переліку наукових фахових видань України (категоріяБ). Видання включено до наукометричної бази SCOPUS.*

https://hait.od.ua/index.php/journal/article/view/247

3. *Khamitov V. M.* .; Boltenkov V. O. .; Antoshchuk S. G. A Method for Operative Sharing Confidential Images Among a Group of Trusted Users. AAIT. 9 (2). P. 200 -207. https://doi.org/10.15276/aait.09.2026.14. *Видання включено до переліку наукових фахових видань України (категорія Б)* .https://aait.od.ua/index.php/journal/article/view/252

4. *V. Khamitov*, S. Antoshchuk. Application of nonlinear discrete maps to construct pseudo-chaotic cryptosystems . *Proceedings of Odessa Polytechnic University*, 2025. Issue 2(72). P. 186-203. https://doi.org/10.15276/opu.2.70.2024.19. *Видання включено до переліку наукових фахових видань України (категорія Б)*

https://pratsi.op.edu.ua/index.php/pratsi/article/view/558

5. *Dyadyura, K., Prokopovich, I., Khamitov, V., Sikach, T., Vershkov, O.* Application of the Dynamic Programming Method in Process Measurement Problems When Assessing Interoperability. *Lecture Notes in Mechanical Engineering.* 2025. P. 699–711. https://DOI: 10.1007/978-3-031-82746-4_62

Видання включено до наукометричної бази SCOPUS

6. *Dyadyura K., Oborskyi G., Prokopovych I., Khamitov V., Holubiev M.* (2024). Optimal management in the operation of complex technical systems. *Journal of*

Engineering Sciences (Ukraine). 2024. Vol. 11(1). P. B1–B9. https://doi.org/10.21272/jes.2024.11(1).b1. *Видання включено до наукометричної бази SCOPUS.*

Наукові праці апробаційного характеру

7. Дмитришин Д. В., *Хамітов В. М.*, Болтьонков В. О., Антощук С. Г. Використання нелінійних дискретних відображень для побудови псевдохаотичних криптосистем. *Інформатика. Культура. Техніка*. 2025. Т.2. С. 209-214. https://doi.org/10.15276/ict.02.2025.31. *Видання включено до переліку наукових фахових видань України (категорія Б).*

https://ict.od.ua/index.php/journal/uk/issue/view/3

8. *Khamitov V.*, Dmytryshyn D., Gray D., and Stokolos A. Analytic summation of series involving higher-order derivatives of Chebyshev polynomials of the second kind and their applications to convolved linear recurrent sequences arXiv:2605.03200v2 [math.CV] https://doi.org/10.48550/arXiv.2605.03200

9. *Хамітов В. М.*, Болтьонков В. О. Формування інтегрального показника якості шифрування зображень //Global Interdisciplinary Summit: Frontier of Science and Future Technologies. Proceedings of International Scientific and Practical Conference. April 3, 2026 in Khalifa University Campus, Dubai, UAE. Prague: Publishing house Education and Science s.r.o., 2026. P. 143 – 146.

10. *Khamitov Vitaly*, Boltenkov Viktor. Method for exchange of confidential images to a group of trusted users //Collection of Scientific Papers with the Proceedings of the 8th International Scientific and Practical Conference «Global Directions in Scientific Research and Technological Development» (April 6-8, 2026, Valencia, Spain). European Open Science Space. 2026. P. 68 – 70.

11. *Хамітов В.М.*, Болтьонков В.О. Формування інтегрального показника якості шифрування зображень. Сучасні інформаційні технології та системи штучного інтелекту: матеріали 2-ї Міжнародної науково-практичної

конференції. Частина 2. Харків -Яремче, 27-29 квітня 2026 р. – Х.: ХНУРЕ, 2026. С. 44-45

12. *Хамітов В.М*. Аналіз можливостей формування групи довірених користувачів для роботи із конфіденційними зображеннями *Матеріали XVI Міжнародної наукової конференції «Modern Information Technology – 2026»*, Одеса, 14–15 травня 2026 р. С. 179 – 180.

13. *В. Хамітов*, В. Болтьонков, С. Антощук. Система обміну конфіденційними зображеннями у групі довірених користувачів для медичного закладу. Сучасні технології біомедичної інженерії : матеріали *V Міжнародної науково-технічної конференції (6−8 травня 2026 р., м. Одеса, Україна).Odesa : Ecologiya, 2026. С. 182-184.

ABSTRACT

Khamitov V. M. Models and methods for increasing the confidentiality and integrity of image sharing for a group of trusted users . – Qualification scientific work in the form of a manuscript.

Dissertation for the degree of Doctor of Philosophy in the specialty 122 "Computer Science" (12 - Information Technologies). – Odesa National Polytechnic University, Ministry of Education and Science of Ukraine, Odessa, 2026 .

The introduction substantiates the relevance of the work, which is related to the development of a model and methods for increasing the confidentiality and integrity of image exchange for a group of trusted users . The object, subject, goal, tasks and methods of the research are determined; the scientific novelty and practical significance of the results obtained are given; the personal contribution of the applicant is highlighted, basic data on the approbation of the work, publications, information on the structure and general characteristics of the dissertation work are given .

The first chapter of the dissertation analyzes the problem of increasing the confidentiality and integrity of image sharing for a group of trusted users .

The main approaches to increasing the confidentiality and integrity of image exchange for a group of trusted users are analyzed . It is determined that one of the promising research topics in increasing confidentiality and integrity is protective image transformation based on chaotic mappings .

Based on the results of the analysis, the goal and objectives of the research were formulated.

In the second chapter of the dissertation, a method for generating pseudorandom sequences based on the Tent mapping is developed .

To compare the quality of encryption by different methods based on known quality metrics and the ability to make a reasoned choice of stream and block ciphers, it is proposed to form an integral quality metric.

The first point of scientific novelty has been formulated: an integrated encryption quality criterion has been improved, which combines various encryption quality metrics (correlation, entropy, and resistance metrics), constructed using the ideal point method, which allowed for a comprehensive assessment of encryption quality and a reasoned selection of stream and block ciphers.

In this chapter, we propose a new dynamical system, namely a generalized Tenth mapping with control, which stabilizes cycles of a given length. These cycles depend on the system parameters and the initial value; these quantities are a short key for generating a long pseudorandom sequence.

The mathematical basis for constructing new methods for generating pseudorandom cryptosystems is the one-dimensional Tent mapping with predicative control additionally introduced into this mapping.

A method for generating pseudorandom sequences based on the Tent mapping is proposed. An analysis of the main statistical characteristics of the developed pseudorandom sequences for a given key is carried out, which indicates their pseudorandom nature, the absence of regularities between individual parts of the sequence, which allows us to recommend them for use in cryptographic methods.

The advantage of the presented solution is the short key length and the independence of the algorithm from the hardware and software platform used.
Based on the proposed method of generating a pseudorandom sequence, the following image encryption method was developed.

1. A short key is generated. The key is stored on the transmitting side and transmitted to the receiving side.

2. An image is represented as an array of elements, each assigned a three-dimensional vector of decimal values. Using standard methods, these decimal sequences are converted into bit sequences. To encrypt the image using a short key, a pseudo-random decimal sequence is generated and transformed into bit sequences. These sequences are then added element-by-element modulo 2 to the components of the three-dimensional image vector. This method is widely known as the Vernam cipher (or XOR cipher).

3. The encrypted image is transmitted to the receiving side. On the receiving side, the exact same pseudo-random sequence is generated based on the short key (the decimal sequence is converted into a bit sequence), and the encrypted image is decrypted using the same XOR operation.

It is shown that the developed image encryption method works much faster than traditional methods, which is very important for the efficiency of professional encrypted image exchange systems. This is explained by the following factors: first, the Vernam cipher is based on simple mathematical operations; second, in this cipher, the scattering and scrambling operations are combined, while in standard ciphers they are performed sequentially.

The developed method of image encryption using the integral quality indicator is almost as good as modern standards of stream and block encryption, which allows it to be recommended for a wide range of tasks related to increasing the confidentiality of image exchange .

The second point of scientific novelty is formulated: a method of image encryption based on a chaotic Tent mapping with control is proposed, which allows

generating a long pseudo-random sequence based on a short key (seed), which significantly increases the speed of encryption and decryption while maintaining the stability of encryption according to the integral quality criterion.

In the third chapter of the dissertation, a model for constructing pseudorandom sequences based on the collapsed numbers of the k - section of the Fibonacci sequence is proposed.

It is shown that among recurrent integer sequences used for data analysis and enhancing information cryptographic security, the Fibonacci sequence and its generalizations are the most popular. This paper further generalizes Fibonacci numbers by proposing the convolved numbers of the k-section of the Fibonacci sequence. The properties of the resulting sequences are defined, and new relationships between their elements are established. A further development of Fibonacci-type sequences is proposed, based on the connection between the derivatives of Chebyshev polynomials of the second kind and the Chebyshev polynomials themselves, as well as on the connection of convolved numbers of the k-section of the Fibonacci sequence with the derivatives of Chebyshev polynomials of the second kind through Lucas numbers. A series of identities connecting Fibonacci and Lucas numbers has been obtained. It is demonstrated that the higher-order derivatives of Chebyshev polynomials prove to be an efficient basis for solving certain problems in number theory, namely, the construction of new integer sequences. Thus, the study yields a family of generalized sequences with higher-order growth and more complex coupling coefficients than those of the well-known Fibonacci sequences. This makes the obtained generalized sequences suitable for sparse data compression and for solving a number of problems in the field of ensuring information integrity. The originality of the resulting sequences is proven; according to the submitted application, they have been registered in the On-Line Encyclopedia of Integer Sequences (OEIS) under numbers A395431, A393329, A395902, A396356, A396457, and A395532, which confirms the potential of the proposed approach for generating various sequences that can be used to improve the reliability of information systems.

The proposed methodology for studying the sequence of convolved numbers of the *k*-intersection of the Fibonacci sequence is based on the rejection principle, which has demonstrated the potential of the proposed approach for forming various sequences that can be used to enhance the reliability of information systems.

The third point of scientific novelty is formulated: a model for constructing pseudorandom sequences has been further developed, which is based on the connection between the derivatives of Chebyshev polynomials of the second kind and Chebyshev polynomials , as well as on the connection of the collapsed numbers of the *k* - section of the Fibonacci sequence with the derivatives of Chebyshev polynomials of the second kind through Luke numbers, which made it possible to obtain a family of generalized Fibonacci sequences that can be used to increase the level of ensuring the integrity of information when it is exchanged in a group of trusted users.

*In the fourth chapter***,** a method for the rapid exchange of confidential images for a group of trusted users is developed and its research is conducted.

A methodology for studying the effectiveness of group key agreement protocols is proposed. It is shown that when forming groups of trusted users with a small number of users and low dynamics, the most effective is the combination of the Burmester-Desmedt protocol and the Montgomery elliptic curve.

A method for exchanging confidential images of a group of trusted users has been developed. Image confidentiality is ensured by using encryption using pseudo-random sequences based on a modified chaotic Tent mapping. In addition, a protocol for forming a group of trusted users who are allowed access to images has been developed. Image storage is provided by six levels of protection. The protocol is based on the application of operations on Montgomery elliptic curves.

Simulation modeling of the developed method was conducted. The modeling demonstrated the operability of the method on a time scale close to real time and scaling based on the fast Burmester-Desmedt protocol .

The fourth point of scientific novelty is formulated: a method for exchanging images of a group of trusted users has been developed, which is characterized by multi-

level protection using a protective transformation based on a modified chaotic Tent mapping and a high-speed protocol based on Montgomery elliptic curves, which allowed increasing the speed of encryption and decryption while maintaining stability.

In general, the results of the testing indicate the practical suitability of the proposed methods for implementation in real-time systems. The conclusions obtained on the basis of experimental measurements and comparisons with basic approaches confirm the feasibility of their use in information systems.

The results of the dissertation work were implemented in the activities of the state enterprise «Ukrainian Scientific Research Institute of Transport Medicine of the Ministry of Health of Ukraine» (act of the State Enterprise Ukrainian Scientific Research Institute of Transport Medicine of the Ministry of Health of Ukraine dated March 2, 2026), in the activities of the Military Medical Clinical Center of the Southern Region (certificate dated March 5, 2026) and were reflected in the educational and scientific research process of the Odesa National Polytechnic University .

Keywords: information technology, protective image transformation, encryption, group information exchange protocols, image transformation quality criterion , deterministic chaos, chaotic mapping Tent , *k* - section of the Fibonacci sequence.

LIST OF PUBLICATIONS

Publications where the main scientific results of the dissertation are published

1. Dmitrishin DV; *Khamitov V.M* .; Antoshchuk SG; Boltenkov VO A Modified Image Encryption Algorithm Based on the chaotic Tent Map. *Herald of Advanced Information Technology* . 2026. 9(1). R. 9–19.

https://doi.org/10.15276/hait.09.2026.01 .

The publication is included in the scientometric SCOPUS databases

https://hait.od.ua/index.php/journal/article/view/247

2. Khamitov *V.M.*; Dmitrishin D.V.; Stokolos A.M.; Gray D.A. Convolved Numbers of K-Section of the Fibonacci Sequence: Properties, Consequences. *Herald of Advanced Information Technology* . 2026. 9 (2). R. 129–139. https://doi.org/10.15276/hait.09.2026.09 . *The publication is included in the scientometric SCOPUS database* .

https://hait.od.ua/index.php/journal/article/view/247

3. *Khamitov V. M.*; Boltenkov V.O.; Antoshchuk S.G. A Method for Operative Sharing Confidential Images Among a Group of Trusted Users. AAIT. 9 (2). P. 200 - 207. https://doi.org/10.15276/aait.09.2026.14 . *The publication is included in the list scientific professional publications of Ukraine (category B).* https://aait.od.ua/index.php/journal/article/view/252

4. *V. Khamitov* , S. Antoshchuk. Application of nonlinear discrete maps to construct pseudo-chaotic cryptosystems. *Proceedings of Odessa Polytechnic University* , 2025. Issue 2(72). R. 186-203. https://doi.org/10.15276/opu.2.70.2024.19 . *The publication is included in the list scientific professional publications Ukraine (category B)*

https://pratsi.op.edu.ua/index.php/pratsi/article/view/558

5. Dyadyura , K., Prokopovich, I., *Khamitov , V.* , Sikach , T., Vershkov, O. Application of the Dynamic Programming Method in Process Measurement Problems When Assessing Interoperability. *Lecture Notes in Mechanical Engineering.* 2025. R. 699–711. https://DOI: 10.1007/978-3-031-82746-4_62 *Edition included to scientometric SCOPUS databases*

6. Dyadyura K., Oborskyi G., Prokopovych I., *Khamitov V.* , Holubiev M. (2024). Optimal management in the operation of complex technical systems. *Journal of Engineering Sciences (Ukraine)*. 2024. Vol. 11(1). R. B1–B9. https://doi.org/10.21272/jes.2024.11(1).b1 . *The edition is included in the scientometric edition SCOPUS database* .

Scientific works of approbation character

7. Dmytryshyn D. V., *Khamitov V. M.* , Boltyonkov V. O., Antoshchuk S. G. Use nonlinear discrete mappings for construction pseudo-chaotic cryptosystems . *Informatics.Culture. Technology*. 2025. Vol. 2. P. 209-214. https://doi.org/10.15276/ict.02.2025.31 .

8. *Khamitov V.* , Dmytryshyn D., Gray D., and Stokolos A. Analytic summation of series involving higher-order derivatives of Chebyshev polynomials of the second kind and their applications to convolved linear rec*urrent sequences arXiv:2605.03200v2 [math.CV] https://doi.org/10.48550/arXiv.2605.03200

9. *Khamitov V. M.* , Boltyonkov V. O. Formation integral indicator qualities encryption images //Global Interdisciplinary Summit: Frontier of Science and Future Technologies. Proceedings of International Scientific and Practical Conference. April 3, 2026 in Khalifa University Campus, Dubai, UA E . Prague : Publishing house Education and Science s.r.o. , 2026. R. 143 - 146.

10. *Vitaly Khamitov*, Viktor Boltenkov . Method for exchange of confidential images to a group of trusted users //Collection of Scientific Papers with the Proceedings of the 8 th International Scientific and Practical Conference "Global Directions in Scientific Research and Technological Development" (April 6-8, 2026, Valencia, Spain). European Open Science Space. 2026. R. 68-70.

11. *Khamitov V. M.* , Boltenkov V. O. Formation integral indicator qualities encryption images . Modern informational Artificial intelligence technologies and systems : materials of the 2nd International scientific and practical Conferences . Part 2. Kharkiv -Yaremche, April 27-29 , 2026. – Kh.: KhNURE, 2026. P. 44-45

12. *Khamitov V.M.* Analysis opportunities formation of a group of trustees users for work from confidential images *Materials of the XVI International scientific Conference "Modern Information Technology - 2026"* , Odessa, May 14–15, 2026. Pp. 179 – 180.

13. *V. Khamitov* , V. Boltyonkov , S. Antoshchuk . Exchange system confidential images in the group trusted users for a medical institution. Modern technologies of biomedical engineering: materials of the Vth International scientific and technical conference (May 6−8, 2026, Odessa, Ukraine) . Odesa : Ecologiya , 2026. P. 182-184.

ЗМІСТ

ВСТУП

Актуальність теми. Дисертаційну роботу присвячено актуальному завданню розробці моделі та методів підвищення конфіденційності та цілісності обміну зображеннями високої роздільної здатності для групи довірених користувачів. У дисертаційній роботі на основі отриманих теоретичних та експериментальних досліджень знайдено рішення важливого науково-технічного завдання побудови методів підвищення конфіденційності та цілісності обміну зображеннями для групи довірених користувачів на основі хаотичних відображень та послідовностей.

Незважаючи на чисельні дослідження, що присвячені вирішенню цього завдання, які пов’язані з удосконаленням методів захисних перетворень (шифрування) зображень, їх використання обмежується не тільки можливостями забезпечення конфіденційності та цілісності, а й їхньою швидкодією та залежністю від програмно-апаратної реалізації, тобто та ресурсозалежністю. Це призводить до протиріччя між затребуваністю методів захисних перетворень зображень, що ґрунтуються на хаотичних відображеннях, з одного боку, та обмеженнями щодо їх використання, що пов’язані з показниками швидкодії та ресурсозалежності, з другого.

Це протиріччя може бути усунене за рахунок вирішення актуальної та важливої науково-прикладної задачі, яка полягає в підвищенні конфіденційності та цілісності обміну зображеннями для групи довірених користувачів шляхом удосконалення моделей та методів захисного перетворення зображень на основі хаотичних відображень для підвищення швидкодії та/або зменшення ресурсозалежності.

Зв’язок роботи з науковими програмами, планами, темами. Дисертаційну роботу виконано у відповідності до пріоритетних тематичних напрямів наукових досліджень і науково-технічних розробок на період до 31 грудня року, наступного після припинення або скасування воєнного стану в

Україні (Постанова Кабінету Міністрів України від 30.04.2024 р. № 476), згідно п. 1.2.1.1, 1.2.1.4, 1.2.4.6 і 1.2.1.7 «Основних наукових напрямів та найважливіших проблем фундаментальних досліджень у галузі природничих, технічних, суспільних і гуманітарних наук Національної академії наук України на 2019–2023 роки» (постанова Президії НАН України від 30.01.2019 р. № 30) та також у відповідності до планів науково-дослідних робіт Національного університету «Одеська політехніка» при виконанні держбюджетної теми: НДР роботи № 719-61/161 – «Інтелектуальна підтримка прийняття рішень при проєктуванні кісткових замінників для лікування воєнних травм» (номер державної реєстрації 0124U000388).

Дисертант приймав участь у виконанні вказаних тем як співвиконавець (акт впровадження від 25.12.2025) (Додаток Г).

Метою дослідження є підвищення рівня забезпеченості конфіденційності та цілісності цифрових зображень шляхом удосконалення методів захисних перетворень на основі хаотичних відображень.

Для досягнення мети дослідження необхідно вирішити такі завдання:

– провести аналіз основних проблем, обмежень та викликів, які виникають задачах створення механізмів забезпечення конфіденційності та цілісності обміну зображеннями для групи довірених користувачів;

– удосконалити критерій якості шифрування для оцінки якості шифрування зображень;

– удосконалити метод шифрування цифровими зображень на основі хаотичного відображення Tent з управлінням;

– удосконалити модель побудови псевдовипадкових послідовностей Фібоначчі;

– розробити метод обміну цифровими зображеннями для групи довірених користувачів;

– провести експериментальні дослідження, апробацію і впровадження отриманих теоретичних результатів.

Об’єкт дослідження – процес обміну цифровими зображеннями для групи довірених користувачів зображення.

Предмет дослідження – моделі та методи забезпечення конфіденційності та цілісності обміну зображеннями для групи довірених користувачів.

Методи дослідження – системний аналіз; процесний підхід – для вивчення процесів, які відбуваються при обміні цифровими зображеннями для групи довірених користувачів; дискретна математика та теорія множин – для опису моделей з застосуванням хаотичних відображень та послідовностей; стеганографічні методи та теорія динамічних систем для удосконалення методів підвищення конфіденційності та цілісності обміну зображеннями для групи довірених користувачів.

Наукова новизна отриманих результатів. Основний науковий результат полягає у розв’язанні важливої науково-практичної задачі підвищення конфіденційності та цілісності обміну зображеннями для групи довірених користувачів в інформаційних системах прикладного призначення.

У рамках виконаних досліджень отримано такі наукові результати:

1. удосконалено інтегральний критерій якості захисних перетворень, який поєднує різні метрики якості шифрування (кореляційні, ентропійні та метрики резистентності), що побудований методом ідеальної точки, що дозволило проводити комплексне оцінювання якості шифрування та проводити обґрунтований вибір потокових та блочних шифрів;

2. запропоновано метод захисного перетворення зображень на основі хаотичного відображення Тент з управлінням, що дозволило на підставі короткого ключа (насіння) згенерувати довгу псевдовипадкову послідовність, що значно підвищило швидкодію шифрування та дешифрування при збереженні стійкості шифрування за інтегральним критерієм якості;

3. отримала подальший розвиток модель побудови псевдовипадкових послідовностей, яка заснована на зв'язку між похідними поліномів Чебишева другого роду та поліномами Чебишева, а також на зв'язку згорнутих чисел k-

перетину послідовності Фібоначчі з похідними поліномів Чебишева другого роду через числа Люка, що дало можливість отримати сімейство узагальнених послідовностей Фібоначчі, які можуть бути використані для підвищення рівня забезпечення цілосності інформації при її обміні у групі довірених користувачів;

4. розроблено метод обміну зображеннями групи довірених користувачів, який відрізняється багаторівневим захистом з застосуванням захистного перетворння на основі модифікованого хаотичного відображення Тент та швидкодіючого протоколу на основі еліптичних кривих Монтґомері, що дозволило підвищило швидкодію шифрування та дешифрування при збереженні стійкості.

Практичне значення одержаних результатів. Розроблений в дисертаційній роботі метод обміну цифровими зображеннями групи довірених користувачів, який відрізняється багаторівневим захистом з застосуванням шифрування на основі модифікованого хаотичного відображення Тент, дозволив підвищити швидкодію шифрування та розшифрування при збереженні стійкості.

Розроблена в дисертаційній роботі модель побудови псевдовипадкових послідовностей дозволяє отримати сімейство узагальнених послідовностей Фібоначчі, які можуть бути використані для підвищення рівня забезпечення цілісності інформації для широкого кола завдань криптографічного захисту інформації. Отримані послідовності є оригінальними і згідно з поданою заявою були представлені в енциклопедії OEIS під номером A395431 (Додаток Е).

Розроблені в роботі наукові положення та практичні результати отримали впровадження у діяльності державного підприємства «Український науково-дослідний інститут медицини транспорту Міністерства охорони здоров'я України» (*акт ДПУКРНДІ МТ МОЗ України від 02 березня 2026 р.*) (Додаток Б), у діяльності Військово-медичного клінічного центру Південного регіону (*довідка від 05 березня 2026 р.*) (Додаток В) та знайшли відображення у навчальному (*довідка про впровадження результатів № 2100/61-07 від 30 грудня 2025 року*) (Додаток Д) та у науково-дослідницькому процесі (*довідка про впровадження результатів №*

704/61-07 від 24.04.2026) (Додаток Г) Національного університету «Одеська політехніка».

Особистий внесок здобувача. Основні наукові положення, висновки і рекомендації, що містяться в дисертації та виносяться на захист, отримано здобувачем особисто в період з 2022 по 2026 рік (Додаток А) .

У статті [1] внесок здобувача полягає в розробці методу шифрування зображень виходячи з хаотичного відображення Tent, який дозволив на підставі короткого ключа (насіння) згенерувати довгу псевдовипадкову послідовність; в статті [2] – отримала подальшого розвитку модель побудови псевдовипадкових послідовностей; у статтях [3, 10] – розроблено метод обміну зображеннями групи довірених користувачів, який відрізняється багаторівневим захистом, у статті [4] – запропоновано застосування для формування псевдовипадкових послідовністей нової динамічної системи, а саме узагальнене відображення Тент з керуванням, яке стабілізує цикли заданої довжини; у статті [5, 13] – показано важливість забезпечення захисту інформації в складних організаційно-технічних системах; у статті [6] – показано важливість забезпечення захист інформації в складних організаційно-технічних системах; у роботі [7] – показано доцільність нелінійних дискретних відображень для побудови псевдохаотичних криптосистем; у роботі [8, 11] – запропоновано інтегральний показник якості шифрування зображень; у роботі [9, 12] – досліджено метод обміну конфіденційними зображеннями з групою довірених користувачів.

Апробація результатів дисертації. Основні положення і практичні результати дисертаційної роботи доповідалися та одержали схвалення на таких конференціях:

– XI Міжнародній науково-практичній конференції «ІНФОРМАТИКА. КУЛЬТУРА. ТЕХНІКА» «ІКТ-25»;

– 8th International Scientific and Practical Conference «Global Directions in Scientific Research and Technological Development» (April 6-8, 2026, Valencia, Spain);

– International Scientific and Practical Conference. April 3, 2026 in Khalifa University Campus, Dubai, UAE;

– 2-й Міжнародній науково-практичній конференції. Харків -Яремче, 27-29 квітня 2026;

– XVI Міжнародній науковій конференції «Modern Information Technology – 2026», Одеса, 14–15 травня 2026;

– 5th International Scientific and Technical Conference “Modern technologies of biomedical engineering” May 06-08, 2026, Odesa, Ukraine.

Публікації. Основні результати дисертаційної роботи викладено у 13 публікаціях, зокрема 6 статей, з них – 4 статті у фахових періодичних виданнях України з технічних наук, з яких 2 – у категорії А (індексується в Scopus); 2 – у категорії Б, 2 статті у інших виданнях, 7 тез доповідей у матеріалах міжнародних наукових конференцій.

Структура і обсяг роботи. Дисертація складається з вступу, чотирьох розділів, висновків, списку використаних джерел і додатків. Повний обсяг дисертації складає 200 сторінок, в тому числі: 144 сторінки основного тексту, 53 рисунки і 6 таблиць, список використаних джерел зі 102 найменувань і 7 додатків

РОЗДІЛ 1. АНАЛІЗ ПРОБЛЕМИ ОБМІНУ КОНФІДЕНЦІЙНИМИ ЗОБРАЖЕННЯМИ ДЛЯ ГРУПИ ДОВІРЕНИХ КОРИСТУВАЧІВ

Інтенсивний перехід на дистанційні принципи функціонування підприємств та організацій, що спостерігається у глобальних масштабах, призвів до інтенсивного впровадження прикладних інформаційних технологій у процеси обміну даними у вигляді як текстових так і текстографічних документів, що представляються у вигляді цифрових, табличних даних, рисунків, графіків, діаграм, підписів, віз, резолюцій, які є по суті 2-D масивами даних (зображеннями). Тобто обмін зображеннями займає особливе місце у процесах обміну даними в інформаційних системах різного прикладного призначення. Однією з суттєвих проблем для організації обміну зображеннями є необхідність забезпечення високого рівня конфіденційності, цілісності та безпеки інформації, яка передається.

Прикладом галузі, де важливу роль відіграє обмін зображеннями, є медицина, особливо телемедицина – область надання медичної допомоги пацієнтам віддалено, коли пацієнт і постачальник медичних послуг рознесені в просторі. Передача медичних цифрових зображень використовується в багатьох додатках телемедицини: дистанційна хірургія, віддалена діагностика та інших. Рентгенівські знімки, УЗД, результати комп'ютерної томографії, зображення головного мозку та магнітно-резонансної томографії пацієнта, містять конфіденційну інформацію, включаючи особисту. Але передача такої інформації відбувається як по відкритих так й по корпоративних каналах зв'язку. Тому конфіденційність і безпека медичних зображень вкрай важлива для захисту особистої інформації користувачів від доступу неавторизованих осіб.

Іншими прикладами, де обмін зображеннями вимагає високого рівня конфіденційності та безпеки, є результати відеоспостереження для «інтернету речей», супутникові знімки високої роздільної здатності для геоінформаційних систем, доказові зображення для дистанційної судової медицини тощо [1-4].

Швидкий розвиток та впровадження інформаційних технологій (ІТ) та досягнення в області штучного інтелекту (ШІ) супроводжується не лише підвищенням ефективності обробки інформації та зростаючим позитивним впливом на всі сфери сучасного суспільства, але й появою нових загроз інформаційній безпеці. Вони створюють сприятливі умови для зловмисників, оскільки надають можливість перехоплення, знищення, фальсифікації та інших незаконних маніпуляцій з інформацією, яка подана у різних форматах представлення: тестові документи, аудіо файли, зображення та відеофайли тощо. Поєднання ШІ та людського фактору становить особливу небезпеку. У цьому випадку нейронні мережі виступають своєрідним «підсилювачем», підвищуючи як ефективність зловмисників, так і ймовірність помилки користувача. Людина традиційно вважається однією з найслабших ланок в інформаційній безпеці. Хоча використання ШІ суттєво зменшує навантаження на людину, воно також може створити нові ризики, пов'язані з надмірною залежністю від інтелектуальних систем, недостатньою обізнаністю користувачів та неправильним використанням технологій. В результаті зростає ймовірність порушень конфіденційності, цілісності та доступності інформації. Тому дослідження, які пов’язані з підвищенням конфіденційності, цілісності інформації є своєчасними та актуальними.

1.1 Використання захисних перетворень як спосіб забезпечення інформаційної безпеки зображень

Ефективним методом забезпечення інформаційної безпеки зображень є використання захисних перетворень.

1.1.1 Аналіз сучасних захисних перетворень

Проведений аналіз літературних джерел показав, що для забезпечення інформаційної безпеки використовуються такі основні перетворення:

– криптографічні перетворення (шифрування): симетричні шифри (використання одного й того ж ключа для шифрування та розшифрування (блокові шифри, такі як AES та потокові шифри) та асиметричні шифри (двоключове шифрування), використання відкритого та закритого ключа (RSA, шифрування на еліптичних кривих ECC);

– перетворення для контролю цілісності та автентичності: хешування: генерація «відбитка» даних фіксованої довжини, незворотне перетворення (SHA-256, SHA-3), електронний підпис (підтвердження авторства та незмінності документа), коди автентифікації повідомлень із секретним ключем;

– стеганографічні перетворення: обфускація передачі інформації шляхом її вбудовування в «контейнери» (зображення, аудіофайли, цифровий шум).

В основі розробки та реалізації сучасних безпечних перетворень інформації використовуються теоретичні розділи дискретної та прикладної математики.

1.1.2 Вимоги до сучасних захисних перетворень

Цифрова стеганографія розглядає різні методи вбудовування секретних даних, таких як відео, зображення, аудіо, текст або файли, в інші мультимедійні застосунки з використанням закритого ключа. Прихована інформація називається секретним повідомленням, а контейнер, який вбудовується секретний файл, називається файлом-контейнером. Контейнером може бути будь-який мультимедійний файл, наприклад, відео, аудіо, зображення або текст. Отриманий у результаті операції вбудовування файл називається стегофайлом.

Незважаючи на величезні досягнення в галузі стеганографії, рівень впровадження стеганографії у програмних додатках реального часу, де конфіденційність інформації має вирішальне значення, таких як оборонні документи, судово-медичні звіти та медичні зображення, все ще залишається відкритим питання компромісу між можливістю інтеграції та спотворенням файлу контейнера.

Більш надійним способом забезпечення конфіденційності та збереження зображень є їх захисне перетворення шифруванням. Шифрування — це процес перетворення медіаданих таким чином, щоб доступ до них мали лише уповноважені особи (рис. 1). Шифрування запобігає підробці оригінальної інформації та позбавляє неавторизованих осіб доступу до неї. У схемі шифрування оригінальне зображення знаходиться у відкритому вигляді та зашифровано за допомогою алгоритму шифрування.

Рисунок 1.1 – Загальна схема захисного перетворення шифруванням при передачі зображення

Зашифрований файл можна прочитати лише після розшифрування. Основною метою шифрування є збереження конфіденційності переданої інформації. Важливою особливістю будь-якого алгоритму шифрування є використання ключа шифрування, який визначає вибір певного варіанту

перетворення серед можливих для алгоритму. Уповноважений одержувач може легко розшифрувати повідомлення за допомогою автентичного ключа, наданого відправником одержувачам.

Шифрування забезпечує три стани інформаційної безпеки.

Цілісність – запобігання зміні інформації під час передачі або зберігання за допомогою шифрування.

Конфіденційність – приховування інформації від неавторизованих користувачів під час передачі або зберігання за допомогою шифрування.

Ідентифікаційність – автентифікація джерела інформації та запобігання запереченню відправником того, що дані були надіслані ним.

Мета шифрування полягає в тому, щоб забезпечити доступ до даних лише користувачеві; він отримує ключ і алгоритм для розшифрування зашифрованих даних.

В той же час ефективні традиційні способи шифрування текстових файлів, наприклад, стандарт блокового шифрування AES мало придатні для шифрування зображень. Відомо, що між сусідніми пікселями зображення існує висока кореляція. Зображення по своїй природі громіздкі і мають високу надмірність, тому їх важко обробляти традиційними методами шифрування. Крім того, традиційні шифри вимагають для шифрування та розшифрування великого комп'ютерного часу, що практично унеможливлює обмін зображеннями в реальному масштабі часу. Альтернативою у такому разі виступають методи шифрування з урахуванням хаотичних відображень [5-7].

1.2 Аналіз одновимірних хаотичних відображень та їх особливостей

Хаотична динаміка є область прикладної математики, яка досліджує поведінку систем, чутливих до початкових умов. Хаотичні відображення є прикладами таких систем, які демонструють складність простих правил. Хаотичні системи, завдяки своїй складності та непередбачуваності, пропонують

перспективні рішення для забезпечення конфіденційності та цілісності даних. Важливо, що хаотичні системи є випадковими; вони слідують суворим правилам, та їх поведінка може бути непередбачуваною. Незважаючи на свою складність, хаотичні відображення мають свої закони та структури, які можуть бути вивчені та проаналізовані. Хаотичні системи також мають особливі властивості, такі як чутливість до початкових умов, що означає, що навіть невеликі зміни в початкових умовах можуть призвести до значних відмінностей у майбутній поведінці системи. Ця властивість часто ілюструється "ефектом метелика", коли малі зміни можуть призвести до великих наслідків [8] .

Хаотичні відображення знаходять застосування у розробці схем захисту мультимедійних даних, таких як відео та аудіо. Хаотичні системи використовуються для генерації ключів шифрування, які потім застосовуються до потоків даних, забезпечуючи захист від несанкціонованого доступу. Крім того, хаотичні відображення використовуються для створення водяних знаків, які захищають авторські права на цифровий контент. Хаотичні відображення застосовуються для забезпечення конфіденційності та незмінності зображень шляхом шифрування. Шифрування зображень з використанням хаотичних відображень ґрунтується на перетворенні пікселів зображення відповідно до алгоритмів, що базуються на хаотичних функціях. Серед найчастіше використовуваних хаотичних систем виділяють логістичне відображення та відображення Тент. Ці відображення мають сильну чутливість до початкових умов, що забезпечує високий рівень безпеки при шифруванні. Основна ідея полягає в тому, щоб змінити порядок пікселів зображення та їх значення таким чином, щоб відновлення вихідного зображення без знання ключа стало неможливим.

Застосування хаотичних зображень для шифрування зображень має кілька важливих переваг:

– такі методи забезпечують високий рівень складності шифру, що ускладнює його зламування;

– хаотичні системи дозволяють генерувати ключі високої ентропії, що робить їх стійкими до атак шляхом повного перебору.

Одним із популярних підходів до шифрування зображень за допомогою хаотичних відображень є використання методу перестановки пікселів [9]. У цьому випадку координати пікселів змінюються відповідно до хаотичної послідовності, що призводить до значної дезорганізації вихідного зображення. Інший підхід полягає у зміні значень пікселів за допомогою хаотичних функцій, що забезпечує додатковий рівень захисту. Комбінація цих методів дозволяє створювати складніші та надійніші алгоритми шифрування.

Незважаючи на очевидні переваги, використання хаотичних відображень у криптографії має обмеження. Одним із головних викликів є необхідність точного відтворення початкових умов та параметрів системи для успішного розшифрування даних. Навіть невеликі помилки можуть призвести до неможливості відновлення вихідного зображення. Крім того, хаотичні системи можуть бути вразливими до певних типів атак, наприклад, до аналізу їх динамічних властивостей або добору параметрів.

Одними з найвідоміших одновимірних хаотичних відображень є логістичне відображення та відображення Тент. У разі зміни параметрів цих відображень можна спостерігати перехід від стабільного стану до хаотичної поведінки.

Розглянемо два найбільш популярних одновимірних хаотичних відображення та їх особливості [10,11].

1.2.1 Логістичне відображення

Логістичне відображення описується рівнянням:

$$x_{n+1} = r \cdot x_n (1 - x_n),$$

де r – параметр, що визначає ступінь хаосу.

При значеннях r між 3,57 та 4,0 система демонструє хаотичну поведінку. Це відображення дозволяє генерувати складні послідовності, які можуть бути

використані для перемішування пікселів зображення і створення випадкових ключів для шифрування.

Дослідити поведінку відображення можна за допомогою біфуркаційної діаграми. Біфуркаційна діаграма – це графічне уявлення, що показує, як динамічна поведінка системи змінюється залежно від параметра. Біфуркаційна діаграма демонструє, як різні значення параметра r впливають на стійкість та поведінку системи, включаючи переходи від періодичної до хаотичної поведінки. Біфуркаційна діаграма логістичного відображення наведена на рисунку 1.2.

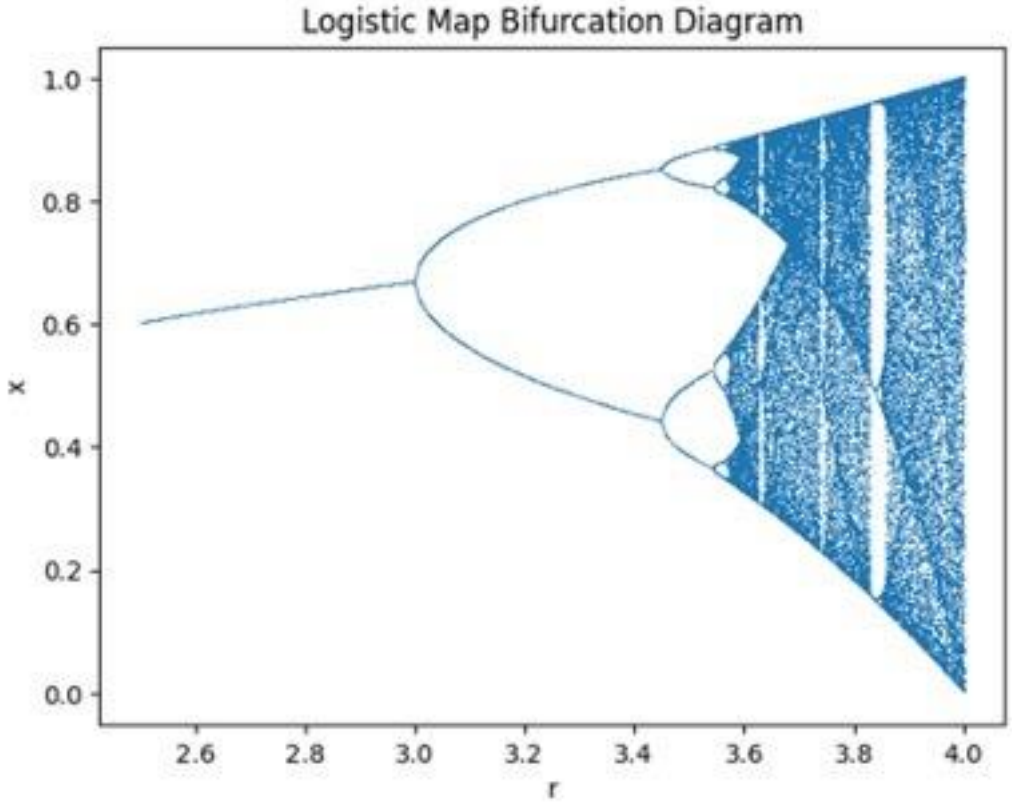


Рисунок 1.2 – Біфуркаційна діаграма логістичного відображення

На рисунку 1.2 спостерігаються основні стадії логістичного відображення.

1. Стабільна рівновага ($0 < r < 3$): При малих значеннях r система завжди прагне однієї фіксованої точки. На графіку це одна суцільна лінія.

2. Подвоєння періоду ($3 < r \approx 3{,}57$): відбувається перша біфуркація – лінія роздвоюється на дві («вилка»). Тепер система не завмирає в одній точці, а коливається між двома значеннями. Зі зростанням *r* цикл подвоюється: 2 точки, потім 4, 8, 16 і так далі. Це називається каскадом Фейгенбаума.

3. Хаос ($r > 3{,}57$): Система стає вкрай чутливою до початкових умов. На діаграмі це схоже на зафарбовані області, де значення розподілені хаотично.

4. Вікна порядку: Навіть усередині хаосу зустрічаються вузькі вертикальні «просвіти» (наприклад, в районі $r \approx 3{,}87$), де система раптово повертається до стабільних циклів (наприклад, періоду 3).

Ще однією характеристикою хаотичних відображень є показник Ляпунова λ (Lyapunov exponent), який кількісно визначає швидкість розбіжності близьких траєкторій, що є ключовою ознакою хаотичної поведінки [12] . На рисунку 1.3 наведено показник Ляпунова для логістичного відображення. Показник Ляпунова кількісно описує хаос у логістичному відображенні: він негативний для періодичних режимів і стає позитивним під час переходу до детермінованого хаосу (після точки $r \approx 3{,}57$).

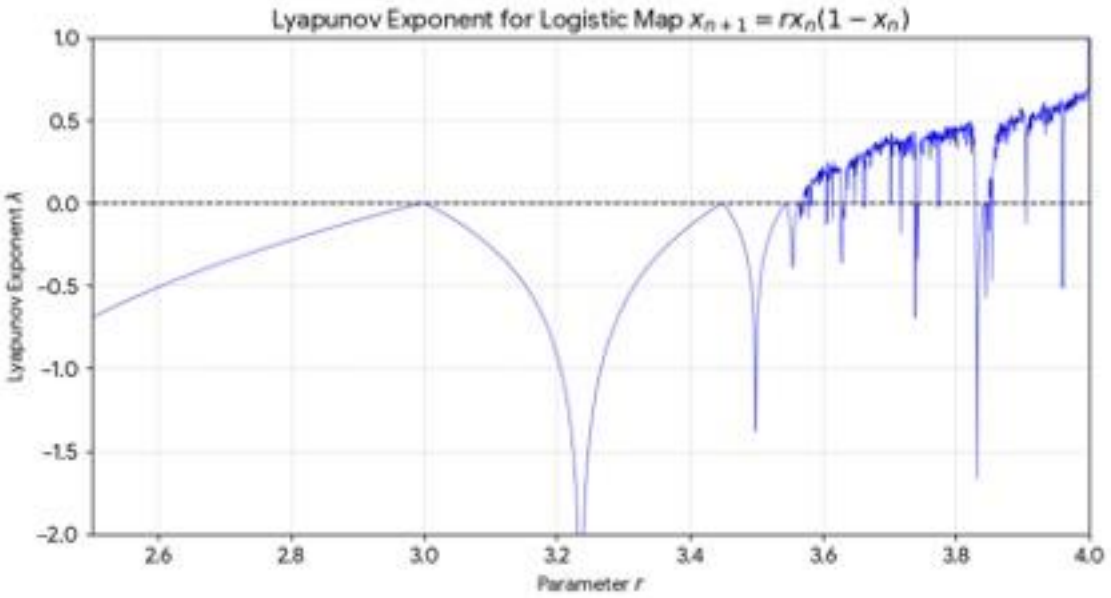


Рисунок 1.3 – Показник Ляпунова для відображення логістики.

1.2.2 Відображення Тент

Відображення Тент (англ. *Tent map*) – проста математична модель, яка використовується для опису хаотичних систем [13]. Назва відображення пов'язана з його графіком, який нагадує форму намету (*tent*) (рис. 1.4)

Формула відображення Тент виглядає наступним чином:

$$x_{n+1} = \begin{cases} \mu x_n, & 0 \le x_n < \frac{1}{2}, \\ \mu(1 - x_n), & \frac{1}{2} \le x_n \le 1, \end{cases}$$

де: x_n – поточне значення;

x_{n+1} – Значення на наступному кроці;

μ – Параметр, що визначає ступінь хаотичності відображення (зазвичай $0 < \mu \le 2$).

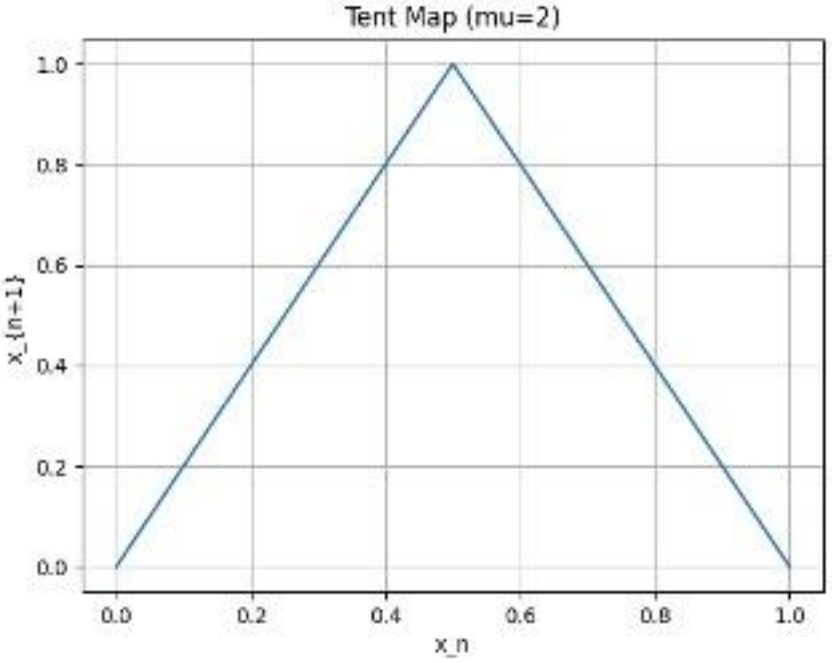


Рисунок 1.4 – Графік відображення Тент.

Біфуркаційна діаграма відображення Тент наведена на рисунку 1.5.

Структура біфуркаційної діаграми. На відміну від логістичного відображення, де перехід до хаосу йде через нескінченний каскад подвоєння періодів (сценарій Фейгенбаума), діаграма Тенту виглядає інакше:

– при $0 < \mu < 1$ єдиною стійкою нерухомою точкою є $x = 0$. Будь-яка траєкторія з часом притягується до нуля;

– при $\mu = 1$ відбувається біфуркація . З'являється континуум нерухомих точок, якщо розглядати граничний випадок, але за $\mu > 1$ точка $x = 0$ втрачає стійкість;

– при $1 < \mu < 2$ с система демонструє хаотичну поведінку, але «наповнює» не весь інтервал [0,1]. Хаос обмежений певною підмножиною (інтервалами), які поступово розширюються і зливаються зі збільшенням μ ;

– при $\mu = 2$ виникає точка "повного хаосу". Відображення стає топологічно пов'язаним логістичним відображенням при $r = 4$. У цьому режимі траєкторія системи щільно заповнює весь інтервал [0,1].

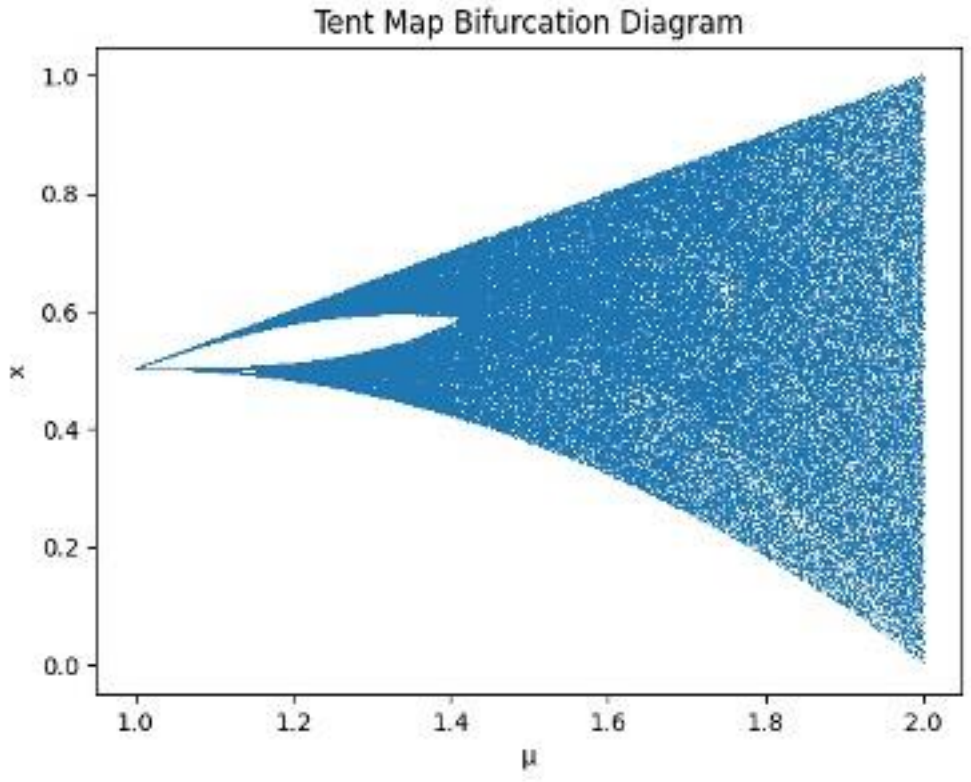


Рисунок 1.5 – Біфуркаційна діаграма відображення Тент

Ключові особливості біфуркаційної діаграми Тент полягають у наступному [14]:

– відсутність вікон періодичності: у класичному відображенні Тент немає стабільних періодичних орбіт, у той час як у логістичному відображенні всередині хаотичної зони зустрічаються острівці порядку;

– чутливість до початкових умов. Система є класичним прикладом детермінованого хаосу.

Біфуркаційні діаграми відображення Тент та логістичного відображення демонструють різний характер динамічної поведінки систем. Відображення Тент має простішу структуру, тоді як логістичне відображення показує складні переходи між періодичними та хаотичними станами.

Картина показника Ляпунова для відображення Тент наведена на рисунку 1.6.

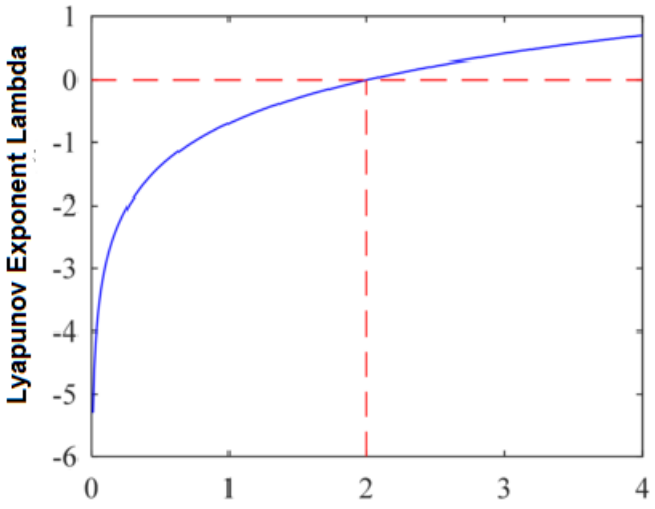


Рисунок 1.6 – Показник Ляпунова відображення Тент

Для відображення Тент показник Ляпунова дорівнює $\lambda = \ln 2\mu$.

Якщо $\mu > 0{,}5$, то $\lambda > 0$ (рис. 1.6), що вказує на хаотичну поведінку системи та чутливість до початкових умов.

Наведені діаграми демонструють наступні особливості відображення Тент:

– простоту реалізації. Тент має просту математичну формулу, що робить його зручним для реалізації в різних додатках, включаючи криптографію і генерацію випадкових чисел;

– хаотичну поведінку. При значенні параметра $\mu>2$ відображення демонструє хаотичну поведінку, коли система стає вкрай чутливою до початкового стану. Навіть мінімальні зміни в початкових умовах призводять до різних результатів;

– можливість застосовуватися у криптографії. Відображення Тент може використовуватися та активно використовується для шифрування даних та генерації псевдовипадкових послідовностей завдяки своїй простоті та хаотичним властивостям при певних параметрах;

– динамічні властивості. Тент має властивість чутливості до початкових умов, і має позитивний показник Ляпунова при $\mu>2$, що підтверджує його хаотичну поведінку. Простір значень обмежений інтервалом [0,1], що спрощує нормалізацію даних;

– ефективність.

Але незважаючи на простоту та хороші статистичні властивості при реалізації, особливо в цифрових системах, Тент має низку істотних недоліків, таких як [15]:

– проблеми точності у цифрових системах. При реалізації на комп'ютері з кінцевою розрядністю хаотичні системи можуть вироджуватися. Замість хаосу орбіти можуть потрапити у короткі цикли, що різко знижує псевдовипадковість послідовності;

– чутливість до точності параметрів. Невеликі зміни параметра або помилки округлення можуть призвести до значних відхилень у поведінці системи, що ускладнює прогнозування довгострокових характеристик;

– аналітичну простота. У криптографічних застосуваннях занадто проста структура відображення тенту (шматково-лінійна) може дозволити атакуючому

відновити ключ або параметри системи, якщо він отримає частину вихідної послідовності;

– не ідеальність рівномірного розподілу. Хоча теоретично Тент відображення забезпечує рівномірний розподіл, дискретна реалізація може призводити до зсувів у розподілі ймовірностей, що потребує додаткових методів постобробки.

Тому для усунення вказаних недоліків Тент відображення запропоновано розробляти захисні перетворення зображень на базі удосконалення відображення Тент.

1.2.3 Шифр Вернама та його зв'язок з хаотичним шифруванням зображень

Шифр Вернама також відомий як одноразовий блокнот (One-Time Pad), є одним із найнадійніших методів шифрування даних. Він був розроблений в 1917 році американським інженером Гілбертом Вернамом і заснований на використанні випадкового ключа, який має бути такою ж довжиною, як і вихідне повідомлення. Основний принцип роботи шифру полягає в побітовій операції XOR між даними та ключем [16] .

Для шифрування зображень використовується той самий принцип – кожен піксель зображення перетворюється за допомогою XOR із відповідним елементом ключа. Це дозволяє отримати повністю зашифроване зображення, яке неможливо розшифрувати без точного ключа.

Базова ідея шифру Вернама виглядає так:

$$C = P \oplus K,$$

$$P = C \oplus K,$$

де: P – відкритий текст (або зображення);

K – ключ (випадкова бітова послідовність);

C – шифртекст;

$\oplus$ – операція XOR (побітове виключне АБО).

Теоретична основа абсолютної криптографічної стійкості була закладена Клодом Шенноном у роботі *Communication Theory of Secrecy Systems* у 1949 р.,

де доведено, що шифр Вернама забезпечує абсолютну криптографічну стійкість (perfect secrecy) при виконанні нижче наведених трьох умов [17].

Умова 1. Ключ має бути абсолютно випадковим.

Умова 2. Довжина ключа і файлу, що шифрується, повинні бути рівні.

Умова 3. Ключ може застосовуватися лише один раз (звідси назва одноразовий блокнот).

На сьогоднішній день шифр Вернама – єдиний симетричний шифр із математично доведеною абсолютною криптографічною стійкістю.

Оскільки випадкові числа існують лише у природі, умову 1 важко виконати у реальних умовах. Зусилля деяких дослідників спрямовані на генерацію випадкових послідовностей.

Як рішення використовують псевдовипадкові послідовності, що генеруються різними алгоритмами, зокрема хаотичними відображеннями.

Шифрування зображення шифром Вернама здійснюється в такий спосіб [18].

1. Зображення перетворюється на бінарний формат попіксельним обходом (рис. 1.7). Кожному пікселю відповідає двійковий код.

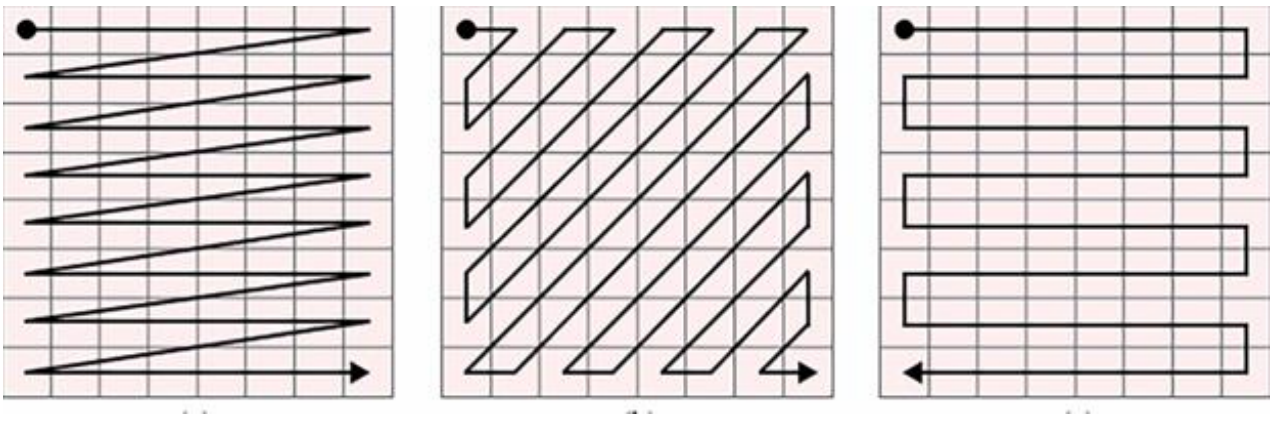


Рисунок 1.7 – Варіанти попіксельного обходу зображення.

2. Для шифрування зображення генерується псевдовипадковий ключ, довжина якого повинна збігатися з кількістю бітів у зображенні.

3. Шифрування: за допомогою операції XOR кожен біт зображення поєднується з відповідним бітом ключа. Це призводить до створення зашифрованого зображення, яке виглядає як довільний набір даних.

$$C_i = P_i \oplus K_i,$$

де C_i – зашифрований біт;

P_i – біт вихідного зображення;

K_i – біт ключа.

4. Розшифрування: Для відновлення вихідного зображення використовується той же ключ. Процес дешифрування також виконується за допомогою операції XOR:

$$P_i = C_i \oplus K_i.$$

Шифр Вернама має наступні переваги при шифруванні зображень:

– абсолютна безпека. При правильному використанні шифр Вернама забезпечує абсолютну безпеку, оскільки кожен можливий ключ рівноймовірний;

– легкість у використанні. Шифрування та розшифрування виконуються за допомогою простих операцій складання за модулем 2;

– збіг прямого та зворотного алгоритмів. Шифрування і розшифрування виконуються за допомогою однакових операцій, що є не типовим для інших симетричних шифрів.

Порівняємо швидкість шифрування зображень шифром Вернама та блочним шифром AES .

Нехай шифрується зображення розміром 1200×800 пікселів. Припустимо, що зображення глибиною 24 біти на піксель (по 8 біт на канал RGB). Об'єм даних: $1200 \cdot 800 \cdot 3 \approx 2{,}88$ МБ.

Припустимо, що для шифру Вернама швидкість обробки 1 ГБ/с (типова швидкість для XOR-операцій на сучасних процесорах) час шифрування зображення складе 2,88 МБ/1000 МБ/с≈2,88 мс.

AES працює з блоками даних розміром 128 біт (16 байт). Для зображення об'ємом 2.88 МБ знадобиться 2880000 Б/16 Б/блок=180000 блоків. Кожен блок проходить через кілька раундів шифрування (10 раундів для AES-128, 12 для AES-192, 14 для AES-256). Швидкість шифрування AES-256 складає 50-200 МБ/с і час виконання складає 14-58 мс.

Таким чином, шифр Вернама працює на порядки швидше, тому що він використовує просту операцію XOR, в той час як AES вимагає більш складних математичних операцій.

Недоліком шифру Вернама є проблеми із ключем: генерація, безпечне зберігання та передача довгих ключів може бути складним завданням.

Хаотичні відображення – динамічні системи, що мають властивість чутливості до початкових умов, детермінований хаос і складну поведінку. Це робить їх ідеальними для генерації псевдовипадкових послідовностей. Ці послідовності можуть бути використані як ключі для шифру Вернама, що забезпечує високий рівень захисту. Сенс у тому, щоб використовувати хаотичну систему для генерації ключа, який потім застосовується у побітовій операції XOR з вихідними даними. Хаотичні відображення, такі як Тент, здатні генерувати ключі з високим ступенем випадковості і непередбачуваності. Це дозволяє значно ускладнити задачу розшифровки даних без знання початкових параметрів хаотичної системи і самого ключа. У цьому випадку хаотична система генерує ключ, який використовується для шифрування побітового кожного пікселя зображення. Оскільки хаотичні системи мають високу чутливість до початкових умов, навіть мінімальна зміна параметрів призводить до зовсім іншого ключа, що робить процес розшифровки практично неможливим для зловмисників. Додатковою перевагою використання хаотичних відображень є їхня здатність генерувати ключі, адаптовані під розмір та структуру даних. Наприклад, для шифрування зображень можна використовувати хаотичні послідовності, які враховують розміри зображення, кількість пікселів та їх

розташування. Це забезпечує індивідуальність ключа кожного зображення, підвищуючи рівень безпеки.

Сучасні дослідження показують, що використання хаотичних відображень для генерації ключів дозволяє покращити стійкість шифру Вернама до різних видів атак, включаючи статистичний аналіз. Крім того, комбінування хаотичних систем із шифром Вернама може бути застосовним у реальному часі, наприклад, для захисту відеопотоків або динамічних зображень [19].

Для забезпечення безпеки псевдовипадкових ключів важливо, щоб початкові умови хаотичного відображення були справді випадковими та непередбачуваними.

Інтеграція хаотичних відображень у шифр Вернама є перспективним напрямом у шифруванні зображень. Це поєднання може значно підвищити рівень безпеки шифрування, забезпечуючи захист даних в умовах сучасних загроз.

1.3 Рекурентні числові послідовності

Послідовність Фібоначчі є однією з найвідоміших рекурентних числових послідовностей, що має простий закон формування та особливі математичні властивості. У шифруванні вона використовується як компонент псевдовипадкових та гібридних генераторів, включаючи схеми шифрування зображень та потокові шифри [20].

Послідовність задається рекурентним співвідношенням:

$$F_n = F_{n-1} + F_{n-2}, F_0 = 0, \quad F_1 = 1.$$

Перші елементи послідовності Фібоначчі: 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, ...З послідовністю Фібоначчі тісно пов'язана послідовність Люка.

Послідовність Люка L_n визначається майже так само, як і Фібоначчі:

$$L_n = L_{n-1} + L_{n-2}.$$

Але початкові умови є іншими:

$$L_0 = 2, L_1 = 1.$$

Перші її значення:

$$2,\ 1,\ 3,\ 4,\ 7,\ 11,\ 18,\ 29,\ 47,\ \ldots$$

Обидві послідовності є пов'язані:

$$L_n = F_{n-1} + F_{n+1},$$

або:

$$L_n = F_n + 2F_{n-1}.$$

Це означає, що обидві послідовності можна використовувати як окремо, так і спільно для створення псевдовипадкових структур [21,22].

Цілочислені послідовності регіструюсь в Онлайн-енциклопедія цілісних послідовностей OEIS. OEIS (On-Line Encyclopedia of Integer Sequences) - це найбільша у світі онлайн-енциклопедія цілісних послідовностей, що містить сотні тисяч послідовностей, що використовуються в криптографії, інформатиці, теорії чисел [23]. Енциклопедію заснував математик Ніл Слоун (NJA Sloane) у 1964 році для систематизації своїх досліджень. Спочатку вона існувала у вигляді паперової книги, але в 1996 була запущена онлайн-версія, яка зараз підтримується фондом The OEIS Foundation Inc OEIS є базою знань про дискретні послідовності, де кожна послідовність має унікальний ідентифікатор виду A000045.

Кожна послідовність у OEIS включає наступні відомості:

– ID (наприклад, A000045);

– перші члени послідовності;

– формули генерації;

– рекурентні співвідношення;

– посилання на літературу;

– код для генерації (Python , PARI , Maple);

– коментарі та застосування.

В OEIS послідовності Фібоначчі та Люка представлені як класичні лінійні рекурентні ряди:

– Фібоначчі (A000045) – як найвідоміша послідовність,

– Люка (A000032) – її сполучений аналог.

Існують також узагальнені числа Фібоначчі, які розміщені в OEIS наступним чином:

Узагальнені числа Фібоначчі - OEIS A001045.

Узагальнені числа Фібоначчі (Generalized Fibonacci Numbers) розширюють послідовність Фібоначчі , дозволяючи використовувати довільні початкові значення [24]:

$$G(n) = G(n-1) + G(n-2),$$

де $G(0) = \text{a}$;

$G(1) = b$ – довільні початкові значення.

Приклад (для $a = 3$, $b = 5$):3,5,8,13,21,34, ...

Узагальнені числа Фібоначчі мають ті ж властивості , що й класичні , але можуть бути використані для моделювання інших систем.

Послідовність трибоначчі (Tribonacci Numbers) - OEIS A000073

Це тричлена узагальнена послідовність Фібоначчі :

$$T(n) = T(n-1) + T(n-2) + T(n-3),$$

де $T(0) = 0, T(1) = 0, T(2) = 1.$

Перші кілька чисел: 0,0,1,1,2,4,7,13,24,44,81, ...

Ця послідовність використовується в задачах комбінаторики та моделювання систем із трьома компонентами.

Послідовність тетраначчі (Tetranacci Numbers) : OEIS A000078.

Це чотиричленна узагальнена послідовність:

$Q(n) = Q(n-1) + Q(n-2) + Q(n-3) + Q(n-4)$,де$Q(0) = 0, Q(1) = 0, Q(2) = 0, Q(3) = 1.$

Перші кілька чисел: 0,0,0,1,1,2,4,8,15,29,56,108, ...

k- бонначі (k - bonacci Numbers).

Це подальше узагальнення, в якому кожен член є сумою попередніх k членів:

$$F_k(n) = F_k(n-1) + F_k(n-2) + \cdots + F_k(n-k),$$

де перші $k-1$ члени дорівнюють 0, а $F_k(k-1) = 1$.

Приклад для $k = 5$ (пентабоначі): 0,0,0,0,1,1,2,4,8,16, ...

Числа Фібоначчі часто використовуються в криптографії для створення динамічних та важкопередбачуваних алгоритмів захисту даних. Основна ідея полягає у використанні математичних властивостей послідовності для генерації ключів, перемішування даних або створення псевдовипадкових чисел.

Основне застосування чисел Фібоначчі наступне:

– генерація ключів (Key Generation). Послідовність використовується для створення довгих ключів. Наприклад, значення чисел Фібоначчі можуть визначати величину зсуву в шифрах (як у вдосконаленому шифрі Цезаря або Віженера);

– шифрування зображень. Числа Фібоначчі застосовуються для скремблювання (перемішування) пікселів. Позиція кожного пікселя змінюється на основі значення числа Фібоначчі, що перетворює картинку на візуальний «шум»;

– генерація псевдовипадкових чисел (PRNG). Існує спеціальний тип генератора – генератор Фібоначчі, що запізнюється (Lagged Fibonacci Generator), який використовує вирази:

$$S_n = S_{n-1} + S_{n-2};\ \ S_n \equiv S_{n-j} \star S_{n-k} (\mathrm{mod} m),\ 0 < j < k$$

до створення високоякісних випадкових чисел.

– стеганографія. Послідовність допомагає визначити безпечні місця в цифровому файлі (наприклад, у найменш значних бітах зображення) для прихованого вкладення секретного повідомлення.

Безумовними перевагами при використанні послідовностей Фібоначчі є швидкість та передбачуваність.

Алгоритми на базі Фібоначчі часто працюють швидше за класичні системи типу блокових шифрів AES, тому що вимагають менше обчислювальних раундів.

Оскільки послідовність детермінована (кожне число суворо випливає з попередніх), без використання складної функції хешування або випадкового сольового значення такі шифри можуть бути вразливі для криптоаналізу.

Використання послідовностей Фібоначчі у безпечних перетвореннях даних базується на введенні надмірності шляхом подання даних у системі чисельності Фібоначчі. Це дозволяє ефективно виявляти та виправляти помилки завдяки структурі коду, яка виключає дві або більше послідовних "1". Це забезпечує високу надійність передачі даних та сприяє розробці ефективних алгоритмів кодування та пошуку. Це базується на теоремі Цекендорфа, яка стверджує, що кожне натуральне число можна однозначно представити як суму різних чисел Фібоначчі, при цьому жодні два сусідні числа не з'являються в послідовності. Розробка та оцінка систем чисельності на основі Фібоначчі являє собою перехід від чистої математики до прикладної інженерії. Цей розвиток прогресує шляхом зростання гнучкості (параметризації) та складності алгебраїчної структури.

Щодо основ безпечних перетворень інформації, то енциклопедія OEIS визначає кілька фундаментальних послідовностей [25].

1. Канонічне представлення (код Цекендорфа)

Базова послідовність для цієї бази - A000045 (самі числа Фібоначчі: 0, 1, 1, 2, 3, 5, 8, 13).

Однак для інформатики похідні мають більше значення:

A003714: Числа Фібоначчі (фіббінарні числа). Це числа, двійкове представлення яких не містить двох послідовних одиниць. Точніше, це справжні кодові слова бази Фібоначчі. Приклад послідовності: 0, 1, 2, 4, 5, 8, 9, 10, 16

A000119: Кількість способів подання числа як суми різних чисел Фібоначчі. Ця послідовність є важливою для оцінки надлишковості бази. Якщо існує більше однієї можливості, база може містити скрыту інформацію (стеганографія).

Для потокових шифрів та комп'ютерної арифметики OEIS пропонує:

A000045 з розширенням до негативних індексів

A001906: Числа Фібоначчі із парними індексами. Вони часто є основою для спеціальних кодів, стійких до певних типів зсувів бітів.

На основі проведеного аналізу виділені наступні захисні властивості послідовностей Фібоначчі.

Інформаційні властивості. Коефіцієнт надмірності: вказує, скільки додаткових бітів потрібно для кодування порівняно зі звичайною двійковою системою. Фібоначчі завжди пропонує вищу надмірність, але за рахунок завадостійкості.

Щільність даних: оцінює, наскільки ефективно заповнюється інформаційний простір. Наприклад, коди Фібоначчі мають нижчу щільність, оскільки комбінації числа 11 не допускаються.

Завадостійкість та надійність.

Властивості самосинхронізації: Найважливіший критерій оцінки. Базовий код вважається високоякісним, якщо помилка в одному біті не призводить до втрати всього блоку даних. Коди Фібоначчі (з маркером 11) оцінюються вище, ніж коди Хаффмана або класичні двійкові коди. Відстань Хеммінга : Оцінює мінімальну кількість переходів (інверсій бітів), необхідних для перетворення одного кодового слова в інше.

Обчислювальна складність.

Арифметична ефективність: Як швидко процесор може об'єднувати чи множити числа. У системах Фібоначчі арифметика є складнішою, ніж у двійкових системах (через операції згортання та розгортання); тому оцінюються кількість тактів на операцію.

Послідовність Фібоначчі сама по собі не є криптографічно стійким генератором, проте застосовується:

– у модифікованому вигляді;

– у поєднанні з хаотичними системами;

– при використанні в перестановних шарах.

Таким чином послідовність Фібоначчі є ефективним компонентом легких криптографічних схем, особливо у шифруванні зображень.

Ряд дослідників підтверджують досить високу якість псевдовипадкових послідовностей, що генеруються рядами Фібоначчі. Дослідження послідовностей Фібоначчі та його модифікацій представляє значний інтерес для розробки сучасних методів захисту, зокрема систем хаотичного шифрування цифрових зображень [26, 27].

Аналіз показує доцільність провести подальше дослідження послідовностей Фібоначчі та їх застосування для захисту зображень.

1.4 Тестування псевдовипадкових послідовностей

Якість алгоритмів шифрування зображень багато в чому залежить від якості псевдовипадкових послідовностей, що використовуються.

1.4.1 Аналіз тестів для перевірки якості псевдовипадкових послідовностей.

Досліджування якості псевдовипадкових послідовностей має вирішальне значення при побудові захисних перетворень. Якщо псевдовипадкова послідовність має передбачуваність або статистичну закономірність (виконання першої умови теореми Шеннона), це може призвести до зниження стійкості системи шифрування і створення вразливостей для криптоаналізу.

Для оцінки якості псевдовипадкових послідовностей використовуються спеціальні статистичні тести, що дозволяють визначити ступінь їхньої випадковості та відсутність кореляцій. Перевірка містить аналіз розподілу бітів,

частоти появи шаблонів, серій однакових значень, ентропії та інших характеристик. Результати тестування дозволяють зробити висновок про придатність генератора псевдовипадкових чисел для застосування задач захисту зображень [28].

Нижче розглядаються основні методи тестування псевдовипадкових послідовностей, що застосовуються в системах шифрування зображень, а також аналізуються результати їх використання для оцінки стійкості криптографічної алгоритму. Існує ряд тестів для перевірки якості псевдовипадкових послідовностей, кожен з яких має свої особливості, переваги та обмеження.

Тести з пакету NIST вважаються стандартом оцінки криптографічної стійкості генераторів, оскільки вони охоплюють широкий спектр статистичних властивостей, включаючи частоту, послідовності, матричний ранг та інші. Однак вони вимагають великих обсягів даних та значних обчислювальних ресурсів, що робить їх менш зручними для повсякденного використання [29].

Тести Diehard є більш простою альтернативою, що включає такі перевірки, як Birthday Spacing Test, Rank of Matrix Test та Monkey Test. Незважаючи на їхню зручність, вони вважаються застарілими для сучасних криптографічних завдань [30].

Пакет тестів Dieharder – це вдосконалена версія Diehard , яка поєднує класичні тести з новими методиками, включаючи тести з NIST та власні розробки. Цей інструмент відрізняється універсальністю, гнучкістю налаштування та підтримкою різних генераторів, але потребує глибокого розуміння статистики для інтерпретації результатів [31].

Основні тести у наборі NIST наведені нижче.

1. Частотний (Frequency) тест: перевіряє співвідношення нулів та одиниць у послідовності (має бути приблизно 50/50).

2. Частотний тест усередині блоку: аналогічна перевірка, але для окремих блоків бітів.

3. Тест на серії (Runs): аналізує загальну довжину безперервних послідовностей однакових бітів.

4. Тест на найдовшу серію одиниць у блоці (Longest Run of Ones in a Bloc*k*): перевіряє, чи не є серії одиниць аномально довгими.

5. Тест рангів бінарних матриць (Binary Matrix Rank): оцінює лінійну залежність між підрядками фіксованої довжини.

6. Спектральний тест (Discrete Fourier Transform): шукає періодичні повторення (патерни) у послідовності за допомогою перетворення Фур'є.

7. Тест на збіг шаблонів, що не перекриваються (Non- overlapping Template Matching): шукає надто часту появу певних коротких бітових комбінацій.

8. Тест на збіг шаблонів, що перекриваються (Overlapping Template Matching): аналогічно попередньому, але з урахуванням перекриттів.

9. Статистичний тест Маурера (Maurer 's Universal Statistical): оцінює ступінь стисливості послідовності (випадкові дані не повинні ефективно стискатися).

10. Тест на лінійну складність (Linear Complexity): перевіряє довжину найкоротшого регістру зсуву з лінійним зворотним зв'язком (LFSR), що генерує цю послідовність.

11. Серіальний тест (Serial): аналізує частоту появи всіх можливих комбінацій бітів заданої довжини.

12. Тест на приблизну ентропію (Approximate Entropy): порівнює частоти блоків, що перекриваються, двох сусідніх довжин.

13. Тест кумулятивних сум (Cumulative Sums): перевіряє відхилення часткових сум елементів послідовності від нуля.

14. Тест на довільні відхилення (Random Excursions): аналізує кількість відвідувань певних станів у випадковому блуканні.

15. Варіантний тест на довільні відхилення (Random Excursions Variant): розширена перевірка відхилень для 18 різних станів.

Серед тестів в NIST (так званий скорочений пакет) заслуговують уваги наступні.

Frequency Test (Тест частоти): Перевіряє, чи рівномірно розподілені 0 та 1 у послідовності.

Runs Test (Тест серій): Перевіряє довжину послідовних серій однакових бітів.

Longest Run of Ones Test (Тест на найдовшу серію одиниць): Перевіряє, чи довжина найдовшої серії одиниць відповідає очікуваному значенню.

Block Frequency Test (Тест частоти блоків): Аналізує рівномірність розподілу бітів у заданих блоках.

FFT Test (Тест на основі швидкого перетворення Фур'є): Перевіряє наявність періодичних структур у послідовності.

Результат проходження кожного тіста супроводжується величиною *p-value*.

p-value в тестах на псевдовипадковість – це ймовірність того, що ідеальний, абсолютно випадковий генератор видав би послідовність, так само мало схожу на випадкову (або ще менш схожу), як і послідовність, що тестується. Якщо $p \in [0.01, \dots, 0.99]$, тест вважається успішним. Якщо $p < 0.01$ або $p > 0.99$ це може вказувати на відхилення від випадковості.

Важлива відмінність NIST від інших тестових пакетів полягає в наступному.

NIST перевіряє не тільки окремі *p- value* , але й додатково частку успішних послідовностей (якщо тест проводиться на багатьох блоках) та рівномірність розподілу *p- value* , яка перевіряється за критерієм χ^2.

Пакет Dieharder при попередньому розгляді представляється найповнішим і найсучаснішим (рис. 1.8).

Dieharder – це вдосконалена версія Diehard , яка поєднує класичні тести з новими методиками, включаючи тести з NIST та власні розробки. Цей інструмент відрізняється універсальністю, гнучкістю налаштування та

підтримкою різних генераторів, але вимагає глибокого розуміння статистики для інтерпретації результатів.

Dieharder tests:

Test Number	Test Name
-d 0	Diehard Birthdays Test
-d 1	Diehard OPERM5 Test
-d 2	Diehard 32x32 Binary Rank Test
-d 3	Diehard 6x8 Binary Rank Test
-d 4	Diehard Bitstream Test
-d 5	Diehard OPSO
-d 6	Diehard OQSO Test
-d 7	Diehard DNA Test
-d 8	Diehard Count the 1s (stream) Test
-d 9	Diehard Count the 1s Test (byte)
-d 10	Diehard Parking Lot Test
-d 11	Diehard Minimum Distance (2d Circle) Test
-d 12	Diehard 3d Sphere (Minimum Distance) Test
-d 13	Diehard Squeeze Test
-d 14	Diehard Sums Test
-d 15	Diehard Runs Test
-d 16	Diehard Craps Test
-d 17	Marsaglia and Tsang GCD Test
-d 100	STS Monobit Test
-d 101	STS Runs Test
-d 102	STS Serial Test (Generalized)
-d 200	RGB Bit Distribution Test
-d 201	RGB Generalized Minimum Distance Test
-d 202	RGB Permutations Test
-d 203	RGB Lagged Sum Test

Рисунок 1.8. – Повний зміст пакету Dieharder .

Результати тесту Dieharder дають можливість глибоко проаналізувати властивості псевдовипадкових послідовностей. Якщо кілька тестів дають статус "FAILED" або "WEAK", це може вказувати на недостатню випадковість генератора, що є неприпустимим для криптографічних або наукових додатків.

У пакеті Dieharder існує кілька тестів, які називають "мавпячими" (Monkey Tests). Ці тести пов'язані з аналізом частоти появи певних послідовностей символів (бітів) у випадковому рядку. Назва "мавпячі тести" походить від концепції "мавпи, що друкує на друкарській машинці", яка випадково натискає клавіші, створюючи послідовності символів. Якщо мавпа друкує досить довго,

вона теоретично може написати будь-який текст, наприклад твори Шекспіра. У контексті тестів випадковості, "мавпячий тест" перевіряє, наскільки ймовірно, що випадкова послідовність бітів містить певні шаблони, які ми очікуємо побачити в дійсно випадковому рядку.

Приклади "мавпячих тестів" у Dieharder [30, 31].

Diehard OPSO (Overlapping Pairs Sparse Occupancy Test) Цей тест перевіряє, скільки разів зустрічаються різні пари (довжини 2) з 8-бітових послідовностей (256 можливих значень). Ідея тесту в тому, що якщо послідовність дійсно випадкова, то всі 256 можливих пар повинні зустрічатися приблизно однаково часто, без значних відхилень .

Diehard OQSO (Overlapping Quadruples Sparse Occupancy Test):

Цей тест аналогічний OPSO, але аналізує більш довгі послідовності - 4-символьні (4 байти або 32 біти).

Перевіряється, наскільки рівномірно розподілені всі можливі комбінації послідовностей довжиною 4 у випадковому рядку.

Diehard DNA Test. Цей тест моделює послідовності ДНК, де кожна "літера" представлена одним із чотирьох символів: A, C, G, T. Аналізується, наскільки рівномірно розподілені ці символи та їх комбінації, щоб перевірити випадковість у біологічно значущих послідовностях.

В рамках порівняльного аналізу пробне тестування псевдовипадкової послідовності довжиною 5000 біт, згенерованої модифікованим . відображенням Тент, проведено на повних пакетах NIST та Dieharder . Пробне тестування показало «провал» тестованої послідовності на шести тестах Dieharder . Водночас ця послідовність пройшла повний тест NIST з хорошими значеннями *p- value* . Це викликає недовіру до пакету Dieharder . Крім того, встановлена висока складність настроювання Dieharder .

Вирішено далі використовувати NIST у повному чи скороченому до п'яти основних тестів варіантах.

1.4.2. Метрики якості шифрування зображень

При оцінці алгоритмів шифрування зображень недостатньо перевірити візуальну «невпізнанність» зашифрованого зображення. Необхідний формальний кількісний аналіз, що дозволяє оцінити наступні показники:

– стійкість до статистичного аналізу;

– чутливість до зміни вхідних даних;

– ступінь руйнування структури зображення;

– рівномірність розподілу пікселів.

Для цього використовується ряд спеціальних метрик [32,33].

1. *Коефіцієнт кореляції.* Це одна з найважливіших метрик оцінки якість для шифрування. Вона вимірює взаємозв'язок між сусідніми пікселями.

В оригінальному зображенні кореляція сусідніх пікселів близька до 1 (вони схожі).

*У зашифрованому зображенні к*ореляція має бути близька до 0, що говорить про відсутність структури та успішне приховування даних.

Хороший алгоритм шифрування руйнує кореляцію між сусідніми пікселями. Аналіз виконується у трьох напрямах горизонтальному, вертикальному та діагональному.

Деякі джерела рекомендують обчислювати коефіцієнт кореляції пікселів за антидіагональним напрямком [34] .

На графіку розподілу пікселів (корелограмі) упорядковані точки оригіналу перетворюються на шумову картину (рис. 1.9).

2. *Ентропія Шеннона.*

Ентропія оцінює рівень невизначеності зображення та розраховується за формулою:

$$\boldsymbol{H(X) = -\sum_{i=1}^{N} p(x_i)\log_2 p(x_i).}$$

Максимальне значення ентропії для 8-бітного зображення: $H(X) \approx 8$. При якісному шифруванні метрика прагне значення максимальної ентропії.

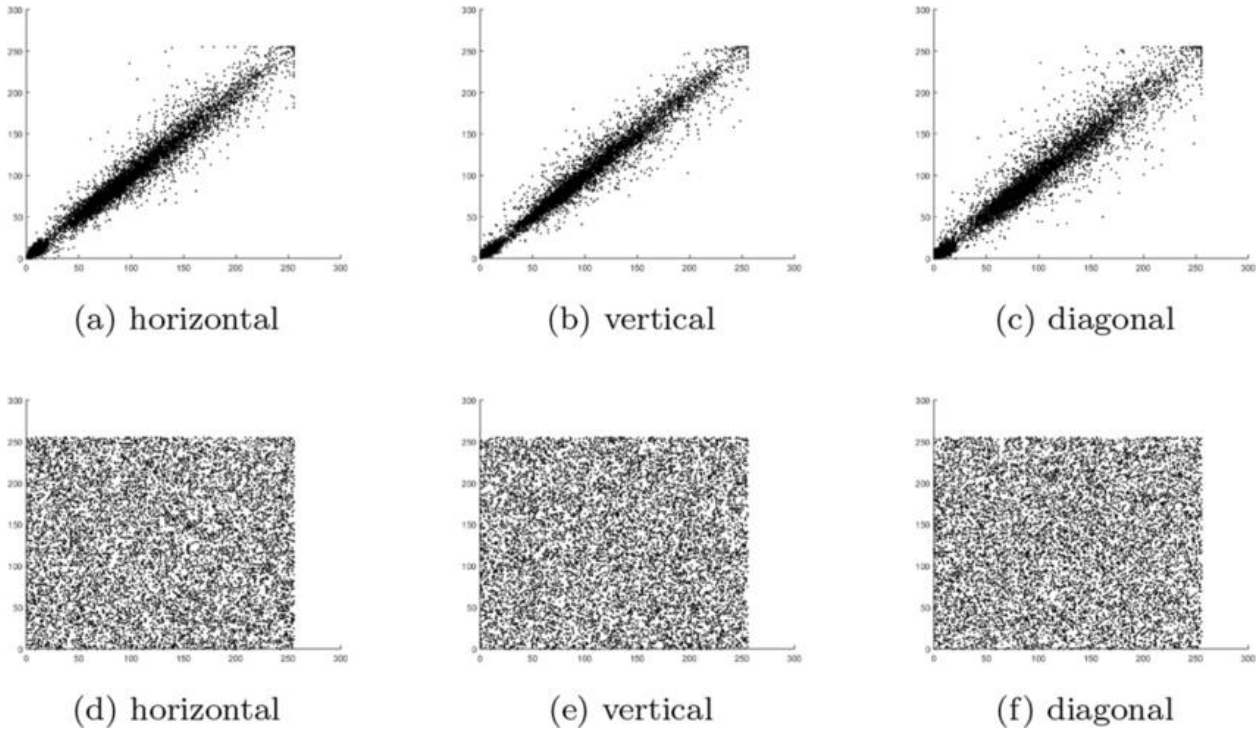


Рисунок 1.9 – Коефіцієнт кореляції пікселів (a , b , c – оригінальне зображення , d , e , f – зашифроване зображення) [35] .

3. *Метрики дифузії (мінливості) зображення* під час його шифрування.

NPCR (Number of Pixels Change Rate)

Вказує, який відсоток пікселів змінився при малій зміні вхідного зображення.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \cdot H} \times 100\%,$$

де: $D(i,j) = 1$ якщо піксель змінився; $D(i,j) = 0$, якщо піксель не змінився;

$W,\ H$ – розміри зображення.

Значення $NPCR > 99\%$ вказує на високоякісне шифрування.

UACI (Unified Average Changing Intensity):

$$UACI = \frac{1}{W \cdot H} \sum_{i,j} \frac{| C_1(i,j) - C_2(i,j) |}{255} \times 100\%$$

Ця метрика оцінює середню інтенсивність змін пікселів у зашифрованому зображенні $_1 i$ зашифрованому зображенні $_2$, оригінали яких відрізняються одним пікселем .

Для якісного алгоритму шифрування значення $UACI$ близько 33% (для 8-бітних зображень)

У процесі розробки різних методів перетворення зображень часто виникає потреба порівняння якості перетворення. Застосування для такого порівняння перерахованого набору метрик якості є досить складним багатокритеріальним завданням. Вирішення такої задачі виконується методом експертного оцінювання та породжує певні труднощі. Доцільно вирішити задачу приведення перерахованого набору метрик якості до єдиного показника якості.

1.5 Аналіз можливостей формування групи довірених користувачів для роботи із конфіденційними зображеннями

Формування групи довірених користувачів можливе шляхом вирішення завдання вироблення спільного секретного ключа кількома учасниками. Це завдання лежить в основі захищених групових комунікацій, розподілених систем та сучасних протоколів захищеного обміну даними. Фундаментальною основою таких систем є класичний протокол Діффі = Хеллмана, який був запропонований для двох учасників [36].

Базова модель формування групи довірених користувачів має такий вигляд. Розглядається кінцева множина з N користувачів:

$$U = \{U_1, U_2, \dots, U_N\}.$$

Мета протоколу - обчислення загального ключа (загального секрету):

$$K \in \mathcal{K}.$$

Доступ до конфіденційного контенту отримує лише користувач, який має спільний груповий ключ (загальний секрет).

Протокол Діффі-Хеллмана, запропонований у 1976 році, став поворотним моментом у криптографії, оскільки вперше дозволив двом сторонам безпечно виробляти спільний секрет відкритим каналом без попереднього обміну ключами. Його основа на момент опублікування спиралася на обчислювальну складність завдання дискретного логарифмування в кінцевих групах, що унеможливило практичне відновлення секрету при розумних параметрах. Ця ідея заклала фундамент для всієї сучасної криптографії з відкритим ключем і безпосередньо вплинула розвиток протоколів формування довірених груп .

Однак класична схема Діффі-Хеллмана спочатку була розрахована тільки на двох учасників, це швидко виявило її обмеження в умовах реальних систем, де потрібна захищена групова комунікація. Вже в 1980-1990-х роках почалися спроби розширення протоколу на розраховані на багато користувачів сценарії [37]. Найпростіші підходи використовували послідовне нарощування секрету, коли кожен учасник по черзі модифікував значення, але такі схеми страждали від високої затримки та слабкої стійкості до динамічної зміни складу групи.

Наступним важливим кроком стала поява структурованих групових протоколів, серед яких особливо вирізняється схема Бурместера-Демстедта , запропонована 1994 року [38]. Ця схема заклала основу для подальших досліджень у галузі Group Key Agreement (GKA) — протоколів узгодження ключів у групах довірених користувачів. Протокол Бурместера-Демстедта показав, що можна організувати користувачів в кільцеву топологію і досягти обчислення загального ключа з лінійною складністю за кількістю учасників. Це стало значним покращенням порівняно з методом Діффі-Хеллмана і продемонструвало, що груповий обмін ключами можна зробити досить оперативним. Проте ця схема мала обмеження: її стійкість до динамічним змін групи тобто. до масштабування залишалася низькою, а перерахунок ключа при додаванні або видаленні учасників був дорогим.

Паралельно розвивалися загальніші дослідження групових протоколів узгодження ключів, які прагнули покращити масштабованість і гнучкість. У цих роботах поступово формувалася ідея переходу від лінійних структур до ієрархічних. Ключовим напрямом стало використання дерев ключів, де обчислення торкаються лише частини учасників. Такий підхід дозволив знизити складність оновлень і зробити протоколи придатними для великих і довірених користувачів, що динамічно змінюються.

Деревоподібні структури в групових протоколах Діффі-Хеллмана з'явилися як природна відповідь на дві проблеми ранніх схем: квадратичну складність обмінів і слабку масштабованість при зміні складу групи. Ідея полягає в тому, щоб замінити "все з усіма" або кільцеву топологію на ієрархію, де обчислення локалізуються у вузлах дерева, а глобальний ключ формується на вершині [39].

Криптографія на еліптичних кривих – сучасний метод асиметричного шифрування, що забезпечує високу безпеку при малому розмірі ключів (наприклад, 256-бітний ключ на еліптичній кривій еквівалентний 3072-бітному ключу RSA) при тому рівні захищеності. Криптографія на еліптичних кривих (ECC) – це сучасний метод асиметричного шифрування, що забезпечує високу безпеку при малому розмірі ключів (наприклад, 256-бітний ключ ECC еквівалентний 3072-бітному ключу RSA). Вона базується на операції множення точки P на еліптичній кривою на скаляр k : Q = k P , де знаючи Q і P, практично неможливо знайти k [40;41] .

Сьогодні відомо 10 форм еліптичних кривих [42] (рис. 1.10).

Усі форми еліптичних кривих мають свої особливості [43,44]. Це стосується головним чином обчислювальних витрат на виконання операцій з точками на еліптичних кривих. До цих операцій відносяться композиція точок, що здійснюється додаванням точок та їх подвоєнням.

Найбільш уживаними на сьогоднішній день є три форми електричних кривих. Це криві у формі Вейєрштраса, Монтгомері, Едвардса.

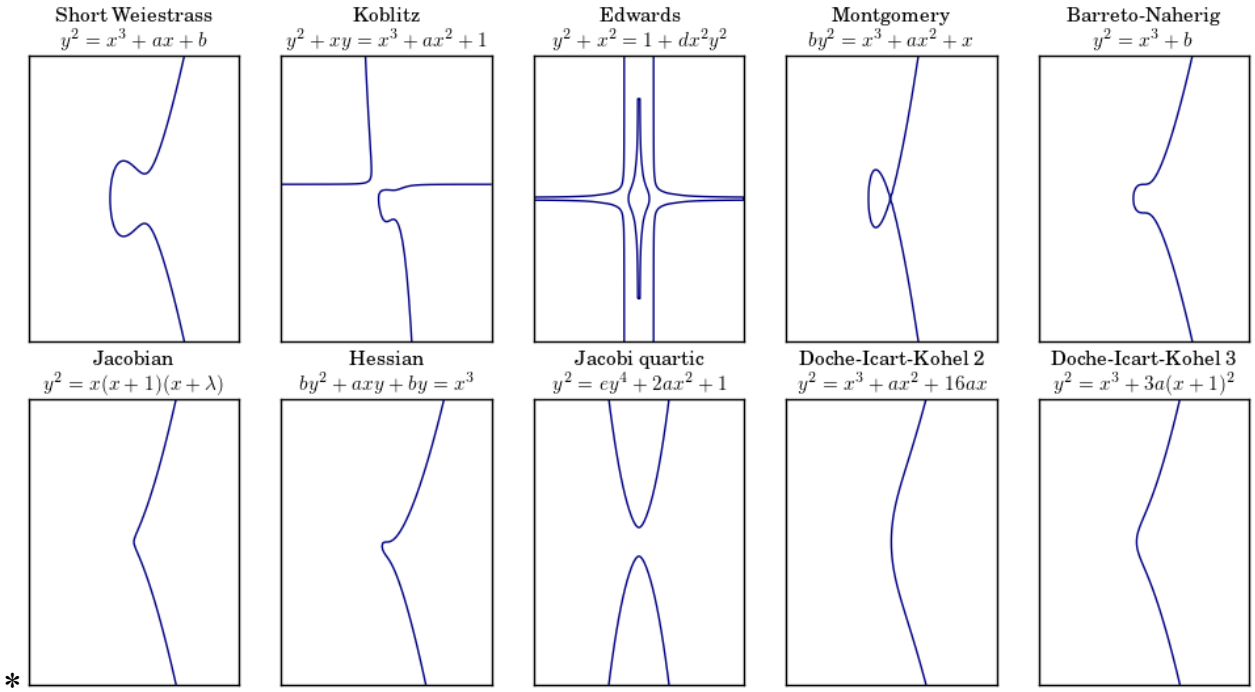


Рисунок 1.10 – Форми еліптичних кривих [42].

Крива Вейєрштрасса – найпоширеніший вид, представлений рівнянням:

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

Крива Монтгомері представляється у вигляді:

$$By^2 = x^3 + Ax^2 + x.$$

Крива Едвардса має вигляд:

$$x^2 + y^2 = 1 + dx^2y^2.$$

Оскільки завдання формування групи довірених користувачів нас цікавить оперативність виконання операцій, найбільш перспективною для дослідження є крива у формі Монтгомері. Криві Монтгомері дозволяють виконувати операції складання точок на кривій, не обчислюючи координати y, що робить їх ефективнішими для оперативних обчислень [45-47]. Крім того, відомі так звані сходи Монтгомері – алгоритм, який використовується для ефективного обчислення скалярного добутку на кривих Монтгомері. Він дозволяє швидко обчислювати добуток скалярного значення (особистого секретного ключа) та точки на кривій. Сходи Монтгомері використовують бінарне подання скалярного

значення для послідовного виконання операцій складання та подвоєння точок на кривій.

Таким чином, у задачі формування групи довірених користувачів необхідно досліджувати різні протоколи формування розширеної групи, зокрема, протокол Бурместера-Демстедта, деревоподібний протокол. Ці протоколи необхідно оцінити з точки зору швидкодії різних еліптичних кривих, зокрема на кривої Монтгомері.

1.6. Особливості дистанційної обробки медичних конфіденційних зображень

В останні десятиліття в медицині відкриваються нові можливості в галузі медичної візуалізації за рахунок впровадження передових пристроїв та сучасних інформаційних технологій. Медичні зображення стали найважливішим інформаційним ресурсом медичних працівників. Сьогодні широкий спектр технологій медичної візуалізації у світі діагностики допомагає лікарям отримувати високоякісні зображення для точнішої діагностики захворювань. Сюди, зокрема, відносяться такі зображення [48]:

– магнітно-резонансні томограми;

– комп'ютерні томограми;

– цифрові зображення ультразвукового дослідження;

– комп'ютерні рентгенограми та оцифровані рентгенівські знімки;

– цифрові ангіограми;

– оцифровані маммограми;

– позитронно- (фотонно-) емісійні томограми (PET, SPECT).

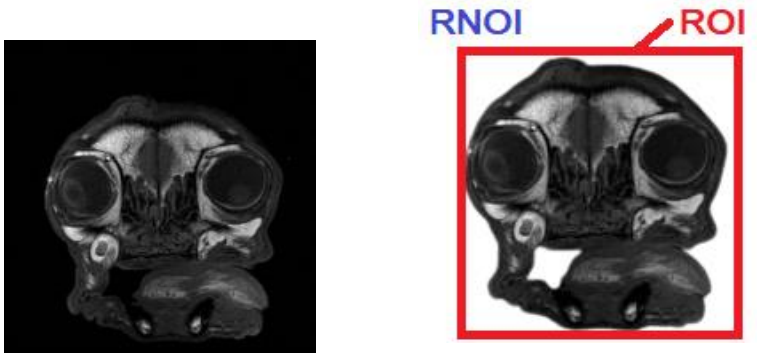
Паралельно швидко розвивається інший процес. Сьогодні величезна кількість медичних зображень та інформації про пацієнтів передається між різними географічно віддаленими організаціями для аналізу та оцінки. Це фактично є основою формування нової галузі медичної науки та практики – телемедицини [49-51]. Телемедицина включає телеконсультації,

теледіагностику, телехірургію, телерадіологію та інші види дистанційних медичних послуг. Зараз особлива увага приділяється захисту медичних зображень та інформації про пацієнтів, що міститься в них. Тут особливо важливо забезпечити конфіденційність та незмінність зображень. Конфіденційність та цілісність стали серйозною проблемою при передачі медичних зображень відкритими каналами зв'язку. Важливість безпечного обміну медичними зображеннями змушує міжнародні організації охорони здоров'я розробляти спеціальні стандарти щодо безпеки медичних даних. Одним із таких стандартів є DICOM [52-53]. DICOM (Digital Imaging and Communications in Medicine) – медичний галузевий стандарт створення, зберігання, передачі та візуалізації цифрових медичних зображень та документів обстежених пацієнтів. DICOM підтримується основними виробниками медичного обладнання та медичного програмного забезпечення Medical Imaging & Technology Alliance.

DICOM надає медичним працівникам та організаціям рекомендації та механізми для забезпечення в телемедичній конфіденційності та цілісності зображень. Конфіденційність повинна гарантувати, що тільки довірені особи або системи мають право доступу до інформації, якою іде обмін. Цілісність повинна гарантувати, що інформація не була змінена або спотворена. Служба конфіденційності необхідна для запобігання несанкціонованому доступу до зображень, що передаються, тоді як забезпечення цілісності необхідне для перевірки і виявлення можливої фальсифікації зображень [53]. Кожен піксель зображення може бути необхідний процесу діагностики, і будь-яке спотворення може призвести до помилкової діагностики.

Оскільки медичні зображення мають специфічну природу, вони складаються з двох розділів, які називаються областю інтересу (ROI, region of interest) і областю нецікавості (RONI, region of no interest) (рис. 1.11) [54]. ROI вважається важливою областю, оскільки в ній міститься вразлива та конфіденційна інформація, тому значення пікселів мають вирішальне значення у

процесі діагностики. Через це модифікація ROI категорично заборонена. З іншого боку, RONI, а точніше, фон зображення – це область, яка не містить важливої інформації. Згідно з DICOM всі коментарі до зображення (діагностичні висновки, призначення) можуть вноситися лише в RONI.



а) б)

Рисунок 1.11 – Область інтересу (region of interest, ROI) і область нецікавості (region of no interest, RONI) для медичного зображення.

1.7 Висновки до першого розділу

У першому розділі дисертації було проведено ґрунтовний аналіз актуальності та сучасного стану проблеми підвищення конфіденційності та цілісності обміну зображеннями для групи довірених користувачів. Досліджено існуючі рішення, їх основні характеристики та тенденції розвитку. Підкреслено, що підвищення конфіденційності та цілісності обміну зображеннями є критично важливим для телемедицині, інтернету речей, передачі супутникових знімків.

В ході огляду були виявлені основні закономірності хаотичних відображень і можливості використання їх для захисту конфіденціальних зображень, розглянуто послідовності Фібоначчі і їх потенціальні можливості. Детально проаналізовано шляхи побудови груп довірених користувачів для

сумісного аналізу конфіденціальних зображень. Встановлено, що існуючі методи мають певні недоліки, такі як недостатня захищеність, низька швидкодія. Крім того, аналіз літератури виявив суттєві обмеження при використанні методів хаотичного шифрування для захисту зображень.

Таким чином, отримані результати аналізу підтверджують необхідність подальших досліджень і розробки нових моделей та методів підвищення конфіденційності та цілісності обміну зображеннями, які були б більш е надійними, захищеними і швидкодіючими.

Сформульовано мету та задачі дослідження.

Метою дослідження є підвищення рівня забезпечення конфіденційности та цілісності зображень шляхом удосконалення методів шифрування на основі хаотичних відображень.

Для досягнення мети дослідження необхідно вирішити такі завдання:

– удосконалити критерій якості шифрування для оцінки якості шифрування зображень;

– удосконалити метод шифрування зображень на основі хаотичного відображення Tent з управлінням;

– удосконалити модель побудови псевдовипадкових послідовностей Фібоначчі;

– провести експериментальні дослідження, апробацію і впровадження отриманих теоретичних результатів.

РОЗДІЛ 2. РОЗРОБКА МЕТОДУ ГЕНЕРАЦІЇ ПСЕВДОХАОТИЧНИХ ПОСЛІДОВНОСТЕЙ НА ОСНОВІ ВІДОБРАЖЕННЯ ТЕНТ

У розділі пропонується нова динамічна систему, а саме узагальнене відображення Тент з керуванням, яке стабілізує цикли заданої довжини. Ці цикли залежать від параметрів системи та початкового значення; ці величини є коротким ключем для генерації довгої псевдохаотичної послідовності.

Математичною основою для побудови нових методів генерації псевдохаотичних криптосистем є одновимірне відображення Тент із додатково введеним у це відображення предикативного управління.

2.1 Метод генерації псевдохаотичних послідовностей на основі відображення Тент

Враховуючі [55], розглянемо нелінійне рівняння з дискретним часом:

$$x_{n+1} = f(x_n), \quad n = 1, 2, \ldots , \tag{2.1}$$

де

$$f(x) = H\left(1/2 - |x - 1/2|\right) = \begin{cases} H\,x, x \le 1/2; \\ H(1-x), x > 1/2, \end{cases} \tag{2.2}$$

$x \in (-\infty, +\infty)$, $H \ge 2$.

Відображення (2.2) називається узагальненим відображенням Тент.

Множина називається інваріантною для рівняння (2.1), якщо для будь-якого $x_0 \in U$ справедливо, що $f^{(k)}(x_0) \in U$, $k = 1, 2, \ldots$. Можна показати, що при $H > 2$ в рівнянні (2.1) інваріантною множиною буде множина канторового типу: замкнута, потужності континуум. Зазначимо, що кожна точка інваріантної множини може бути представленою у вигляді

$$\sum_{j=1}^{\infty} \frac{\alpha_j}{H^j}, \text{ де } \alpha_j \in \{0, H-1\}.$$

Ця множина включає зліченна підмножина всіх періодичних точок відображення (2.2). Якщо x_0 не належить інваріантній множині, то відповідна послідовність $\{f^{(k)}(x_0)\}_{k=1}^{\infty}$ прагне до $-\infty$. Такі інваріантні множини називаються репелерами відображення (2).

Множина $\{\eta_1, \dots, \eta_T\}$ називається T-циклом відображення (2), якщо числа $\eta_1, \dots, \eta_T$ різні та $\eta_{j+1} = f(\eta_j)$, $j = 1, \dots, T-1$, $\eta_1 = f(\eta_T)$, при цьому кожна точка T-циклу називається T-періодичною точкою. Мультиплікатор циклу рівняння (1) визначається формулою $\mu = f'(\eta_T) \cdot \dots \cdot f'(\eta_1)$, т.е. $\mu = \pm H^T$.

Як відомо [56], локальна асимптотична стійкість циклу визначається умовою (достатньою): мультиплікатор по абсолютній величині менше одиниці. Оскільки $|\mu| = H^T > 1$, то любий цикл рівняння (1) є нестійким. Крім того, якщо $H > 2$, то майже для будь-якої початкової точки відповідна траєкторія йде на нескінченність.

Поряд із рівнянням (1) розглянемо рівняння

$$x_{n+1} = F(x_n), \quad n = 1, 2, \dots, \tag{3}$$

де $F(x) = f(\vartheta x + (1-\vartheta) f^{(T)}(x))$, ϑ – деяке дійсне число, яке називається керуючим параметром і підлягає визначенню.

Рівняння (3) називається системою управління рівняння (1).

Нехай $\{\eta_1, \dots, \eta_T\}$ – цикл рівняння (1). Так як $\vartheta\eta_k + (1-\vartheta) f^{(T)}(\eta_k) = \eta_k$, то $F(\eta_k) = f(\eta_k)$, це означає, що цикл рівняння (2.1) також буде циклом рівняння (2.3). Зауважимо, що зворотне твердження у загальному випадку невірне.

Мультиплікатор λ того ж циклу $\{\eta_1, \dots, \eta_T\}$ для рівняння (2.3) можна знайти згідно [57]:

$$\lambda = \mu(\vartheta + (1-\vartheta)\mu)^T.$$

Можливі два випадки: $\mu > 0$ та $\mu < 0$. Умова локальної асимптотичної стійкості T-циклу рівняння (2.3) при $\mu = H^T$:

$$|\lambda| = \left| H^T \left(\vartheta + (1-\vartheta) H^T\right)^T \right| < 1,$$

звідки

$$\frac{H^T - \frac{1}{H}}{H^T - 1} < \vartheta < \frac{H^T + \frac{1}{H}}{H^T - 1} \tag{2.4}$$

Якщо $\mu = -H^T$, то умова локальної асимптотичної стійкості циклу рівняння (2.5):

$$|\lambda| = \left| H^T \left(\vartheta - (1-\vartheta) H^T \right)^T \right| < 1,$$

звідки

$$\frac{H^T - \frac{1}{H}}{H^T + 1} < \vartheta < \frac{H^T + \frac{1}{H}}{H^T + 1}. \tag{2.5}$$

***Теорема* 1** [55]. Якщо виконано нерівності (4), то будь-яке рішення рівняння (3) обмежено (тобто для будь-якої початкової точки) $x_0 \in (-\infty, +\infty)$ відповідна траєкторія обмежена). Більше того, будь-який T-цикл $\{\eta_1, \ldots, \eta_T\}$ цього рівняння, для якого величина $\mu = f'(\eta_T) \cdot \ldots \cdot f'(\eta_1)$ позитивна, локально асимптотично стійкий.

***Теорема* 2** [55]. Якщо виконана нерівність (5), $\frac{H^T - \frac{1}{H}}{H^T + 1} < \vartheta \le \frac{H^T}{H^T + 1}$, то множина $[0, H/2]$ є інваріантною множиною рівняння (1) (тобто для будь якої початкової точки $x_0 \in [0, H/2]$ відповідна траєкторія обмежена значеннями 0 и $H/2$). Больш того, любий T-цикл $\{\eta_1, \ldots, \eta_T\}$ цього рівняння, для якого величина $\mu = f'(\eta_T) \cdot \ldots \cdot f'(\eta_1)$ від'ємна, локально асимптотично стійкий.

2.1.1 Генерація псевдохаотичної послідовності

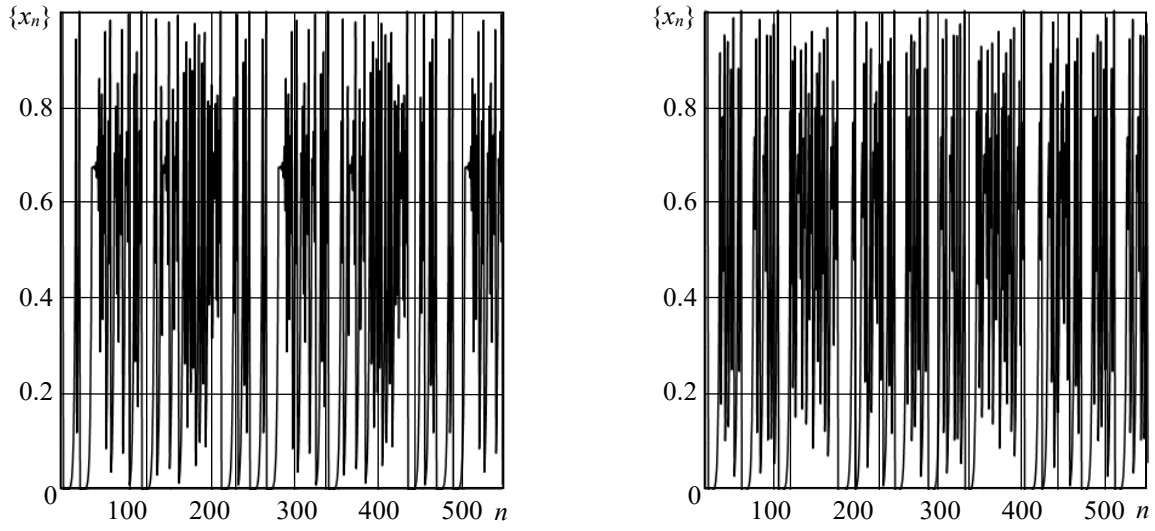
Для генерації псевдохаотичної послідовності пропонується використовувати динамічну систему (3), у якій ϑ задовольняє умову (4) або (5).

При цьому сама послідовність визначається через T-періодичні точки $\{\eta_1, \ldots, \eta_T\}$. Тут T – достатньо велике число. Щоб виключити короткі підцикли, число T потрібно обирати простим. Всього існує $\frac{2^{T-1} - 1}{T}$ циклів довжини T, тобто

великих T циклів дуже багато, тому ймовірність потрапити на конкретний цикл дуже мала. З огляду на хаотичність динамічної системи (1) довгий цикл практично не відрізняється від довільної нециклічної траєкторії. Цей цикл залежить від вихідної точки $x_0 \in (0,1)$, від числа T и параметрів H и ϑ.

В силу хаотичності динамічної системи (1) довгий цикл практично не відрізняється від довільної обмеженої нециклічної траєкторії. Цей цикл залежить від вихідної точки $x_0 \in (0,1)$, від числа T и параметрів H и ϑ.

Однак, що на практиці для $H > 2$ будь яка траєкторія рівняння (1) буде йти на нескінченність в силу округлення результатів. На рис. 2.1 представлені типові T -періодичні траєкторії рівняння (1) при $T = 223$, $H = 2.070801$, $x_0 = 0.9$.



a) *b*)

Рисунок 2.1 – T -періодичні траєкторії рівняння (1) при $T = 223$, $H = 2.070801$, $x_0 = 0.9$: *a*) величина $\mu = f'(\eta_T) \cdot \ldots \cdot f'(\eta_1)$ від'ємна; *b*) величина $\mu = f'(\eta_T) \cdot \ldots \cdot f'(\eta_1)$ позитивна

Щоб практично будувати періодичні траєкторії, треба використовувати рівняння (3). Тоді знайдений цикл залежить від початкової точки $x_0 \in (0,1)$, від числа T та від параметрів H та ϑ, які можуть містити достатньо багато

десяткових знаків. Така складна залежність робить цикл фактично необчислюваним для кібератак.

Цей цикл локально асимптотично стійкий. Це означає, що отримана траєкторія залежить від незначних збурень, похибок обчислень і округлень. Більше того, можна очікувати, що при одних і тих же значеннях x_0 , T, H, ϑ будуть виходити однакові цикли на комп'ютерах різних типів.

Важливим питанням є питання точності обчислень (тобто числа коректних десяткових цифр дрібної частини). Загалом кажучи, ця точність повинна залежати від довжини циклу. Експерименти показують [55], що точність слід вибирати не менше, ніж $1.05 \cdot T \lg(H)$.

Однак послідовність $\{\eta_1, \dots , \eta_T\}$ не є псевдовипадковою – порядок елементів повністю визначено. Тому потрібний додатковий трюк. Справа в тому, що в результаті обчислень можна гарантувати q вірних десяткових знаків у точках циклу $\{\eta_1, \dots , \eta_T\}$, де через q позначена величина точності обчислень. Таким чином, є $T \cdot q$ десяткових цифр, у тому числі можна будувати псевдохаотичну послідовність. Наприклад, так: слід задати деякі числа T_0, T_1, та точність обчислювань брати $q = T_1 + 2T_0$ $(T_1 + 2T_0 > 1.05 \cdot T \lg(H))$. Для кожного числа η_j взяти десяткові цифри дробової частини, починаючи з розряду з номером $T_0 + 1$, закінчуючи номером $T_1 + T_0$. Позначимо ці множини $\{\eta_{j1}, \dots , \eta_{jT_1}\}$, $j = 1, \dots, T$. Для формування ключової послідовності получили $T \cdot T_1$ десятинних цифр.

Сама ключова послідовність може мати, наприклад, такий вигляд

$$\mathrm{I}_1 = \{\eta_{11}, \eta_{12}, \dots , \eta_{1T_1}, \eta_{21}, \dots, \eta_{2T_1}, \dots, \eta_{T1}, \dots, \eta_{TT_1}\} \tag{2.6}$$

або

$$\mathrm{I}_2 = \{\eta_{11}, \eta_{21} \dots , \eta_{T1}, \eta_{12}, \dots, \eta_{T2}, \dots, \eta_{1T_1}, \dots, \eta_{TT_1}\}. \tag{2.7}$$

Можна формувати послідовність і іншими способами.

Розглянемо завдання вибору параметрів ключа.

Насінням генерації псевдохаотичної послідовності є ключ:

$$Key = [T,\ H,\ \pm\alpha,\ x_0].$$

Тут числа α або $-\alpha$ використовуються для обчислення керуючого параметра $\vartheta = \dfrac{H^T + \alpha\dfrac{1}{H}}{H^T - 1}$ або $\vartheta = \dfrac{H^T - \alpha\dfrac{1}{H}}{H^T + 1}$ відповідно.

Чим ближче до нулю α, тим ближче до нулю мультиплікатор циклу, тим швидше початкова точка притягнеться до цього циклу.

Тому доцільно обрати $0 < \alpha < 0.005$. Практичні експерименті показують, що при такому α початкова точка попадає на цикл не більш, ніж за 20 ітерацій. Це означає, що число T_0 у формулі $q = T_1 + 2T_0$ можна брати рівним 20. При цьому число T_1 можна брати просто рівним T. Період T має бути простим числом у діапазоні між 100 і 500. Великі числа призводять до різкого зростання часу обчислень. Початкова точка x_0 повинна вибиратися з інтервалу $(0, 1)$.

Періодичні траєкторії чутливі до зміни параметрів ключа. Візьмемо, наприклад, такі параметри послідовності:

$$x_0 = 0.9,\ T = 223,\ \vartheta = \frac{H^T + 0.001\cdot\dfrac{1}{H}}{H^T - 1},\ H \in \{2.070801,\ 2.0708011\},$$

тобто

$$Key = [223,\ \{2.070801,\ 2.0708011\},\ 0.001,\ 0.9].$$

Обчислимо дві відповідні періодичні траєкторії та їх різницю z_n. Отримана траєкторія зображена на рисунку 2.2.

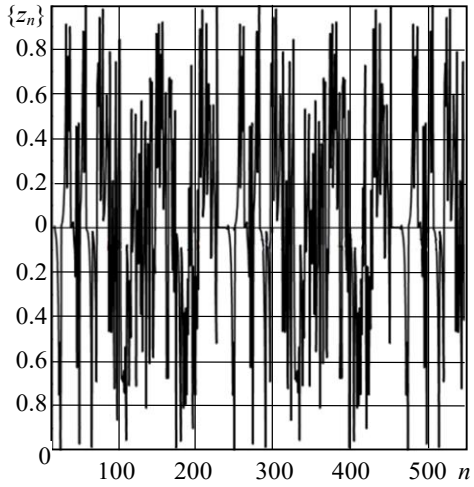


Рисунок 2.2 – Різниця двох T-періодичних траєкторій рівняння (2.3) при

$$Key = \left[223,\ \{2.070801,\ 2.0708011\},\ 0.001,\ 0.9\right]$$

В силу сильної чутливості параметр H можна вибирати досить близьким до двійки, наприклад, $H \in (0,\ 2.2)$, а всю невизначеність вкладати у такі значні десяткові цифри.

Візьмемо ключ: $Key = \left[223, 2.0708011,\ \{0.001,\ -0.001\},\ 0.9\right]$. Обчислимо дві відповідні періодичні траєкторії та їх різницю z_n. Отримана траєкторія зображено на рисунку 2.3.

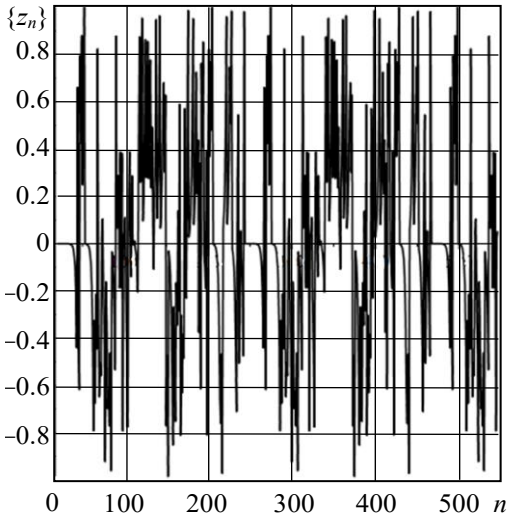


Рисунок 2.3 – Різниця двох T-періодичних траєкторій рівняння (2.3) при

$$Key = \left[223, 2.0708011,\ \{0.001,\ -0.001\},\ 0.9\right]$$

Аналогічно побудуємо різницю траєкторій при $Key = [223, 2.0708011, \{0.001, 0.0011\}, 0.9]$ (рис. 2.4), $Key = [223, 2.0708011, 0.001, \{0.9, 0.9001\}]$ (рис. 2.5).

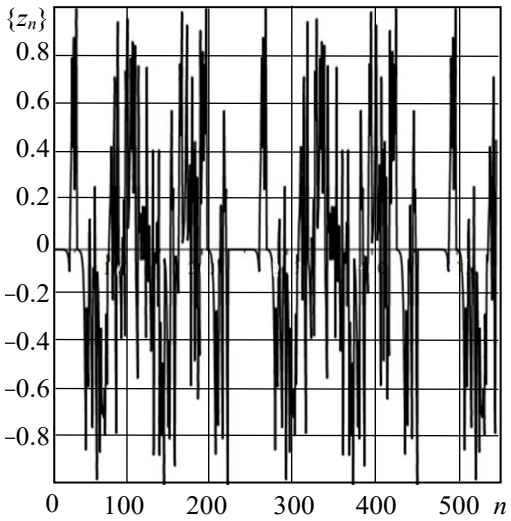


Рисунок 2.3 – Різниця двох T-періодичних траєкторій рівняння (3) при $Key = [223, 2.0708011, \{0.001, 0.0011\}, 0.9]$

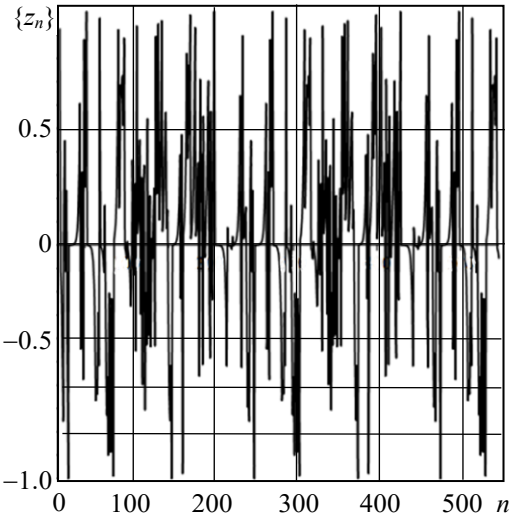


Рисунок 2.5 – Різниця двох T-періодичних траєкторій рівняння (3) при $Key = [223, 2.0708011, 0.001, \{0.9, 0.9001\}]$

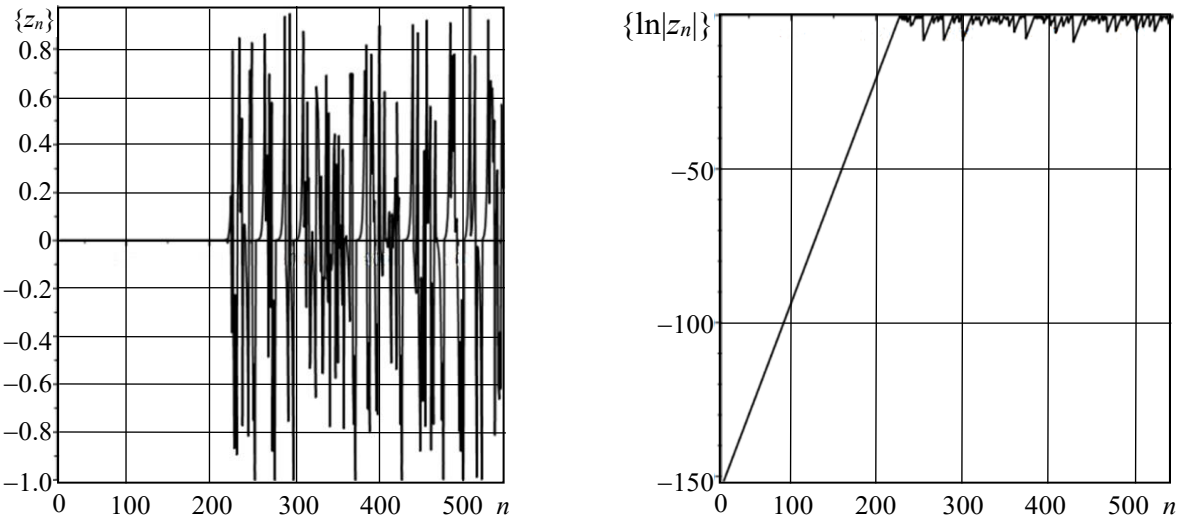
Розглянемо чутливість ключової послідовності до параметра T (періоду), тобто обчислимо дві відповідні періодичні траєкторії x_n та y_n (побудовані для $T = 223$ та $T = 227$ відповідно) та їх різниця z_n при ключі:

$$Key = \left[\{223,\ 227\}, 2.0708011,\ 0.001,\ 0.9\right].$$

Отримана траєкторія та точки послідовності $\{\ln(|z_n|)\}$ наведені на рисунку 2.6.

Аналіз результатів показав, що при $n < 210$ величини значень двох траєкторій x_n та y_n близькі між собою, зокрема $|z_n| < 10^{-50}$ при $n < 74$. При $230 < n < 440$ близькими будуть величини x_n та y_{n+4}; далі, при $460 < n < 670$ будуть величини x_n та y_{n+8} тощо. Таким чином, можна зробити висновок: варіація параметру T не дає потрібного розходження ключових послідовностей.

Істотними параметрами ключа є величини H, α, x_0. Якщо ці параметри будуть визначатися хоча б десятьма знаками після коми, то кількість різних варіантів ключів буде порядку 10^{30}, тобто біля 100 біт. При необхідності можна підвищити криптостійкість методу, використовуючи кілька ключів.



a *b*

Рисунок 2.6 – Різниця двох T-періодичних траєкторій рівняння (2.3) при $Key = \left[\{223,\ 227\}, 2.0708011,\ 0.001,\ 0.9\right]$: *a* – послідовність $\{z_n\}$; *b* – послідовність $\{\ln(|z_n|)\}$

2.2 Дослідження розроблених псевдохаотичних послідовностей

2.2.1 Дослідження статистичних характеристик псевдохаотичних послідовностей

Проведемо дослідження деяких статистичних характеристик псевдохаотичних послідовностей (2.6) та (2.7) при ключі $Key = [223,\ 2.070811,\ 0.001,\ 0.9]$.

Побудуємо гістограму та визначимо *середнє та середньоквадратичне відхилення* для послідовності (2.6).

Послідовність містить T^2 елементів. У нашому випадку 49729 елементів.

Середнє: $S = 4.4795...$, що трохи відхиляється від теоретичного середнього 4.5 рівномірно розподіленої дискретної випадкової величини.

Середньоквадратичне відхилення: $\sigma = 2.8634...$, теоретичне значення 2.8722….

Гістограми для перших 1000 елементів послідовності, елементів з номерами від 2000 до 3000 та всіх елементів послідовності (49729) наведено на рисунку 2.7 (розбиття проводилось на всім ділянок).

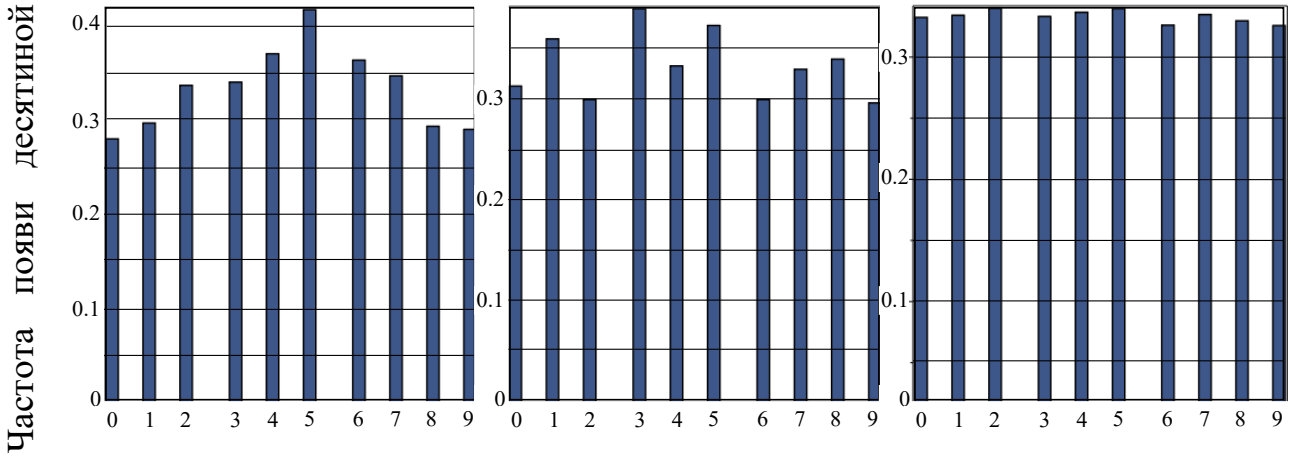
Таким чином, окремі ділянки послідовності не мають суворого рівномірного розподілу, хоча їх розподіли близькі до рівномірного.

Для подальшого аналізу властивостей послідовності $[I_1[j]: j = 1..49729]$ визначимо три величини:

накопичувальне середнє $\bar{I}_1(k) = \frac{1}{k}\sum_{j=1}^{k} I_1[j],\ k = 1, \dots, T^2$;

накопичувальне середньоквадратичне відхилення $\delta_1(k) = \frac{1}{k-1}\sum_{j=1}^{k}\left(I_1[j] - \bar{I}_1(k)\right)^2$;

накопичувальну дисперсію $\sigma_1(k) = \sqrt{\delta_1(k)},\ k = 2, \dots, T^2$.



a *b* *c*

Рисунок 2.7. Гістограма для послідовності: $a - [\mathrm{I}_1[j]: j = 1..1000]$; $b -$ $[\mathrm{I}_1[j]: j = 2000..3000]$; $c - [\mathrm{I}_1[j]: j = 1..49729]$, які побудовані при $T = 223$, $H = 2.0708011$,

$$\vartheta = \frac{H^T + 0.001 \cdot \dfrac{1}{H}}{H^T - 1},\ x_0 = 0.9$$

Тут звичайне вибіркове середнє одно $\bar{\mathrm{I}}_1(T^2)$, а вибіркова дисперсія $\sigma_1(T^2)$. Для побудови графіків накопичувальних середнього та дисперсії виведемо рекурентні формули для цих величин.

Оскільки $$\bar{\mathrm{I}}_1(k) = \frac{k-1}{k}\frac{1}{k-1}\sum_{j=1}^{k-1}\mathrm{I}_1[j] + \frac{1}{k}\mathrm{I}_1[k],$$

то

$$\bar{\mathrm{I}}_1(k) = \frac{k-1}{k}\bar{\mathrm{I}}_1(k-1) + \frac{1}{k}\mathrm{I}_1[k],\ \bar{\mathrm{I}}_1(1) = \mathrm{I}_1[1]. \qquad (2.8)$$

Далі:

$$\left(\mathrm{I}_1[j] - \bar{\mathrm{I}}_1(k)\right)^2 = \left(\mathrm{I}_1[j]\right)^2 - 2\mathrm{I}_1[j]\bar{\mathrm{I}}_1(k) + \left(\bar{\mathrm{I}}_1(k)\right)^2,$$

звідки

$$\delta_1(k) = \frac{1}{k-1}\sum_{j=1}^{k}\left(\mathrm{I}_1[j]\right)^2 - \frac{2}{k-1}\bar{\mathrm{I}}_1(k)\sum_{j=1}^{k}\mathrm{I}_1[j] + \frac{k}{k-1}\left(\bar{\mathrm{I}}_1(k)\right)^2 = \frac{1}{k-1}\sum_{j=1}^{k}\left(\mathrm{I}_1[j]\right)^2 - \frac{k}{k-1}\left(\bar{\mathrm{I}}_1(k)\right)^2.$$

Позначимо

$$\bar{\mathrm{I}}_1^{(2)}(k)=\frac{1}{k-1}\sum_{i=1}^{k}\left(\mathrm{I}_1[j]\right)^2,$$

Тоді

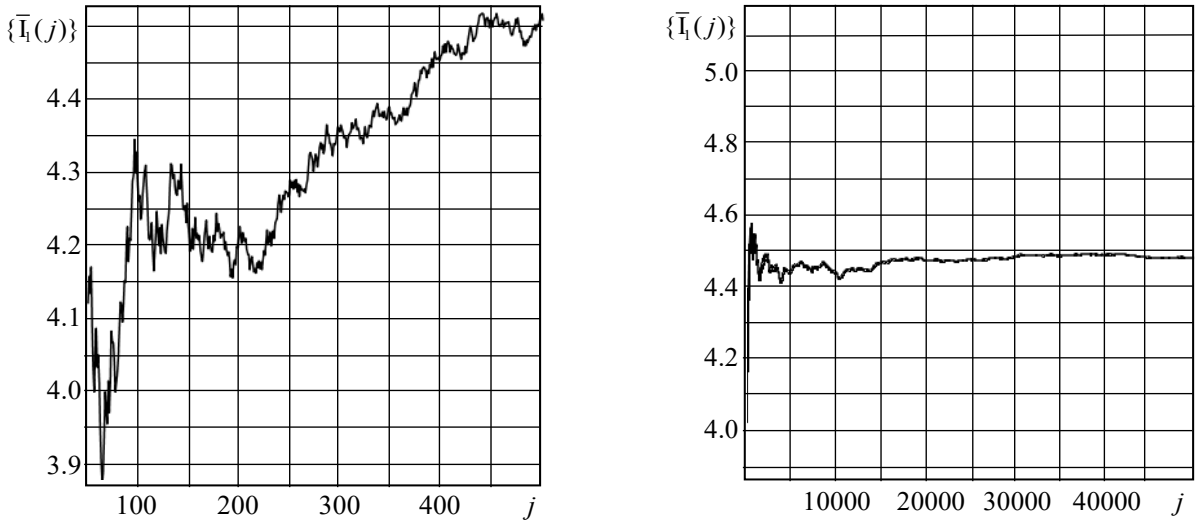
$$\bar{\mathrm{I}}_1^{(2)}(k)=\frac{k-2}{k-1}\frac{1}{k-2}\sum_{j=1}^{k-1}\left(\mathrm{I}_1[j]\right)^2+\frac{1}{k-1}\left(\mathrm{I}_1[k]\right)^2=\frac{k-2}{k-1}\bar{\mathrm{I}}_1^{(2)}(k-1)+\frac{1}{k-1}\left(\mathrm{I}_1[k]\right)^2.$$

Таким чином, справедливо рекурентне співвідношення

$$\begin{cases}\delta_1(k)=\bar{\mathrm{I}}_1^{(2)}(k)-\dfrac{k}{k-1}\left(\bar{\mathrm{I}}_1(k)\right)^2;\\ \bar{\mathrm{I}}_1^{(2)}(k)=\dfrac{k-2}{k-1}\bar{\mathrm{I}}_1^{(2)}(k-1)+\dfrac{1}{k-1}\left(\mathrm{I}_1[k]\right)^2.\end{cases}\tag{2.9}$$

При цьому $k=3,\ldots,N$ та $\bar{\mathrm{I}}_1^{(2)}(2)=\left(\mathrm{I}_1[1]\right)^2+\left(\mathrm{I}_1[2]\right)^2$.

Графіки величин $\{\bar{\mathrm{I}}_1(j)\}_{j=1}^{500}$, $\{\bar{\mathrm{I}}_1(j)\}_{j=1}^{T^2}$ зображені на рисунку 2.8. Графіки величин $\{\sigma_1(j)\}_{j=1}^{500}$, $\{\sigma_1(j)\}_{j=1}^{T^2}$ зображені на рисунку 2.9.



a *b*

Рисунок 2.8 – Графіки величин: *a* – $\{\bar{\mathrm{I}}_1(j)\}_{j=1}^{500}$; *b* – $\{\bar{\mathrm{I}}_1(j)\}_{j=1}^{T^2}$

Таким чином, відсутність періодичності у поведінці графіків накопичувальних середнього та дисперсії сигналізує про відсутність закономірностей між окремими частинами послідовності, що може свідчити про її псевдохаотичний характер.

Аналогічний аналіз проведемо для послідовності (2.). При цьому врахуємо, що у формулах (2.8), (2.9) індекс 1 треба замінити на 2.

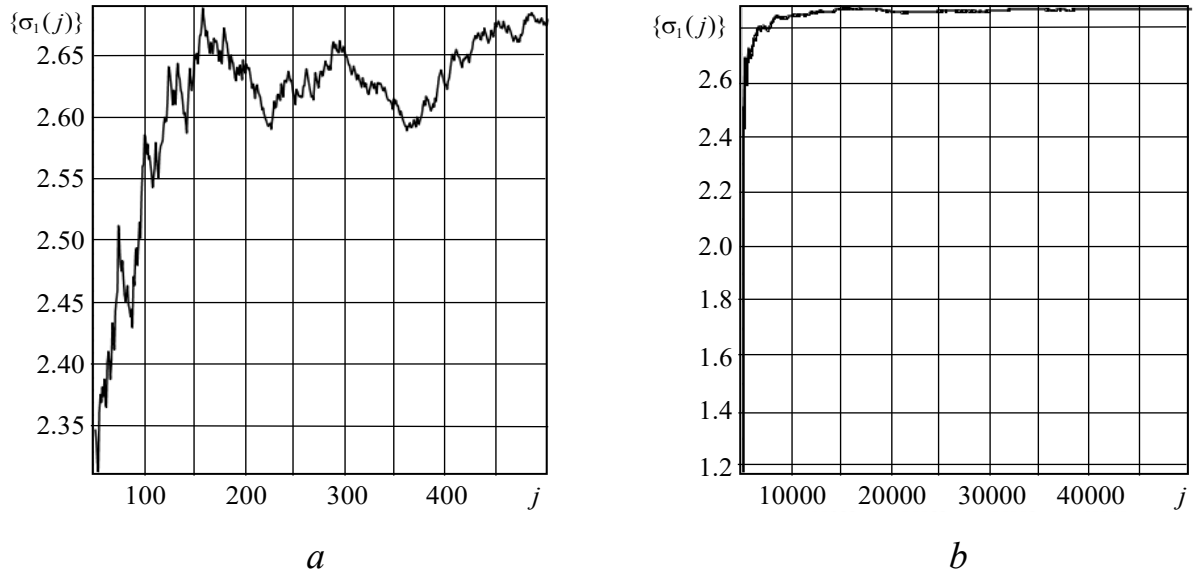


Рисунок 2.9 – Графіки величин: a – $\{\sigma_1(j)\}_{j=1}^{500}$; b – $\{\sigma_1(j)\}_{j=1}^{T^2}$

Нижче наводяться відповідні графіки (рис. 2.10, 2.11, 2.12).

Таким чином, проведений аналіз основних статистичних характеристик псевдохаотичних послідовностей (2.6) та (2.7) при ключі $Key = [223,\ 2.070811,\ 0.001,\ 0.9]$ свідчить про їх псевдохаотичний характер, про відсутність закономірностей між окремими частинами послідовності що дозволяє їх рекомендувати для використання у криптографічних методах.

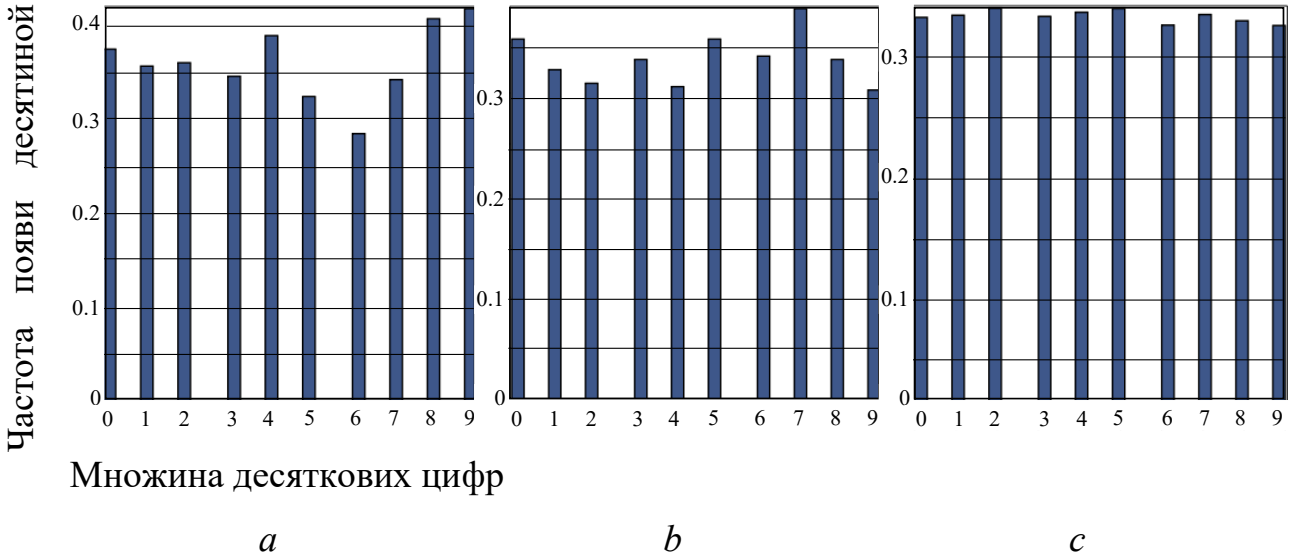


Рисунок 2.10 – Гістограма для послідовності: a – $[\mathrm{I}_2[j]: j = 1..1000]$;

b – $[\mathrm{I}_2[j]: j = 2000..3000]$; c – $[\mathrm{I}_2[j]: j = 1..49729]$, яка побудована при $T = 223$,

$$H = 2.0708011,\ \vartheta = \frac{H^T + 0.001 \cdot \frac{1}{H}}{H^T - 1},\ x_0 = 0.9$$

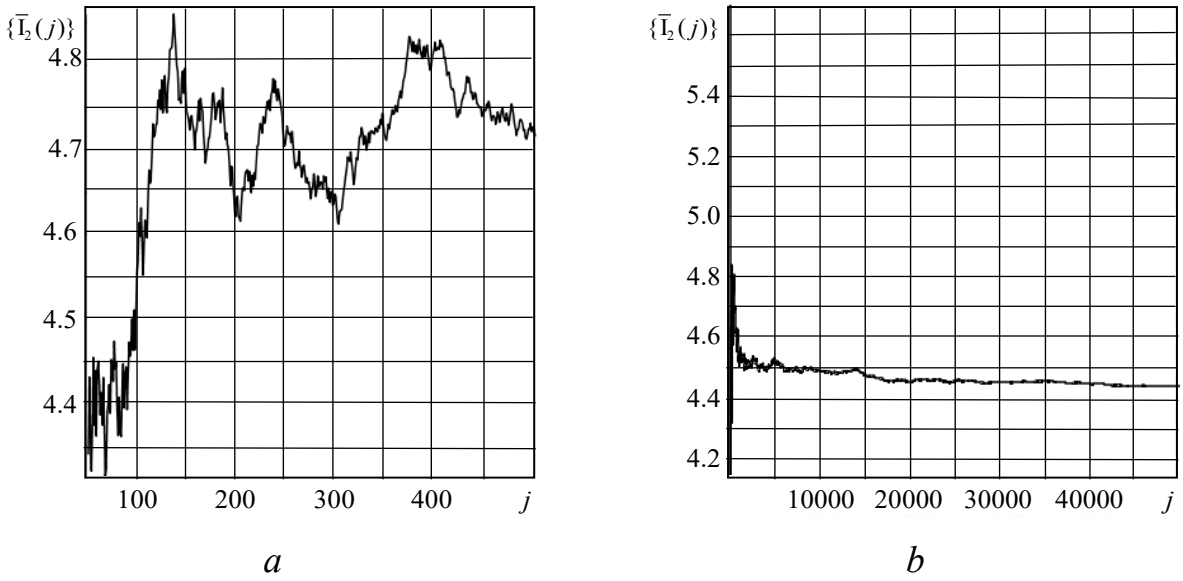
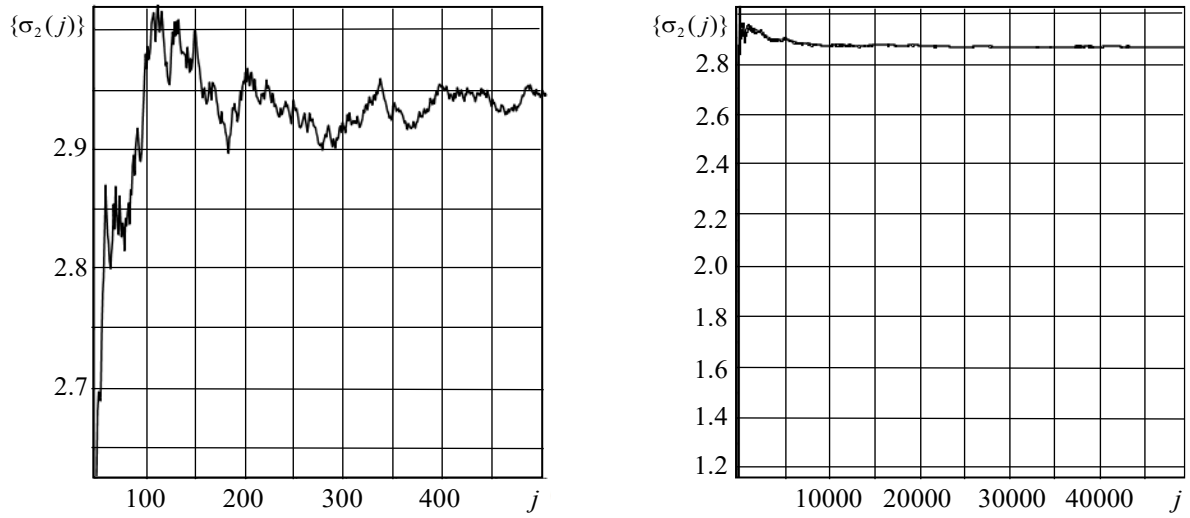


Рисунок 2.11 – Графіки величин: a – $\{\bar{\mathrm{I}}_2(j)\}_{j=1}^{500}$; b – $\{\bar{\mathrm{I}}_2(j)\}_{j=1}^{T^2}$



A *b*

Рисунок 2.12 – Графіки величин: *a* – $\{\sigma_2(j)\}_{j=1}^{500}$; *b* – $\{\sigma_2(j)\}_{j=1}^{T^2}$

2.2.2 Дослідження псевдохаотичних послідовностей візуальним способом

Існує відома проблема в тестуванні псевдохаотичної послідовності на некорельованість, яка полягає в тому, що використання точкових характеристик (середнє, дисперсія), так само як і кореляційної функції або навіть функції, що залежать від моментів більш високих порядків, може виявитися неефективним.

Тому додатково застосуємо візуальний спосіб дослідження, для якого здійснимо лінійні перетворення, щоб провести візуалізацію – формування зображення у градаціях сірого:

– розіб'ємо послідовність $[\mathrm{I}_1[j]: j = 1..49729]$ на елементи, що складаються з послідовних трійок десяткових чисел;

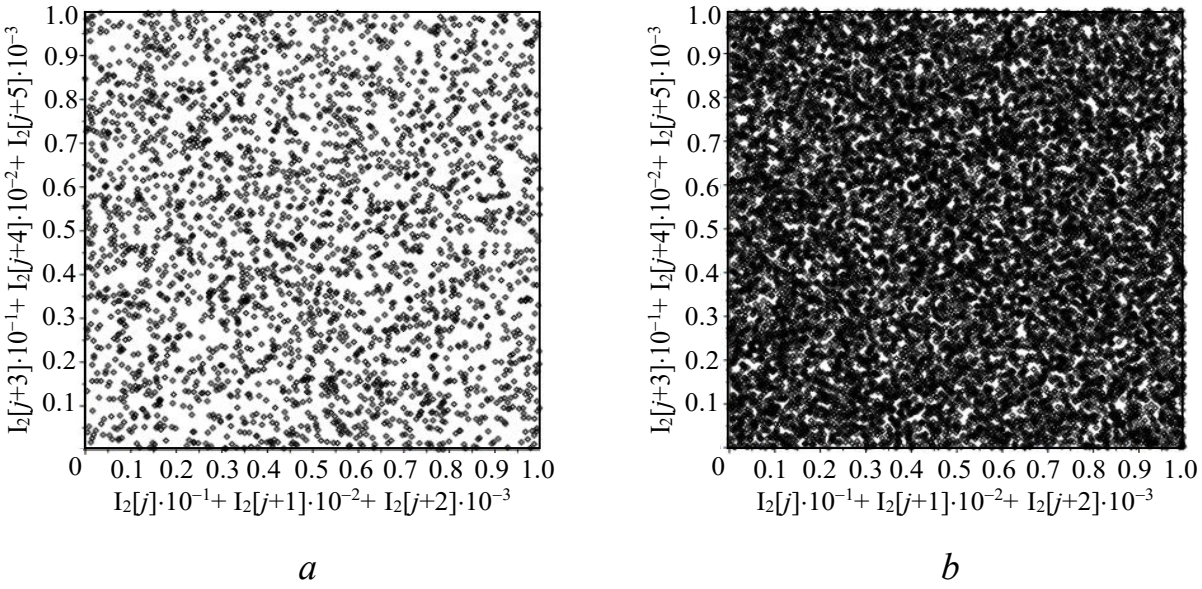
– поділимо отримані трицифрові числа на 10^3. Одержуємо нову послідовність, що складається з десяткових чисел, що визначаються трьома першими розрядами:

$$\left[\mathrm{I}_1[j]\cdot 10^{-1} + \mathrm{I}_1[j+1]\cdot 10^{-2} + \mathrm{I}_1[j+2]\cdot 10^{-3} : j = 1..49727\right].$$

– зобразимо на площині точки з координатами:

$$\left\{\mathrm{I}_1[j]\cdot 10^{-1} + \mathrm{I}_1[j+1]\cdot 10^{-2} + \mathrm{I}_1[j+2]\cdot 10^{-3},\ \mathrm{I}_1[j+3]\cdot 10^{-1} + \mathrm{I}_1[j+4]\cdot 10^{-2} + \mathrm{I}_1[j+5]\cdot 10^{-3}\right\}. \qquad (10)$$

Отримане зображення дозволить візуально оцінити хаотичність послідовних трійок чисел. На рисунку 2.13 наведені точки з координатами (2.10) для $j = 1..3000$ та $j = 5000..20000$. Можна бачити відсутність явної кореляції у послідовності (2.6).



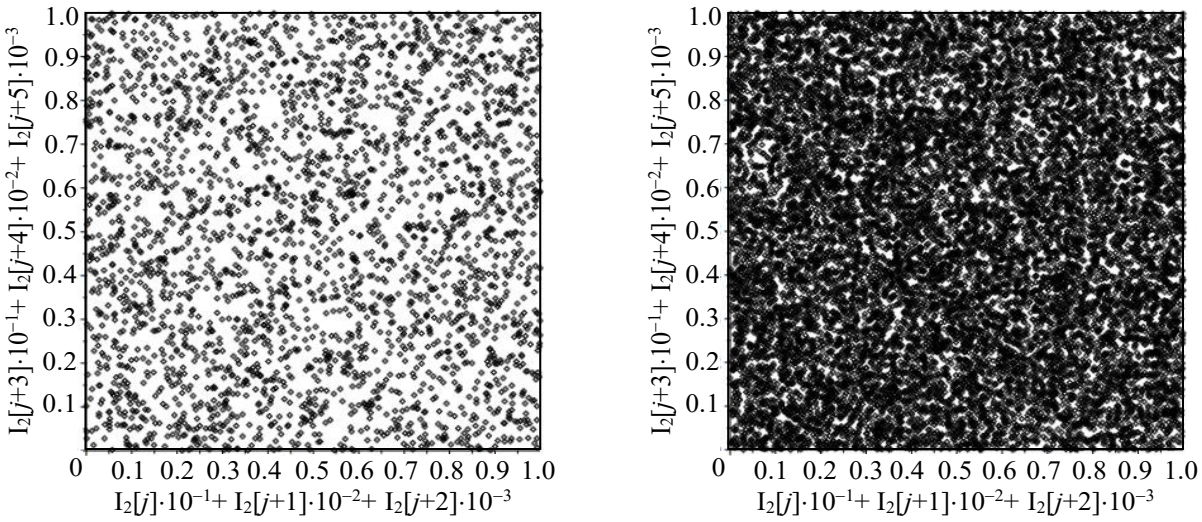
a *b*

Рисунок 2.13 – Точки с координатами (10) для: *a*) $j = 1..3000$ и *b*) $j = 5000..20000$, які згенеровано послідовністю (6) при $T = 223$, $H = 2.0708011$, $\vartheta = \dfrac{H^T + 0.001 \cdot \dfrac{1}{H}}{H^T - 1}$, $x_0 = 0.9$

Аналогічно на рисунку 2.14 представлено послідовність (2.7).

Візуальний аналіз відповідних графіків показує, що послідовність (2.7) є більш некорельованою, ніж (2.6).

Однак слід відмітити, що послідовність (6) будується послідовно з обчисленням точок циклу $\{\eta_1, \ldots, \eta_T\}$, у той час, як для побудови послідовності (2.7) необхідно знати відразу весь цикл, що призводить до зменшення швидкодії алгоритму та збільшення пам'яті, що використовується.



a *b*

Рисунок 2.14 – Точки с координатами (10) (с заміною індексу 1 на 2) для: *a*) $j = 1..3000$ и *b*) $j = 5000..20000$, які згенеровано послідовністю (6) при $T = 223$,

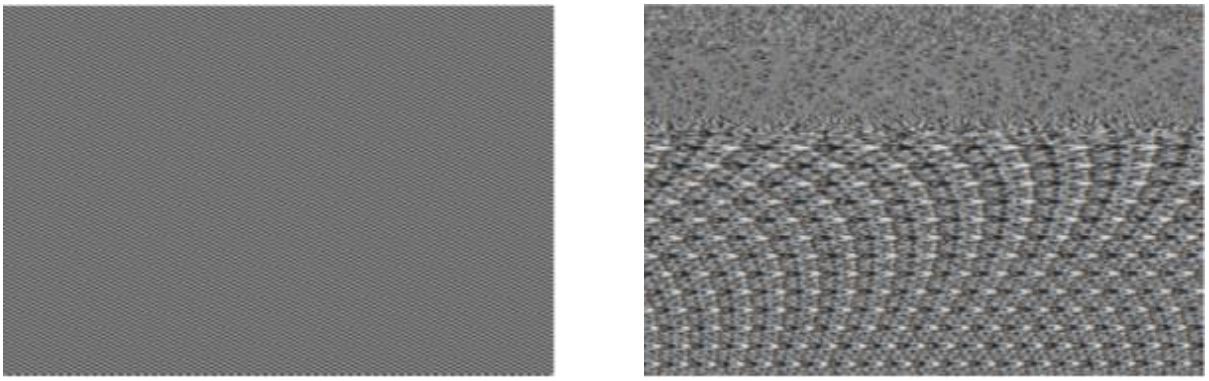
$$H = 2.0708011,\ \vartheta = \frac{H^T + 0.001 \cdot \frac{1}{H}}{H^T - 1},\ x_0 = 0.9$$

Також для наочності можна провести візуалізацію – формування кольорового зображення. Для цього з послідовності $[\mathrm{I}[j]: j = 1..N]$ генеруються три послідовності $R = [0.1 \cdot \mathrm{I}[j]: j = 1..N],\ G = [0.1 \cdot \mathrm{I}[j+1]: j = 1..N],\ B = [0.1 \cdot \mathrm{I}[j+2]: j = 1..N]$.

Тобто кожному значенню послідовності знаходиться відповідне значення пікселя за допомогою згенерованих послідовностей R, G, B, що видповідає кольору у форматі *RGB*.

Візьмемо, наприклад, висоту зображення $h = 438$ пікселів, ширину $w = 648$ пікселів. Всього використовується 279936 пікселів. Згенеруємо послідовність $[j \bmod 10: j = 1..N]$ (число N обирається не менш, ніж 279938), яка є явно корельованою. При цьому гістограма, середнє та дисперсія цієї послідовності буде, як у рівномірно розподіленої. Для порівняння згенеруємо послідовність перших цифр дробної частини виразу $\sin(j^2 + 1),\ j = 1..N$. Побудуємо зображення цих послідовностей у форматі *RGB* (рис. 2.16).

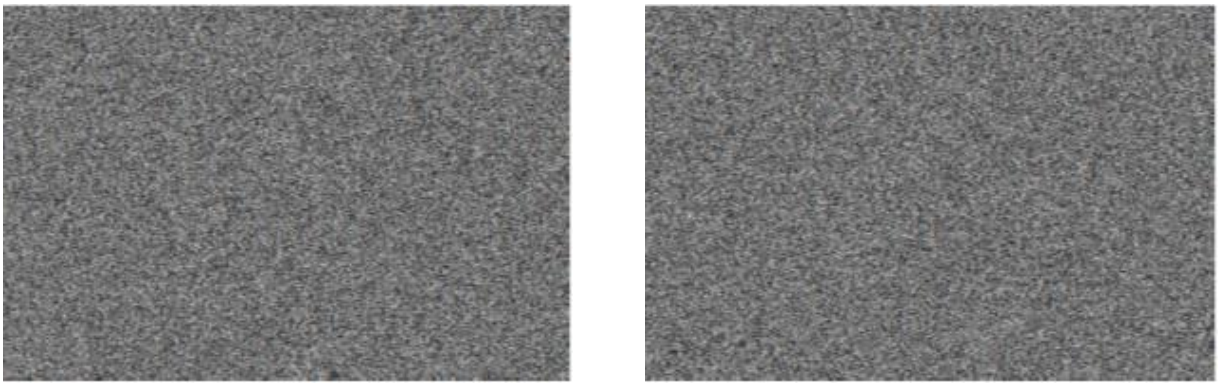
Так як будь яка кореляція повинна виявлятися у вигляді візуальної регулярності, можна стверджувати, що послідовності, що генерують зображення на рисунку 2.15, сильно корельовані.



a *b*

Рисунок 2.15 – Зображення у формате *RGB* для послідовностей:
a) $[j \bmod 10 : j = 1..N]$; *b*) $[trunc(10 \cdot \sin(j^2 + 1)) : j = 1..N]$.

Аналогічне зображення побудовано для послідовностей (2.6) та (2.7) (рис. 2.16).

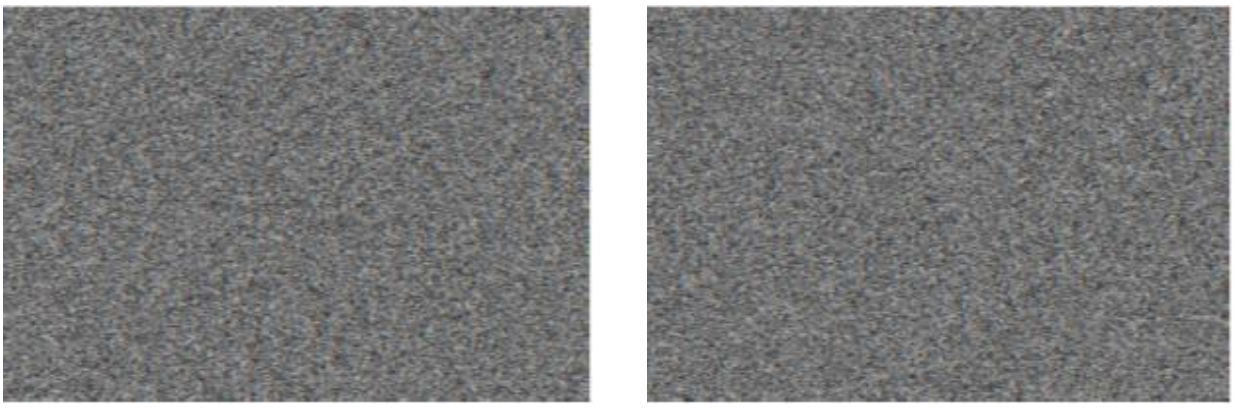


a *b*

Рисунок 2.16 – Зображення у формате *RGB* для послідовностей (6) (*a*) та (7) (*b*)

Для цих послідовностей регулярна структура візуально не спостерігається. Для візуального порівняння приведемо зображення у форматі *RGB* для послідовності перших 286000 десяткових цифр чисел π та e (рисунок 2.17).

-



a *b*

Рисунок 2.17 – Зображення в форматі *RGB* для послідовностей перших 286000 десяткових цифр чисел: *a*) π; *b*) e

Порівняння зображень, що наведені на рисунках 2.17 та 2.18 свідчить про схожу випадковість розробленої послідовності з управлінням та десяткових цифр чисел π та e. Але останні не є секретними та непередбачуваними.

Запропоновано метод генерації псевдохаотичних послідовностей на основі відображення Тент:

Крок 1. Згенерувати псевдохаотичну послідовність, елементи якої укладені між нулем і одиницею, і скласти поелементно по модулю 1 з послідовностями R, G та B. Зрозуміло, що замість однієї псевдохаотичної послідовності, можна згенерувати три різні подібні послідовності.

Нехай послідовність $[\mathrm{I}[j]: j = 1..N]$ згенерована згідно з правилом (2.6) або (2.7) з відповідним ключом: $Key = [T,\ H,\ \pm\alpha,\ x_0]$.

Визначимо послідовність

$$\left[\sum_{k=1}^{p} \mathrm{I}[j+k-1]\cdot 10^{-k} : j = 1..N+1-p\right], \qquad (2.11)$$

де $1 \le p \le 15$ (експерименті показують, що достатньо брати $p = 2$ або 3).

Якщо T таке, що відповідне N менш ніж n, то необхідно згенерувати кілька ключових послідовностей (з різними ключами).

Крок 2. Зашифрувати елементи. Нехай $r-i$-й елемент послідовності R, $\alpha-i$-й елемент ключової послідовності.

Зашифрований елемент $\hat{r}$ в найпростішому випадку буде обчислюватися за формулою

$$\hat{r}=\{r+\alpha\}, \tag{2.12}$$

де функція $\{\cdot\}$ означає цілу частину числа.

Крок 3. Виконати перемасштабування.

Формула (2.12) допускає:

$$r=\begin{cases}\hat{r}-\alpha, & \hat{r}-\alpha>0;\\ 1+\hat{r}-\alpha, & \hat{r}-\alpha<0.\end{cases} \tag{2.13}$$

Формула (2.13) дозволяє однозначно відновити значення вихідного пікселя за зашифрованим значенням у всіх випадках, крім $\hat{r}-\alpha=0$. У цьому випадку можливі два варіанти $r=0$ або 1. Для того, щоб унеможливити неоднозначність, можна виконати перемасштабування послідовностей R, G и B: $X\to(1-\varepsilon)X$, де ε — мале число, більш ніж 10^{-15}. Тоді у випадку $\hat{r}-\alpha=0$ обов'язково $r<1$, тобто $r=0$. Фізично перемасштабування означає відсутність суто білого кольору. Для малих ε цей факт практично нічого не змінює. Зрозуміло, що за потреби можна виконати і зворотне перемасштабування $X\to X/(1-\varepsilon)$.

2.3 Метод шифрування зображення на підставі запропонованої генерації псевдовипадкової послідовності

Наведені вище дослідження показали, що цикл згенерованої псевдовипадкової послідовності фактично є необчислюваним для кібератак. Цей цикл є локально асимптотично стійким. Це означає, що отримана траєкторія залежить від незначних збурень, помилок обчислень та округлень. Більше того, можна очікувати, що при одних і тих же значеннях x_0, T, H, ϑ будуть виходити однакові цикли різних комп'ютерах. Важливим питанням є питання точності

обчислень. Загалом ця точність повинна залежати від довжини циклу. Обчислювальні експерименти показують, що потрібно вибирати і розрядність:

$$Digits = T + 2(k_1 + k_2),\ k_1, k_2 \approx 10 - 15,\ k_1 < k_2.$$

У цьому випадку можна використовувати всі значущі цифри чисел для побудови ключових псевдохаотичних послідовностей (для посилення хаотичності можна використовувати цифри з позиції k_1 до $T + k_1 - 1$). Початкових точок може бути кілька. Можна генерувати послідовності, змінюючи параметри T, H и ϑ.

Практичні рекомендації щодо вибору керуючого параметру:

$$\vartheta = \frac{H^T - \alpha_1 \frac{1}{H}}{H^T + 1} \text{ або } \vartheta = \frac{H^T + \alpha_2 \frac{1}{H}}{H^T - 1}, (\ 0 < \alpha_1 < 0.001,\ 0 < \alpha_2 < 0.001).$$

Далі можна ще більше посилити хаотичність ключової послідовності: спочатку вибирати всі числа із послідовності $\{x_j\}_{j=T_0}^{T_0+T}$ (T_0 - деяке задане число), що стоять на k_1 місті після коми у кожному x_j, далі таким же чином обирати числа, що стоять на $k_1 + 1$ місті тощо. Згенерована послідовність містить pT^2 елементи, де p – число початкових точок.

Насінням генерації є ключ $Key = [T, H, \alpha_1, \alpha_2, \{x_0\}]$, де $\{x_0\}$ – множина початкових точок. Якщо параметри $H, \alpha_1, \alpha_2, \{x_0\}$ визначаються m цифрами, то можливих варіантів послідовностей більш $10^{(3+p)m}$. Такий простір ключової послідовності зламати неможливо.

На основі запропонованого методу генерації псевдовипадкової послідовності розроблено метод шифрування зображень.

Структура методу шифрування зображень виглядає наступним чином.

1. Генерується короткий ключ $Key = [T, H, \alpha_1, \alpha_2, \{x_0\}]$. Ключ зберігається на стороні, що передає, і передається на приймальну сторону.

2. Зображення з висотою h пікселів та шириною w пікселів складається з $n = h \cdot w$ пікселів, тобто розглядається як масив елементів, кожному з яких приписаний тривимірний вектор десяткових чисел. Ці числа мають 15 розрядів і укладені між нулем та одиницею. Вектор (0, 0, 0) визначає піксель чорного кольору, а вектор (1, 1, 1) білого кольору. Координати характеризують відтінки червоного, зеленого та синього кольорів відповідно. Іноді розглядається четверта координата, яка характеризує прозорість кольору. Для шифрування зображення на підставі короткого ключа треба згенерувати псевдохаотичну послідовність, елементи якої укладені між нулем і одиницею, і поелементно скласти по модулю 2 з послідовностями R, G и B. Це відомий шифр Вернама (або XOR cipher). Замість однієї псевдохаотичної послідовності, можна згенерувати три різні подібні послідовності.

3. Зашифроване зображення передається на приймальну сторону. На приймальній стороні на підставі короткого ключа генерується така сама псевдовипадкова послідовність і зашифроване зображення розширюється також операцією XOR.

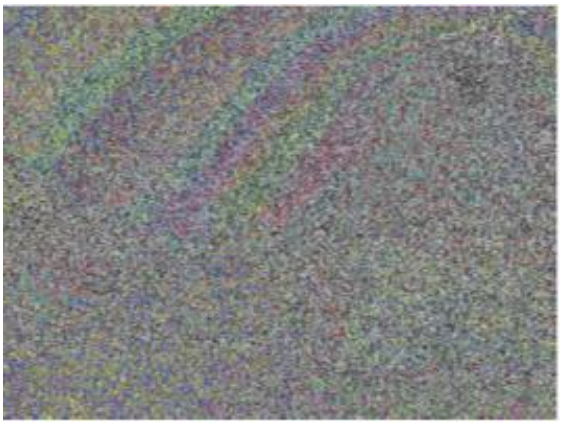
Застосуємо наведений вище метод шифрування зображень. Зображення з висотою h пікселів та шириною w пікселів містить $n = h \cdot w$ пікселів. Тобто зображення можна розглядати як масив з n елементів, кожному з яких приписано тривимірний вектор десяткових чисел. Ці числа мають 15 розрядів і укладені між нулем та одиницею. Вектор (0, 0, 0) визначає піксель чорного кольору, а вектор (1, 1, 1) білого кольору. Координати характеризують відтінки червоного, зеленого та синього кольорів відповідно. Іноді розглядається четверта координата, яка характеризує прозорість кольору.

Розглянемо зображення, подане на рисунку 2.19. Воно складається з 238572 пікселів ($h = 423$, $w = 564$). Для шифрування візьмемо ключ $Key = [223,\ 2.070811,\ 0.001,\ 0.9]$ та згенеруємо ключову послідовність. Вона містить 49729 елементів. Необхідно згенерувати додаткові послідовності. Зробимо це, вибираючи ключі $Key_j = [223,\ 2.07081j,\ 0.001,\ 0.9]$, $j = 2..6$. Об'єднана ключова

послідовність містить $49729 \cdot 6 = 298374$ елементів, що достатньо виконання процесу шифрування. Результати процесу шифрування за допомогою послідовностей (2.6) (2.7) Зашифроване таким чином зображення представлене на рисунку 2.19.

Рисунок 2.18 – Тестове зображення для шифрування

a

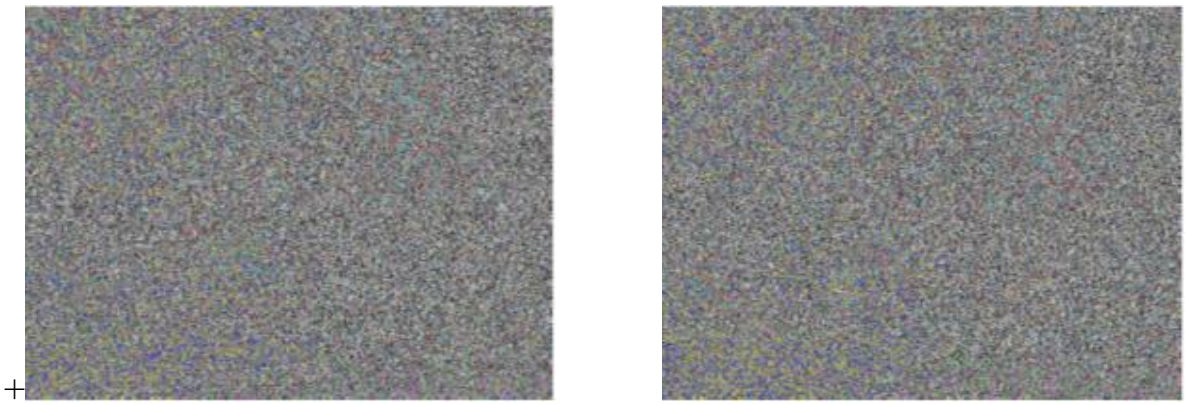


b

Рисунок 2. 19 – Зашифроване тестове зображення з використанням послідовності (2.6) (випадок *a*) та (2.7) (випадок *b*)

На шифрованих зображеннях простежується регулярна структура.

Якщо використовувати модифіковану версію (2.14), то зашифровані зображення виглядають без наявності видимої регулярної структури (рисунок 2.20).



a *b*

Рисунок 2.20 – Зашифроване тестове зображення з використанням модифікації (2.14) при $p = 2$ для послідовності (2.6) (випадок *a*) та (2.7) (випадок *b*)

Розглянемо ще один приклад (тестове зображення наведено на рисунку 2.21).

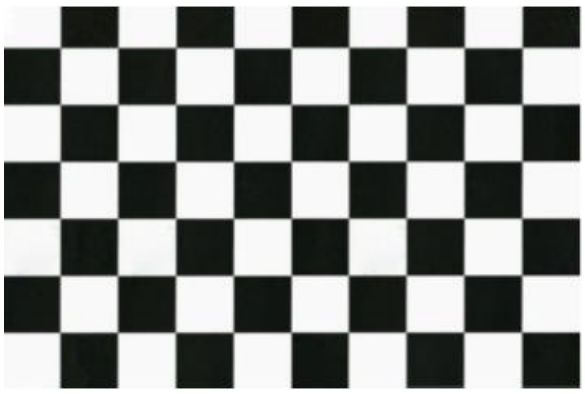
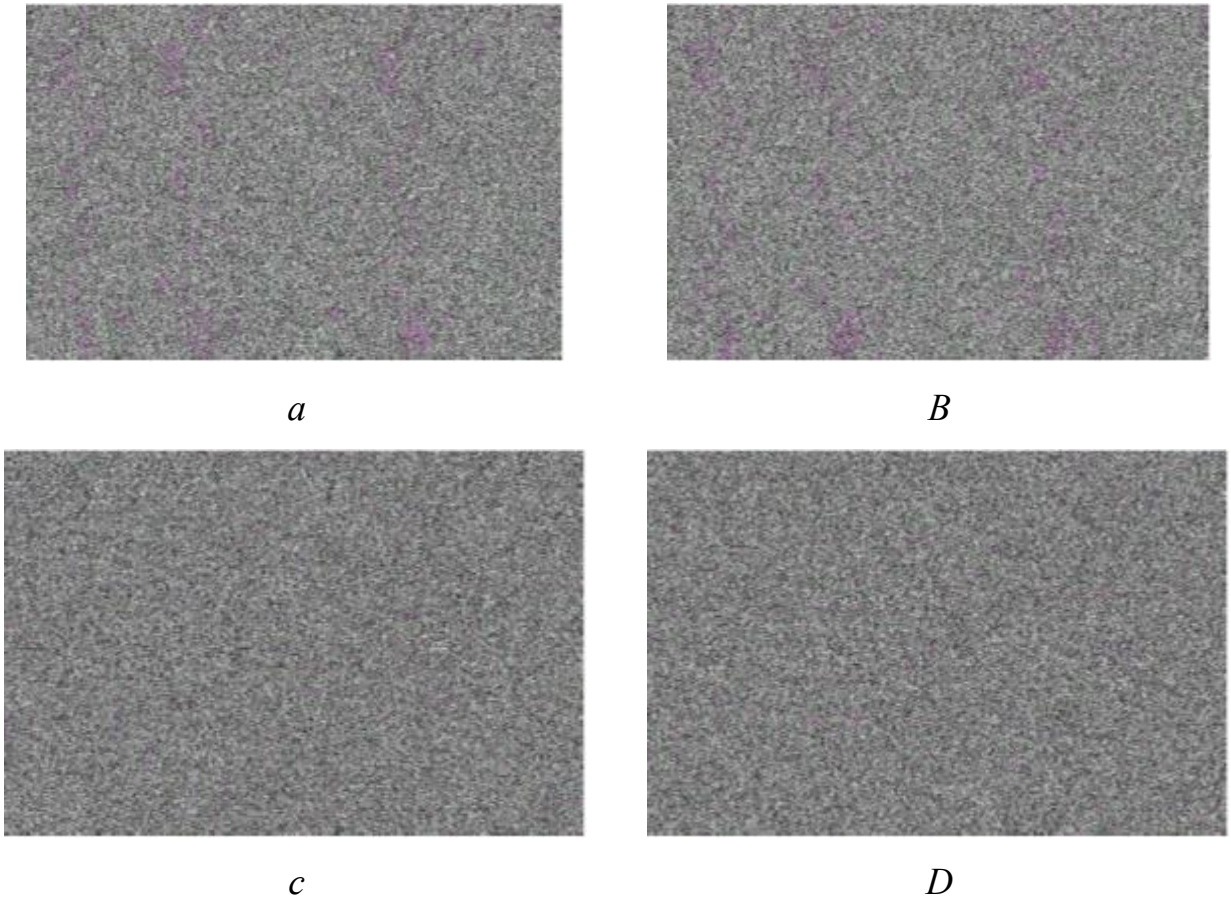


Рисунок 2.21 –Тестове зображення для шифрування

Результати шифрування представлені на рисунку 2.22. Видно, що просте використання послідовностей (2.6) і (2.7) призводить до регулярної структури (випадки *a* та *b*). При модифікації (2.14) ($p = 2$) видима регулярність зашифрованого зображення зникає.



a *B*

c *D*

Рисунок 2.22 – Зашифроване тестове зображення для послідовностей (2.6) та (2.7): без модифікації (випадки *a* та *b*); з модифікацією (2.14) (випадки *c* та *d*)

2.4 Метод формування інтегрального показника якості шифрування зображень

2.4.1 Формування інтегрального показника якості шифрування зображень

Для порівняння якості шифрування запропонованим методом на підставі відомих метрик якості необхідно сформувати інтегральну метрику якості.

Метрики якості шифрування зображень дозволяють оцінити, наскільки ефективно та безпечно зображення було зашифровано. Нижче розглянуто такі метрики.

Кореляція. Якісний алгоритм шифрування має максимально знизити кореляцію між сусідніми пікселями. Коефіцієнт кореляції вказує на лінійний зв'язок між сусідніми пікселями. При ефективному шифруванні він має бути близьким до нуля [58].

Коефіцієнт кореляції розраховується за такими співвідношеннями:

$$\begin{cases} r_{xy} = \dfrac{\operatorname{cov}(x,y)}{\sqrt{D(x)D(y)}}, \\ \operatorname{cov}(x,y) = E(\left[x - E(x)\right]\left[y - E(y)\right], \\ E(x) = \dfrac{1}{N}\sum\limits_{i=1}^{N} x_i, \\ E(y) = \dfrac{1}{N}\sum\limits_{i=1}^{N} y_i, \\ D(x) = \dfrac{1}{N}\sum\limits_{i=1}^{N}\left[x_i - E(x)\right], \\ D(y) = \dfrac{1}{N}\sum\limits_{i=1}^{N}\left[y_i - E(y)\right], \end{cases}$$

де x и y – пара сусідніх пікселів, $E(x)$ и $E(y)$ – математичне очікування інтенсивності пікселів, $D(x)$ и $D(y)$ – дисперсія інтенсивності.

Для врахування кореляції між сусідніми пікселями коефіцієнт кореляції повинен оцінюватися для всіх можливих геометричних розташувань сусідніх пікселів: горизонтального – r_{xy}^{horiz}, вертикального – r_{xy}^{vert}, діагонального – r_{xy}^{diag}, антидіагонального – r_{xy}^{diag}. Для оцінки «найслабшого» напряму придушення кореляції пікселів вихідного зображення запропоновано розраховувати максимальний коефіцієнт кореляції.

$$r_{xy}^{\max} = \max\left\{ r_{xy}^{horiz} + r_{xy}^{vert} + r_{xy}^{diag} + r_{xy}^{antidiag} \right\}.$$

Інформаційна ентропія зашифрованого зображення.

Інформаційна ентропія зашифрованого зображення С розраховується як:

$$H(C) = \sum_{i=0}^{2^N - 1} p(m_i) \log \frac{1}{p(m_i)} (bit),$$

де N – кількість різних значень пікселів ($N = 256$ для 8-бітного зображення). Для ідеального шифру 8 біт.

Локальна ентропія. Більш точною мірою випадковості зашифрованого зображення є ентропія, розрахована для локальних блоків зображення. Навіть якщо зашифроване зображення має дуже високу ентропію Шеннона по всьому зображенню, зображення може містити деякі блоки з низькою ентропією. У цьому сенсі воно не є ідеально зашифрованим, незалежно від того, наскільки високою є його глобальна ентропія [59,60].

Локальна ентропія розраховується за співвідношенням

$$\overline{H(C)} = \sum_{i=1}^{k} \frac{H(S_k)}{k}(bit) \ ,$$

де $S_1, S_2, ..., S_k$ – випадково вибрані k блоків зображення, які не перекриваються, з T_B пікселями кожен, та знаходяться всередині зашифровані зображення.

Обчислюються $H(S_k)$ $i \in \{1,2,...,k\}$ та далі оцінюється $\overline{H(C)}$. Для ідеального шифру $\overline{H(C)}$ також містить 8 біт.

Метрики резистентності к атакам.

Метрика NPCR (Number of Pixels Change Rate) використовується з метою оцінки лавинного ефекту алгоритму шифрування. Вона вимірює, наскільки сильно змінюється зашифроване зображення після шифрування при зміні одного пікселя у вихідному зображенні. Формується відповідно до алгоритму шифрування зашифроване зображення $C^{(1)}$. Далі у вихідному зображенні змінюється один піксель і для зміненого зображення формується зашифроване зображення $C^{(2)}$. *NPCR* розраховується як

$$NPCR = \frac{1}{N}\sum_{i=1}^{N}\left(\frac{C^{(1)} \otimes C^{(2)}}{255}\right)\cdot 100\%,$$

де N – число пікселів в зображенні,

$\otimes$ – операція XOR.

NPCR показує, яка доля пікселів змінилась при зміні одного бита в вихідному зображенні. Теоретично ідеальне значення *NPCR* 99.6%.

Метрика UACI (Unified Average Changing Intensity) використовується для оцінки якості шифрування зображень. Вона показує наскільки сильно

змінюється інтенсивність пікселів при зміні одного пікселю в початковому зображенні.

UACI розраховується по співвідношенню:

$$UACI = \frac{1}{N}\sum_{i=1}^{N}\left(\frac{C^{(1)} - C^{(2)}}{255}\right)\cdot 100\% \cdot$$

Теоретичне ідеальне значення *UACI* 33.4% (у припущенні, що інтенсивність пікселів $C^{(1)}$ и $C^{(2)}$ має рівномірний розподіл).

Для всебічної оцінки якості шифрування зображення запропоновано таку систему критеріїв якості, засновану на перерахованих метриках:

$$\begin{cases} Crit_1 = r_{xy}^{\max} \\ Crit_2 = H(C) \\ Crit_3 = \overline{H(C)} \\ Crit_4 = NPCR \\ Crit_5 = UACI \end{cases}.$$

При порівняльному аналізі якості шифру з відомими алгоритмами шифрування така багатокритеріальна система складна для винесення рішення про перевагу застосування того чи іншої варіанта захисного перетворення зображення. Запропоновано сформувати інтегрований показник якості шифрування з урахуванням системи вище наведених критеріїв. Це здійснено формуванням згортки критеріїв. Для формування згортки застосований спосіб відстані від ідеальної точки. Ідеальною точкою називається вектор значень критеріїв, у якому кожен із n критеріїв досягає свого найкращого значення $Crit_i^{ideal\_point}, i = \overline{1,n}$.

Тоді інтегральний показник якості *IntQI*

$$IntQI = \left(\sum_{i=1}^{n}\lambda_i^p (Crit_i - Crit_i^{ideal\_point})^p\right)^{\frac{1}{p}},$$

де $\lambda_i, i = \overline{1,n}$ – нормуючі коефіцієнти;

p – натуральний показник ступеню.

Застосовуючи до вищенаведеної формули норму L_2 маємо:

$$IntQI = \sqrt{\sum_{i=1}^{5} \lambda_i^2 (Crit_i - Crit_i^{ideal\_point})^2} \ .$$

Розроблений інтегральний критерій дозволяє проводити комплексне оцінювання якості шифрування та проводити обґрунтований вибір потокових та блочних шифрів.

2.4.2 Експериментальна оцінка якості розробленого алгоритму шифрування

Для оцінки якості розробленого алгоритму шифрування Modified Tent Cipher (MTC) було проведено наступний попередній експеримент. Експеримент проводився на платформі Win10 (64-біт) з процесором Intel Core i7-9750H з частотою 2.60 GHz та 8 GB of RAM.

20 зображень розміром 564×423 пікселів були зашифровані шифром MTC, сучасним українським потоковим шифром ДСТУ 8845:2019 «Струмок» з ключем довжиною 256 біт [61] та блоковим шифром AES з довжиною ключа 256 біт [62]. Для всіх зашифрованих зображень обчислювалися вказані вище критерії якості та $IntQI$. Усереднені за 20 зображеннями показники наведені у таблиці 2.1. Приклад шифрування зображення шифром MTC наведено на рис. 2.24. Зашифровані шифрами зображення Strumok-256 та AES-256 візуально не відрізняються від наведеного на рисунку 2.24. При розрахунку локальної ентропії із зашифрованих зображень випадково вибиралися k=16 блоків розміром 32×32 пікселя. Експерименти проводилися на платформі Win10 (64-біт) з процесором Intel Core i7-9750H із частотою 2.60 GHz та 8 GB of RAM.

Крім того, для кожного алгоритму шифрування фіксувався час зашифрування/розшифрування.

З досвіду моделювання систем шифрування прийнято такі значення нормуючих коефіцієнтів: $\lambda_1 = 10^4$, $\lambda_2 = 10^5$ bit^{-1}, $\lambda_3 = 10^4$ bit^{-1}, $\lambda_4 = 10^2$, $\lambda_5 = 10^2$.

При таких значеннях нормуючих коефіцієнтів значення *IntQI* для більшості систем шифрування складає 25...50.

Відмітимо, що при розрахунку *IntQI* критерії *NPCR* та *UACI* беруться не в процентному виразі, а у вигляді десяткового дробу.

Результати розрахунків низки критеріїв та інтегрального показника якості при шифруванні різними шифрами наведено в таблицях 2.1 та 2.2.

а б

Рисунок 2.23 – Приклади початкового та зашифрованого шифром МТС зображення.

Таблиця 2.1 – Критерії якості шифрування

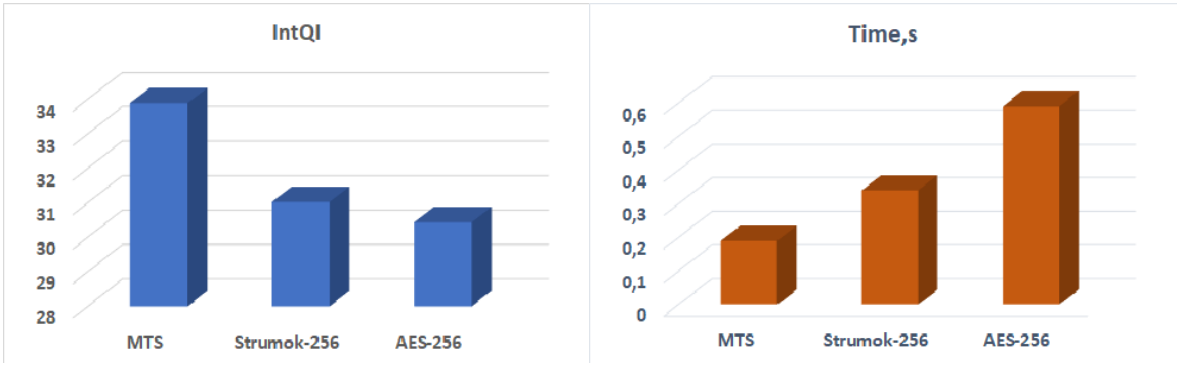
Критерії якості	МТС	Strumok-256	AES-256
$Crit_1 = r_{xy}^{\max}$	0,0021	0,0019	0,0019
$Crit_2 = H(C)$	7.99961	7.99984	7.99990

$Crit_3 = \overline{H(C)}$	7.9018	7.9123	7.9031
$Crit_4 = NPCR$	98.87	98.91	98.93
$Crit_5 = UACI$	33.18	33.27	33.29
	33.88	31.02	30.43

Таблиця 2.2 – Середній час шифрування/розшифрування одного зображення

Шифр	MTC	Strumok-256	AES-256
Час, с	0,19	0,34	0,59

Графічно порівняльні показники якості та швидкодії шифрів показані на рисунку 2.24.



а) б)

Рисунок 2.24 – Порівняльні показники якості та швидкодії шифрів.

Таким чином, експерименти показали, що розроблений метод шифрування зображень за інтегральним показником якості майже не поступається сучасним стандартам потокового та блокового шифрування.

2.4.3 Перевірка якості псевдовипадкових послідовностей, що генеруються модифікованим методом Тент з керуванням

Перевірку якості псевдовипадкових послідовностей, що генеруються модифікованим методом Тент з управлінням, було проведена на платформі Win10(64-біт) з процесором Intel Core i7-9750H з частотою 2.60 GHz і 8 GB of RAM.

Перевірялася двійкова послідовність довжиною 5000 біт за допомогою пакету тестів NIST. До його складу входять 15 статистичних тестів, метою яких є визначення міри випадковості двійкових послідовностей.

У кожному тесті розраховується так звана величина *p-value*. *P-value* – це значення, яке є ймовірністю того, що досліджуваний генератор послідовності створить послідовність, принаймні, такої ж якості, як істинна гіпотетично. Якщо *p-value* дорівнює 1, це означає, що послідовність, що тестується, абсолютно випадкова; якщо воно дорівнює 0, то послідовність цілком передбачувана. *P-value* порівнюється з рівнем значущості α, і якщо воно більше α, то нульова гіпотеза приймається, і послідовність вважається випадковою. В іншому випадку нульова гіпотеза відкидається. У тестах використовують значення $\alpha = 0.01$.

Це означає, якщо *p-value* ≥ 0.01, послідовність вважається випадковою з рівнем довіри 99%. Якщо *p-value* < 0.01, випадковість послідовності відкидається з рівнем довіри 99%. Чим нижче *p-value*, то сильніше свідчення проти нульової гіпотези.

Результати тестування, що наведені у таблиці 2.3, показують високу якість псевдовипадкової послідовності, що генерується модифікованим методом Тент.

Таблиця 2.3 – Перевірка якості псевдовипадкових послідовностей, що генеруються модифікованим методом Тент з керуванням

№ тесту	Назва тесту	Значення *p-value*
1	Frequency (Monobit) Test (Частотний побітовий тест)	0, 452
2	Frequency Test within a Block (Частотний блоковий тест)	0,634
3	Runs Test (Тест на послідовність однакових бітів)	0, 745
4	Test for the Longest Run of Ones in a Block (Тест на найдовшу послідовність одиниць у блоці)	0,344
5	Binary Matrix Rank Test (Тест рангів бінарних матриць)	0,811
6	Discrete Fourier Transform (Spectral) Test (Спектральний тест)	0,407
7	Non- overlapping Template Matching Test (Тест на збіг шаблонів, що не перекриваються)	0,591
8	Overlapping Template Matching Test (Тест на збіг шаблонів, що перекриваються)	0,588
9	Maurer's "Universal Statistical" Test (Універсальний статистичний тест Маурера)	0,423
10	Linear Complexity Test (Тест на лінійну складність)	0, 391
11	Serial Test (Тест на періодичність/Серіальний тест)	0,865
12	Approximate Entropy Test (Тест приблизної ентропії)	0,843
13	Cumulative Sums (Cusum) Test (Тест кумулятивних сум)	0,322
14	Random Excursions Test (Тест на довільні відхилення)	0, 460
15	Random Excursions Variant Test (Варіант тесту на довільні відхилення)	0, 467

2.5 Висновки до другого розділу

У розділі запропоновано новий підхід для генерації довгих псевдохаотичних послідовностей. Система може бути використана для шифрування даних, наприклад, зображень та захисту інформації від несанкціонованого доступу. Перевагою наведеного рішення є коротка довжина ключа та незалежність алгоритму від застосовуваної апаратно-програмної платформи.

У той самий час розроблений метод шифрування зображень працює значно швидше, що дуже важливо задля оперативності систем професійного обміну зашифрованими зображеннями. Це пояснюється низкою факторів. По-перше, шифр Вернама ґрунтується на простих математичних операціях. По-друге, у цьому шифрі операції розсіювання та перемішування поєднані, тоді як у стандартних шифрах вони виконуються послідовно.

Розроблений метод шифрування зображень за інтегральним показником якості майже не поступається сучасним стандартам потокового та блокового шифрування, що дозволяє його рекомендувати для широкого кола завдань, які пов’язані з підвищенням конфіденційності обміну зображеннями.

Таким чином, в розділі 2 отримано такі наукові результати:

– удосконалено інтегральний критерій якості шифрування, який поєднує різні метрики якості шифрування (кореляційні, ентропійні та метрики резистентності), що побудований методом ідеальної точки, що дозволило проводити комплексне оцінювання якості шифрування та проводити обґрунтований вибір потокових та блочних шифрів;

– запропоновано метод шифрування зображень на основі хаотичного відображення Tent з управлінням, що дозволило на підставі короткого ключа (насіння) згенерувати довгу псевдовипадкову послідовність, що значно підвищило швидкодію шифрування та дешифрування при збереженні стійкості шифрування за інтегральним критерієм якості.

РОЗДІЛ 3. МОДЕЛЬ ПОБУДОВИ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ НА ОСНОВІ ЗГОРНУТИХ ЧИСЕЛ K-ПЕРЕТИНУ ПОСЛІДОВНОСТІ ФІБОНАЧЧІ

Одна з можливих схем шифрування даних пов'язана з потоковими шифрами, в яких використовується досить довга псевдовипадкова послідовність. Для підвищення криптостійкості шифр додатково застосовують алгоритми лінійного зсуву. Такі зрушення генеруються лінійними рекурентними послідовностями. В розділі проведено подальше узагальнення чисел Фібоначчі, а саме, згорнуті числа k-перетину послідовності Фібоначчі. В процесі дослідження використано сучасні методи теорії чисел. Проведено визначення властивостей отриманих послідовностей, знаходження нових зв'язків між їх елементами, що може сприяти подальшому забезпеченню підвищення конфіденційності та цілісності обміну зображеннями.

Роль поліномів Чебишева складно переоцінити: вони становлять потужний апарат під час вирішення різноманітних прикладних завдань: теорії інтерполяції, теорії апроксимації, чисельного аналізу, теорії динамічних систем, теорії чисел тощо. Проте похідні поліномів Чебишева особливо високих порядків у літературі зустрічаються значно рідше, переважно щодо загальних властивостей ортогональних поліномів.

3.1 Узагальнення чисел Фібоначчі – згорнуті числа k-перетину послідовності Фібоначчі

Послідовність Фібоначчі визначається рекурентними співвідношеннями

$$x_{n+2} = x_{n+1} + x_n, \;\; n = 1, 2, \ldots \;, \tag{3.1}$$

та початковими умовами $x_1 = 1$, $x_2 = 1$.

В свою чергу послідовность Люка визначається тими самими співвідношеннями та початковими умовами $x_1 = 1$, $x_2 = 3$.

Відповідно до електронної енциклопедії OEIS [23] ці послідовності мають свій номер: для послідовності Фібоначчі $\{F_n\}_{n=1}^{\infty} = \{1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots\}$ номер A000045; для послідовності Люка $\{L_n\}_{n=1}^{\infty} = \{1, 3, 4, 7, 11, 18, 29, 47, 76, 123, \ldots\}$ A000032.

відповідно.

Інші приклади лінійних рекурентних послідовностей другого порядку з різними початковими умовами можна знайти в [63]. Наприклад, рекурентна послідовність $x_{n+2} = 3x_{n+1} - x_n$, $n = 1, 2, \ldots$, з початковими умовами $x_1 = 1$, $x_2 = 3$ визначає переріз послідовності Фібоначчі $\{F_{2n}\}_{n=1}^{\infty} = \{1, 3, 8, 21, 55, \ldots\}$ з номером в OEIS A001906, а з початковими умовами $x_1 = 1$, $x_2 = 2$ перетин $\{F_{2n-1}\}_{n=1}^{\infty} = \{1, 2, 5, 13, 34, \ldots\}$ з номером в OEIS A001519.

Ще один приклад. Позначимо $\Phi_{n,k} = F_{nk}/F_k$, $n = 1, 2, \ldots$, $k = 1, 2, \ldots$. Так як число nk є кратним k, то всі числа $\Phi_{n,k}$ цілі [20]. Крім того, для кожного $k = 1, 2, \ldots$ послідовность $\{\Phi_{nk}\}_{n=1}^{\infty}$ визначається рекурентним співвідношенням

$$x_{n+2} = L_k x_{n+1} - (-1)^k x_n, \quad n = 1, 2, \ldots, \tag{3.2}$$

та початковими умовами $x_1 = 1$, $x_2 = L_k$ [7, 8].

Числа $\Phi_{n,k}$ можна виразити напряму через числа Люка [21]

$$\Phi_{n,k} = \sum_{j=0}^{\left[\frac{n-1}{2}\right]} (-1)^{(k-1)j} \binom{n-1-j}{j} (L_k)^{n-1-2j}. \tag{3.3}$$

Для кожного k послідовність $\{\Phi_{nk}\}_{n=1}^{\infty}$ має свій номер в [23], однак не має спеціальної назви. Тому пропонується цю послідовність називати k-перетином послідовності Фібоначчі. Відповідні номера в OEIS: $k = 1$, A000045

(послідовність Фібоначчі), $k=2$, A001906 (перетин послідовності Фібоначчі); $k=3$, A001076; $k=4$, A004187; $k=5$, A049666; $k=6$, A049660; $k=7$, A049667; $k=8$, A049668; $k=9$, A049669 тощо

Зазначимо, що досить повно вивчені також числа, що породжуються загальними рекурентними співвідношеннями другого порядку. $x_{n+2}=\alpha x_{n+1}\pm x_n$, $n=1,2,\ldots$, однак саме послідовність $\{\Phi_{n,k}\}_{n=1}^{\infty}$ породжується «золотим перетином» (виражається через числа $\varphi=\frac{1}{2}\left(1+\sqrt{5}\right)$, $\varphi^{-1}=\frac{1}{2}\left(-1+\sqrt{5}\right)$).

Наступне узагальнення послідовності Фібоначчі пов'язане зі згорнутими числами. Згорнуте число Фібоначчі визначається так:

$$F_n^{(0)}=F_n,\quad F_n^{(s)}=\sum_{j=0}^{n-1}F_{j+1}F_{n-j}^{(s-1)},\ s=1,2,3,\ldots\ . \tag{3.4}$$

З формул (3.4) слідує, що

$$F_1^{(s)}=1,\ F_2^{(s)}=s+1.$$

При визначенні згорнутих чисел використовують модифікацію формул (3.4) (простий зсув за індексами), де $F_{s+1}^{(s)}=1$, $F_{s+2}^{(s)}=s+1$ и $F_n^{(s)}=0$ при $n<s$ [22].

Оскільки форма задання згорнутих чисел через (3.4) більш зручна, то надалі використовується саме вона.

Для кожного s послідовність $\{F_n^{(s)}\}_{n=1}^{\infty}$ має свій номер в OEIS:

$\{F_n^{(1)}\}_{n=1}^{\infty}=\{1,2,5,10,20,38,\ldots\}$ - A001629; $\{F_n^{(2)}\}_{n=1}^{\infty}=\{1,3,9,22,51,111,\ldots\}$ - A001628; $\{F_n^{(3)}\}_{n=1}^{\infty}=\{1,4,14,40,105,256,\ldots\}$ - A001872; $\{F_n^{(4)}\}_{n=1}^{\infty}=\{1,5,20,65,190,511,\ldots\}$ - A001873 тощо.

Послідовність $\{F_n^{(s)}\}_{n=1}^{\infty}$ визначається лінійним рекурентним співвідношенням порядку вище за другий. Наприклад, для $s=1$ згорнуті числа Фібоначчі задовольняють співвідношенню [21]:

$x_{n+4} = 2x_{n+3} + x_{n+2} - 2x_{n+1} - x_n,\ \ n = 1, 2, \ldots$. Ці рекурентні співвідношення легко можна получити методом функцій (метод буде розглянуто далі). Зв'язок між функціями і рекурентними співвідношеннями докладно описана, наприклад, в [21].

Для чисел з k -перетину послідовності Фібоначчі також можна визначити згорнуті числа згідно з формулою, аналогічною (3.4), тобто

$$\Phi_{n,k}^{(1)} = \sum_{j=0}^{n-1} \Phi_{j+1,k} \Phi_{n-j,k}\ ,\ \ \Phi_{n,k}^{(s)} = \sum_{j=0}^{n-1} \Phi_{j+1,k} \Phi_{n-j,k}^{(s-1)}\ ,\ s = 2,3, \ldots\ . \tag{3.5}$$

Так як $\Phi_{n,1} = F_n$, то $\Phi_{n,1}^{(s)} = F_n^{(s)}$.

Використані формули зв'язку між похідними поліномів Чебишева другого роду та власне поліномами Чебишева другого роду [12]. Як побічні результати, отримані різні тотожності, пов'язані з числами Фібоначчі, Люка, біноміальними коефіцієнтами, згорнутими числами Фібоначчі та числами k -перетину послідовності Фібоначчі.

Слід відмітити, що послідовності $\left\{\Phi_{n,k}^{(s)}\right\}_{n=1}^{\infty}$ для $k = 3,4, \ldots,\ s = 1,2, \ldots$ не наведені в енциклопедії OEIS [5].

Співвідношення (3.1) можна розглядати як лінійне різницеве рівняння із заданими початковими умовами. Коріння відповідного характеристичного рівняння дорівнює φ и $-\varphi^{-1}$, а частинний розв’язок подається у формі

$$F_n = \frac{\varphi^n - (-\varphi)^{-n}}{\varphi + \varphi^{-1}} = \frac{1}{\sqrt{5}}\left(\varphi^n - (-\varphi)^{-n}\right). \tag{3.6}$$

Аналогічно,

$$L_n = \varphi^n + (-\varphi)^{-n}. \tag{3.7}$$

Функція $f(z) = \dfrac{z}{1 - z - z^2}$ є породжувальною функцією для послідовності Фібоначчі [21]; що означає:

$$\frac{z}{1-z-z^2}=\sum_{j=1}^{\infty}F_j\,z^j\ .$$

Для перетину послідовності Фібоначчі $\{F_{2n}\}_{n=1}^{\infty}$ породжувальною функцією буде $\hat{f}(z)=\frac{z}{1-3z+z^2}$, при цьому $\frac{z}{1-3z+z^2}=\sum_{j=1}^{\infty}F_{2j}\,z^j$.

Розглянемо k -перетин послідовності Фібоначчі. Використовуючи (3.2) та зв'язок між породжувальною функцією та рекурентними співвідношеннями, можна визначити породжувальну функцію для $\Phi_{j,k}$ [20, p.230]:

$$\hat{f}_k(z)=\frac{z}{1-L_k z+(-1)^k z^2},$$

при цьому $\frac{z}{1-L_k z+(-1)^k z^2}=\sum_{j=1}^{\infty}\Phi_{j,k}\,z^j$ $(\hat{f}_0(z)=f(z),\hat{f}_1(z)=\hat{f}(z))$.**

Для згорнутих чисел Фібоначчі $F_n^{(s)}$ породжувальна функція визначається [22]:

$$\tilde{f}(z)=\frac{z}{\left(1-z-z^2\right)^{s+1}};\ \frac{z}{\left(1-z-z^2\right)^{s+1}}=\sum_{j=1}^{\infty}F_j^{(s)}\,z^j\ .$$

Функція $g(z,t)=\frac{1}{1-2t\,z+z^2}$ називається породжувальною функцією для поліномів Чебишева другого роду $U_n(t)$ [13], так що

$$\frac{1}{1-2t\,z+z^2}=\sum_{j=0}^{\infty}U_j(t)z^j\ ,$$

де [14]: $U_n(t)=\sum_{j=0}^{\left[\frac{n}{2}\right]}(-1)^j\binom{n-j}{j}2^{n-2j}t^{n-2j}$.

Так як $z\,g(z/i,i/2)=f(z)$, $z\,g(z,3/2)=\hat{f}(z)$ $(i^2=-1)$, то [20]

$$(-i)^{n-1}U_{n-1}(i/2)=F_n,\tag{3.8}$$

$$U_{n-1}(3/2)=F_{2n}.\tag{3.9}.$$

Далі, $z\,g(z/i,(i/2)L_k)=\hat{f}_k(z)$, k - непарне, $z\,g(z,(1/2)L_k)=\hat{f}_k(z)$, k - парне. Тоді

$$\Phi_{n,k}=\frac{F_{nk}}{F_k}=\begin{cases}(-i)^{n-1}U_{n-1}\left(\dfrac{i}{2}L_k\right), k-odd,\\ U_{n-1}\left(\dfrac{1}{2}L_k\right), k-even\end{cases} \tag{3.10}$$

Повернемося до згорнутих чисел Фібоначчі $F_n^{(s)}$. Знайдемо

$$\frac{\partial^s}{\partial t^s}g(z,t)=2^s s!\frac{z^s}{\left(1-2tz+z^2\right)^{s+1}}=\sum_{j=0}^{\infty}U_j^{(s)}(t)z^j=\sum_{j=s}^{\infty}U_j^{(s)}(t)z^j=\sum_{j=1}^{\infty}U_{j+s-1}^{(s)}(t)z^{j+s-1}$$

$$\left(U_j^{(s)}(t)=0,\ j<s\right).$$

Тоді $$\frac{z}{\left(1-2tz-z^2\right)^{s+1}}=\frac{1}{2^s s!}\sum_{j=1}^{\infty}U_{j+s-1}^{(s)}(t)z^j,$$

отже,

$$F_n^{(s)}=\frac{(-i)^{n-1}}{2^s s!}U_{n+s-1}^{(s)}(i/2). \tag{3.11}$$

Аналогічно,

$$F_{2n}^{(s)}=\frac{1}{2^s s!}U_{n+s-1}^{(s)}(3/2). \tag{3.12}$$

Формули (3.10), (3.11), (3.12) є узагальненням відомих формул (3.8) и (3.9).

3.2 Зв'язок між похідними поліномів Чебишева та поліномами Чебишева другого роду

Наступні результати у суттєвому отримані на підставі формул зв'язку між похідними поліномів Чебишева другого роду $U_n^{(s)}(z)$ (s – порядок похідної) та власне поліномів Чебишева другого роду $U_n(z)$. Наведемо ці формули [65].

$$U_n^{(s)}(z)=s!\sum_{j=0}^{\left[\frac{n-s}{2}\right]}(-1)^j\binom{n-j}{j}\binom{n-2j}{s}2^{n-2j}z^{n-2j-s}, \tag{3.13}$$

$$\frac{1}{2^s s!}U_{n+s-1}^{(s)}\left(\frac{1}{2}\left(z^{\frac{1}{2}}+z^{-\frac{1}{2}}\right)\right)=z^{-\frac{n-1}{2}}\sum_{j=0}^{n-1}\binom{n+s-1-j}{s}\binom{s+j}{s}z^j, \tag{3.14}$$

$$\frac{1}{2^s s!}U_{n+s-1}^{(s)}\left(\frac{1}{2}\left(z^{\frac{1}{2}}+z^{-\frac{1}{2}}\right)\right)=z^{-\frac{n-1}{2}}(1-z)^{-(2s+1)}\sum_{j=0}^{s}(-1)^j\binom{n+2s}{j}\binom{n+s-1-j}{n-1}\left(z^j-z^{n+2s-j}\right), \tag{3.15}$$

$$\frac{2^s}{s!}\left(1-z^2\right)^s U_{n+s-1}^{(s)}(z)=(-1)^s\sum_{j=0}^{s}(-1)^j\binom{n+s-1-j}{n-1}\binom{n+2s}{j}U_{n+2s-1-2j}(z). \tag{3.16}$$

Формули типу Біне для згорнутих чисел Фібоначчі виходять з (3.11), (3.14), (3.15) при підстановці замість z величину $-\varphi^2$:

$$F_n^{(s)}=(-1)^{n-1}\varphi^{-n+1}\sum_{j=0}^{n-1}(-1)^j\binom{n+s-1-j}{s}\binom{s+j}{s}\varphi^{2j},$$

$$F_n^{(s)}=\frac{\varphi^{-n+1}}{\left(1+\varphi^2\right)^{2s+1}}\sum_{j=0}^{s}\binom{n+2s}{j}\binom{n+s-1-j}{n-1}\left(-(-1)^n\varphi^{2j}+\varphi^{2(n+2s-j)}\right). \tag{3.17}$$

З формул (3.17) та (3.6) витікає формула зв'язку між згорнутими числами Фібоначчі та числами Фібоначчі:

$$F_n^{(s)}=5^{-s}\sum_{j=0}^{s}\binom{n+2s}{j}\binom{n+s-1-j}{n-1}F_{n+2s-2j}. \tag{3.18}$$

При виводі (3.18) використовувались формули:

$$\frac{\varphi^{-n+1}}{\left(1+\varphi^2\right)^{2s+1}}=\frac{\varphi^{-n}\varphi^{-s}}{\left(\varphi+\varphi^{-1}\right)^{2s}\left(\varphi+\varphi^{-1}\right)}, \qquad \frac{-(-1)^n\varphi^{-(n+2s-2j)}+\varphi^{n+2s-2j}}{\varphi+\varphi^{-1}}=F_{n+2s-2j}.$$

Формулу (3.18) також можна получить з (3.16), підставляючи $z=i/2$. Ця формула суттєво уточнює формулу (1.12) з [21].

При $s=1$: $F_n^{(1)}=\frac{1}{5}\left(nF_{n+2}+(n+2)F_n\right)$.

При $s=2$: $F_n^{(2)}=\frac{1}{25}\left(\frac{1}{2}n(n+1)F_{n+4}+n(n+4)F_{n+2}+\frac{1}{2}(n+3)(n+4)F_n\right)$.

Відзначимо, що послідовності $\left\{F_n^{(s)}\right\}_{s=1}^{\infty}$ представлені в OEIS номерами: при $n=2$ - A000027, $n=3$ - A000096, $n=4$ - A006503, $n=5$ - A006504 тощо.

Продиференціюємо тотожність (3.16)

$$\frac{2^s}{s!}s(1-z^2)^{s-1}(-2z)U_{n+s-1}^{(s)}(z)+\frac{2^s}{s!}(1-z^2)^s U_{n+s-1}^{(s+1)}(z)=(-1)^s\sum_{j=0}^{s}(-1)^j\binom{n+s-1-j}{n-1}\binom{n+2s}{j}U_{n+2s-1-2j}^{(1)}(z),$$

підставимо $z=i/2$, застосуємо формулу (3.11), одержимо

$$4s5^{s-1}F_n^{(s)}+2(s+1)5^s F_{n-1}^{(s+1)}=2\sum_{j=0}^{s}\binom{n+2s}{j}\binom{n+s-1-j}{n-1}F_{n+2s-2j-1}^{(1)},$$

звідки

$$F_n^{(s)}=-\frac{2(s-1)}{5s}F_{n+1}^{(s-1)}+\frac{1}{5^{s-1}s}\sum_{j=0}^{s-1}\binom{n+2s-1}{j}\binom{n+s-1-j}{n}F_{n+2s-2j-2}^{(1)}. \qquad (3.19)$$

Формула (3.19) дозволяє отримувати різні наслідки. Наприклад, при $s=2$:

$$F_n^{(2)}=\frac{1}{10}\left((n+1)F_{n+2}^{(1)}-2F_{n+1}^{(1)}+(n+3)F_n^{(1)}\right).$$

Якщо врахувати (3.18), то формула (3.19) набуде вигляду

$$F_n^{(s)}=\frac{1}{5^{s-1}s}\sum_{j=0}^{s-1}\binom{n+2s-1}{j}\binom{n+s-1-j}{n}\left(F_{n+2s-2j-2}^{(1)}-\frac{2(s-1)}{5}F_{n+2s-2j-1}\right).$$

З (3.19) неважко отримувати й інші тотожності, що пов'язують згорнуті числа Фібоначчі.

Для чисел k-перетину послідовності Фібоначчі формули Біне очевидні. З формули (3.11) при $s=0$ та $z=\begin{cases}(i/2)L_k, k-odd,\\ (1/2)L_k, k-even\end{cases}$ відразу слідує формула (3.3).

Зазначимо, що формула (3.10) є наслідком формул (3.7), (3.13) при $s=0$ и $z=-\varphi^{2k}$.

Для згорнутих чисел k -перетину послідовності Фібоначчі $\Phi_{n,k}^{(s)}$ виконуюча функція визначається аналогічно випадку $F_n^{(s)}$:

$$f_k^{(s)}(z)=\frac{z}{\left(1-L_k z+(-1)^k z^2\right)^{s+1}};\ \frac{z}{\left(1-L_k z+(-1)^k z^2\right)^{s+1}}=\sum_{j=1}^{\infty}\Phi_{j,k}^{(s)} z^j .$$

Дійсно згідно з [20, с. 216] та [64] отримуємо

$$\frac{z}{1-L_k z+(-1)^k z^2}\cdot\frac{1}{1-L_k z+(-1)^k z^2}=\sum_{j=1}^{\infty}\left(\sum_{l=0}^{n-1}\Phi_{l+1,k}\Phi_{n-l,k}\right)z^j=\sum_{j=1}^{\infty}\Phi_{j,k}^{(1)} z^j ,$$

$$\frac{z}{\left(1-L_k z+(-1)^k z^2\right)^{s}}\cdot\frac{1}{1-L_k z+(-1)^k z^2}=\sum_{j=1}^{\infty}\left(\sum_{l=0}^{n-1}\Phi_{l+1,k}\Phi_{n-l,k}^{(s-1)}\right)z^j=\sum_{j=1}^{\infty}\Phi_{j,k}^{(s)} z^j .$$

Звідки

$$\Phi_{n,k}^{(s)}=\frac{1}{2^s s!}\begin{cases}(-i)^{n-1}U_{n+s-1}^{(s)}\left(\frac{i}{2}L_k\right),\ k-odd,\\ U_{n+s-1}^{(s)}\left(\frac{1}{2}L_k\right),\ k-even\end{cases}. \tag{3.20}$$

Формула типу Біне для згорнутих чисел $\Phi_{n,k}^{(s)}$ виходить з (3.14), (3.15), (3.20) при підстановці замість z величини $-\varphi^{2k}$ якщо k - непарний та φ^{2k} якщо k - парний:

$$\Phi_{n,k}^{(s)}=(-1)^{k(n-1)}\varphi^{k(-n+1)}\sum_{j=0}^{n-1}(-1)^{jk}\binom{n+s-1-j}{s}\binom{s+j}{s}\varphi^{2jk},$$

$$\Phi_{n,k}^{(s)}=\frac{\varphi^{-k(n+2s)}}{\left(\varphi^k+\varphi^{-k}\right)^{2s+1}}\sum_{j=0}^{s}(-1)^{(k-1)j}\binom{n+2s}{j}\binom{n+s-1-j}{n-1}\left(-(-1)^{kn}\varphi^{2kj}+\varphi^{2k(n+2s-j)}\right).$$

З формул (3.16), (3.6) виходить формула (повна аналогія з формулою (3.18)):

$$\Phi_{n,k}^{(s)}=5^{-s}\left(F_k\right)^{-2s-1}\sum_{j=0}^{s}(-1)^{(k-1)j}\binom{n+2s}{j}\binom{n+s-1-j}{n-1}F_{k(n+2s-2j)} . \tag{3.21}$$

Еквівалентна формула

$$\Phi_{n,k}^{(s)}=5^{-s}\left(F_k\right)^{-2s}\sum_{j=0}^{s}(-1)^{(k-1)j}\binom{n+2s}{j}\binom{n+s-1-j}{n-1}\Phi_{(n+2s-2j),k} .$$

Окремі випадки при $s=1$, $s=2$:

$$\Phi_{n,k}^{(1)} = \frac{1}{5(F_k)^2}\left(n\Phi_{n+2,k} + (-1)^{k-1}(n+2)\Phi_{n,k}\right);$$

$$\Phi_{n,k}^{(2)} = \frac{1}{25(F_k)^4}\left(\frac{1}{2}n(n+1)\Phi_{n+4,k} + (-1)^{k-1}n(n+4)\Phi_{n+2,k} + \frac{1}{2}(n+3)(n+4)\Phi_{n,k}\right).$$

Відмітимо, що $\Phi_{3,1}^{(s)} = \frac{1}{2}(s+1)(s+4)$, $\Phi_{3,2}^{(s)} = \frac{1}{2}(s+1)(9s+16)$ послідовність $\{\Phi_{3,3}^{(s)}\}_{s=1}^{\infty} = \{50,99,164,245,342,\ldots\}$ має спеціальну назву, «число блукань по кубічних ґратах» [5], номер в OEIS - A005570.

Послідовності $\{\Phi_{n,k}^{(s)}\}_{n=1}^{\infty}$ для $k = 3,4,\ldots$, $s = 1,2,\ldots$ не представлені в енциклопедії OEIS [21].

Для послідовності $\{\Phi_{n,3}^{(1)}\}_{n=1}^{\infty} = \{1,8,50,280,1476,7472,36836,\ldots\}$ відповідний скріншот представлено на рисунку 3.1. Аналогічні результати виходять всім послідовностей $\{\Phi_{n,k}^{(s)}\}_{n=1}^{\infty}$, $k = 3,4,\ldots$, $s = 1,2,\ldots$. Цікаво відзначити, що в OEIS не представлені навіть послідовності $\{\Phi_{n,k}\}_{n=1}^{\infty}$, $k = 13,14,15,\ldots$.

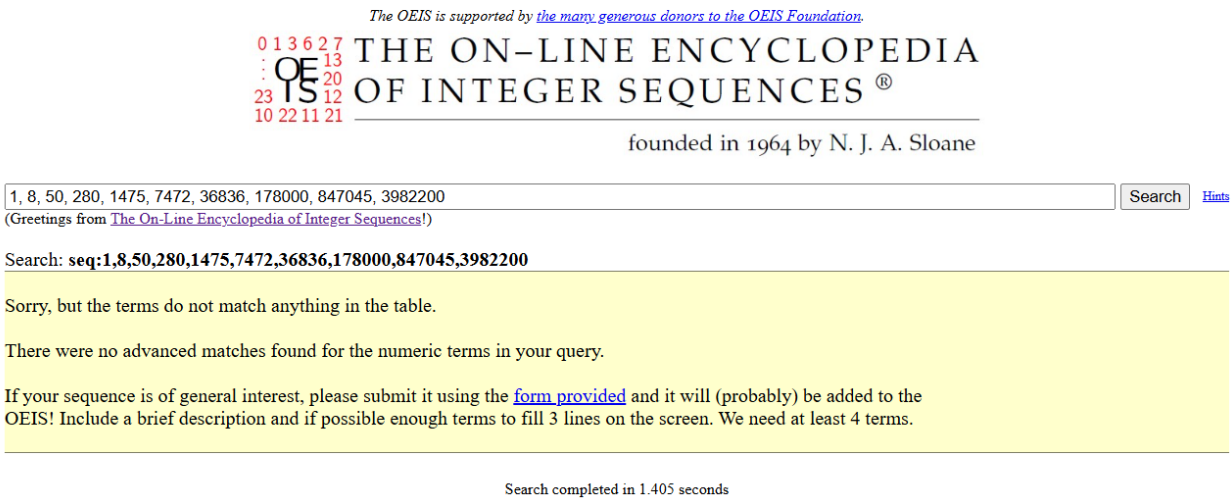


Рисунок 3.1 – Скриншот перевірки номера послідовності $\{\Phi_{n,3}^{(1)}\}_{n=1}^{\infty}$

З формул (3.10), (3.13), (3.21) слід, що

$$\Phi_{n,k}^{(s)} = \sum_{j=0}^{\left\lfloor \frac{n-1}{2} \right\rfloor} (-1)^{(k-1)j} \binom{n+s-1-j}{j} \binom{n+s-1-2j}{s} (L_k)^{n-1-2j} .$$

Тоді

$$\sum_{j=0}^{\left\lfloor \frac{n-1}{2} \right\rfloor} (-1)^{(k-1)j} \binom{n+s-1-j}{j} \binom{n+s-1-2j}{s} (L_k)^{n-1-2j} = 5^{-s} (F_k)^{-2s-1} \sum_{j=0}^{s} (-1)^{(k-1)j} \binom{n+2s}{j} \binom{n+s-1-j}{n-1} F_{k(n+2s-2j)} . \quad (3.22)$$

3.3 Опис знайденої послідовності для енциклопедії OEIS

Опис послідовності $\left\{\Phi_{n,k}^{(s)}\right\}_{n=1}^{\infty}$ для OEIS може бути представленим:

- за визначенням

$$\Phi_{n,k} = F_{nk} / F_k , \quad \Phi_{n,k}^{(1)} = \sum_{j=0}^{n-1} \Phi_{j+1,k} \Phi_{n-j,k} , \quad \Phi_{n,k}^{(s)} = \sum_{j=0}^{n-1} \Phi_{j+1,k} \Phi_{n-j,k}^{(s-1)} , \ s = 2,3, \ldots .$$

- через виконуючу функцію

$\Phi_{n,k}^{(s)}$ – коефіцієнти розкладання в ряд виконує функції

$$f(z) = \frac{z}{\left(1 - L_k z + (-1)^k z^2\right)^{s+1}} ;$$

- за формулою Біне

$$\Phi_{n,k}^{(s)} = \frac{\varphi^{-k(n+2s)}}{\left(\varphi^k + \varphi^{-k}\right)^{2s+1}} \sum_{j=0}^{s} (-1)^{(k-1)j} \binom{n+2s}{j} \binom{n+s-1-j}{n-1} \left(-(-1)^{kn} \varphi^{2kj} + \varphi^{2k(n+2s-j)}\right);$$

- явна формула через числа Фібоначчі

$$\Phi_{n,k}^{(s)} = 5^{-s} (F_k)^{-2s-1} \sum_{j=0}^{s} (-1)^{(k-1)j} \binom{n+2s}{j} \binom{n+s-1-j}{n-1} F_{k(n+2s-2j)} ;$$

- через рекурентну послідовність

Визначимо лінійну форму $\left(1-L_k z+(-1)^k z^2\right)^{s+1}=\Lambda\left(1, z, z^2, \ldots, z^{2s+2}\right)$;

рекурентна послідовність:

$$\Lambda\left(x_{n+2s+2}, x_{n+2s+1}, \ldots, x_n\right)=0,\ x_j=\Phi_{j,k}^{(s)},\ j=1, \ldots, n+2s+1.$$

Тотожності, що пов'язують числа Фібоначчі, числа Люка, біноміальні числа відомі з давніх-давен, і це співтовариство поповнюється чи не щодня [21]. У розділі наведено наслідки цих тотожностей. Зрозуміло, більшість з цих тотожностей відомі (або легко виводяться і відомі), проте деякі тотожності є оригінальними. З формули (3.4) одержуємо

$$\sum_{j=0}^{n-1} F_{j+1}F_{n-j}=\frac{1}{5}\left(nF_{n+2}+(n+2)F_n\right),$$

$$\sum_{j=0}^{n-1} F_{j+1}\left((n-j)F_{n+2-j}+(n+2-j)F_{n-j}\right)=\frac{1}{5}\left(\frac{1}{2}n(n+1)F_{n+4}+n(n+4)F_{n+2}+\frac{1}{2}(n+3)(n+4)F_n\right),$$

Звідки

$$\sum_{j=0}^{n-1}(n-j)F_{j+1}L_{n+1-j}=\frac{1}{10}\left(n(5n+7)F_{n+2}+2(n+2)F_n\right).$$

Використовуючи формулу прикладу 18.7 [20, p.222], отримуємо

$$\sum_{j=1}^{[n/2]} j\binom{n-j}{j}=\frac{1}{5}\left((n-1)F_{n+1}+(n+1)F_{n-1}\right)=\frac{1}{5}\left(nL_n-F_n\right).$$

З (3.18), враховуючі що $F_1^{(s)}=1$, $F_2^{(s)}=s+1$, $F_3^{(s)}=\frac{1}{2}(s+1)(s+4)$, $F_4^{(s)}=\frac{1}{6}(s+1)(s+2)(s+9)$, $F_5^{(s)}=\frac{1}{24}(s+1)(s+2)(s+4)(s+15)$, тоді:

$$\frac{1}{5^s}\sum_{j=0}^{s}\binom{1+2s}{j}F_{1+2s-2j}=1,$$

$$\frac{1}{5^s}\sum_{j=0}^{s}\binom{2+2s}{j}(1+s-j)F_{2+2s-2j}=s+1,$$

$$\frac{1}{5^s}\sum_{j=0}^{s}\binom{3+2s}{j}\binom{2+s-j}{2}F_{3+2s-2j}=\frac{1}{2}(s+1)(s+4),$$

$$\frac{1}{5^s}\sum_{j=0}^{s}\binom{4+2s}{j}\binom{3+s-j}{3}F_{4+2s-2j}=\frac{1}{6}(s+1)(s+2)(s+9),$$

$$\frac{1}{5^s}\sum_{j=0}^{s}\binom{5+2s}{j}\binom{4+s-j}{4}F_{5+2s-2j}=\frac{1}{24}(s+1)(s+2)(s+4)(s+15),$$

тощо (скрізь s - натуральне число).

З визначення чисел $\Phi_{n,k}^{(s)}$ (формула (5)) отримуємо:

$$\sum_{j=0}^{n-1}F_{(j+1)k}F_{(n-j)k}=\frac{1}{5F_k}\left(nF_{(n+2)k}+(-1)^{k-1}(n+2)F_{nk}\right),$$

$$\sum_{j=0}^{n-1}F_{(j+1)k}\left((n-j)F_{(n-j+2)k}+(-1)^{k-1}(n-j+2)F_{(n-j)k}\right)=\frac{1}{5F_k}\left(\frac{1}{2}n(n+1)F_{(n+4)k}+(-1)^{k-1}n(n+4)F_{(n+2)k}+\frac{1}{2}(n+3)(n+4)F_{nk}\right).$$

Враховуючи, що $\Phi_{1,k}^{(s)}=1$, $\Phi_{2,k}^{(s)}=(s+1)L_k$, $\Phi_{3,k}^{(s)}=\frac{1}{2}(s+1)(s+2)L_{2k}+(s+1)^2(-1)^k$,

$$\Phi_{4,k}^{(s)}=\frac{1}{2}(s+1)(s+2)(s+3)(L_k)^3-(s+1)(s+2)(-1)^k L_k \quad \text{(через рівність}$$

$$\frac{1}{2^s s!}U_{2+s}^{(s)}(z)=2(s+1)(s+2)z^2-(s+1),\quad \frac{1}{2^s s!}U_{3+s}^{(s)}(z)=\frac{4}{3}(s+1)(s+2)(s+3)z^3-2(s+1)(s+2)z).$$

Тоді

$$5^{-s}(F_k)^{-2s-1}\sum_{j=0}^{s}(-1)^{(k-1)j}\binom{1+2s}{j}F_{k(1+2s-2j)}=1, \tag{3.23}$$

або

$$(F_k)^{2s+1}=5^{-s}\sum_{j=0}^{s}(-1)^{(k-1)j}\binom{1+2s}{j}F_{k(1+2s-2j)},$$

$$5^{-s}(F_k)^{-2s-1}\sum_{j=0}^{s}(-1)^{(k-1)j}\binom{2+2s}{j}(1+s-j)F_{k(2+2s-2j)}=(s+1)L_k, \tag{3.24}$$

або

$$(F_k)^{2s} = 5^{-s}\frac{1}{(s+1)F_{2k}}\sum_{j=0}^{s}(-1)^{(k-1)j}\binom{2+2s}{j}(1+s-j)F_{k(2+2s-2j)},$$

$$5^{-s}(F_k)^{-2s-1}\sum_{j=0}^{s}(-1)^{(k-1)j}\binom{3+2s}{j}\binom{2+s-j}{2}F_{k(3+2s-2j)} = \frac{1}{2}(s+1)(s+2)L_{2k} + (s+1)^2(-1)^k, \quad (3.25)$$

$$5^{-s}(F_k)^{-2s-1}\sum_{j=0}^{s}(-1)^{(k-1)j}\binom{4+2s}{j}\binom{3+s-j}{3}F_{k(4+2s-2j)} = \frac{1}{6}(s+1)(s+2)(s+3)(L_k)^3 - (s+1)(s+2)(-1)^k L_k. \quad (3.26)$$

Для невеликих значень або виходять формули, які, як правило, вже відкриті раніше (скоріше за все іншими способами). Наприклад, з (3.23), (3.24), враховуючи, що $L_k = F_{2k}/F_k$ (при $s = 1, 2, 3$),

$$F_{2k}(F_k)^2 = \frac{1}{5}\left(F_{4k} + (-1)^{k-1}2F_{2k}\right),$$

$$F_{2k}(F_k)^4 = \frac{1}{25}\left(F_{6k} + (-1)^{k-1}4F_{4k} + 5F_{2k}\right),$$

$$F_{2k}(F_k)^6 = \frac{1}{125}\left(F_{8k} + (-1)^{k-1}6F_{6k} + 14F_{4k} + (-1)^{k-1}14F_{2k}\right),$$

$$L_k = \frac{F_{4k} - (-1)^k 2F_{2k}}{F_{3k} - (-1)^k 3F_k} = \frac{F_{6k} - (-1)^k 4F_{4k} + 5F_{2k}}{F_{5k} - (-1)^k 5F_{3k} + 10F_k},$$

тощо.

З (3.25) при $s = 0, 1, 2, 3$:

$$\frac{F_{3k}}{F_k} = L_{2k} + (-1)^k,$$

$$\frac{1}{5(F_k)^3}\left(3F_{5k} + (-1)^{k-1}5F_{3k}\right) = 3L_{2k} + 4(-1)^k,$$

$$\frac{1}{25(F_k)^5}\left(2F_{7k} + (-1)^{k-1}7F_{5k} + 7F_{3k}\right) = 2L_{2k} + 3(-1)^k,$$

$$\frac{1}{125(F_k)^7}\left(5F_{9k} + (-1)^{k-1}27F_{7k} + 54F_{5k} + (-1)^{k-1}42F_{3k}\right) = 5L_{2k} + 8(-1)^k,$$

тощо.

З (3.26) при $s = 0, 1, 2, 3$:

$$\frac{F_{4k}}{F_k} = (L_k)^3 - (-1)^k 2L_k,$$

$$\frac{1}{5(F_k)^3}\left(2F_{6k} + (-1)^{k-1}3F_{4k}\right) = 2(L_k)^3 - (-1)^k 3L_k,$$

$$\frac{1}{25(F_k)^5}\left(5F_{8k} + (-1)^{k-1}16F_{6k} + 14F_{4k}\right) = 5(L_k)^3 - (-1)^k 6L_k,$$

$$\frac{1}{125(F_k)^7}\left(F_{10k} + (-1)^{k-1}5F_{8k} + 9F_{6k} + (-1)^{k-1}6F_{4k}\right) = (L_k)^3 - (-1)^k L_k,$$

тощо.

Використовуючи формулу (3.22), також можна отримувати чергові тотожності при різних значеннях n, k, s.

3.4 Дослідження послідовності згорнутих чисел k-перетину послідовності Фібоначчі

На підставі отриманих результатів представлення згорнутих чисел k-перетину послідовності Фібоначчі запропоновано нову послідовність. Умовно назвемо її k-послідовність, оскільки вона ще не зареєстрована в енциклопедії OEIS.

Формула для обчислення членів послідовності:

$$\Phi_{n,k}^{(s)} = \Phi(n,k,s) = 5^s \cdot ((F(k))^{-2s-1} \sum_{j=0}^{s} (-1)^{(k-1)j} C_{n+2s}^{j} C_{n+s-1-j}^{n-1} \cdot F(k \cdot (n+2s-2j)),$$

де F(k)– k -е число Фібоначчі.

n – номер елементу;

k – перетин;

s – згортка.

Наведемо деякі приклади.

Для $\Phi_{n,3}^{(1)} = \Phi(n,3,1)$ $n = 1,...,15$ маємо послідовність:

1, 8, 50, 280, 1475, 7472, 36836, 178000, 847045, 3982200, 18538134, 85599912, 392560775, 1789800160,8119213000.

$\Phi_{50,3}^{(1)} = \Phi(50,3,1)$=2365729001618250547238978373530 00.

$\Phi_{50,7}^{(5)} = \Phi(50,7,5)$ =151352341160887204842063863969079166398245…

…90627926336677423637 9 542341783241735.

Це число містить N_{dec}=78 десяткових знаків. Число двійкових знаків можна визначити наступним чином:

$$N_{bin} = N_{dec} \log_2(10) = N_{dec} \cdot 3,322 ,$$

$$N_{dec}=260.$$

Видно, що число $\Phi_{n,k}^{(s)}$ зростає дуже швидко. Можна доказати, що по параметрам k та n ріст експоненціальний, по параметру s – поліноміальний.

Приблизний масштаб числа $\Phi_{n,k}^{(s)}$ визначається як

$$\Phi_{n,k}^{(s)} \approx O(n^s \cdot \varphi^{k(n-1)}) .$$

Справедлива наближена формула

$$D \approx 0,209 \cdot k(n-1) .$$

Можна згенерувати достатньо велике число $\Phi_{n,k}^{(s)}$, однак цифри такого числа детерміновані. Якщо зловмисник знає формулу та три параметри (n,s,k), він швидко відновить усю послідовність цифр.

Тим не менш, число $\Phi_{n,k}^{(s)}$ можна застосовувати як "насіння" для генерації ключа з використанням шифру Вернама.

Пропонується методика дослідження послідовності згорнутих чисел k-перетину послідовності Фібоначчі, заснована на принципі відкидання (Discarding).

Методика складається з наступних етапів:

– задається потрібна довжина псевдовипадкового ключа N_{bin};

– розраховується відповідна йому довжина десяткового числа N_{dec} і множиться на 3. Далі вважаємо, що 3 N_{dec}=D;

– по співвідношенню $D \approx 0,209 \cdot k(n-1)$ підбираються значення k і n;

– в згенерованому числі $\Phi_{n,k}^{(s)}$ відкидаються N_{dec} початкових цифр та N_{dec} кінцевих цифр;

– десяткове число, що залишилося, довжиною N_{dec} перекладається в двійкову форму і використовується як ключ до шифру Вернама.

Методика перевірена на послідовностях довжиною 5000 біт на тестах NIST. Вибрано 5 основних тестів із 15-ти існуючих. Результати перевірки наведено у таблиці 3.1.

З таблиці 3.1 видно, що p-value > 0 для всіх п'яти тестів, тобто запропоновану методику можна застосовувати для формування ключів до шифру Вернама.

Таблиця 3.1 – Дослідження послідовності згорнутих чисел k-перетину послідовності Фібоначчі

Назва тесту	Значення p-value
Frequency (Monobit) Test (Частотний побітовий тест)	0, 211
Test for the Longest Run of Ones in a Block (Тест на найдовшу послідовність одиниць у блоці)	0,377
Discrete Fourier Transform (Spectral) Test (Спектральний тест)	0, 406
Approximate Entropy Test (Тест приблизної ентропії)	0,124
Cumulative Sums (Cusum) Test (Тест кумулятивних сум)	0,239

3.5. Висновки до третього розділу

У розділі проведено подальше узагальнення чисел Фібоначчі, а саме, згорнуті числа *k*-перетину послідовності Фібоначчі. В процесі дослідження використано сучасні методи теорії чисел. Проведено визначення властивостей отриманих послідовностей, знаходження нових зв'язків між їх елементами.

Запропоновано подальший розвиток послідовностей типу Фібоначчі, який заснований на зв'язку між похідними поліномів Чебишева другого роду та власне поліномами Чебишева, а також на зв'язку згорнутих чисел *k*-перетину послідовності Фібоначчі з похідними поліномів Чебишева другого роду через числа Люка.

Отримано ряд тотожностей, що пов'язують числа Фібоначчі та числа Люка. Показано, що похідні поліномів Чебишева вищого порядку виявилися ефективним базисом на вирішення деяких завдань теорії чисел, саме, побудови нових послідовностей. Таким чином, в результаті дослідження отримано сімейство узагальнених послідовностей зі зростанням вищого порядку і

складнішими коефіцієнтами зв'язку ніж у відомих послідовностей Фібоначчі. Це робить отримані узагальнені послідовності ідеальними для стиснення розріджених даних, вирішення низки завдань у сфері захисту.

Доведено, що отримані послідовності є оригінальними і представлені в енциклопедії OEIS, що підтверджує потенціал запропонованого підходу до формування різних послідовностей, які можуть бути використані для підвищення надійності інформаційних систем.

Таким чином, у розділі 3 вирішені наступні завдання:

– знайдені формули представлення згорнутих чисел k -перетину послідовності *Фібоначчі*;

– визначені властивості послідовності *Фібоначчі* $\left\{\Phi_{n,k}^{(s)}\right\}_{n=1}^{\infty}$, знайдені нові зв'язки між елементами послідовності;

– знайдені формули *типу Біне* для згорнутих чисел $\Phi_{n,k}^{(s)}$;

– проведено дослідження послідовності згорнутих чисел k-перетину послідовності Фібоначчі;

– проведено дослідження послідовності згорнутих чисел k-перетину послідовності Фібоначчі як генератора псевдовипадкових чисел та показано, що послідовність може бути використаною для створення високоякісних паролів довірених користувачів.

Таким чином, у третьому розділі одержано наступний пункт наукової новизни: отримала подальшого розвитку модель побудови псевдовипадкових послідовностей, яка заснована на зв'язку між похідними поліномів Чебишева другого роду та поліномами Чебишева, а також на зв'язку згорнутих чисел k-перетину послідовності Фібоначчі з похідними поліномів Чебишева другого роду через числа Люка, що дало можливість отримати сімейство узагальнених послідовностей Фібоначчі, які можуть бути використані для підвищення рівня забезпечення цілісності інформації при її обміні у групі довірених користувачів.

РОЗДІЛ 4. МЕТОД ОПЕРАТИВНОГО ОБМІНУ КОНФІДЕНЦІЙНИМИ ЗОБРАЖЕННЯМИ ДЛЯ ГРУПИ ДОВІРЕНИХ КОРИСТУВАЧІВ

В розділі розглянуто завдання розробки та моделювання методу оперативного обміну конфіденційними зображеннями для групи довірених користувачів на основі розроблених у другому розділі теоретичних засад щодо генерування псевдовипадкових послідовності на основі Тент-відображення, які можуть бути використані для перемішування пікселів зображення.

Сформовані вимоги до методу, що розробляється. Метод повинен забезпечувати:

– конфіденційність та цілісність зображень, виключення можливого несанкціонованого втручання у зображення з метою їх зміни, копіювання або перегляду;

– високу швидкодію, тобто можливість функціонування в режимі, близькому до реального часу;

– можливість легкого масштабування для різної кількості груп довірених користувачів.

4.1 Дослідження ефективності протоколів формування груп довірених користувачів

Розвиток протоколів групового узгодження ключів (Group Key Agreement, GKA) тісно пов'язаний з еволюцією криптографічних методів захищеної розподіленої взаємодії та необхідністю забезпечення конфіденційності групових комунікацій у розрахованих на багато користувачів мережевих систем. Базою для появи GKA-протоколів став класичний протокол Діффі-Хеллмана, запропонований Вітфілдом Діффі та Мартіном Хеллманом у 1976 році [66-68].

Запропонована схема вперше дозволила двом сторонам сформувати спільний секретний ключ по відкритому каналу зв'язку без попереднього обміну секретними параметрами. Основою безпеки протоколу була обчислювальна складність завдання дискретного логарифмування в мультиплікативні групи кінцевих полів [69-70].

Класичний протокол Діффі-Хеллмана був орієнтований виключно на взаємодію двох учасників та не передбачав механізмів безпечного формування загального ключа групи користувачів. Проте розвиток систем колективної обробки даних розрахованих та багатокористувацьких комунікаційних платформ вимагатиме створення механізмів групового узгодження ключів для довільного числа учасників *N*.

Перші спроби розширення протоколу Діффі-Хеллмана на багатокористувацький, випадок з'явилися в 1980-х роках і ґрунтувалися на послідовному виконанні операцій експонентування між учасниками групи. У таких схемах кожен новий учасник вносив свій особистий внесок у формування підсумкового групового ключа.

Незважаючи на концептуальну простоту, дані рішення мали ряд істотних недоліків: високу обчислювальну складність, значну кількість раундів взаємодії, велику залежність від порядку підключення учасників та низьку масштабованість при збільшенні розміру групи.

Подальший розвиток досліджень у галузі GKA-протоколів призвів до появи спеціалізованих схем колективного узгодження ключів, що оптимізовані для різних топологій взаємодії учасників. Одним із найвідоміших рішень став протокол Burmester-Desmedt Group Key Agreement (BD-GKA), запропонований Майком Бурместером та Івонн Десмедт у середині 1990-х років. Основною перевагою даної схеми було фіксоване число раундів взаємодії незалежно від кількості учасників групи, і також лінійна комунікаційна складність [71-76].

У протоколі BD-GKA кожен учасник виконує обмежене число криптографічних операцій і взаємодіє з сусідніми вузлами групи, що забезпечує високу ефективність за порівняно великих розмірах груп.

Паралельно розвивалися ієрархічні підходи до узгодження ключів на основі деревоподібних структур. У Tree-based GKA-протоколах учасники організуються у вигляді бінарного або багатозв'язного дерева, всередині якого виконується поетапне формування проміжних ключів. Такий підхід дозволяє суттєво зменшити глибину координації та скоротити кількість операцій при динамічній зміні складу групи. Протоколи Tree-GKA особливо ефективні у великих розподілених системах, де потрібно регулярне додавання або виключення учасників без повного перетворення групового ключа [76-80].

Окремий напрямок склали Ring-based GKA-протоколи, що використовують кільцеву топологію взаємодії. У таких схемах кожен учасник взаємодіє лише з сусідніми вузлами кільця, а підсумковий ключ формується шляхом послідовної обробки проміжних значень. Кільцева організація забезпечує рівномірний розподіл обчислювального навантаження між учасниками та спрощує організацію децентралізованої взаємодії. Однак, зі збільшенням числа користувачів Ring-GKA-протоколи часто демонструють більш високу сумарну обчислювальну вартість в наслідок зростання кількості залежних операцій та збільшення координаційних накладних витрат.

Спочатку більшість GKA-протоколів будувалися на основі арифметики мультиплікативних груп кінцевих полів, де основними криптографічними операціями були модульні зведення в ступінь. Такі операції вимагали значних обчислювальних ресурсів, особливо під час використання ключів великої довжини для забезпечення необхідного рівня криптографічної стійкості. Зі зростанням вимог до продуктивності розподілених систем та мобільних пристроїв, виникла необхідність переходу до ефективніших криптографічних примітивів.

Істотним етапом розвитку GKA-протоколів стало запровадження криптографії на еліптичних кривих (Elliptic Curve Cryptography, ECC). Використання еліптичних кривих дозволило забезпечити еквівалентний рівень криптографічної стійкості при значно менших розмірах ключів у порівнянні з класичними схемами дискретного логарифмування у кінцевих полях. Це призвело до зменшення обсягу переданих даних, зниження обчислювальних витрат та підвищення загальної продуктивності GKA-протоколів.

Найбільшого поширення набули три основних класи еліптичних кривих: криві Вейєрштраса, Монтгомері та Едвардса.

1. Еліптичні криві Вейєрштраса [81-83].

Еліптичні криві Вейєрштраса задаються рівнянням:

$$E_w(a,b): y^2 = x^3 + ax + b$$

де коефіцієнти a и b належать кінцевому полю F_p .

2. Еліптичні криві Монтгомері [84,85].

Еліптичні криві Монтгомері мають вигляд:

$$E_M(A,B): By^2 = x^3 + Ax^2 + x,$$

де A и B – параметри, що належать кінцевому полю F_p.

Ці криві зручні в реалізації операцій складання і множення, оскільки дозволяють уникнути необхідності обчислення квадратного кореня.

3. Еліптичні криві Едвардса [86-90].

Еліптичні криві Едвардса описуються рівнянням:

$$E_{Ed}(d): x^2 + y^2 = 1 + dx^2y^2,$$

де d є параметром, який також належать кінцевому полю F_p.

Аналіз трьох типів кривих дозволяє стверджувати, що крива Монтгомері вимагає найменші обчислювальні витрати. Операції складання та множення на кривих Монтгомері виконуються швидше, порівняно з іншими типами кривих. Криві Монтгомері використовують ефективний алгоритм обчислення множення точки на скаляр – «сходи Монтгомері» (Montgomery ladder [91-93]). Сходи

Монтгомері виконують операції за фіксовану кількість кроків, незалежно від значень бітів скаляра.

Алгоритм Montgomery Ladder (сходи Монтгомері) є методом скалярного множення точки еліптичної кривої, призначений для забезпечення регулярної структури обчислень (рис. 4.1) [94] . Нехай необхідно обчислити:

$$Q = k\boldsymbol{P},$$

де: $\boldsymbol{P}$ – точка еліптичної кривої;

$k = (k_{n-1},.., k_1\ k_0)_2$ — n-бітний скаляр;

Q — результуюча точка.

Основна ідея алгоритму у тому, що у кожної ітерації виконується однакову кількість операцій незалежно від значення поточного біта скаляра. Завдяки цьому зменшується залежність часу виконання секретних даних.

Алгоритм використовує дві проміжні точки:

$\boldsymbol{R_0}$ та $\boldsymbol{R_1}$, для яких підтримується інваріант: $\boldsymbol{R_1} = \boldsymbol{R_0} + \boldsymbol{P}$.

Ініціалізація. Початкові значення задаються таким чином:

$$\boldsymbol{R_0} = \boldsymbol{O},$$

$$\boldsymbol{R_1} = \boldsymbol{P},$$

де $\boldsymbol{O}$ — нейтральний елемент групи точок еліптичної кривої (точка нескінченності).

Принцип роботи алгоритму наступний.

Біти скаляра обробляються від старшого до молодшого.

Для кожного біта k_i виконуються операції складання та подвоєння точок. Якщо $k_i = 0$, то виконується:

$\boldsymbol{R}_1 \leftarrow \boldsymbol{R}_0 + \boldsymbol{R}_1$,

$\boldsymbol{R}_0 \leftarrow 2\boldsymbol{R}_0$.

Якщо $k_i = 1$,

то виконується:

$\boldsymbol{R}_0 \leftarrow \boldsymbol{R}_0 + \boldsymbol{R}_1$,

$\boldsymbol{R}_1 \leftarrow 2\boldsymbol{R}_1$.

Після обробки всіх бітів результатом є:

$\boldsymbol{Q} = \boldsymbol{R}_0 = k\boldsymbol{P}$.

Основні переваги Montgomery Ladder

1. Регулярна структура обчислень.

2. Передбачуваний час виконання.

3. Висока ефективність для кривих Монтгомері.

Схему алгоритму наведено на рисунку 4.1.

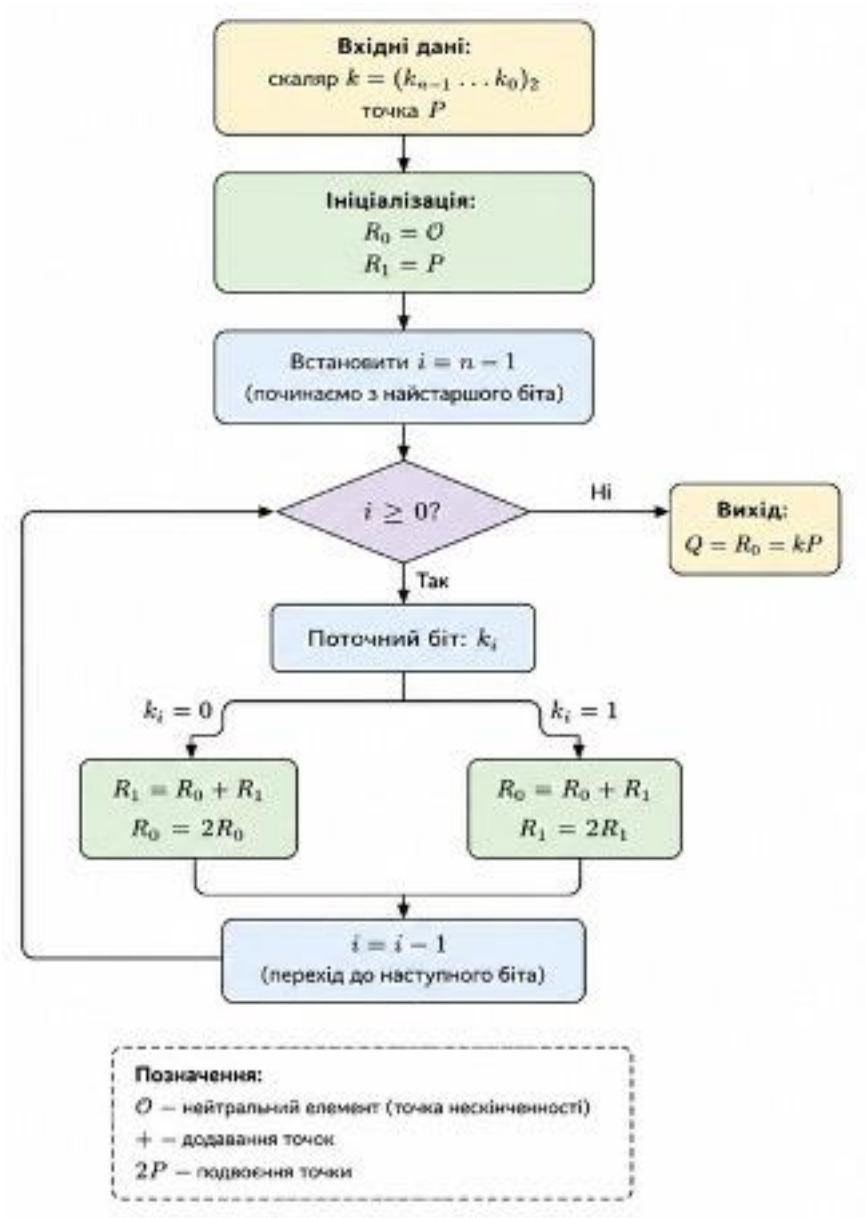


Рисунок 4.1– Схема алгоритму «Сходи Монтгомери» (Montgomery Ladder

Криві Вейєрштраса стали основою більшості міжнародних криптографічних стандартів завдяки універсальності математичного апарату та широкої сумісності з існуючими ECC-бібліотеками. Однак операції над такими кривими найчастіше вимагають порівняно складної арифметики координат.

Криві Монтгомері набули широкого поширення в системах Діффі-Хеллмана, завдяки високій ефективності операцій скалярного множення. У контексті GKA-протоколів застосування кривих Монтгомері дозволило суттєво зменшити вартість операцій групового узгодження ключів у системах з обмеженими обчислювальними ресурсами.

Криві Едвардса та їх модифікації забезпечили подальше підвищення ефективності ECC-арифметики. Симетрична форма рівнянь Едвардса дозволила спростити операції складання точок та зменшити кількість проміжних обчислень. Завдяки цьому Edwards-криві продемонстрували високу продуктивність у розподілених криптографічних протоколах, орієнтованих на інтенсивні операції групового узгодження.

Сучасний етап розвитку GKA-протоколів характеризується переходом від аналізу виключно теоретичної асимптотичної складності до побудови комплексних моделей практичної ефективності. Якщо ранні дослідження обмежувалися оцінкою складності виду (O(N)), (O(N /log N)) або ($O(N^2)$), то сучасні моделі враховують реальні обчислювальні характеристики криптографічних операцій, особливості ECC-реалізацій, вартість координації учасників, затримки синхронізації, навантаження на процесор та мережеву інфраструктуру.

В результаті з'явилися інтегральні моделі ефективності GKA-протоколів, які об'єднують:

- асимптотичну обчислювальну складність;
- кількість ECC-операцій;
- особливості конкретних типів еліптичних кривих.

Подібний підхід дозволяє більш реалістично оцінювати масштабованість та практичне застосування різних GKA-протоколів розрахованих на багато користувачів в умовах сучасних захищених комунікаційних середовищ. Саме інтеграція теоретичних і практичних аспектів оцінки ефективності стає одним з ключових напрямів сучасного розвитку протоколів групового узгодження ключів на основі Діффі-Хеллмана та криптографії на еліптичних кривих.

Постановка задачі:

Нехай є група з N учасників: $G = \{U_1, U_2, \dots, U_N\}$.

Необхідно визначити такий варіант GKA-протоколу та такий тип еліптичної кривої, які забезпечують максимальну ефективність формування загального групового ключа.

В рамках дослідження розглядаються два базові класи GKA- протоколів:

1. Протокол Burmester-Desmedt (BD-GKA);

2. Деревоподібні схеми групового узгодження ключів (TGDH).

Кожен із розглянутих протоколів може бути реалізований на:

- кривих Вейєрштраса;
- кривих Монтгомері;
- кривих Едвардса.

Потрібно визначити область раціонального застосування кожної комбінації складових:

$$\langle Protocol, Curve, N, Latency \rangle,$$

де: $Protocol$ – тип GKA-протоколу;

$Curve$ – тип еліптичної кривої;

N – кількість учасників групи;

$Latency$ – мережна затримка.

Для кількісного порівняння різних варіантів було введено інтегральну функцію ефективності:

$$E(N) = \frac{S(N)}{w_1 C_{comp}(N) + w_2 C_{comm}(N) + w_3 T(N) + w_4 R(N)},$$

де:

$S(N)$ – криптографічна стійкість;

$C_{comp}(N)$ – обчислювальна вартість;

$C_{comm}(N)$ – комунікаційна вартість;

$T(N)$ – часова затримка виконання протоколу;

$R(N)$ – вартість оновлення ключів;

w_i – вагові коефіцієнти.

Оскільки порівнювали криві еквівалентного рівня криптографічної стійкості, величина $S(N)$ приймалася постійною:

$$S(N) = const.$$

В результаті завдання максимізації ефективність зводиться до мінімізації сукупних витрат протоколу.

Обчислювальна модель вартості операцій.

Основне обчислювальне навантаження у GKA-протоколах створює операція скалярного множення точки еліптичної кривої. Для оцінки вартості обчислень була використана агрегована модель:

$$C_{comp} = n_M c_M + n_S c_S + n_A c_A,$$

де n_M – кількість множень у кінцевому полі;

n_S – кількість операцій зведення у квадрат;

n_A– кількість операцій складання;

c_M, c_S, c_A – відносні вартості даних операцій.

Як базова одиниця приймалася вартість множення: $c_M = 1$.

Тоді:

$$c_S \approx 0{,}8 c_M;$$

$$c_A \approx 0{,}05 c_M.$$

Для різних типів еліптичних кривих було отримано такі відносні оцінки вартості.

Криві Вейєрштраса.

Операція складання точки:

$$12M + 2S + 7A$$

Загальна вартість:

$$C_{Wei} = 12c_M + 2c_S + 7c_A$$

Після підстановки:

$$C_{Wei} = 13{,}95$$

Криві Монтгомері.

Для алгоритму «Сходи Монтгомері»:

$$8M + 4S + 6A$$

Отже:

$$C_{Mont} = 8c_M + 4c_S + 6c_A$$

Після підстановки:

$$C_{Mont} = 11{,}5$$

Криві Едвардса.

Для симетричних формул Едвардса:

$$10M + 1S + 6A.$$

Загальна вартість:

$$C_{Ed} = 10c_M + c_S + 6c_A$$

Після підстановки:

$$C_{Ed} = 11{,}1$$

Таким чином, найбільш ефективними з обчислювальної точки зору виявляються криві Монтгомері та Едвардса.

Масштабованість GKA-протоколів.

Однією з ключових характеристик групових протоколів є масштабованість. Під масштабованістю розуміється здатність протоколу зберігати прийнятну продуктивність зі збільшенням числа учасників групи. Формально масштабованість можна визначити через швидкість зростання обчислювальних витрат:

$$Scalability = \frac{1}{\frac{dC(N)}{dN}}.$$

Чим повільніше зростає вартість, тим вища масштабованість системи.

Масштабованість BD-GKA.

Для протоколу Burmester-Desmedt обчислювальна складність зростає лінійно:

$$C_{BD}(N) \sim O(N).$$

Це означає, що кожен новий учасник практично пропорційно збільшує обчислювальне навантаження. Однак для діапазону $N = 10\text{-}20$ дане зростання залишається помірним і практично не призводить до деградації продуктивності.

Масштабованість TGDH.

Для деревоподібних схем:

$$C_{TGDH}(N) \sim O(\log_2 N).$$

Отже, навіть значне збільшення числа учасників наводить лише до помірного зростання витрат. Це робить деревоподібні схеми доцільними для великих розподілених систем.

Вплив затримки мережі.

Найважливішим параметром GKA-протоколів є Latency – мережна затримка. Під Latency розуміється час передачі повідомлень між учасниками групи та виконання одного комунікаційного раунду.

Повний час виконання протоколу визначається виразом:

$$T(N) = r(N)t_{round} + t_{comp},$$

де: $r(N)$ – число раундів;

t_{round} – затримка одного раунду;

t_{comp} – час обчислень.

Протокол Burmester-Desmedt вимагає лише двох раундів $r_{BD} = 2$ незалежно від кількості учасників.

Це є однією з найважливіших переваг BD-GKA у мережах з високою затримкою.

Деревоподібні схеми вимагають більшої кількості фаз обміну, проте виграють за рахунок кращої масштабованості.

Графічна модель інтегральної функції ефективності.

Для аналізу областей домінування різної архітектури було побудовано графічну модель (рис. 4.2):

$$E = f(N, L, C),$$

де: N – кількість учасників;

L – затримка мережі;

C – тип еліптичної кривої.

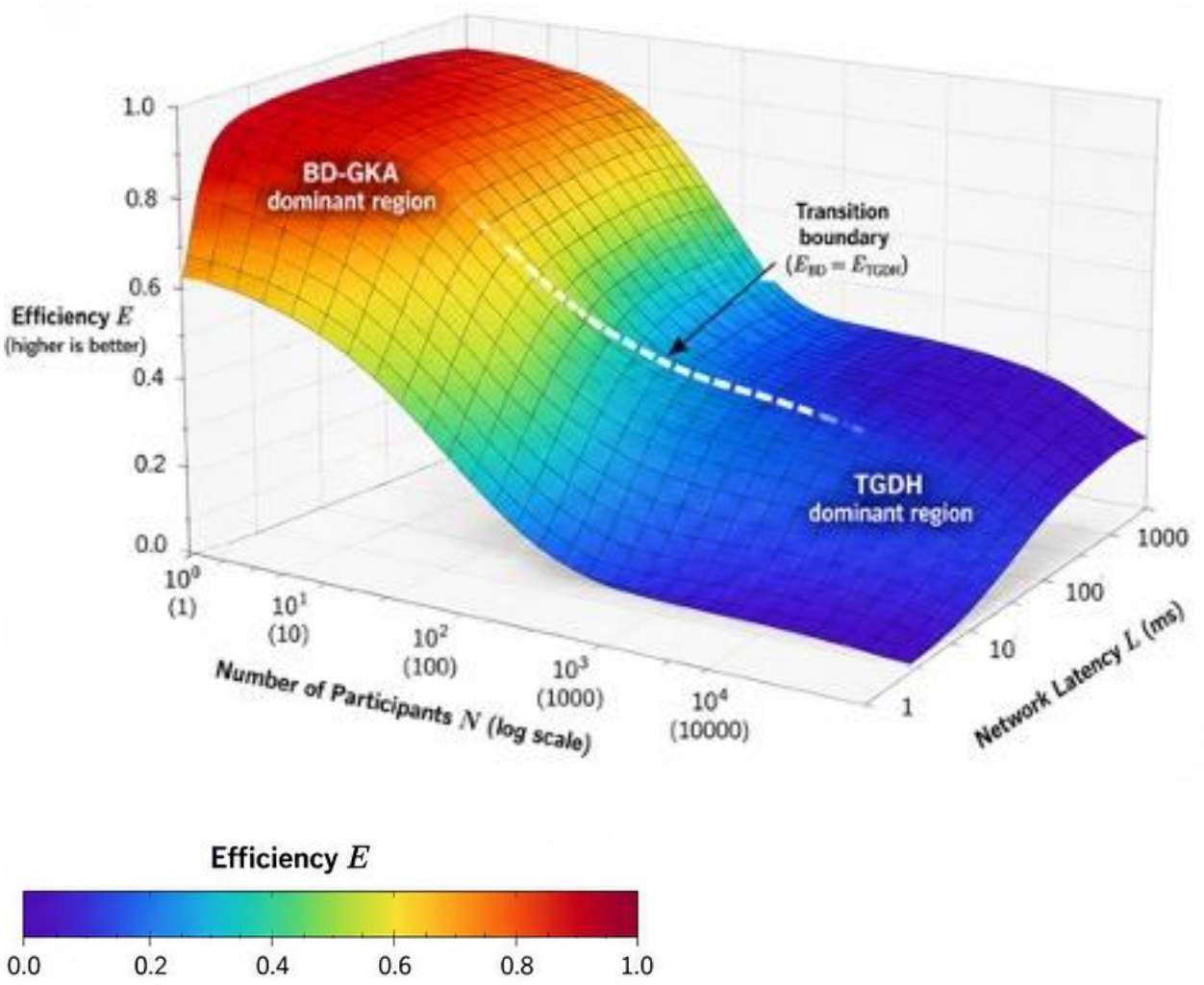


Рисунок 4.2 – Графічна модель інтегральної функції ефективності.

Побудована 3D phase surface дозволяє візуалізувати області домінування різних GKA-архітектур. Цей графік – фазова карта ефективності GKA-протоколів (Group Key Agreement), що показує, в яких умовах який протокол стає кращим.

Осі поверхні. Вісь X – Number of Participants – кількість учасників групи (логарифмічна шкала): то головний параметр масштабованості GKA.

Вісь Y – Network Latency – мережна затримка, зразкові значення: 1мс – локальна мережа, 10-100 мс – інтернет, 1000 мс – супутникові / WAN-мережі.

Вісь Z – Efficiency – нормалізована ефективність: $0 \leq E \leq 1$.

Поверхня показує, як змінюється ефективність GKA при одночасної зміни розміру групи, мережної затримки, вартості ECC-операцій. Це багатовимірна модель оптимальності протоколу.

Ліва частина поверхні відповідає режиму високої ефективності BD-GKA. Це зона домінування BD-GKA. Це означає, що за малих і середніх груп протокол Burmester-Desmedt працює краще.

Причинами цього є те, що BD-GKA має невелику кількість раундів, низьку мережну затримку та просту координацію. Тобто при $N \lesssim 20\text{-}50$ мережеві переваги BD переважують його лінійну вартість обчислень.

Праворуч знаходиться регіон, де домінує TGDH (TGDH = Tree Group Diffie-Hellman). Це означає, що при великих групах дерево стає ефективніше.

Важливим елементом поверхні є біла пунктирна лінія. Це межа фазового переходу. Вона відповідає умові: $E_{BD} = E_{TGDH}$, тобто ліворуч від лінії домінує BD-GKA, а праворуч – TGDH.

Лінія вигнута і це дуже важливий момент. Якби порівняння залежало тільки від *N*, лінія була б вертикальною. Насправді ж вона викривляється, тому що при зростанні затримки вартість додаткових раундів стає критичною. При високій затримці BD-GKA залишається вигідним для групи довше.

Інтерпретація колірної динаміки є наступною.

Червона область – це область високій ефективності (невеликі групи, дешеві ECC-операції).

Зелена зона – це перехідна область, тут починається конкуренція між мережевою вартістю та масштабованістю.

Синя/фіолетова зона – область, де система стає неефективною: тут або надто велика група, або висока складність координації, або висока вартість оновлення.

Побудована тривимірна фазова поверхня ефективності демонструє існування областей домінування різних GKA-протоколів в залежності від розміру групи, мережної затримки та вартості ECC-операцій. Кордон переходу між областями відповідає умові рівності інтегральної ефективності протоколів та інтерпретується як точка фазового переходу системи групового узгодження ключа.

Отримані результати підтверджують відсутність універсально оптимального GKA-протоколу та обґрунтовують необхідність адаптивного вибору схеми групового узгодження ключа в залежності від параметрів середовища виконання.

Проведене моделювання показало, що для груп середньої розмірності $N = 10\text{-}20$ найбільш ефективним рішенням є комбінація: $BD\text{-}GKA + Montgomery$.

Цей результат пояснюється впливом наступних складових:

– мінімальної кількості комунікаційних раундів;

– високої швидкості операцій на еліптичній кривій;

– невеликого розміру групи користувачів;

– низьких комунікаційних накладних витрат;

– простою структурою протоколу.

При збільшенні числа учасників: $N > 20\text{-}30$ деревоподібні схеми починають демонструвати вищу ефективність завдяки логарифмічній масштабованості.

Найбільш ефективними реалізаціями TGDH також виявляються варіанти на кривих Монтгомері та Едвардса.

Криві Вейєрштраса у всіх досліджених сценаріях показали більше високу обчислювальну вартість внаслідок складнішої арифметики групового закону.

Таким чином, у ході дослідження було збудовано комплексну модель вибору оптимального GKA-протоколу на основі інтегрального показника ефективності, що враховує обчислювальну вартість, мережі затримки, комунікаційні витрати, вартість оновлення ключів та масштабованість системи. Показано, що ефективність GKA-протоколів визначається як асимптотичної складністю алгоритму, а й вартістю операцій на конкретному типі еліптичної кривої, а також характеристиками мережі. Встановлено, що для малих та середніх груп найбільш ефективним рішенням є протокол Burmester-Desmedt в поєднанні з кривими Монтгомері, тоді як для великих розподілених систем переважними стають деревоподібні схеми TGDH.

Отримана фазова модель дозволяє формалізувати галузі раціонального застосування різних GKA-архітектур та криптографічних платформ колективної взаємодії.

Далі побудована поверхня Curve-Protocol Sensitivity Surface, як узагальнена тривимірна модель, яка пов'язує параметри кривої, характеристики протоколу та підсумкову чутливість (або вартість/ефективність) системи. Вона сформована шляхом побудови базових кривих кожного протоколу окремо. Розраховуються залежності виду $C(N, curve)$, тобто обчислювальна вартість для різних типів еліптичних кривих (Weierstrass, Montgomery, Edwards). Щоб різні протоколи можна було порівнювати, дані приводяться до загальної шкали. Дискретні точки (отримані з розрахунків/експериментів) перетворюються на безперервну поверхню шляхом сплайн інтерполяції.

У результаті отримано поверхню: $S = f(N, protocol, curve)$, яка показує чутливість протоколу до вибору еліптичної кривої при зростанні масштабу системи (рис. 4.3).

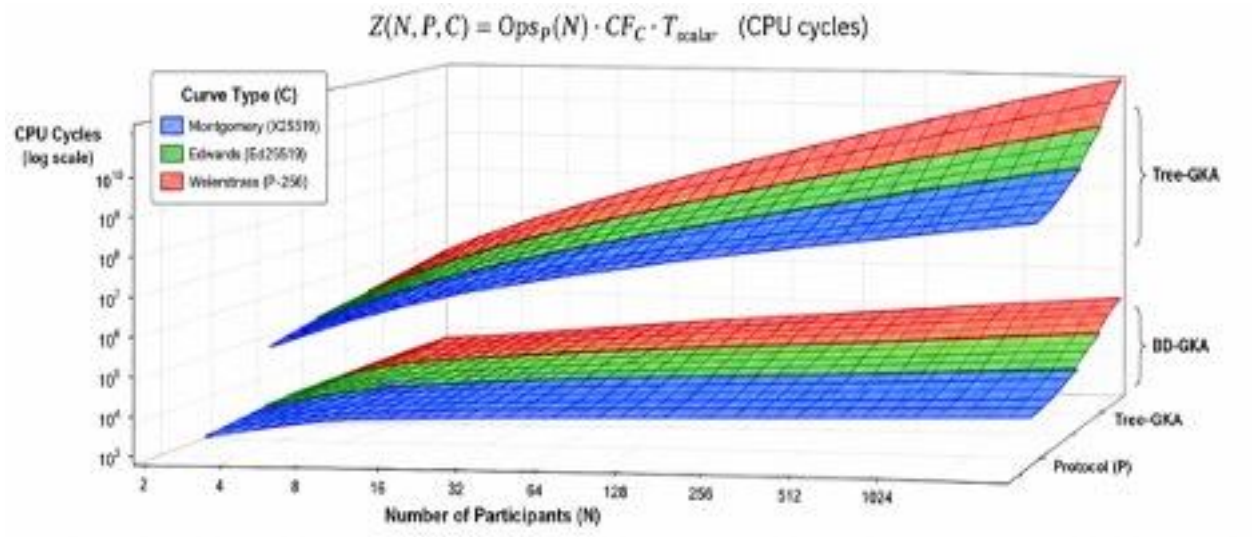


Рисунок 4.3 – Графік Curve-Protocol Sensitivity Surface.

Графік Curve-Protocol Sensitivity Surface демонструє інтегральну залежність обчислювальної вартості GKA-протоколів від числа учасників, типу протоколу та використовуваної еліптичної кривої.

Поверхня відображає спільний вплив архітектури розподілу групового ключа та обчислювальної вартості операцій ECC на підсумкові витрати на CPU cycles. Аналіз поверхні показує, що основним фактором зростання обчислювального навантаження є структура самого протоколу, тоді як тип еліптичної кривої виступає у ролі масштабного коефіцієнта, що змінює абсолютний рівень вартості, але й характер її зростання.

Найбільш важливим висновком є суттєва різниця між протоколами BD-GKA та Tree-GKA. Поверхня Tree-GKA розташовується значно вище і демонструє виражене нелінійне зростання при збільшення числа учасників. Це пов'язано з залежністю виду $N\log_2 N$, при якій збільшення розміру групи призводить до прискореного зростання числа операцій. Геометрично це проявляється як зростаюча кривизна поверхні: при малих значеннях N зростання вартості помірне, проте при переході до великих груп нахил поверхні стає дедалі більше крутим. Таким чином, Tree-GKA характеризується погіршенням

масштабованості при зростанні числа учасників та поступовим переходом системи в обчислювально важкий режим. На противагу цьому поверхня BD-GKA має майже лінійний характер. Її нахил залишається порівняно постійним навіть за значного збільшення числа учасників, що відповідає лінійній залежності. Практично це означає, що обчислювальне навантаження зростає передбачувано і без різкого погіршення масштабованості. Поверхня BD-GKA залишається суттєво нижче Tree-GKA на всьому діапазоні N, що свідчить про значно менші обчислювальні витратаи та кращу придатність протоколу для великих груп користувачів.

Додатковий рівень аналізу пов'язаний з типом використовуваної еліптичної кривої. Всередині кожної протокольної поверхні спостерігаються три практично паралельні шари, відповідних Montgomery, Edwards та Weierstrass-кривим. Це показує, що вибір кривої не змінює форму масштабування системи, а лише вертикально зміщує поверхню вартості. Криві Монгомери формують мінімальний рівень обчислювальних витрат, Edwards займають проміжне положення, а Weierstrass демонструють найбільшу вартість. Паралельність поверхонь вказує на те, що коефіцієнт вартості ECC залишається практично постійним щодо числа учасників та не впливає на асимптотичний характер зростання.

Показана на рисунку 4.4 Tree-GKA Cost Surface by Curve демонструє обчислювальну вартість Tree-GKA для різних типів еліптичних кривих.

Поверхня має виражену кривизну і швидко зростає при збільшенні числа учасників. Це відображає характер залежності $N\log_2 N$, характерний для деревоподібної схеми розподілу ключа.

При малих розмірах групи зростання обчислювального навантаження залишається порівняно помірним, однак у міру збільшення N поверхня стає все більш крутою, що вказує на погіршення масштабованості.

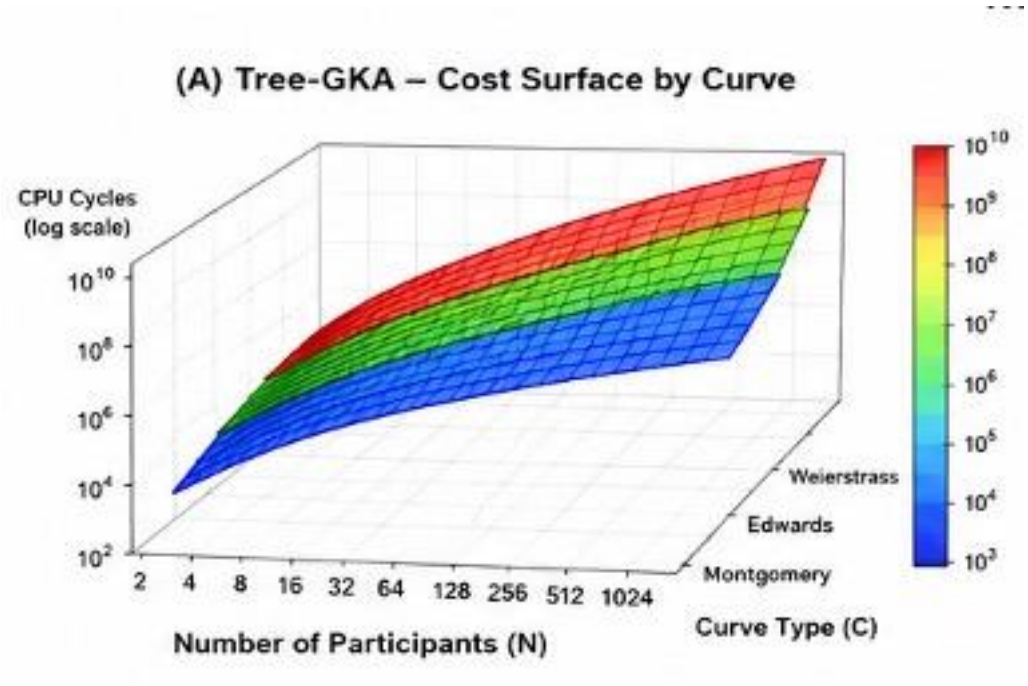


Рисунок 4.4 – Обчислювальна вартість Tree-GKA для різних типів еліптичних кривих.

Особливо це помітно в області великих груп, де навіть невелике збільшення числа учасників призводить до суттєвого зростання CPU cycles. Поділ поверхні на три шари показує вплив типу кривої : Montgomery забезпечує мінімальну вартість, Edwards – проміжну, а Weierstrass – максимальну. При цьому відстань між шарами залишається майже постійною, що підтверджує незалежність curve-factor від числа учасників. Таким чином, графік показує, що основна причина зростання обчислювальної вартості Tree-GKA пов'язана саме з архітектурою протоколу, а вибір кривої лише посилює чи послаблює це зростання.

Наведена на рисунку 4.5 BD-GKA Cost Surface by Curve демонструє принципово інший характер поведінки системи.

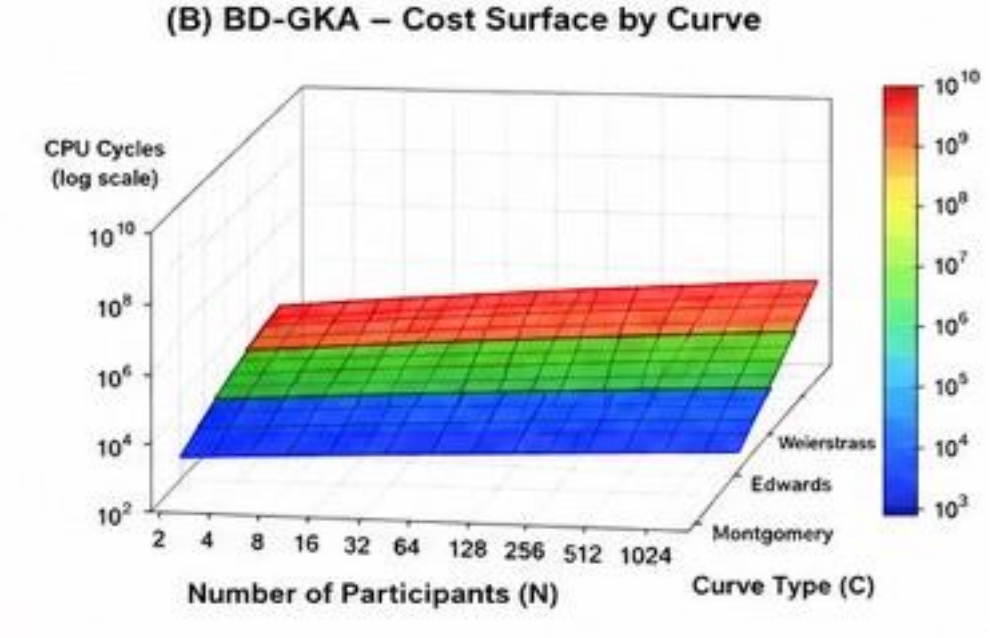


Рисунок 4.5 – Обчислювальна вартість BD-GKA для різних типів еліптичних кривих.

Поверхня має майже лінійний вигляд та значно менший нахил. Це відповідає залежності $3(N-1)$, яка є характерною для BD-GKA. На відміну від Tree-GKA, тут відсутнє виражене прискорення зростання обчислювального навантаження: збільшення числа учасників призводить до майже пропорційного збільшення вартості. Навіть при великих значеннях *N*, поверхня залишається порівняно плоскою, що вказує на гарну масштабованість протоколу. Аналогічно попередньому графіку спостерігається вертикальний поділ за типами кривих, проте самі поверхні залишаються паралельними і не розходяться зі зростанням числа учасників. Це означає, що вплив ECC-кривої зберігає характер постійного мультиплікативного коефіцієнта та не впливає на форму масштабування. У сукупності графік підтверджує, що BD-GKA забезпечує значно більш стійке та передбачуване зростання обчислювальної вартості в порівнянні з Tree-GKA.

На рисунку 4.6 показана Curve Sensitivity (Normalized to Montgomery), ця поверхня має особливо важливе значення. Тут вартість всіх кривих нормована щодо Montgomery-кривих, прийнятих за одиничний базовий рівень.

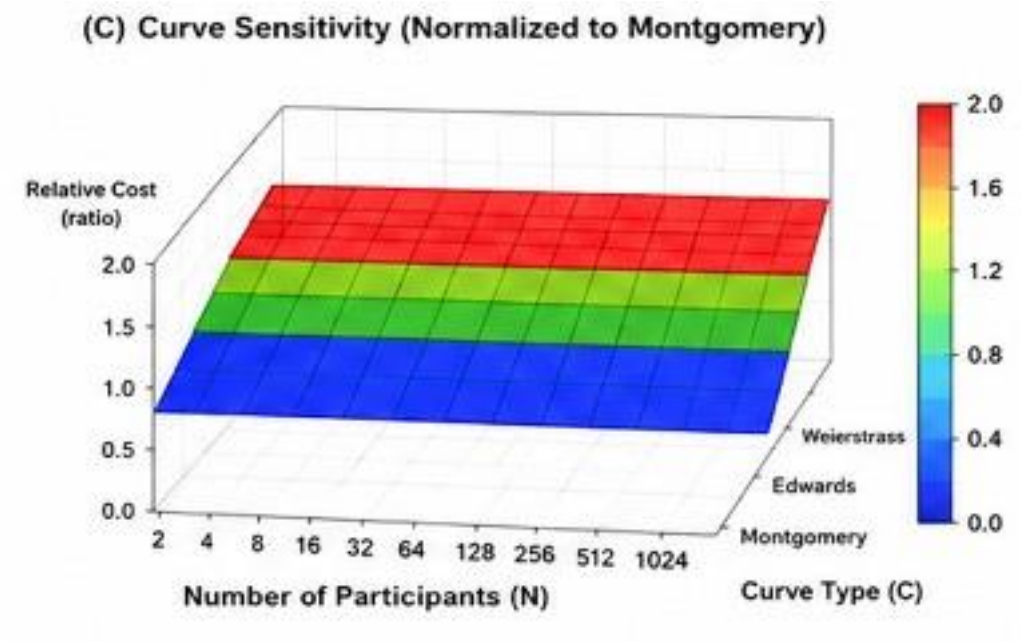


Рисунок 4.6 – Обчислювальна вартість, нормована до кривої Монтгомері.

Поверхня практично не змінюється вздовж осі числа учасників, а відмінності між Montgomery, Edwards та Weierstrass залишаються постійними на всьому діапазоні *N*. Це означає, що відносна вартість ECC-реалізацій не залежить від розміру групи і може розглядатися як стабільний коефіцієнт масштабування. Іншими словами, тип кривої не впливає на асимптотичну поведінку протоколу, а лише змінює абсолютну вартість однієї криптографічної операції. Такий результат підтверджує коректність моделі:

$$Z(N, P, C) = f(N, P) \cdot g(C),$$

де протокольна складність та вартість ECC є незалежними компонентами загального обчислювального навантаження.

Сукупний аналіз трьох останніх графіків показує, що вибір топології GKA, робить значно більший вплив на масштабованість системи, ніж вибір конкретної еліптичної кривої.

Tree-GKA формує швидко зростаючу обчислювальну поверхню і гірше переносить збільшення кількості учасників, тоді як BD-GKA демонструє майже лінійне зростання і зберігає стійкість навіть великих груп. Тип кривої, у свою чергу, визначає лише рівень обчислювальної вартості. Montgomery-криві мінімізують витрати, Weierstrass-криві збільшують їх, а Edwards займають проміжне положення.

Таким чином, графіки підтверджують, що архітектура координації групового ключового обміну є визначальним фактором ефективності GKA-систем, тоді як реалізація виконує роль додаткового коефіцієнта.

Окремо досліджено питання масштабованості групи, що формується. Масштабованість визначається тим, наскільки швидко росте обчислювальна вартість зі збільшенням N [94, 95].

Використана загальна модель:

$$Scale(N) = \alpha \cdot f_{proto}(N) \cdot k_{curve},$$

де: $f_{proto}(N)$ – складність протоколу;

k_{curve} – коефіцієнт вартості операцій на кривій;

$\alpha -$ базова вартість операції на кривий.

На рисунках 4.7 – 4.9 наведено графіки масштабованості для різних протоколів.

На основі вище наведених графиків побудовано поверхню інтегральної залежності обчислювальних витрат GKA – протоколів одночасно від двох факторів (рис. 4.10). На цій 3D-поверхні показана інтегральна залежність обчислювальних витрат GKA-протоколів одночасно від двох факторів: числа учасників N та моделі еліптичної кривої.

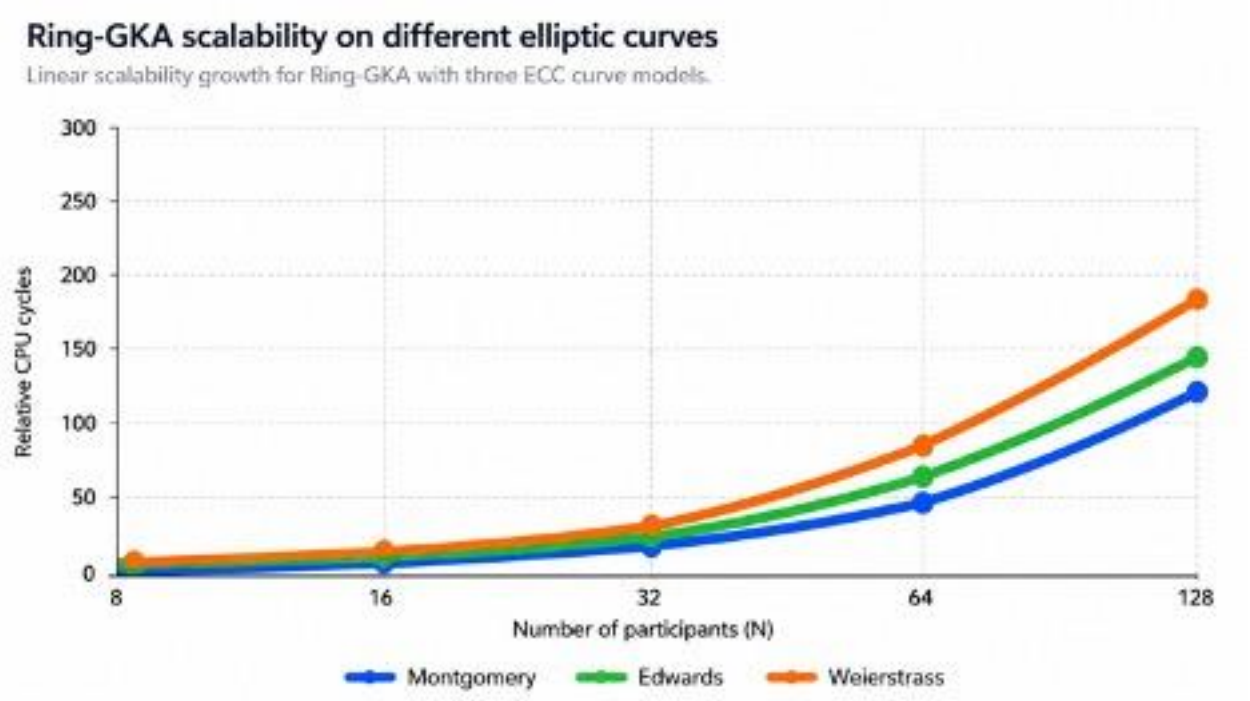


Рисунок 4.7 – Масштабованість для протоколу Діффі-Хеллмана.

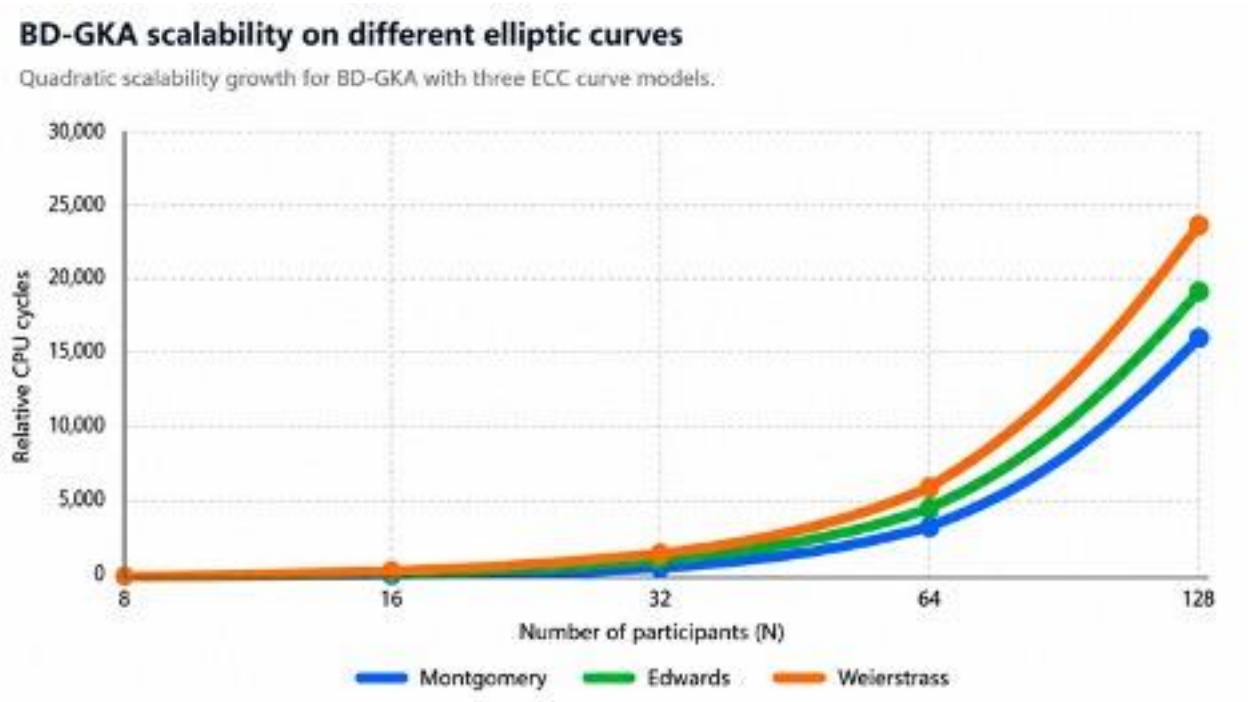


Рисунок 4.8 – Масштабованість для протоколу Бурместера-Десмедта.

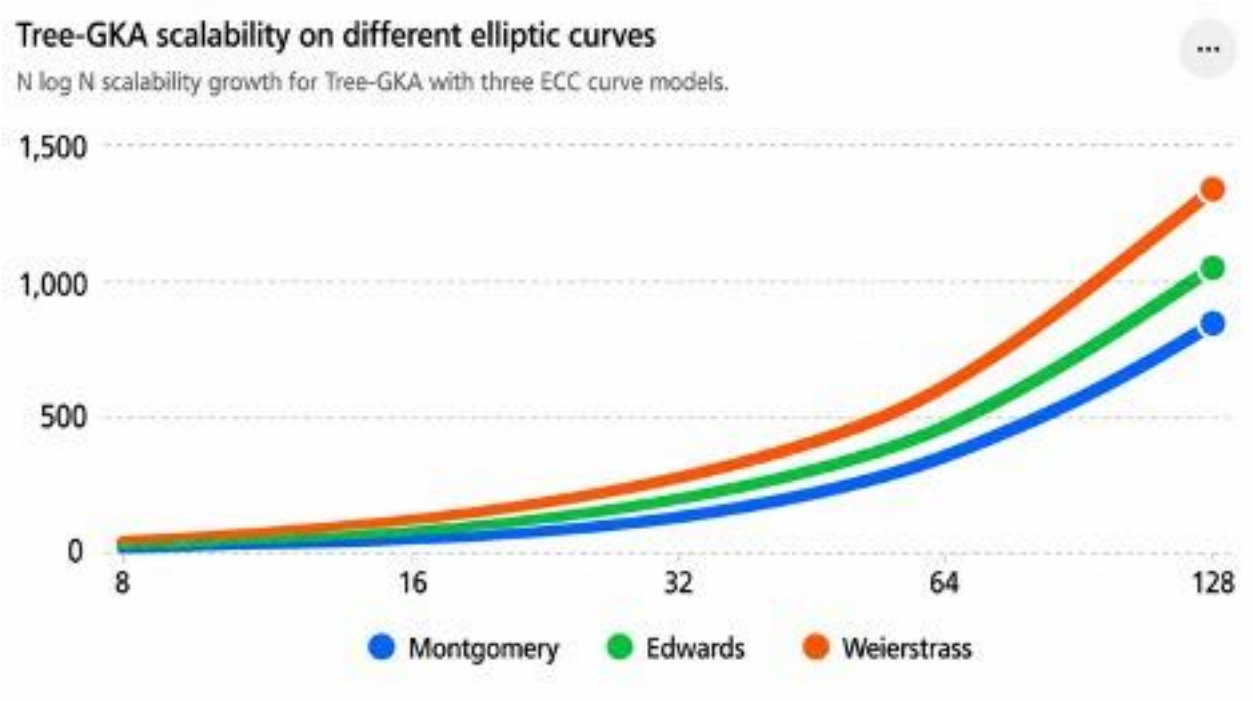


Рисунок 4.9 – Масштабованість для деревоподібного протоколу.

Поверхня поєднує три рівні складності протоколів – лінійний $O(N)$, квазілінійний $O(N \log N)$ і квадратичний $O(N^2)$, а також враховує відмінності обчислювальної вартості операцій на кривих Montgomery, Edwards та Weierstrass.

В основі побудови лежить модель:

$$C(N, proto, curve) = f_{proto}(N) \cdot k_{curve},$$

де $f_{proto}(N)$ – описує асимптотику протоколу;

k_{curve} – відображає відносну вартість операцій на обраній моделі еліптичної кривою.

Зокрема, при побудові поверхні взяті такі значення:

$$k_{\text{Montgomery}} = 1;$$

$$k_{\text{Edwards}} \approx 1{,}15;$$

$$k_{\text{Weierstrass}} \approx 1{,}45.$$

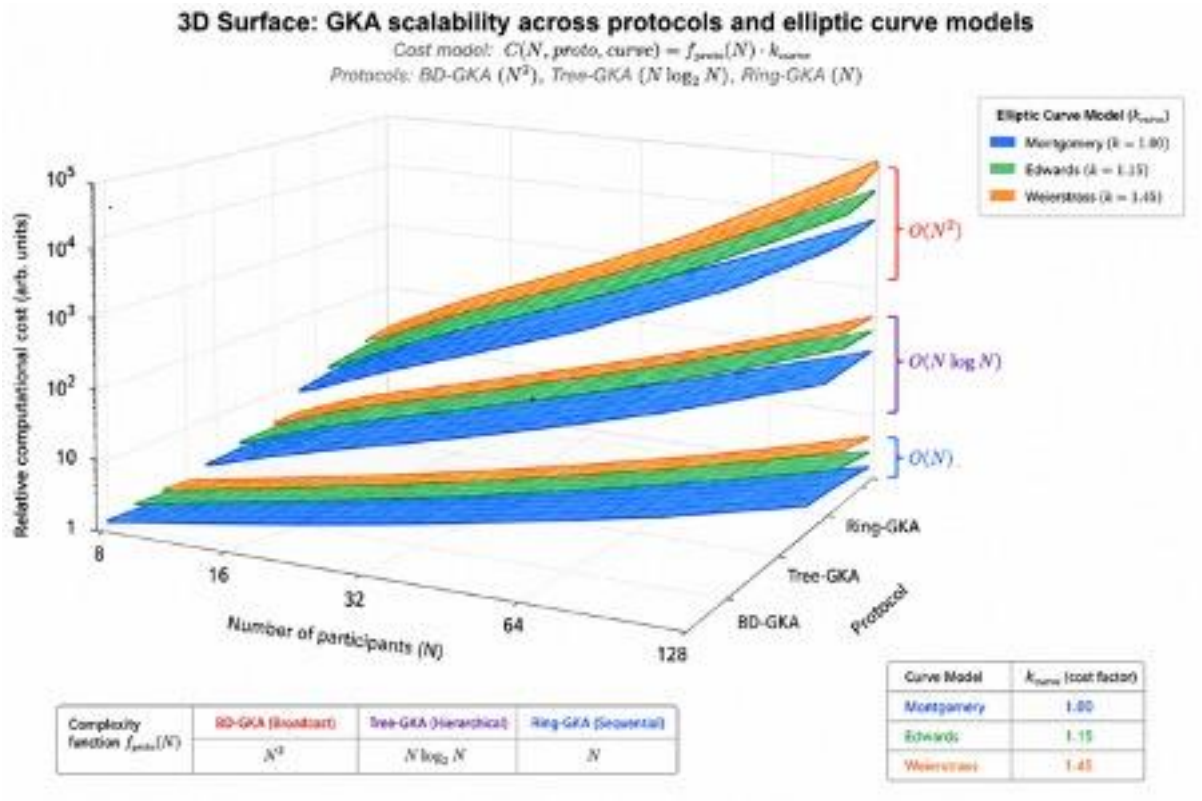


Рисунок 4.10 – Інтегральна масштабованість для різних протоколів та типів еліптичних кривих.

По осі X відкладено кількість учасників групи, по осі Y – тип протоколу, а по вертикальній осі Z – відносна обчислювальна вартість у логарифмічний масштаб. Логарифмічна шкала дозволяє одночасно спостерігати як малі, так і дуже великі значення витрат, що виникають при зростанні N.

Нижній шар поверхні відповідає Ring-GKA з лінійною складністю $f_{Ring}(N) = N$.

Тут зростання вартості відбувається найплавніше. Навіть при збільшенні числа учасників обчислювальне навантаження зростає практично пропорційно до розміру групи. Це вказує на високу масштабованість кільцевої архітектури та робить Ring-GKA найбільш стійким до зростання N.

Середній шар відповідає Tree-GKA:

$$f_{Tree}(N) = N\log_2 N$$

Зростання витрат тут помітно швидше за лінійне, проте суттєво повільніше квадратичного. Ієрархічна структура дерева зменшує глибину координації та розподіляє обчислення між вузлами, завдяки чому Tree-GKA займає проміжне положення між ефективністю та керованістю групового обміну ключами.

Верхній шар описує BD-GKA:

$$f_{BD}(N) = N^2$$

Саме тут спостерігається найбільш різке зростання поверхні. При збільшенні числа учасників вартість зростає квадратично, оскільки кількість необхідних взаємодій між учасниками швидко збільшується. Тому при великих BD-GKA стає суттєво менш масштабованим у порівнянні з Tree- та Ring-архітектурами.

Відмінності кольорів всередині кожного шару показують вплив типу еліптичної кривої. *Синя поверхня* (Montgomery) має мінімальну висоту, оскільки операції на таких кривих вимагають найменших обчислювальних витрат. *Зелена поверхня* (Edwards) розташовується вище, а *помаранчева* (Weierstrass) демонструє максимальну вартість обчислень. Таким чином, модель кривої виступає як мультиплікативний коефіцієнт, що посилює або зменшує базову асимптотику протоколу.

Графік також показує важливий практичний ефект: відмінності між моделями кривих стають особливо помітні при великих *N*. На малих розмірах групи вплив коефіцієнта k_{curve} відносно невеликий, проте при квадратичному зростанні BD-GKA навіть невелике збільшення вартості однієї ECC-операції призводить до значного зростання загального обчислювального навантаження.

Практичний висновок із графіка поверхні полягає в тому, що вибір топології протоколу надає більший вплив на масштабованість системи, ніж вибір

конкретної моделі еліптичної кривої. Однак всередині однієї і тієї ж топології використання Montgomery-кривих дозволяє суттєво знизити абсолютні обчислювальні витрати. Тому для великих динамічних груп найефективнішою комбінацією є Ring-GKA або Tree-GKA спільно з Montgomery-кривими, тоді як BD-GKA на Weierstrass-кривих представляє найбільш ресурсомісткий сценарій.

Для перевірки адекватності розробленої вище моделі були складено три моделюючі програми формування груп довірених користувачів за різними протоколами – програма для моделювання протоколу Діффі-Хеллмана, розширена на N користувачів, програма моделювання протоколу Бурместера-Десмедта, програма моделювання деревоподібного протоколу. Схеми всіх трьох програм представлені на рисунках 4.11 – 4.13.

Всі програми використовують еліптичну функцію Монтгомері, яка в процесі попереднього аналізу показала себе найбільш ефективною з погляду обчислювальних витрат.

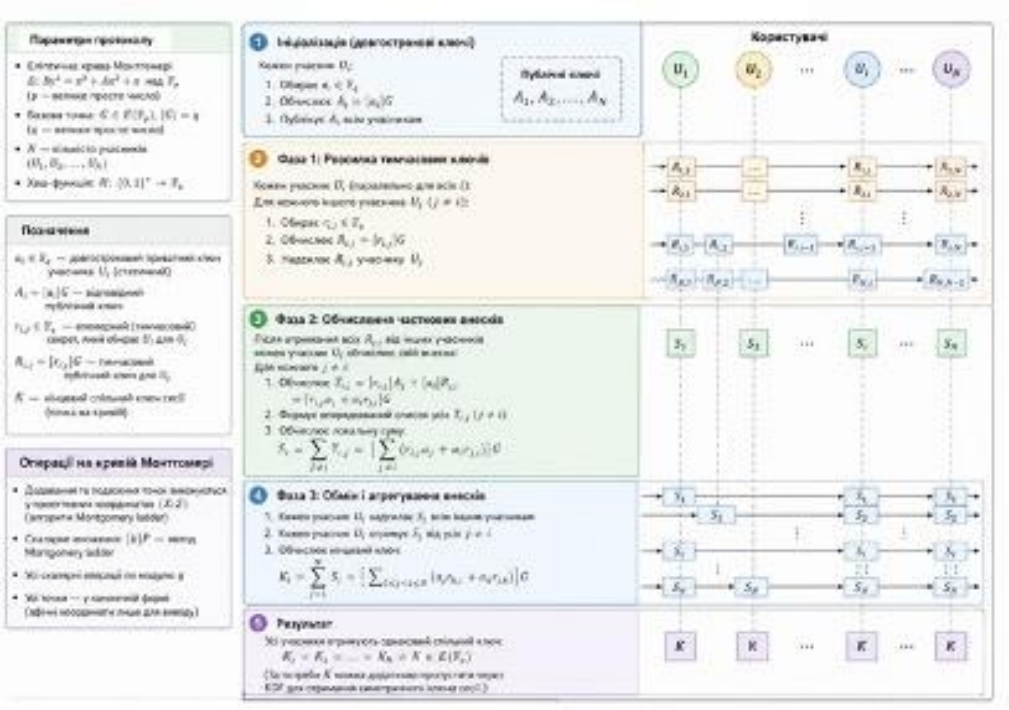


Рисунок 4.11 – Схема моделюючої програми для протоколу Діффі-Хеллмана для N користувачів.

Моделююча програма для протоколу Діффі-Хеллмана складається з трьох фаз:

– розсилка початкових ключів;

– обчислення проміжних відкритих ключів;

– формування загального секрету.

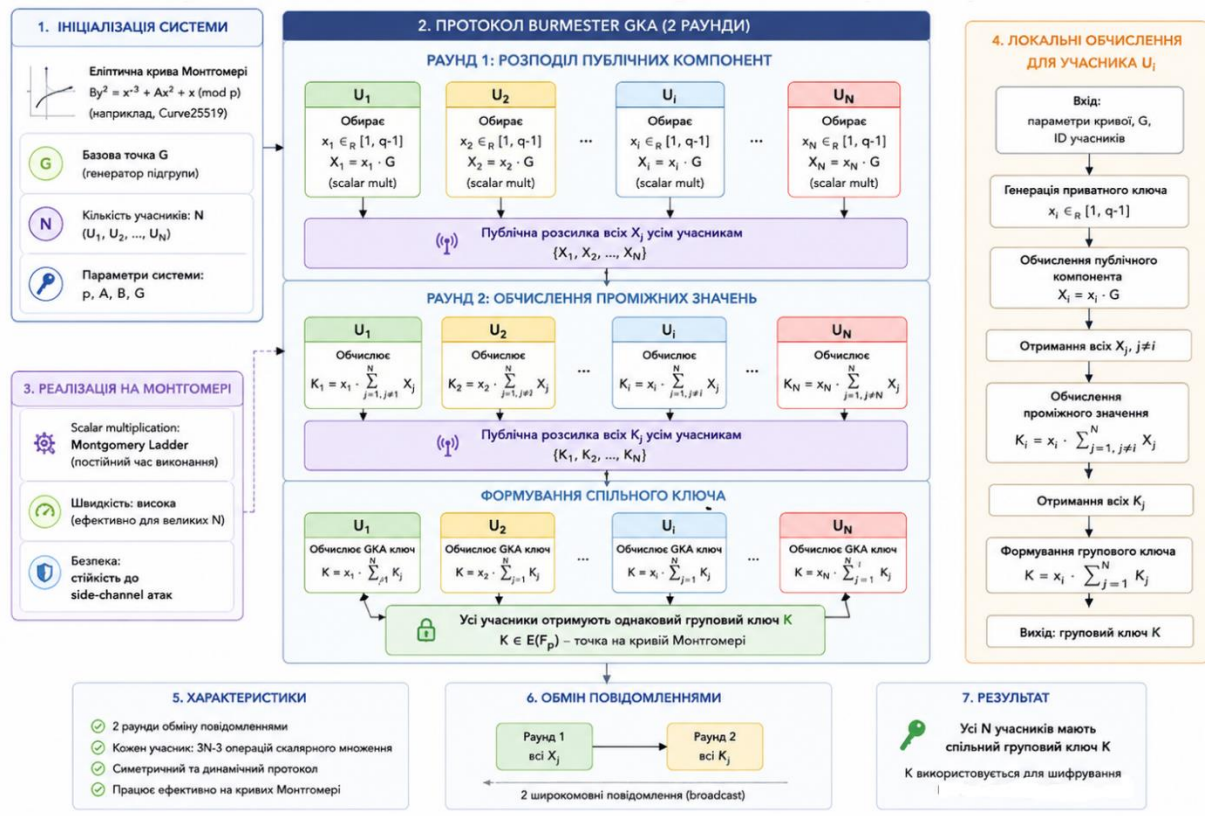


Рисунок 4.12 – Схема моделюючої програми для протоколу Бурместера-Десмедта для N користувачів .

Програма моделювання протоколу Бурместера-Десмедта містить два попередніх раунди:

– розподіл відкритих ключів;

– обчислення проміжних значень відкритих ключів.

Кінцевий етап програми містить формування загального секрету.

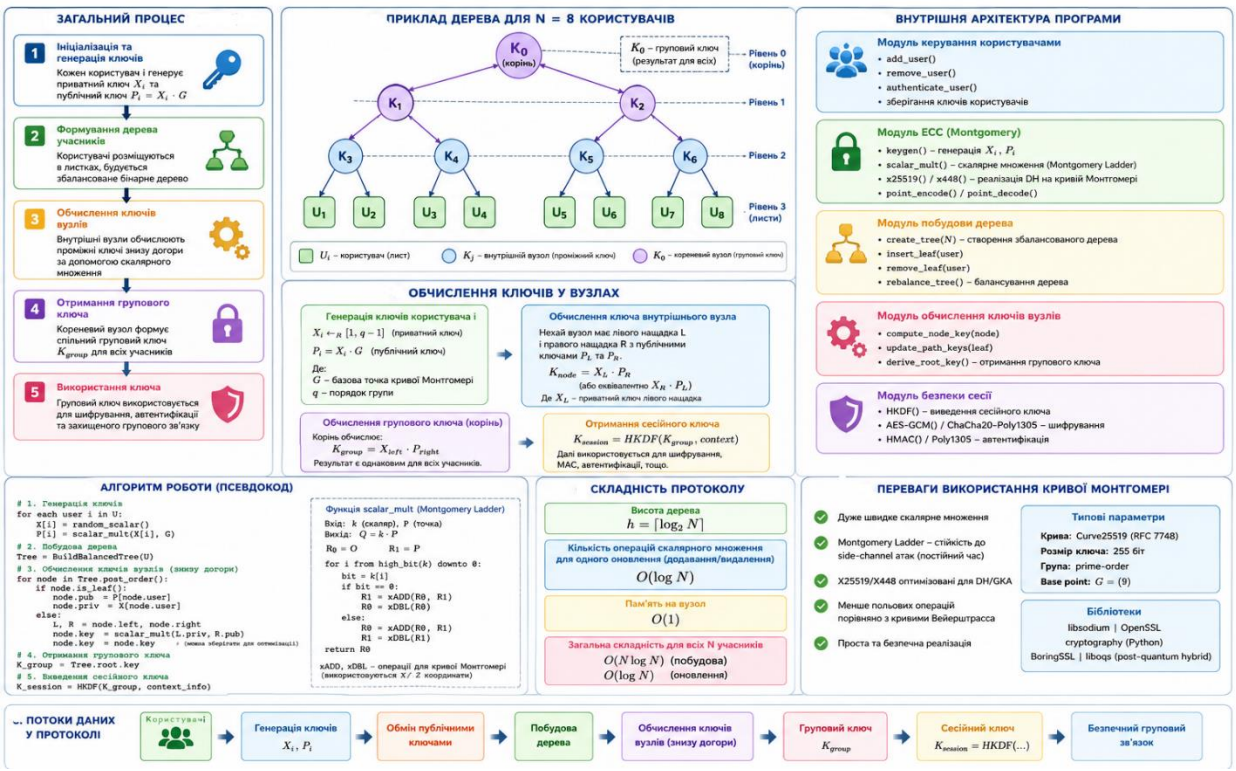


Рисунок 4.13 – Схема моделюючої програми для деревоподібного протоколу з N користувачами.

Моделююча програма для деревоподібного протоколу містить такі модулі: модуль управління користувачами, модуль операцій на еліптичної кривої Монтгомері, модуль побудови дерева, модуль обчислення загального секрету в корені дерева.

Моделювання за допомогою всіх трьох програм здійснювалося для 10-20 користувачів (комп'ютери з операційною системою Win10 та частотою процесорів ~2-4 ГГц). Моделювання повністю підтвердило основні результати сформульованої вище моделі. Зокрема, встановлено, що з малого числа користувачів поєднання протоколу Бурместера-Десмедта та еліптичної кривої Монтгомері забезпечує найвищу обчислювальну ефективність, програми з таким поєднанням працюють у режимі реального часу. Промодельовано групи з

незначною динамікою – кількість тих, хто приєднується до групи користувачів або користувачів, які виходять із групи, не перевищувало трьох.

Моделювання показало, що для малодинамічних груп ефективність застосування ефективності протоколу Бурместера-Десмедта та деревоподібного протоколу мало відрізняються. Таким чином, для груп з невеликим числом користувачів та малою динамікою найбільш ефективними є поєднання протоколу Бурместера-Десмедта та еліптичної кривої Монтгомері.

4.2. Розробка методу обміну конфіденційними зображеннями для групи довірених користувачів

В основу пропонованого методу обміну зображеннями для групи довірених користувачів, який забезпечує їх багаторівневий захист (в сенсі конфіденційності та збереження), покладений описаний в попередньому розділі модифікований метод шифрування зображень на підставі хаотичного відображення Тент з управлінням. Даний метод дозволяє генерувати досить довгу псевдовипадкову послідовність високої якості. Далі ця послідовність застосовується для зашифрування чи розшифрування зображення шифром Вернама. Попередньо оброблюване зображення перетворюється на форму вектора. Для зашифрування або розшифрування користувач повинен мати згенеровану алгоритмом Тент псевдовипадкову послідовність великої довжини. Передача такої послідовності відкритими каналами зв'язку викликає певні труднощі.

Тому в модифікованому алгоритмі шифрування Тент передбачено формування короткого ключа, що містить параметри для генерації псевдовипадкової послідовності («насіння») . Короткий сеансовий ключ формує адміністратор, який управляє процесом обміну зображеннями у групі довірених користувачів. Цей короткий ключ передається користувачам, які розгортають

його в псевдовипадкову послідовність необхідної довжини. Шифрування зображення на підставі хаотичного перетворення Тент є першим рівнем захисту.

На другому рівні захисту короткий сеансовий ключ модифікованого алгоритму шифрування Тент шифрується шифром Вернама з ключем, побудованим з використанням послідовності згорнутих чисел k-перетину послідовності Фібоначчі A002026.

На третьому рівні захисту запропоновано підхід до формування групи довірених користувачів та отримання спільного секрету [96-99].

Адміністратор системи формує сеансову групу довірених користувачів, яким дозволено доступ до зображень. Зазначимо, що користувачі можуть як шифрувати зображення та виставляти їх у групу, так і розшифровувати виставлені зображення для аналізу. Оскільки цій групі довірених користувачів короткий ключ модифікованого перетворення Тент передається відкритими каналами зв'язку, цей ключ повинен бути зашифрований блоковим шифром . Отже, у групі користувачів має бути сформований загальний ключ для розшифровки ключа першого рівня. Запропоновано спершу формувати спільний секретний ключ для групи користувачів конфідентів згідно з модифікованим протоколом Діффі-Хеллмана на еліптичних кривих.

Сформовано наступний протокол узгодження загального секрету на еліптичній кривій Монтгомері.

Початкові установки протоколу.

1. Адміністратор формує групу з N користувачів-конфідентів: $U_1, U_2, ..., U_N$, при цьому адміністратор – користувач U_1.

2. Адміністратор вибирає та оголошує загальні параметри еліптичної кривої Монтгомері, кінцеве поле F_p, базову точку-генератор **P** та порядок групи n.

Функціонально-логічна схема протоколу включає наступні операції.

1) Генерація ключів – кожен користувач $U_i, i = \overline{1, N}$ вибирає випадкове ціле число ($x_i (1 < x_i < n-1)$), яке є його закритим ключем.

2) Циклічний ітеративний обмін.

Крок 1: користувач U_1 обчислює точку на $\mathbf{X_1} = x_1 \cdot \mathbf{P}$ та відправляє його користувачу U_2.

Крок 2: користувач U_2 одержує точку на еліптичній кривій $\mathbf{X_1}$, обчислює нову точку $\mathbf{X_2} = x_2 \cdot \mathbf{X_1} = x_2 \cdot (x_1 \cdot \mathbf{P})$ та відправляє його користувачу U_3.

Крок *i*: користувач U_i одержує точку на еліптичній кривій $\mathbf{X_{i-1}}$ від U_{i-1}, обчислює нову точку $\mathbf{X_i} = x_i \cdot \mathbf{X_{i-1}}$ та відправляє її користувачу U_{i+1}. …

Крок *N*: Останній користувач U_N одержує точку на еліптичній кривій $\mathbf{X_{N-1}}$ та обчислює точку $\mathbf{X_N} = x_N \cdot \mathbf{X_{N-1}} = (x_N x_{N-1} \ldots x_1) \cdot \mathbf{P}$.

3) Поширення секрету: Точка (її координати) $\mathbf{X_N}$ розсилається адміністратором усім користувачам.

4) Обчислення загального секрету: Кожен учасник U_i одержує точку $\mathbf{X_N}$, множить її на свій секретний ключ і отримує спільний секрет: $\mathbf{CS} = x_i \cdot \mathbf{X_N}$.

У разі необхідності розширення групи довірених користувачів, тобто додавання нового користувача, необхідно здійснити такі дії.

1. Коли новий користувач U_{new} повинен приєднатися до групи, він генерує свій закритий ключ та відкритий ключ $\mathbf{P_{new}} = k_{new} \cdot \mathbf{P}$.

2. Існуючі користувачі передають свої відкриті ключі новому користувачеві.

3. Новий користувач також передає свій відкритий ключ всім користувачам.

4. Обчислення загального секрету відбувається так:

Кожен користувач обчислює новий спільний секрет, використовуючи свої закриті ключі та відкриті ключі решти учасників.

Для користувача U_i, загальний секрет буде обчислюватися наступним чином:

$$\mathbf{CS_i} = x_i \cdot \mathbf{P_{new}} + \sum_{j \neq i} x_i \cdot \mathbf{P_j} .$$

Вище показано, що протокол Бурместера-Десмедта значно ефективніший за класичний Діффі-Хеллмана за рахунок економного обміну ключами при тій же стійкості.

Тому альтернативним рішенням на другому рівні захисту, яке досліджено, було використання протоколу Бурместера-Десмедта узгодження загального секрету на еліптичній кривій Монтгомері, який передбачає наступну послідовність дій (рис.4.14):

Перший етап:

Кожен учасник U_i обирає випадкове число x_i (закритий ключ) та публікує свою точку на кривій: $\mathbf{W_i} = x_i$.

Другий етап:

Кожен учасник U_i обчислює та публікує проміжне значення $\mathbf{X_i}$, яке використовує відкриті ключі сусідів:

$$\mathbf{X_i} = (x_i \cdot \mathbf{Z_{i+1}}) - (x_i \cdot \mathbf{Z_{i-1}}),$$

де $\mathbf{Z_{i+1}}$ и $\mathbf{Z_{i-1}}$ – публічні точки «сусідів» справа и зліва у логічному кільці користовучів (рис. 4.1).

Обчислювання ключа:

Після обміну значеннями $\mathbf{X_i}$ кожен учасник може обчислити підсумковий загальний секрет **CS**. Після того як всі учасники U_i обмінялись значеннями $\mathbf{X_i}$,

кожен користувач U_i, знаючі свій секрет $\mathbf{X_i}$ та одержані від інших відкриті ключі сусідів обчислює загальний секретний ключ **CS** за наступною формулою:

$$\mathbf{X_i} = (x_i \cdot \mathbf{Z_{i+1}}) - (x_i \cdot \mathbf{Z_{i-1}})$$

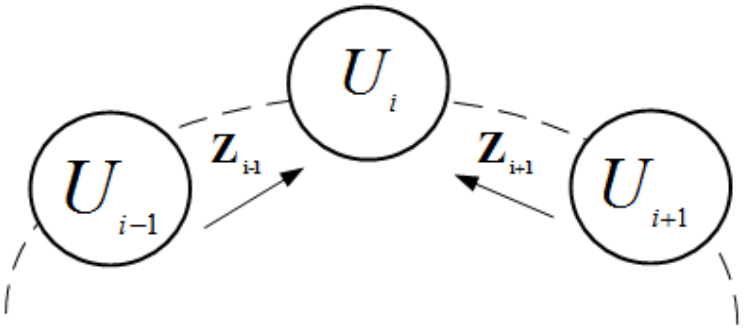


Рисунок 4.14 – Схема протоколу Бурместера-Десмедта.

$$\mathbf{CS} = N \cdot x_i \cdot \mathbf{Z_{i-1}} + (N-1) \cdot \mathbf{X_i} + (N-2) \cdot \mathbf{X_{i+1}} + \ldots + \mathbf{X_{i+n-2}},$$

де N – загальна кількість учасників;

x_i – секретний ключ поточного користувача;

$\mathbf{Z_{i-1}}$ – відкритий ключ сусіда зліва;

$\mathbf{X_i}$ – значення відкриті ключі сусідів, що отримані на другому етапі.

Зазначимо, що всі індекси обчислюються за модулем N.

Основна перевага протоколу Бурместера-Десмедта – масштабованість: протокол виконується всього за два раунди взаємодії, незалежно від кількості учасників.

Ще одним розглянутим варіантом економічного різновиду схеми Діффі-Хеллмана, як вказано вище, є ієрархічна або деревоподібна схема (Tree-based Group Diffie-Hellman). Згідно з цим варіантом, всі учасники об'єднуються в

бінарне дерево, кожен з учасників є «листом» дерева на рівні k. На кожному рівні дерева, загальний парний секрет для вузлів, що становлять пари учасників, може бути обчислений за формулою:

$$\mathbf{X}_i = \mathbf{X}_{2i-1,2i} = (x_{2i-1}x_{2i}) \cdot \mathbf{P}.$$

На наступному (батьківському) рівні обчислюються ключі від пар, утворених парами нижнього (дочірнього) рівня тощо.

Цей процес повторюється рекурсивно вгору по дереву, доки не буде обчислено ключ кореневого вузла. На верхньому (кореневому) рівні, загальний секрет для всіх учасників утворюється так:

$$\mathbf{X}_N = \mathbf{X}_{root} = (x_1x_2...x_N) \cdot \mathbf{P}.$$

Далі все відбувається як у протоколі Діффі-Хеллмана.

Переваги деревоподібної схеми.

Логарифмічна масштабованість.

Помітно менший трафік: якщо у звичайній схемі число пересилань $O(n)$, то в деревоподібній схемі число пересилок $O(\log_2 N)$. Кількість обчислень і повідомлень, що пересилаються, зростає не лінійно, а логарифмічно. Так, наприклад, для групи з 16 чоловік шлях до кореня становить всього 4 кроки, а не 16. Це дозволяє ефективно працювати у великих групах.

Висока динамічність.

Деревоподібна схема ідеально підходить для груп, склад учасників яких змінюється (наприклад, коли для аналізу зображень можуть бути потрібні додаткові фахівці). При вході одного додаткового учасника змінюється не все дерево, лише вузли шляху від учасника до кореня. Інші гілки дерева залишаються недоторканими і використовують свої старі проміжні ключі, що економить обчислювальні ресурси та підвищує оперативність.

На рисунку 4.15 детально показано деревоподібну схему для 8-ми учасників. Червоним кольором показана гілка , що підлягає коригування , якщо восьмий учасник увійшов пізніше інших.

У загальному випадку, деревоподібна схема працює швидше, ніж схема Бурместера-Десмедта , особливо для великих груп учасників, завдяки меншій кількості обмінів та можливості паралельної обробки. Протокол Бурместера-Десмедта може бути повільнішим через лінійну кількість обмінів. Крім того, деревоподібна схема виграє за швидкістю у разі послідовного приєднання до групи нових учасників.

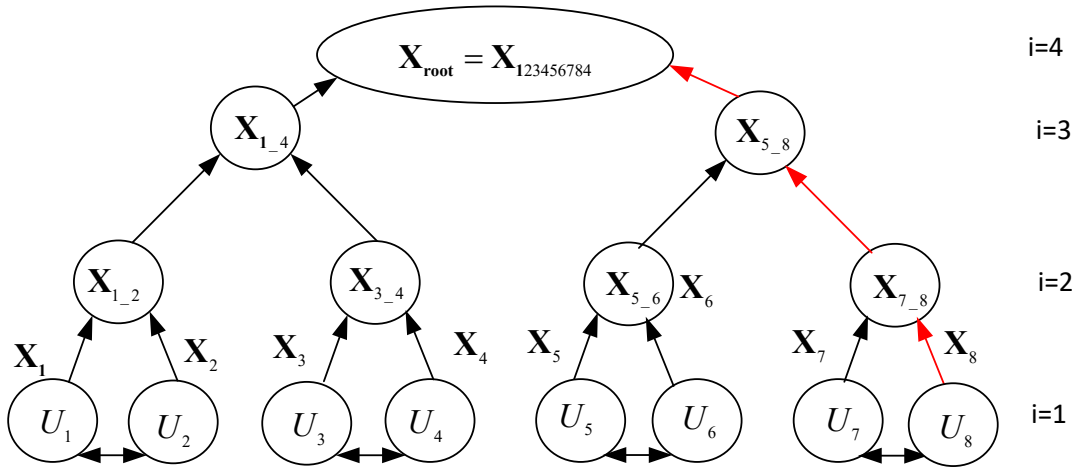


Рисунок 4.15 – Деревоподібна схема для восьми учасників (4 кроки).

Залежно від кількості користувачів у сеансовій групі та від очікуваної кількості можливих додаткових учасників адміністратор приймає рішення про застосування протоколу Бурместера-Десмедта або деревоподібного протоколу.

Четвертим рівнем захисту у запропонованому методі є хешування загального секрету, отриманого в протоколі Діффі-Хеллмана:

$$CS' = Hash(CS_x),$$

де *Hash* – стандартизована хеш-функція (наприклад, SHA-3);

CS_x – x-координата точки $\mathbf{CS}$.

Значення, яке одержано, CS' — є ключом з яким шифрується короткий ключ $KeyI$ відображення Тент (п'ятий рівень захисту):

$$k = CS',$$

$$KeyII = E_k(KeyI).$$

На шостому рівні захисту ключ $KeyII$ роздається всім довіреним користувачам. Вони можуть генерувати сеансову псевдовипадкову послідовність відображення Тент і зашифровувати/розшифровувати конфіденційні зображення цього сеансу. Структурно-логічна схема розробленого методу обміну конфіденційними зображеннями групи довірених користувачів наведено на рисунку 4.16.

На рисунку 4.17 показано ланцюжок ключів (KeyChain) для розробленого методу.

Разом із запрошенням до групи адміністратор Admin виділяє кожному користувачу $U_i, i = \overline{1,N}$ параметри еліптичної кривої Монтгомері та початкову точку ***P***. Далі відповідно до протоколу Бурместера- Десмедта кожен користувач отримує загальний груповий секрет **CS**.

За допомогою цього секрету та псевдовипадкової послідовності Фібоначчі A002026 користувач розшифровує короткий хаотичний ключ Тент послідовності (цей ключ був зашифрований блоковим шифром AES).

В результаті користувач розгортає повний ключ Тент і формує хаотичну послідовність необхідної довжини.

Далі застосовується шифр Вернама, і користувач має можливість зашифровувати та/або розшифровувати зображення, аналізувати та коментувати їх.

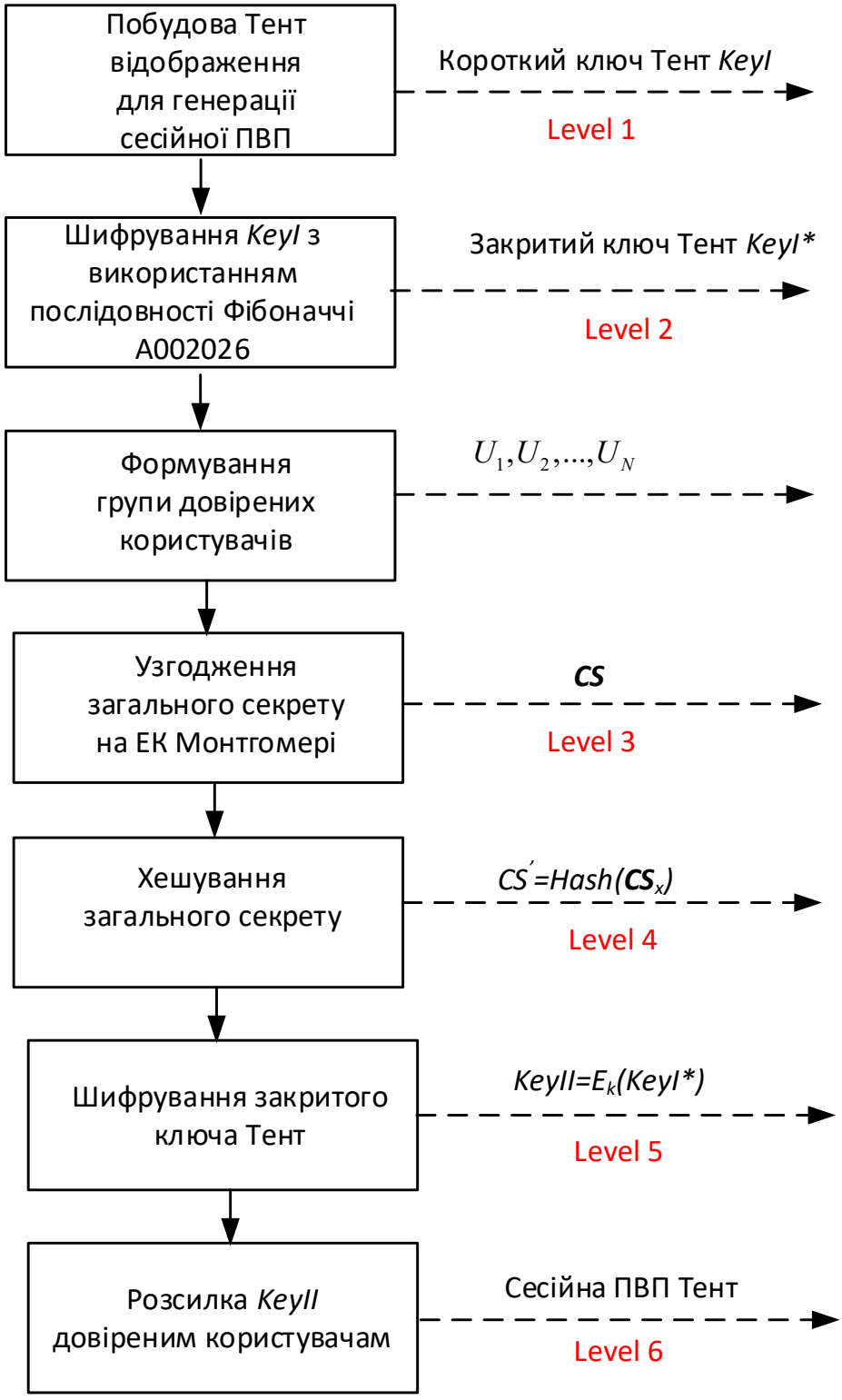


Рисунок 4.16 – Структурно-логічна схема розробленого методу

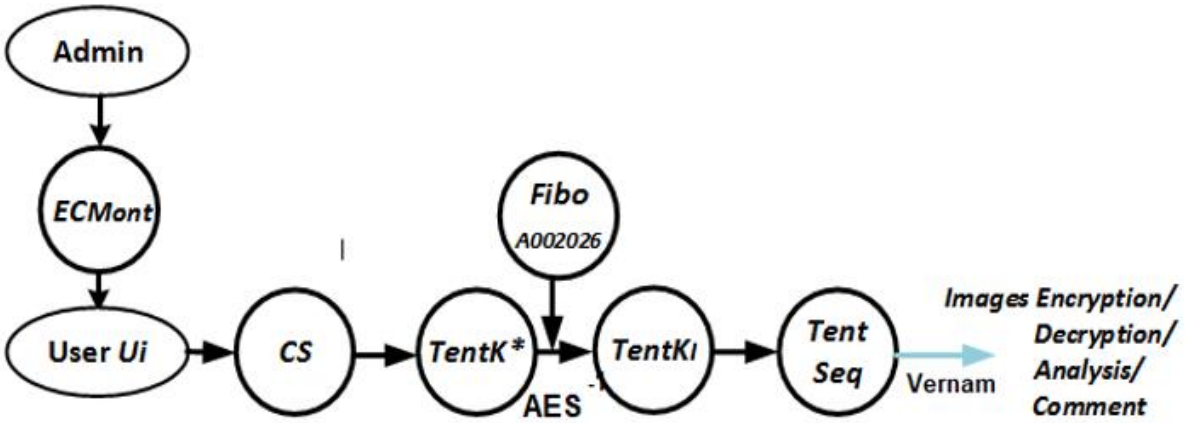


Рисунок 4.17 – Ланцюжок ключів (KeyChain) для розробленого методу.

4.3 Моделювання розробленого методу обміну конфіденційними зображеннями для групи довірених користувачів

Програмне моделювання методу проводилося на платформі Win10(64-бит) с процесором Intel Core i7-9750H з частотою 2.60 GHz и 8 GB RAM.

Сформовано модифіковане відображення Тент із набором коротких ключів:

$KeyI_j = [223,\ 2{,}07081j,\ 0.001,\ 0.9]$, $j = 1,...,6$.

Група учасників-конфідентів обиралась у складі N=5, 10, 20, 30. В якості еліптичної кривої Монтгомері обрана крива Curve25519 [100-102]. Вона була розроблена Деніелом Бернстайном та є однією з найбільш популярних еліптичних кривих для криптографічних застосунків. Крива задається наступним рівнянням:

$$y^2 = x^3 + 486662x^2 + x \,.$$

Графік кривої наведено на рисунку 4.18.

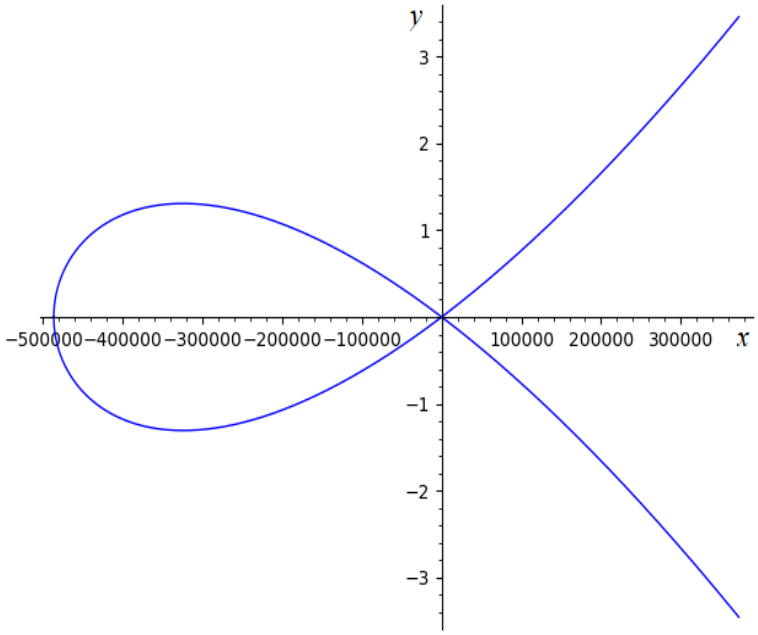


Рисунок 4.18 – Графік кривої Монтгомері Curve25519.

Крива визначена над полем F_p з простим модулем $p = 2^{255} - 19$ (звідси її назва). Крива Curve25519 рекомендована для застосування NIST завдяки низці наступних переваг:

– великий порядок групи, що становить $2^{252} + 27742317777372353535851937790883648493$, що забезпечує високий рівень безпеки.

– швидкі операції. Алгоритми для операцій на Curve25519 оптимізовані для швидкості. Це дозволяє ефективно виконувати операції навіть у пристроях з обмеженими ресурсами.

– мала кількість операцій. Для обчислення точок на кривій потрібно менше операцій, ніж інших кривих, що робить її більше продуктивною.

Генераторна точка G обрана с координатами $G = (9, y_G)$.

Значення $x_G = 9$ було обрано оскільки це значення невелике та просте, що спрощує подальші обчислення.

Для хешування використовувалась функція SHA-3-256 (Keccak).

Для шифрування $KeyII = E_k(KeyI)$ використано стандарт блочного шифру AES-256.

В процесі моделювання були програмно реалізовані як протокол Диффи-Хелмана, так і протокол Бурместера-Десмедта. Реєструвався процесорний час T на виконання всіх операцій згідно зі структурно-логічною схемою розробленого методу (рис. 4.16). Результати моделювання наведено у таблиці 4.1.

Таблиця 4.1. Витрати процесорного часу виконання повної послідовності операцій (згідно до рис. 4.16)

Кількість учасників в групі *N*	Узгодження загального секрету за протоколом Діффі-Хеллмана *T*, с	Узгодження загального секрету згідно з протоколом Бурместера-Десмедта *T*, с
5	2, 18	0.86
10	3.98	1.23
20	7.34	3.44
30	13.43	5.65

Аналіз одержаних результатів (табл. 4.1) демонструє високу оперативність протоколу Бурместера-Десмедта. Крім того, наведені у таблиці 4.1 вказують на масштабування методу із застосуванням цього протоколу: зі зростанням числа

користувачів N економія процесорного часу порівняно із застосуванням протоколу Діффі-Хеллмана помітно зростає. Моделювання розробленого методу підтвердило правильність закладених в основу алгоритмічних рішень та показало можливість роботи запропонованого методу обміну конфіденційними зображеннями групи довірених користувачів в масштабі часу, близькому до реального.

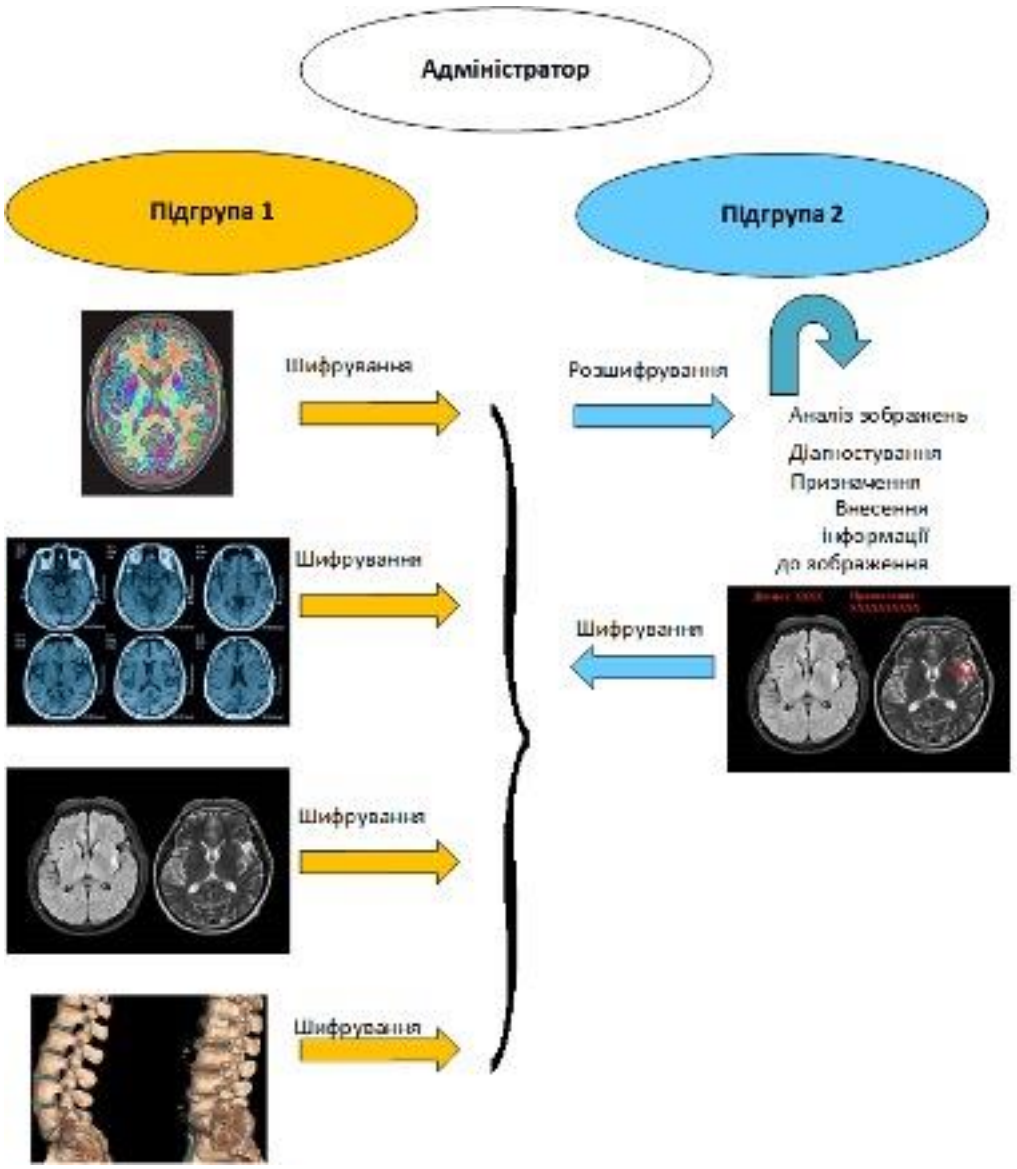
4.4 Функціональна схема прототипу системи обміну конфіденційними зображеннями у групі довірених користувачів для медичного закладу

На основі розробленого методу побудовано прототип системи обміну конфіденційними зображеннями для діагностики в медичному закладі. Функціональна схема прототипу системи представлена рисунку 4.19.

Перед початком сеансу адміністратор формує групу довірених користувачів. Група складається із двох підгруп. До підгрупи 1 входять користувачі, які є власниками зображень. Ними можуть бути як окремі пацієнти, так і лікарі, які репрезентують зображення для діагностики з віддалених відділень медичного закладу. У віддалених відділеннях може бути діагностичне обладнання, що дозволяє отримувати зображення для діагностики. Однак у відділеннях можуть бути відсутні фахівці високої кваліфікації, які можуть проаналізувати зображення, здійснити діагностику та призначити лікування. До підгрупи 2 входять фахівці, які є експертами у діагностиці представлених зображень.

Ініціалізація системи. Адміністратор перед початком сеансу встановлює параметри модифікованого відображення Тент, яке буде застосовуватися для генерації псевдовипадкової послідовності. Крім того, він обирає параметри

послідовності згорнутих чисел *k*-перетину послідовності Фібоначчі, яка буде застосовуватися для генерації сеансового ключа.



Рисунку 4.19 – Функціональна схема прототипу системи.

Формування групи. Відповідно до переліку довірених користувачів адміністратор формує групу. Залежно від кількості користувачів підгрупи 2 та необхідності підключення додаткових користувачів в цю підгрупу,

адміністратор обирає протокол формування групи. Це може бути протокол Бурместера-Десмедта чи деревоподібний протокол.

Після формування групи у кожного користувача є ключ до шифру AES , яким він може послідовно розшифрувати параметри сеансових параметрів модифікованого Тент відображення.

Шифрування. Користувачі підгрупи 1 зашифровують зображення шифром Вернама з псевдовипадковою послідовністю, отриманої за допомогою відображення Тент. Зашифровані зображення користувача підгрупи 1 викладаються в загальне користування групи. Користувачі підгрупи 2 вибирають зображення, що належать до їхньої професійної компетенції. Далі вони розшифровують ці зображення і приступають до їхнього аналізу. В результаті аналізу користувачі підгрупи 2 встановлюють діагнози, формулюють призначення і вносять цю інформацію у відповідне зображення. Вказана текстова інформація також є конфіденційною, тому вона вноситься безпосередньо до файлу зображення на неінформативні ділянки. Для цього застосовується наприклад утиліта. Далі користувачі підгрупи 2 зашифровують проаналізовані зображення шифром Вернама з псевдовипадковою сеансовою послідовністю. Користувачі підгрупи 1 можуть розшифрувати проаналізовані зображення та ознайомитись з результатами їх аналізу.

Для здійснення перерахованих функцій сформовано програмне забезпечення, яке включає такі програмні компоненти:

– формування псевдовипадкової послідовності із заданими початковими параметрами виходячи з модифікованого відображення Тент;

– формування випадкових послідовностей з послідовності згорнутих чисел *k*-перетину послідовності Фібоначчі A002026;

– прямого та зворотного перетворення файлів зображення у векторну форму;

– шифрування шифром Вернама;

– формування групи довірених користувачі на підставі протоколів на еліптичній кривій Монтгомері.

Прототип системи випробувано за участю одного з медичних закладів. У процесі лабораторних випробувань перевірено вище зазначені протоколи формування групи. Випробування проведені для груп з числом учасників до 12 і кількістю зображень до 32. Встановлено, що часові затримки здійснення операцій із забезпечення конфіденційності і цілісності зображення не перевищують 0,5 секунди, тобто система працює майже в реальному масштабі часу. Випробування в цілому підтвердили правильність прийнятих розробки методу алгоритмічних і програмних рішень. Прийнято рішення про застосування розробленої системи в одному з медичних закладів.

4.5 Висновки до четвертого розділу

Запропоновано методику дослідження ефективності протоколів групового узгодження ключів. Показано, що при формуванні груп довірених користувачів груп з невеликим числом користувачів та малою динамікою найбільш ефективним є поєднання протоколу Бурместера-Десмедта та еліптичної кривої Монтгомері.

Розроблено метод обміну конфіденційними зображеннями групи довірених користувачів. Конфіденційність зображень забезпечується шифруванням із застосуванням псевдовипадкових послідовностей на основі модифікованого хаотичного відображення Тент.

Розроблено протокол формування групи довірених користувачів, яким дозволено доступ до зображень. Збереження зображень забезпечується шістьма

рівнями захисту. Протокол ґрунтується на застосуванні операцій на еліптичних кривих Монтґомері.

Проведено імітаційне моделювання розробленого методу. Моделювання продемонструвало працездатність методу в масштабі часу, близькому до реального, та масштабування на основі швидкодіючого протоколу Бурместера-Десмедта.

Випробування в цілому підтвердили правильність прийнятих розробки методу алгоритмічних і програмних рішень. Прийнято рішення про застосування розробленої системи в медичних закладах.

Сформульовано пункт наукової новизни: розроблено метод обміну зображеннями групи довірених користувачів, який відрізняється багаторівневим захистом з застосуванням захисного перетворення на основі модифікованого хаотичного відображення Тент та швидкодіючого протоколу на основі еліптичних кривих Монтґомері, що дозволило підвищило швидкодію шифрування та дешифрування при збереженні стійкості.

Загалом, результати апробації свідчать про практичну придатність запропонованих методів до впровадження в системи реального часу. Висновки, отримані на основі експериментальних вимірювань та порівнянь із базовими підходами, підтверджують доцільність їх використання в інформаційних системах.

ВИСНОВКИ

Дисертаційне дослідження містить нові наукові результати, які є результатом вирішення актуального наукового завдання, яке полягає підвищенні конфіденційності та цілісності обміну зображеннями для групи довірених користувачів шляхом удосконалення моделей та методів перетворення зображень на основі хаотичних відображень шляхом підвищення їх швидкодії та/або зменшення ресурсозалежності.

При проведенні дослідження отримано наступні наукові та практичні результати.

1. Визначено, що розробка моделей та методів підвищення конфіденційності та цілісності обміну зображеннями високої роздільної здатності для групи довірених користувачів є актуальною в області комп'ютерних наук. Показано протиріччя, яке полягає в тому, що з одного боку, методи захисних перетворень зображень, що ґрунтуються на хаотичних відображеннях є затребуваними; з іншого боку, існують обмеження використання, що пов’язані з показниками швидкодії та ресурсозалежності самих хаотичних відображень. Запропоновані шляхи, що направлені на усунення цього протиріччя, та присвячені вирішенню важливої науково-практичної задачі підвищенні конфіденційності та цілісності обміну зображеннями для групи довірених користувачів.

2. Удосконалено інтегральний критерій якості захисних перетворень, який поєднує різні метрики якості шифрування (кореляційні, ентропійні та метрики резистентності), що побудований методом ідеальної точки, що дозволило проводити комплексне оцінювання якості шифрування та проводити обґрунтований вибір потокових та блочних шифрів.

3. Запропоновано застосовувати дискретну динамічну систему, а саме узагальнене відображення Тент з керуванням, яке стабілізує цикли заданої довжини. Система може бути використана для шифрування даних, наприклад,

зображень та захисту інформації від несанкціонованого доступу. Перевагою наведеного рішення є коротка довжина ключа та незалежність алгоритму від застосовуваної апаратно-програмної платформи.

На основі запропонованої дискретної динамічної системи розроблено метод захисного перетворення зображень на основі хаотичного відображення Тент з управлінням, що дозволило на підставі короткого ключа (насіння) згенерувати довгу псевдовипадкову послідовність, що значно підвищило швидкодію шифрування та дешифрування при збереженні стійкості шифрування за інтегральним критерієм якості.

4. Отримала подальшого розвитку модель побудови псевдовипадкових послідовностей, яка заснована на зв'язку між похідними багаточленів Чебишева другого роду та поліномами Чебишева, а також на зв'язку згорнутих чисел k-перетину послідовності Фібоначчі з похідними поліномів Чебишева другого роду через числа Люка, що дало можливість отримати сімейство узагальнених послідовностей Фібоначчі, які можуть бути використані для підвищення рівня забезпечення цілісності інформації при її обміні у групі довірених користувачів.

Отримано сімейство узагальнених послідовностей зі зростанням вищого порядку і складнішими коефіцієнтами зв'язку ніж у відомих послідовностей Фібоначчі. Це робить отримані узагальнені послідовності ідеальними для стиснення розріджених даних, вирішення низки завдань у сфері перетворення інформації. Доведено, що отримані послідовності є оригінальними і можуть бути представлені в енциклопедії OEIS, що підтверджує потенціал запропонованого підходу до формування різних послідовностей, які можуть бути використані для підвищення надійності інформаційних систем. В енциклопедії OEIS їм присвоєно номер.

5. Розроблено метод обміну зображеннями групи довірених користувачів, особливостями якого є наступне:

– конфіденційність зображень забезпечується застосуванням шифрування із застосуванням псевдовипадкових послідовностей на основі модифікованого хаотичного відображення Тент;

– збереження зображень забезпечується шістьма рівнями захисту;

– швидкодіючий протокол на основі операцій на еліптичних кривих Монтґомері, що дозволило підвищити швидкодію шифрування та дешифрування при збереженні стійкості.

Моделювання продемонструвало працездатність методу в масштабі часу, близькому до реального.

6. Розроблено та апробовано відповідні алгоритми на основі запропонованих моделей і методів. Розроблені в роботі методи отримали впровадження у діяльності державного підприємства «Український науково-дослідний інститут медицини транспорту Міністерства охорони здоров'я України» (акт ДПУКРНДІ МТ МОЗ України від 02 березня 2026 р.), у діяльності Військово-медичного клінічного центру Південного регіону (довідка від 05 березня 2026 р.) та знайшли відображення у навчальному та науково-дослідницькому процесі Національного університету «Одеська політехніка». Це довело ефективність запропонованих рішень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Hoppe F., et al. Imaging with Confidence: Uncertainty Quantification for High-Dimensional Undersampled MR Images // *Computer Vision – ECCV 2024* / eds. A. Leonardis, E. Ricci, S. Roth et al. – Cham : Springer, 2025. – (Lecture Notes in Computer Science ; Vol. 15136). – DOI: 10.1007/978-3-031-73229-4_25H.

2. Al-Ghaili M., et al. A Review on Role of Image Processing Techniques to Enhancing Security of IoT Applications // *IEEE Access*. – 2023. – Vol. 11. – P. 101924–101948. – DOI: 10.1109/ACCESS.2023.3312682.

3. Li T., Wang Z., Kyba C. C. M. et al. Satellite Imagery Reveals Increasing Volatility in Human Night-Time Activity // *Nature*. – 2026. – Vol. 652. – P. 379–386. – DOI: 10.1038/s41586-026-10260-w.

4. Kozhevnikov O. A. Forensic Intelligence Based on Photo Image Analysis // *Bulletin of Kharkiv National University of Internal Affairs*. – 2025. – Vol. 111, № 4. – P. 353–366. – DOI: 10.32631/v.2025.4.28.

5. Holt A. Chaotic Maps // *Network Performance Analysis*. – London : Springer, 2008. – P. 125–146. – DOI: 10.1007/978-1-84628-823-4_7.

6. Dachselt F., Schwarz W. Chaos and Cryptography // *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*. – 2001. – Vol. 48. – P. 1498–1509.

7. Yang M., Bourbakis N., Li S. Data, Image, Video Encryption // *IEEE Potentials*. – 2004.

8. Diab O., Sobky T., Serag Eldin W., Mahmoud A., Zaky H., Hogo M. Fast Simple Image Encryption Technique Based on Chaos Based System // *2023 International Telecommunications Conference (ITC-Egypt)*. – 2023. – DOI: 10.1109/ITC-Egypt58155.2023.

9. Dinu A., Frunzete M. Image Encryption Using Chaotic Maps: Development, Application, and Analysis // *Mathematics*. – 2025. – Vol. 13, № 16. – P. 2588. – DOI: 10.3390/math13162588.

10. Lin C.-F., Lin Y.-X., Chang S.-H. Medical Image Encryption Using Chaotic Mechanisms: A Study // *Bioengineering*. – 2025. – Vol. 12, № 7. – P. 734. – DOI: 10.3390/bioengineering12070734.

11. Amutha R., Phamila A. V. Chaotic Cosine and Logistic Map Based Robust Image Encryption with Dual-Stage Confusion–Diffusion Architecture // *Scientific Reports*. – 2026. – DOI: 10.1038/s41598-026-40337-5.

12. Moghimi Moghaddam S. S., Rashtchi V., Azarpeyvand A. Parallel Chaos-Based Image Encryption Algorithm: High-Level Synthesis and FPGA Implementation // *The Journal of Supercomputing*. – 2024. – Vol. 80. – P. 10985–11013. – DOI: 10.1007/s11227-023-05784-1.

13. Ramalingam B., Ravichandran D., Annadurai A. A. et al. Chaos Triggered Image Encryption – A Reconfigurable Security Solution // *Multimedia Tools and Applications*. – 2018. – Vol. 77. – P. 11669–11692. – DOI: 10.1007/s11042-017-4811-x.

14. Biswas H. R. Investigation of Chaotic Features of the Family of Generalized Tent Maps // *Journal of Applied Mathematics and Computation*. – 2024. – Vol. 8, № 2. – P. 93–99. – DOI: 10.26855/jamc.2024.06.001.

15. Irfan M., Asif Khan M. Cryptographically Secure Pseudo-Random Number Generation Using a Robust Chaotic Tent Map: A Novel Approach // *Cogent Engineering*. – 2025. – Vol. 12, № 1. – DOI: 10.1080/23311916.2025.255875.

16. G. Vernam, “Cipher printing telegraph systems for secret wire and radio telegraphic communications,” J. American Inst. Elec. Eng., vol. 45, no. 2, pp. 295-301, Feb. 1926.

17. Shannon CE. Collected Papers / Edited by NJA Sloane and Aaron D. Wyner. - IEEE press, 1993. - 923 c .

18. Ho, S.-W., Chan, T., Grant, A., & Uduwerelle , C. (2017). Error-Free Perfect Secrecy Systems. B RF Schaefer, H. Boche, A. Khisti, & HV Poor (Eds.), *Information Theoretic Security and Privacy of Information Systems* (pp. 21-50). chapter, Cambridge: Cambridge University Press.

19. Etem , Taha; Kaya, Turgay . (2019). A novel True Random Bit Generator design for image encryption. Physica A: Statistical Mechanics and its Applications, (), 122750-. doi:10.1016/j.physa.2019.122750

20. Koshy, T. “Fibonacci and Lucas Numbers with Applications”. John Wiley & Sons.2019.

21. Hoggatt, V. E. & Lind, D. A. “Compositions and Fibonacci Numbers”. The Fibonacci Quarterly. 1969; 7 (3): 253–266. DOI: https://doi.org/10.1080/00150517.1969.12431151.

22. Hoggatt, V. E. & Bicknell-Johnson, M. “Fibonacci convolution sequences”. Fibonacci Quarterly. 1977: 15: 117–122. DOI: https://doi.org/10.1080/00150517.1977.12430465.

23. Sloane N. J. A. (Ed.). *The On-Line Encyclopedia of Integer Sequences* [Електронний ресурс]. – Режим доступу: OEIS (дата звернення: 13.05.2026).

24. Coufal P., Trojovský P. Repdigits as Product of Terms of *k*-Bonacci Sequences // *Mathematics*. – 2021. – Vol. 9, № 6. – P. 682. – DOI: 10.3390/math9060682.

25. Stockmeyer P. K. An Exploration of Sequence A000975 // *The Fibonacci Quarterly*. – 2017. – Vol. 55, № 5. – P. 174–185. – DOI: 10.1080/00150517.2017.12427747.

26.Кіх М. В., Нємкова О. А. Покращення статистичних характеристик псевдовипадкових бітових послідовностей модифікованого адитивного генератора Фібоначчі // *Сучасний захист інформації*. – 2024. – № 2(58). – С. 69–76. – DOI: 10.31673/2409-7292.2024.020008.

27. Beletsky A. Y. Synthesis of Cryptoresistant Generators of Pseudorandom Numbers Based on Generalized Galois and Fibonacci Matrixes // *Radio Electronics, Computer Science, Control*. – 2019. – № 3. – P. 86–98.

28. Нємкова О., Кіх М. Порівняльне дослідження тестів для оцінки послідовностей // Кібербезпека: освіта, наука, техніка. — 2024. — № 4(24). — С. 115–132. — DOI: https://doi.org/10.28925/2663-4023.2024.24.115132.

29. Rukhin A., Soto J., Nechvatal J., Smid M., Barker E. та ін. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. — Gaithersburg : National Institute of Standards and Technology, 2010. — 131 p.

30. Marsaglia G. DIEHARD: A Battery of Tests of Randomness. — Florida State University, 1996.

31. Brown R. G. Dieharder. — Duke University Physics Department, 2006

32. Alghamdi Y., Munir A. Image Encryption Algorithms: A Survey of Design and Evaluation Metrics // Journal of Cybersecurity and Privacy. — 2024. — Vol. 4, № 1. — P. 126–152. — DOI: https://doi.org/10.3390/jcp4010007.

33. Yogi B., Khan A. K. Advancements in Image Encryption: Comprehensive Review of Design Principles and Performance Metrics // Computer Science Review. — 2025. — Vol. 57. — Article 100759.

34. Gupta P. A New Medical Image Encryption Algorithm Based on the 1D Logistic Map Associated with Pseudo-random Numbers // Multimedia Tools and Applications. — 2021. — Vol. 80. — P. 18941–18967. — DOI: https://doi.org/10.1007/s11042-020-10325-6.

35. Wen H., Yang L., Bai C. та ін. Exploiting High-quality Reconstruction Image Encryption Strategy by Optimized Orthogonal Compressive Sensing // Scientific Reports. — 2024. — Vol. 14. — Article 8805. — DOI: https://doi.org/10.1038/s41598-024-59277-z.

36. Diffie W., Hellman M. E. New Directions in Cryptography // IEEE Transactions on Information Theory. — 1976. — Vol. 22, № 6. — P. 644–654.

37. Steiner M., Tsudik G., Waidner M. Key Agreement in Dynamic Peer Groups // IEEE Transactions on Parallel and Distributed Systems. — 2000. — Vol. 11, № 8. — P. 769–780.

38. Burmester M., Desmedt Y. A Secure and Efficient Conference Key Distribution System // Advances in Cryptology — EUROCRYPT'94. — Berlin : Springer, 1995. — P. 275–286.

39. Xiong H., Wu Y., Lu Z. A Survey of Group Key Agreement Protocols with Constant Rounds // ACM Computing Surveys. — 2019. — Vol. 52, № 3. — Article 57. — 32 p. — DOI: https://doi.org/10.1145/3318460.

40. Jaiswal P., Kumar A., Tripathi S. Design of Secure Group Key Agreement Protocol Using Elliptic Curve Cryptography // 2014 International Conference on High Performance Computing and Applications (ICHPCA). — Bhubaneswar, India, 2014. — P. 1–6. — DOI: https://doi.org/10.1109/ICHPCA.2014.7045305.

41. Washington L. C. Elliptic Curves: Number Theory and Cryptography. — 2nd ed. — Boca Raton : CRC Press, 2008. — 514 p.

42. Dzurenda P., Ricci S., Hajny J., Malina L. Performance Analysis and Comparison of Different Elliptic Curves on Smart Cards // 2017 15th Annual Conference on Privacy, Security and Trust (PST). — Calgary, Canada, 2017. — P. 36501–36509. — DOI: https://doi.org/10.1109/PST.2017.00050.

43. Sukumar N. K., Ranganathan S. G. A Survey of Security Approaches Based on Elliptic Curve Cryptography // SSRN Electronic Journal. — 2024. — 15 p. — URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4817620 (дата звернення: 04.05.2026).

44. Miao Z. Elliptic Curve Cryptography: Theory, Security, and Applications in Modern Network Security // Theoretical and Natural Science. — 2024. — Vol. 1. — P. 1–12. — URL: https://www.researchgate.net/publication/385535061 (дата звернення: 04.05.2026).

45. Okeya K., Kurumatani H., Sakurai K. Elliptic Curves with the Montgomery-Form and Their Cryptographic Applications // International Conference on Theory and Practice of Public Key Cryptography. — 2000.

46. Priyanka, Singh A. K. A Survey of Image Encryption for Healthcare Applications // Evolutionary Intelligence. — 2023. — Vol. 16. — P. 801–818. — DOI: https://doi.org/10.1007/s12065-021-00683-x.

47. Salameh J. N. B. A New Approach for Securing Medical Images and Patient's Information by Using a Hybrid System // International Journal of Computer Science and Network Security. — 2019. — Vol. 19, № 4. — P. 28.

48. Priyanka, Singh, A.K. A survey of image encryption for healthcare applications. *Evol. Intel.* **16**, 801–818 (2023). https://doi.org/10.1007/s12065-021-00683-x

---

49. J. N. B. Salameh . A New Approach for Securing Medical Images and Patient's Information by Using A hybrid System. International Journal of Computer Science and Network Security (IJCSNS).Volume 19, No. 4, pp. 28-39, 2019.

50. M Magdy, M., Hosny, K.M., Ghali, N.I. *et al.* Security of medical images for telemedicine: a systematic review. *Multimed Tools Appl* **81**, 25101–25145 (2022). https://doi.org/10.1007/s11042-022-11956-7

51. Ulutas G, Ustubioglu A, Ustubioglu B, V Nabiyev V, Ulutas M. Medical Image Tamper Detection Based on Passive Image Authentication. J Digit Imaging. 2017 Dec;30(6):695-709. doi: 10.1007/s10278-017-9961-x. PMID: 28484919; PMCID: PMC5681465.

52. "Digital Imaging and Communications in Medicine (DICOM)" // National Electrical Manufacturers Association. Rosslyn, 2008.

53. Pianykh O.S. "Digital Imaging and Communications in Medicine (DICOM). A Practical Introduction a

54. Balasamy, K., Krishnaraj, N. & Vijayalakshmi, K. Improving the security of medical image through neuro-fuzzy based ROI selection for reliable transmission. *Multimed Tools Appl* **81**, 14321–14337 (2022). //https://doi.org/10.1007/s11042-022-12367-4

55. Search for invariant sets of the generalized tent map / K. Ayers et al. Journal of Difference Equations and Applications. 2023. Vol. 29, no. 9-12. P. 1156–1183. DOI: https://doi.org/10.1080/10236198.2024.2307521.

56. Elaydi S. N. Discrete Chaos: With Applications in Science and Engineering. 2nd ed. Boca Raton : Chapman & Hall/CRC, 2007. 440 pDmitrishin D., Stokolos A., and Iacob J., Average predictive control for nonlinear discrete dynamical systems, Adv. Syst. Sci. Appl. 20(1) (2020), pp. 27 – 49.

57. Dmitrishin D., Stokolos A., Iacob J. Average predictive control for nonlinear discrete dynamical systems. Advances in Systems Science and Applications. 2020. Vol. 20, no. 1. P. 27–49. DOI: https://doi.org/10.25728/assa.2020.20.1.848.

58. Bhattacharjee, S., Gupta, M. & Chatterjee, B. “Time efficient image encryption-decryption for visible and COVID-19 X-ray images using modified chaos-based logistic map”. Appl Biochem Biotechnol. 2023; 195: 2395–2413. DOI: https://doi.org/10.1007/s12010-022-04161-7.

59. Ghouate, N. E., Tahiri, M. A. & Bencherqui, A., et al. “A high-entropy image encryption scheme using optimized chaotic maps with Josephus permutation strategy”. Sci Rep. 2025; 15: 29439. DOI: https://doi.org/10.1038/s41598-025-14784-5.

60. Zou, C., Shang, Y., Yang, Y., Zhou, C. & Liu, Y. “A novel image encryption algorithm with anti-tampering attack capability.” Chaos, Solitons & Fractals. 2024;189 (Part 1): 115638. DOI: https://doi.org/10.1016/j.chaos.2024.115638.

61. Kuznetsov, O., Lutsenko, M. & Ivanenko, D. “Strumok stream cipher: Specification and basic properties”. 2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T). Kharkiv, Ukraine. 2016. p. 59–62. DOI: https://doi.org/10.1109/INFOCOMMST.2016.7905335.

62. AL-Wattar, A. H. “A new approach for the image encryption using AES cipher in ECB mode”. Turkish Journal of Computer and Mathematics Education (TURCOMAT). 2020; 14 (2): 1061–1074. DOI: https://doi.org/10.61841/turcomat.v14i03.14117.

63. “Recursive Sequences”. – Available from: https://www.tanyakhovanova.com/ RecursiveSequences/RecursiveSequences.html. – [Accessed: Jan, 2025].

64. Rivlin, T. J. “Chebyshev polynomials: from approximation theory to algebra and number theory”. *A Wiley International Publ*. 1990.

65. Dmytryshyn, D., Gray, D. & Stokolos, A. **“**Reciprocal polynomials with zeros on the unit circle and derivatives of Chebyshev polynomials of the second kind”. *Arxiv*. 2026. DOI: https://doi.org/10.48550/arXiv.2602.19132.

66. Maurer, U.M., Wolf, S. The Diffie–Hellman Protocol. *Designs, Codes and Cryptography* **19**, 147–171 (2000). https://doi.org/10.1023/A:1008302122286

67. E. Dritsas, M. Trigka and P. Mylonas, "Performance and Security Analysis of the Diffie-Hellman Key Exchange Protocol," *2024 19th International Workshop on Semantic and Social Media Adaptation & Personalization (SMAP)*, Athens, Greece, 2024, pp. 166-171, doi: 10.1109/SMAP63474.2024.00039.

68. Nan Li, "Research on Diffie-Hellman key exchange protocol," *2010 2nd International Conference on Computer Engineering and Technology*, Chengdu, China, 2010, pp. V4-634-V4-637, doi: 10.1109/ICCET.2010.5485276

69. Järpe, E. (2020). An Alternative Diffie-Hellman Protocol. *Cryptography*, *4*(1), 5. https://doi.org/10.3390/cryptography4010005

70. Kar, J. (2017). A Study on Diffie-Hellman Key Exchange Protocols. International Journal of Pure and Apllied Mathematics. https://doi.org/10.12732/IJPAM.V114I2.2

71. Just, M., Vaudenay, S. (1996). Authenticated multi-party key agreement. In: Kim, K., Matsumoto, T. (eds) Advances in Cryptology — ASIACRYPT '96. ASIACRYPT 1996. Lecture Notes in Computer Science, vol 1163. Springer, Berlin, Heidelberg. https://doi.org/10.1007/BFb0034833

72. Burmester, M. (2011). Group Key Agreement. In: van Tilborg, H.C.A., Jajodia, S. (eds) Encyclopedia of Cryptography and Security. Springer, Boston, MA. https://doi.org/10.1007/978-1-4419-5906-5_320 73. Sun, D.-Z., & Tian, Y. (2022).

Member Tampering Attack on Burmester-Desmedt Group Key Exchange Protocol and Its Countermeasure. *Mathematics*, *10*(19), 3685. https://doi.org/10.3390/math10193685

74. Mike Burmester, Yvo Desmedt, A secure and scalable Group Key Exchange system, Information Processing Letters, Volume 94, Issue 3,2005, Pages 137-143.

75. Deng J, Li C, Xu C (2013), Scalable group key exchange protocol with provable security. *COM/PEL*, Vol. 32 No. 2 pp. 612–619, doi: https://doi.org/10.1108/03321641311296990

76. Burmester, M. (2025). Group Key Agreement. P. 1038-1045. In: Jajodia, S., Samarati, P., Yung, M. (eds) Encyclopedia of Cryptography, Security and Privacy. Springer, Cham. https://doi.org/10.1007/978-3-030-71522-9_320

77. Yongdae Kim, Adrian Perrig, Gene Tsudik Tree-based group key agreement . ACM Transactions on Information and System Security (TISSEC), Volume 7, Issue 1 Pages 60 – 96 https://doi.org/10.1145/984334.9843

78. Lee, S., Kim, Y., Kim, K., Ryu, DH. (2003). An Efficient Tree-Based Group Key Agreement Using Bilinear Map. In: Zhou, J., Yung, M., Han, Y. (eds) Applied Cryptography and Network Security. ACNS 2003. Lecture Notes in Computer Science, vol 2846. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-45203-4_28

79. Tripathi, S. (2009). Design of efficient ternary-tree based group key agreement protocol for dynamic groups. https://doi.org/10.1109/COMSNETS.2009.4808834

80. Vijayakumar, P., Naresh, R., Jegatha Deborah, L., and Hafizul Islam, S. (2016) An efficient group key agreement protocol for secure P2P communication. *Security Comm. Networks*, 9: 3952–3965. doi: 10.1002/sec.1578.

81. Abhishek, Kunal, and E. George Dharma Prakash Raj. "Computation of Trusted Short Weierstrass Elliptic Curves for Cryptography." *Cybernetics and Information Technologies*, vol. 21, no. 2, Bulgarian Academy of Sciences, Institute of Information and Communication Technologies, 2021, pp. 70-88. https://doi.org/10.2478/cait-2021-0020.

82. Comalada, S. (1994), On the Weierstrass Class of Semistable Elliptic Curves Over Quadratic Fields. Bulletin of the London Mathematical Society, 26: 137-139. https://doi.org/10.1112/blms/26.2.137

83. J. Chris Eilbeck, Matthew England, Yoshihiro Ônishi; Some new addition formulae for Weierstrass elliptic functions. *Proc. A* 1 November 2014; 470 (2171): 20140051. https://doi.org/10.1098/rspa.2014.0051

84. Farashahi, R. R., Fadavi, M., & Sabbaghian, S. (2024). Faster Complete Addition Laws for Montgomery Curves. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2024(4), 737-762. https://doi.org/10.46586/tches.v2024.i4.737-762

85. Okeya, K., Kurumatani, H., Sakurai, K. (2000). Elliptic Curves with the Montgomery-Form and Their Cryptographic Applications. In: Imai, H., Zheng, Y. (eds) Public Key Cryptography. PKC 2000. Lecture Notes in Computer Science, vol 1751. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-46588-1_17

86. Lange, T. (2025). Edwards Curves. In: Jajodia, S., Samarati, P., Yung, M. (eds) Encyclopedia of Cryptography, Security and Privacy. Springer, Cham. https://doi.org/10.1007/978-3-030-71522-9_243

87. D. J. Bernstein and T. Lange, Faster addition and doubling on elliptic curves, Advances in Cryptology – ASIACRYPT 2007 (Vol. 4833, pp. 29-50), Springer, Berlin/Heidelberg, 2007. https://doi.org/10.1007/978-3-540-76900-2_3

88. Performance analysis of Edwards elliptic curves using vedic mathematics for secure authentication protocols in ECC. (2025). *Pi International Journal of Mathematical Sciences*, *1*(2), 44-55. https://doi.org/10.59828/pijms.v1i2.9

89. Abramov, Serhii and Sokolov, Volodymyr and Abramov, Vadym (2024) Research of the graphic model of the points of the elliptic curve in the Edward form Cybersecurity Providing in Information and Telecommunication Systems II 2024, 3826. pp. 174-181. ISSN 1613-0073

90. Hanwa, A., & Fouotsa, E. (2022). Elliptic divisibility sequences over the Edwards model of elliptic curves. Journal of Discrete Mathematical Sciences and Cryptography, 25(8), 2289–2304. https://doi.org/10.1080/09720529.2020.1822042

91. Joye, M., Yen, SM. (2003). The Montgomery Powering Ladder. In: Kaliski, B.S., Koç, ç.K., Paar, C. (eds) Cryptographic Hardware and Embedded Systems - CHES 2002. CHES 2002. Lecture Notes in Computer Science, vol 2523. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-36400-5_22

92. Haihua Gu , Wenlu Xie , and R.C.C. Cheung. Analysis the Montgomery Ladder Algorithm for Elliptic Curves over Ternary Fields. Proceedings of the 2013 International Conference on Information and Network Security (ICINS 2013) . 2014

93. Giacomo Pope, Krijn Reijnders, Damien Robert, Alessandro Sferlazza, and Benjamin Smith, Simpler and Faster Pairings from the Montgomery Ladder. *IACR Communications in Cryptology*, vol. 2, no. 2, Jul 07, 2025, doi: 10.62056/ah2i893y6

94. Mohammad Al-Khatib, Wafaa Saif. Improved Software Implementation for Montgomery Elliptic Curve Cryptosystem. Computers, Materials & Continua 2022, 70(3), 4847-4865. https://doi.org/10.32604/cmc.2022.021483

94. Chuang, Y.-H. and Tseng, Y.-M. (2010), An efficient dynamic group key agreement protocol for imbalanced wireless networks. Int. J. Network Mgmt., 20: 167-180. https://doi.org/10.1002/nem.7395

95. Shih-Pang Tseng, Yang Yu,and Chien-Min Chen. Improving the Scalability of Data Center Networking with Protocol-independent Source Routing. Sensors and Materials, Vol. 36, No. 6 (2024) 2585–2596

96. Noack and J. Schwenk, "Group key agreement performance in wireless mesh networks," *IEEE Local Computer Network Conference*, Denver, CO, USA, 2010, pp. 176-179, doi: 10.1109/LCN.2010.5735694.

97. Zhang Q, Zhu L, Li Y, et al. A group key agreement protocol for intelligent internet of things system. Int J Intell Syst. 2022;37:699-722. https://doi.org/10.1002/int.22644

98. Bresson E and Catalano D Bao F, Deng R, and Zhou J Constant round authenticated group key agreement via distributed computation *Public Key Cryptography – PKC 2004* 2004 Heidelberg Springer 115-129

99. Bünz, B., Bootle, J., Boneh, D., Poelstra, A., Wuille, P., Maxwell, G.: Bulletproofs: short proofs for confidential transactions and more. In: 2018 IEEE Symposium on Security and Privacy (SP), pp. 315–334 (2018).

100. Intan Muchtadi-Alamsyah & Yanuar Bhakti Wira Tama, 2020. "Implementation of Elliptic Curve25519 in Cryptography," Chapters, in: Kehdinga George Fomunyam (ed.), Theorizing STEM Education in the 21st Century, IntechOpen. DOI: 10.5772/intechopen.88614

101. Yanuar Bhakti Wira Tama, Adam Adam, Aditya Putra Pratama; Algorithm design of curve25519 in Elliptic curve digital signature. AIP Conf. Proc. 15 July 2025; 3301 (1): 040005.

102. Yu-Fang Chen, Chang-Hong Hsu, Hsin-Hung Lin, Peter Schwabe, Ming-Hsien Tsai, Bow-Yaw Wang, Bo-Yin Yang, Shang-Yi Yang. Verifying Curve25519 Software. CCS '14: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. Pages 299 – 300. doi.org/10.1145/2660267.2660370.

ДОДАТОК А

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Праці, які відображають основні наукові результати дисертації

1. Дмитришин Д. В., *Хамитов В. М.*, Болтьонков В. О., Антощук С. Г. Використання нелінійних дискретних відображень для побудови псевдохаотичних криптосистем. *Інформатика. Культура. Техніка*. 2025. Т.2. С. 209-214. https://doi.org/10.15276/ict.02.2025.31. *Видання включено до переліку наукових фахових видань України (категорія Б).*
https://ict.od.ua/index.php/journal/uk/issue/view/3

2. Dmitrishin D. V.; *Khamitov V. M.*; Antoshchuk S. G.; Boltenkov V. O. A Modified Image Encryption Algorithm Based on the chaotic Tent Map. *Herald of Advanced Information Technology* . 2026. 9(1). P. 9–19.
https://doi.org/10.15276/hait.09.2026.01. *Видання включено до переліку наукових фахових видань України (категорія А).*
Видання включено до наукометричної бази SCOPUS
https://hait.od.ua/index.php/journal/article/view/247

3. *Khamitov, V. M.* .; Dmitrishin, D. V. .; Stokolos, A. M. .; Gray, D. A. . Convolved Numbers of K-Section of the Fibonacci Sequence: Properties, Consequences. *Herald of Advanced Information Technology*. 2026. 9 (2). P. 129–139. https://doi.org/10.15276/hait.09.2026.09. *Видання включено до переліку наукових фахових видань України (категоріяБ). Видання включено до наукометричної бази SCOPUS.*
https://hait.od.ua/index.php/journal/article/view/247

4. *Khamitov V. M.* .; Boltenkov V. O. .; Antoshchuk S. G. A Method for Operative Sharing Confidential Images Among a Group of Trusted Users. AAIT. 9 (2). P. 200 - 207. https://doi.org/10.15276/aait.09.2026.14. *Видання включено до переліку*

наукових фахових видань України (категорія Б) .https://aait.od.ua/index.php/journal/article/view/252

5. *V. Khamitov*, S. Antoshchuk. Application of nonlinear discrete maps to construct pseudo-chaotic cryptosystems . *Proceedings of Odessa Polytechnic University*, 2025. Issue 2(72). P. 186-203. https://doi.org/10.15276/opu.2.70.2024.19. *Видання включено до переліку наукових фахових видань України (категорія Б)* https://pratsi.op.edu.ua/index.php/pratsi/article/view/558

6. Dyadyura, K., Prokopovich, I., *Khamitov, V*., Sikach, T., Vershkov, O. Application of the Dynamic Programming Method in Process Measurement Problems When Assessing Interoperability. *Lecture Notes in Mechanical Engineering.* 2025. P. 699–711. https://DOI: 10.1007/978-3-031-82746-4_62

Видання включено до наукометричної бази SCOPUS

7. Dyadyura K., Oborskyi G., Prokopovych I., *Khamitov V*., Holubiev M. (2024). Optimal management in the operation of complex technical systems. *Journal of Engineering Sciences (Ukraine)*. 2024. Vol. 11(1). P. B1–B9. https://doi.org/10.21272/jes.2024.11(1).b1. *Видання включено до наукометричної бази SCOPUS.*

Наукові праці апробаційного характеру

8. *Khamitov V*., Dmytryshyn D., Gray D., and Stokolos A. Analytic summation of series involving higher-order derivatives of Chebyshev polynomials of the second kind and their applications to convolved linear recurrent sequences arXiv:2605.03200v2 [math.CV] https://doi.org/10.48550/arXiv.2605.03200

9. *Хамітов В. М*., Болтьонков В. О. Формування інтегрального показника якості шифрування зображень //Global Interdisciplinary Summit: Frontier of Science and Future Technologies. Proceedings of International Scientific and Practical Conference. April 3, 2026 in Khalifa University Campus, Dubai, UAE. Prague: Publishing house Education and Science s.r.o., 2026. P. 143 – 146.

10. *Khamitov Vitaly*, Boltenkov Viktor. Method for exchange of confidential images to a group of trusted users //Collection of Scientific Papers with the Proceedings of the 8th International Scientific and Practical Conference «Global Directions in Scientific Research and Technological Development» (April 6-8, 2026, Valencia, Spain). European Open Science Space. 2026. P. 68 – 70.

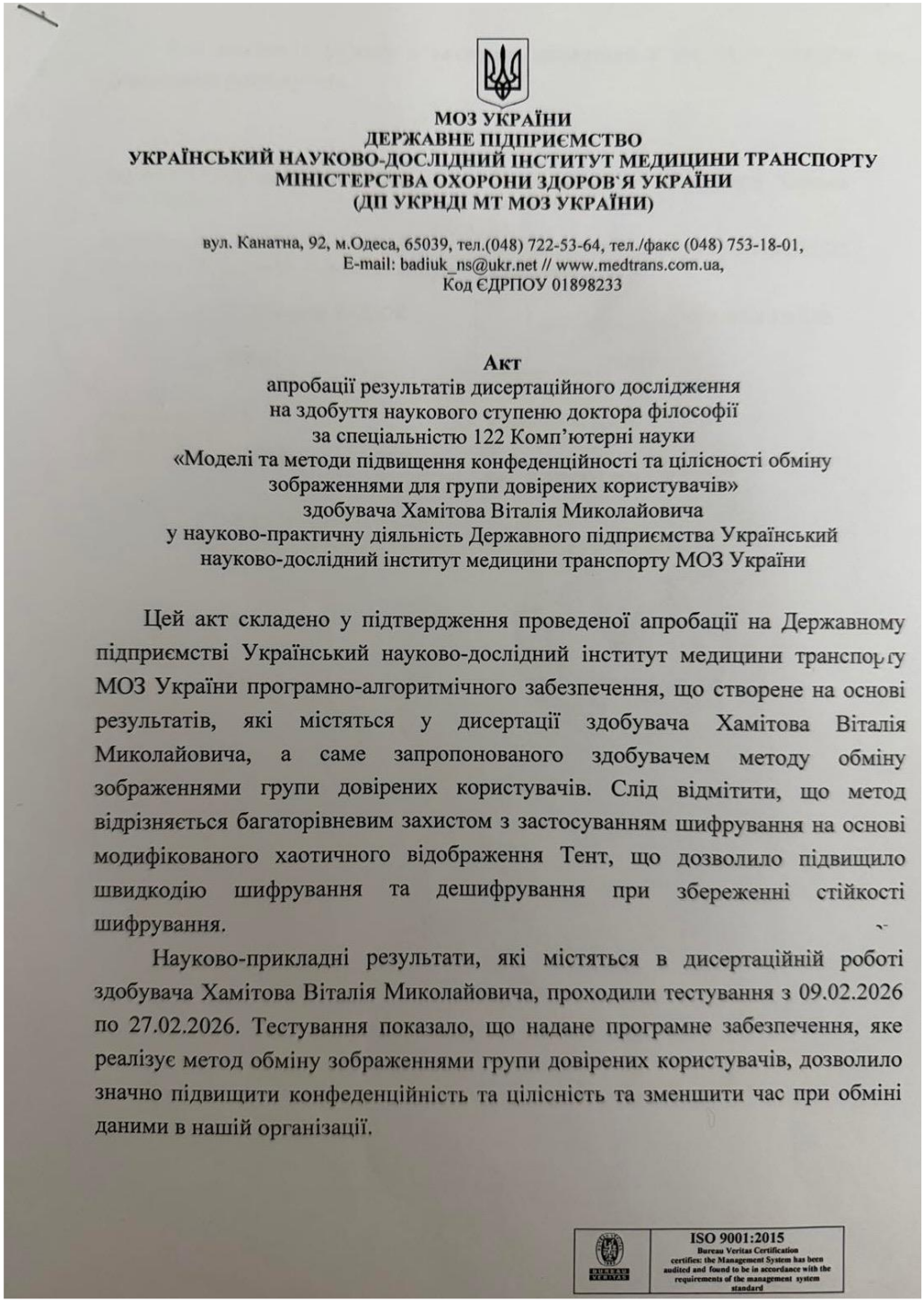
11. *Хамітов В.М*., Болтьонков В.О. Формування інтегрального показника якості шифрування зображень. Сучасні інформаційні технології та системи штучного інтелекту: матеріали 2-ї Міжнародної науково-практичної конференції. Частина 2. Харків -Яремче, 27-29 квітня 2026 р. – Х.: ХНУРЕ, 2026. С. 44-45

12. *Хамітов В.М*. Аналіз можливостей формування групи довірених користувачів для роботи із конфіденційними зображеннями *Матеріали XVI Міжнародної наукової конференції «Modern Information Technology – 2026»*, Одеса, 14–15 травня 2026 р. С. 179 – 180.

13. *В. Хамітов*, В. Болтьонков, С. Антощук. Система обміну конфіденційними зображеннями у групі довірених користувачів для медичного закладу. Сучасні технології біомедичної інженерії : матеріали *V Міжнародної науково-технічної конференції (6−8 травня 2026 р., м. Одеса, Україна).Odesa : Ecologiya, 2026. С. 182-184.

ДОДАТОК Б

Акт про використання результатів дисертаційної роботи у діяльності державного підприємства підприємства «Український науково-дослідний інститут медицини транспорту Міністерства охорони здоров'я України»



МОЗ УКРАЇНИ
ДЕРЖАВНЕ ПІДПРИЄМСТВО
УКРАЇНСЬКИЙ НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ МЕДИЦИНИ ТРАНСПОРТУ
МІНІСТЕРСТВА ОХОРОНИ ЗДОРОВ'Я УКРАЇНИ
(ДП УКРНДІ МТ МОЗ УКРАЇНИ)

вул. Канатна, 92, м.Одеса, 65039, тел.(048) 722-53-64, тел./факс (048) 753-18-01,
E-mail: badiuk_ns@ukr.net // www.medtrans.com.ua,
Код ЄДРПОУ 01898233

Акт
апробації результатів дисертаційного дослідження
на здобуття наукового ступеню доктора філософії
за спеціальністю 122 Комп'ютерні науки
«Моделі та методи підвищення конфеденційності та цілісності обміну зображеннями для групи довірених користувачів»
здобувача Хамітова Віталія Миколайовича
у науково-практичну діяльність Державного підприємства Український науково-дослідний інститут медицини транспорту МОЗ України

Цей акт складено у підтвердження проведеної апробації на Державному підприємстві Український науково-дослідний інститут медицини транспорту МОЗ України програмно-алгоритмічного забезпечення, що створене на основі результатів, які містяться у дисертації здобувача Хамітова Віталія Миколайовича, а саме запропонованого здобувачем методу обміну зображеннями групи довірених користувачів. Слід відмітити, що метод відрізняється багаторівневим захистом з застосуванням шифрування на основі модифікованого хаотичного відображення Тент, що дозволило підвищило швидкодію шифрування та дешифрування при збереженні стійкості шифрування.

Науково-прикладні результати, які містяться в дисертаційній роботі здобувача Хамітова Віталія Миколайовича, проходили тестування з 09.02.2026 по 27.02.2026. Тестування показало, що надане програмне забезпечення, яке реалізує метод обміну зображеннями групи довірених користувачів, дозволило значно підвищити конфеденційність та цілісність та зменшити час при обміні даними в нашій організації.

ISO 9001:2015
Bureau Veritas Certification
certifies: the Management System has been audited and found to be in accordance with the requirements of the management system standard

Акт видано в зв'язку з захистом дисертації і він не є основою для фінансових розрахунків.

Від ДП УКР НДІ медицини транспорту МОЗ України

Заступник директора з інноваційної і міжнародної діяльності та менеджменту, к.мед.н.

_____ Наталія БАДЮК

_____ 2026 р.

Адреса 65044, Одеса,
вул.. Канатна, 92
ДП УКР НДІ медицини транспорту МОЗ України

Від Національного університету "Одеська політехніка"

Заст. директора з наукової роботи ННІКС, к.т.н., доц.

_____ Анатолій КІСІЛЬ

_____ 2026 р.

Адреса 65044, Одеса,
пр. Шевченка, 1
Національний університет "Одеська політехніка"
Тел. (8-048) 705-8328

Узгоджено

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ · НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ПОЛІТЕХНІКА» · 43861328

ДОДАТОК В

Довідка про використання результатів дисертаційної роботи у діяльності Військово-медичного клінічного центру Південного регіону

Відкрита інформація

ЗБРОЙНІ СИЛИ УКРАЇНИ
ВІЙСЬКОВО-МЕДИЧНИЙ
КЛІНІЧНИЙ ЦЕНТР
ПІВДЕННОГО РЕГІОНУ
Код ЄДРПОУ 08199969
«__» _____ 20___р.
№_____
вул. Пироговська, 2
м. Одеса, 65044

ДОВІДКА
про використання результатів дисертаційного дослідження
Хамітова Віталія Миколайовича, представленого
на здобуття наукового ступеню доктора філософії
за спеціальністю 122 Комп'ютерні науки.
Тема дослідження:

«Моделі та методи підвищення конфіденційності та цілісності обміну зображеннями для групи довірених користувачів»

Важливим і перспективним напрямком науково-технічного розвитку залишається розробка та вдосконалення методів підвищення конфіденційності та цілісності обміну зображеннями високої роздільної здатності для групи довірених користувачів. Така задача є потрібною особливо у медицині для зберігання та обміну не тільки персональних даних пацієнтів, а й результатів медичних обстежень у різних форматах. Для її вирішення та широкого впровадження таких технологій, актуальною є задача удосконалення моделей та методів перетворення інформації та зображень на основі хаотичних відображень та формування нових псевдовипадкових послідовностей для підвищення швидкодії та зменшення ресурсозалежності методів захисту інформації.

Результати дисертаційного дослідження Хамітова Віталія Миколайовича «Моделі та методи підвищення конфіденційності та цілісності обміну зображеннями для групи довірених користувачів» використовуються у сфері телемедицини для забезпечення конфіденційності та цілісності обміну медичними даними пацієнтів між медичним персоналом.

Начальник Військово-медичного клінічного центру
Південного регіону
полковник медичної служби Роман КАЛЬЧУК

ВІДКРИТА ІНФОРМАЦІЯ

Військово-клінічний клінічний центр Південного регіону
№ 5401611 від 17.04.2025 14:48:58 арк. 1

ДОДАТОК Г

Довідка про використання результатів дисертаційної роботи у науково-дослідницький діяльності Національного університету «Одеська Політехніка»

Довідка № 764/1-07

про використання результатів дисертаційної роботи
Хамітова Віталія Миколайовича
«Моделі та методи підвищення конфеденційності та цілісності обміну зображеннями для групи довірених користувачів»
у науково-дослідницької діяльності
Національного університету «Одеська Політехніка»

Довідка видана в тому, що у науково-дослідницькій діяльності Національного університету «Одеська політехніка» використані наступні наукові результати, отримані у дисертаційній роботі **Хамітова Віталія Миколайовича**:

- метод шифрування зображень на основі хаотичного відображення Tent з управлінням, що дозволило на підставі короткого ключа (насіння) згенерувати довгу псевдовипадкову послідовність, що значно підвищило швидкодію шифрування та дешифрування при збереженні стійкості шифрування;
- розроблено метод обміну зображеннями групи довірених користувачів, який відрізняється багато рівневим захистом з застосуванням шифрування на основі модифікованого хаотичного відображення Тент.

Дисертацію виконано згідно тематичних планів НДР Одеської політехніки за період 2016 - 2025 рр.

Хамітов Віталій Миколайович був виконавцем у держбюджетній темі № 719-61/161 – «Інтелектуальна підтримка прийняття рішень при проєктуванні кісткових замінників для лікування воєнних травм» (номер держ. реєстрації 0124U000388).

Проректор з наукової та
науково-педагогічної роботи,
д.т.н., професор Дмитро ДМИТРИШИН

Керівник НДР № 719-61/161,
д.т.н., професор Світлана АНТОЩУК

ДОДАТОК Д

Довідка про використання результатів дисертаційної роботи у навчальному процесі Національного університету «Одеська Політехніка»

Україна
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ПОЛІТЕХНІКА»

КОД ЄДРПОУ 43861328

пр.Шевченка, 1, м.Одеса, 65044
Україна
тел. +38 048 7223474
факс. +38 048 7221992
E-mail: mail@op.edu.ua

10.12.2025 № 2100/61-07

на №

ДОВІДКА

про впровадження результатів дисертаційної роботи
Хамітова Віталія Миколайовича
«Моделі та методи підвищення конфеденційності та цілісності обміну зображеннями для групи довірених користувачів»
у освітній діяльності
Національного університету «Одеська Політехніка»

Довідка видана для підтвердження того, що в програмах, навчально-методичних матеріалах та курсах лекцій з дисциплін, які вивчаються на кафедрі Інформаційних систем Інституту комп'ютерних систем бакалаврами спеціальності 122 «Комп'ютерні науки»: «Дискретна математика» та «Технології захисту інформації», використовуються наукові результати, отримані у дисертації Хамітова Віталія Миколайовича, а саме:

– дисципліна «Дискретна математика» – тема «Відображення та функції»;
– дисципліна «Технології захисту інформації» – теми «Шифр Вернама. Потокові шрифти» та «Режими блокових шифрів та їх особливості».

Використані результати дисертації Хамітова Віталія Миколайовича «Моделі та методи підвищення конфеденційності та цілісності обміну зображеннями для групи довірених користувачів» свідчать про глибоке опрацювання наукової літератури за тематикою дисертації. Висновки та пропозиції відзначаються науковою новизною, можливістю реалізації в інформаційних системах, де є необхідність підвищення конфеденційності та цілісності обміну зображеннями для групи довірених користувачів, тому істотно поліпшують матеріал означених дисциплін і сприяють підвищенню якості підготовки фахівців в галузі комп'ютерних наук та інформаційних технологій.

Проректор з науково-педагогічної
та виховної роботи, д.т.н., професор Сергій НЕСТЕРЕНКО

Завідувачка кафедри
інформаційних систем,
д.т.н., професор Олена АРСІРІЙ

04.12.2025 р.

ДОДАТОК Е

Представлення послідовностей в енциклопедії OEIS (№№A395431, A393329, A395902, A396356)

https://oeis.org/search?q=A395431&language=english&go=Search

login

The OEIS is supported by the many generous donors to the OEIS Foundation.

THE ON–LINE ENCYCLOPEDIA OF INTEGER SEQUENCES ®

founded in 1964 by N. J. A. Sloane

A395431 Поиск Указания

(Вас приветствует Онлайн-энциклопедия целочисленных последовательностей)

Поиск: **a395431**

Displaying 1-4 of 4 results found. page 1

Sort: relevance | references | number | modified | created Format: long | short | data

A395431 Self-convolution of A001076. +40 4

0, 0, 1, 8, 50, 280, 1475, 7472, 36836, 178000, 847045, 3982200, 18538134, 85599912, 392560775, 1789800160, 8119213000, 36670415648, 164983381129, 739737725800, 3306651932410, 14740349833400, 65546786425931, 290816440554768, 1287647063875500, 5690631701996400

(list; graph; refs; listen; history; text; internal format)

OFFSET 0,4

LINKS Alois P. Heinz, Table of n, a(n) for n = 0..1591

D. Dmytryshyn, D. Gray, V. Khamitov, and Alex Stokolos, Convolved numbers of k-section of the Fibonacci sequence: properties, consequences, arXiv:2603.08636 [math.CA], 2026; see also alternate link, Herald of Advanced Information Technology. 2026. Vol. 9, No. 2. P. 129-139.

Index entries for linear recurrences with constant coefficients, signature (8,-14,-8,-1).

FORMULA a(n) = 8*a(n-1) - 14*a(n-2) - 8*a(n-3) - a(n-4) for n>=4, a(0)=a(1)=0, a(2)=1, a(3)=8.

a(n) = (4*(n-1)*a(n-1)+n*a(n-2))/(n-2) for n>=3, a(0)=a(1)=0, a(2)=1.

G.f.: z^2/(1-4*z-z^2)^2.

a(n) = ((n-1)*Fibonacci(3*n+3) + (n+1)*Fibonacci(3*n-3))/40.

Binet formula: a(n) = (1/(q^{3*(n+2)}*(q^3+q^{-3})^3))*(n*((-1)^{3*n+1}+q^{6*(n+2)})+(n+2)*((-1)^{3*n+1}q^6+q^{6*(n+1)})), where q=(1+sqrt(5))/2 is the golden ratio A001622.

Gegenbauer polynomials: a(n) = (-i)^{n-1} * C_{n-1}^{(2)}(2i).

E.g.f.: exp(2*x)*(10*x*cosh(sqrt(5)*x) + sqrt(5)*(5*x - 2)*sinh(sqrt(5)*x))/50. - Stefano Spezia, Apr 26 2026

MAPLE
```
a:= proc(n) option remember; `if`(n<4, [0$2, 1, 8][n+1],
      8*a(n-1)-14*a(n-2)-8*a(n-3)-a(n-4))
    end:
seq(a(n), n=0..25);
# Alternative:
a:= n-> (<<0|1|0|0>, <0|0|1|0>, <0|0|0|1>, <-1|-8|-14|8>>^n)[2, 4]:
seq(a(n), n=0..25);  # Alois P. Heinz, Apr 27 2026
```

MATHEMATICA
```
a[n_]:=((n-1)*Fibonacci[3*n+3]+(n+1)*Fibonacci[3*(n-1)])/40; Array[a, 26, 0] (* Stefano Spezia, Apr 26 2026 *)
```

CROSSREFS Cf. A000045 (Fibonacci), A001076 (F(3*n)/2), A001622, A001629.

KEYWORD nonn,easy

AUTHOR Alex Stokolos, Apr 22 2026

STATUS approved

A395902 Triple convolution of the modified Fibonacci sequence F(3n)/2 (A001076). +10 1

0, 0, 0, 1, 12, 99, 688, 4326, 25464, 143018, 775536, 4092207, 21126564, 107136597, 535272864, 2640788828, 12888228336, 62312915172, 298810304672, 1422537514989, 6728698090428, 31643981809111, 148044975160272, 689370668876130, 3196344091219560, 14762394097629870

(list; graph; refs; listen; history; text; internal format)

OFFSET 0,5

LINKS Table of n, a(n) for n=0..25.

D. Dmytryshyn, D. Gray, V. Khamitov, and Alex Stokolos, Convolved numbers of k-section of the Fibonacci sequence: properties, consequences, arXiv:2603.08636 [math.CA], 2026; see also alternate link, Herald of Advanced Information Technology. 2026. Vol. 9, No. 2. P. 129-139.

Index entries for linear recurrences with constant coefficients, signature (12,-45,40,45,12,1).

FORMULA a(n) = Sum_{j=1..n} y(j)*y1(n-j), where y(n) = F(3*n)/2 and y1(n) is the first-order convolution of y.

G.f.: x^3/(1 - 4*x - x^2)^3.

a(n) = (-1)^(n-3) * GegenbauerC(n-3, 3, 2*I).

a(j) = (4*(j-1)*a(j-1) + (j+1)*a(j-2)) / (j-3) for j>=4, with a(0..2)=0, a(3)=1.

a(n) = 12*a(n-1) - 45*a(n-2) + 40*a(n-3) + 45*a(n-4) + 12*a(n-5) + a(n-6) for n>=6, with a(0..5) = (0, 0, 0, 1, 12, 99).

a(n) = (1/800) * (1/2*(n-2)*(n-1)*F(3*n+6) + (n-2)*(n+2)*F(3*n) + 1/2*(n+1)*(n+2)*F(3*n-6)).

a(n) = (q^(-3*n-6) / (q^3+q^(-3))^5) * (1/2*(n-2)*(n-1)*(q^(6*n+12) - (-1)^n) + (n-2)*(n+2)*(q^(6*n+6) - (-1)^n*q^6) + 1/2*(n+1)*(n+2)*(q^(6*n) - (-1)^n*q^12)), where q = (1+sqrt(5))/2.

E.g.f.: exp(2*x) * ((1/10 - 7/200*x)*cosh(sqrt(5)*x) + sqrt(5)*(9/200*x^2 - 1/50*x + 7/1000)*sinh(sqrt(5)*x)).

MAPLE
```
N := 25; a[0]:= 0; a[1]:= 0; a[2]:= 0; a[3]:= 1;
for j from 4 to N do
a[j]:=1/(j-3)*(4*(j-1)*a[j-1]+(j+1)*a[j-2]):
end:
seq(a[k], k = 0 .. N);
```

MATHEMATICA
```
LinearRecurrence[{12, -45, 40, 45, 12, 1}, {0, 0, 0, 1, 12, 99}, 26] (* Amiram Eldar, May 10 2026 *)
```

CROSSREFS Cf. A395431, A001076, A000045, A001622.

KEYWORD nonn,easy

AUTHOR Alex Stokolos, May 08 2026

STATUS approved

A393329 Self-convolution of the sequence b(n) = A004187(n) = F(4*n)/3, where F(n) are Fibonacci numbers. +10 0

0, 0, 1, 14, 145, 1330, 11420, 94066, 752979, 5902890, 45544035, 347016740, 2617376056, 19577124644, 145406256485, 1073550481990, 7885450036085, 57661336389846, 419985058108884, 3048385407665430, 22057531003184695, 159159907730783330, 1145562037717754311, 8226470282415530824

(list; graph; refs; listen; history; text; internal format)

OFFSET 0,4

COMMENTS Part of a family of self-convolutions of Fibonacci-related sequences F(k*n)/F(k).
Related to **A395431**, which is the self-convolution of F(3*n)/F(3).

LINKS Table of n, a(n) for n=0..23.
D. Dmytryshyn, D. Gray, V. Khamitov, and Alex Stokolos, Convolved numbers of k-section of the Fibonacci sequence: properties, consequences, arXiv:2603.08636 [math.CA], 2026; see also alternate link, Herald of Advanced Information Technology. 2026. Vol. 9, No. 2. P. 129-139.
Index entries for linear recurrences with constant coefficients, signature (14,-51,14,-1).

FORMULA a(n) = 14*a(n-1) - 51*a(n-2) + 14*a(n-3) - a(n-4) for n >= 4.
a(n) = (7*(n-1)*a(n-1) - n*a(n-2)) / (n-2) for n >= 3, a(0)=a(1)=0, a(2)=1.
a(n) = Sum_{j=1..n} b(j)*b(n-j), where b(j) = F(4*j)/3.
a(n) = GegenbauerC(n-2, 2, 7/2) for n >= 2.
a(n) = (q^(-4*(n+1)) / (q^4 - q^(-4))^3) * ((n-1)*(q^(8*(n+1)) - 1) - (n+1)*(q^(8*n) - q^8)), where q = (1+sqrt(5))/2.
a(n) = ((n-1)*F(4*n+4) - (n+1)*F(4*n-4)) / 135.
G.f.: x^2 / (1 - 7*x + x^2)^2.
E.g.f.: exp(7*x/2) * ((7*x/45)*cosh(3*sqrt(5)*x/2) + (sqrt(5)*x/15 - 14*sqrt(5)/675)*sinh(3*sqrt(5)*x/2)).

MAPLE
```
N := 15: a[0] := 0: a[1] := 0: a[2] := 1: a[3] := 14:
for j from 4 to N do
a[j] := 14*a[j - 1] - 51*a[j - 2] + 14*a[j - 3] - a[j - 4]:
end do:
seq(a[k], k = 0 .. N);
```

MATHEMATICA LinearRecurrence[{14, -51, 14, -1}, {0, 0, 1, 14}, 24] (* Amiram Eldar, May 17 2026 *)

CROSSREFS Cf. A000045, A004187, **A395431**.

KEYWORD nonn,easy

AUTHOR Alex Stokolos, May 16 2026

STATUS approved

A396356 Triangle of convolved numbers of the 3-section of the Fibonacci sequence. +10 0

1, 8, 1, 50, 12, 1, 280, 99, 16, 1, 1475, 688, 164, 20, 1, 7472, 4326, 1360, 245, 24, 1, 36836, 25464, 9930, 2360, 342, 28, 1, 178000, 143018, 66544, 19615, 3752, 455, 32, 1, 847045, 775536, 419124, 147364, 34965, 5600, 584, 36, 1, 3982200, 4092207, 2518576, 1028195, 290976, 57820, 7968, 729, 40, 1

(list; table; graph; refs; listen; history; text; internal format)

OFFSET 1,2

COMMENTS This triangle represents a two-dimensional diagonal section of the three-dimensional array of convolutions of k-sections of the Fibonacci sequence for the fixed parameter k=3 (where the base 3-section sequence is A001076).
This triangle is part of a family of matrices for general k-sections of Fibonacci convolutions, where the generalized convolved coefficients for any parameter k are completely determined by the Gegenbauer polynomial framework using the respective Lucas numbers L_k. Here L_3 = 4. For k=1, see A000027, A000096, A006503, A006504, A139798. The rows and columns of this triangle expand upon **A395431** and A395902. While those sequences explicitly present alternative generation methods (including iterative convolutions, P-recurrences, and generating functions), the sequences in this triangle can be generated using completely analogous frameworks.

LINKS Table of n, a(n) for n=1..55.
D. Dmytryshyn, D. Gray, V. Khamitov, and Alex Stokolos, Convolved numbers of k-section of the Fibonacci sequence: properties, consequences, arXiv:2603.08636 [math.CA], 2026; see also alternate link, Herald of Advanced Information Technology. 2026. Vol. 9, No. 2. P. 129-139.

FORMULA T(n, s) = A(n-s+1, s) for n >= 1, 1 <= s <= n, where A(m, k) is the convolved number of the 3-section of the Fibonacci sequence with element position m and convolution order k.
A(m, k) = (-i)^(m-1) * GegenbauerC(m-1, k+1, (i/2)*L_3), where i is the imaginary unit and L_3 = 4.
A(m, k) = Sum_{i=0..floor((m-1)/2)} binomial(k+m-1-i, k) * binomial(m-1-i, i) * 4^(m-1-2*i) for m >= 1.
T(n, s) = A(n-s+1, s) for n >= 1, 1 <= s <= n, where A(m, k) is defined by the recurrence: A(1, k) = 1, A(2, k) = 4*k + 4,
A(m, k) = (4*(m + k - 1)*A(m-1, k) + (m + 2*k - 1)*A(m-2, k))/(m-1) for m >= 3.

EXAMPLE T(4, 2) = A(3, 2) = (-i)^2 * GegenbauerC(2, 3, 2*i) = -1 * (-99) = 99.
The triangle starts:

	s=1	s=2	s=3	s=4	s=5	s=6
n=1:	1;					
n=2:	8,	1;				
n=3:	50,	12,	1;			
n=4:	280,	99,	16,	1;		
n=5:	1475,	688,	164,	20,	1;	
n=6:	7472,	4326,	1360,	245,	24,	1;

Example for the recurrence formula:
To find T(3, 1) = A(3, 1), we use the recurrence with m = 3 and k = 1: A(1, 1) = 1 A(2, 1) = 4*1 + 4 = 8 A(3, 1) = (4*(3 + 1 - 1)*A(2, 1) + (3 + 2*1 - 1)*A(1, 1)) / (3 - 1) = (4*3*8 + 4*1) / 2 = (96 + 4) / 2 = 50.
Example for the combinatorial formula:
To find T(4, 2) = A(3, 2), we use the sum with m = 3 and k = 2: A(3, 2) = Sum_{i=0..1} binomial(2+3-1-i, 2) * binomial(3-1-i, i) * 4^(3-1-2*i) = binomial(4, 2)*binomial(2, 0)*4^2 + binomial(3, 2)*binomial(1, 1)*4^0 = 6 * 1 * 16 + 3 * 1 * 1 = 96 + 3 = 99.

MAPLE
```
A := (n, s) -> simplify((-I)^(n-1) * GegenbauerC(n-1, s+1, 2*I)):
for m from 1 to 10 do
    for j from 1 to m do
```

```
            printf("%d, ", A(m-j+1, j));
        end do; end do;
```

CROSSREFS Cf. A001076 (base 3-section), **A395431** (first column), A395902 (second column), A000012 (right edge), A000045.

KEYWORD nonn,tabl,new

AUTHOR Alex Stokolos, May 23 2026

STATUS approved

Додаток Є

Фрагменти вихідного коду програмних інструментальних засобів

```
 BD-GKA (Burmester–Desmedt) на кривій Монтгомері X25519
# BD-GKA (Burmester–Desmedt Group Key Agreement)
# Elliptic Curve: Montgomery Curve X25519
#
from cryptography.hazmat.primitives.asymmetric import x25519
from cryptography.hazmat.primitives.kdf.hkdf import HKDF
from cryptography.hazmat.primitives import hashes
from cryptography.hazmat.primitives.serialization import Encoding,
PublicFormat
import hashlib
import os
import time
# УЧАСНИК ГРУПИ
class Participant:
    def __init__(self, participant_id):
        self.id = participant_id
        # Приватний ключ X25519
        self.private_key = x25519.X25519PrivateKey.generate()
        # Публічний ключ
        self.public_key = self.private_key.public_key()
        # Сусідні значення
        self.left_shared = None
        self.right_shared = None
        # BD value
        self.z_value = None
        # Фінальний груповий ключ
        self.group_key = None
    # ------------------------------------------------------
    # Повернення байтів публічного ключа
    # ------------------------------------------------------
```

```
    def public_bytes(self):
        return self.public_key.public_bytes(
            encoding=Encoding.Raw,
            format=PublicFormat.Raw
        )
    # ------------------------------------------------------
    # Обчислення спільного секрету
    # ------------------------------------------------------
    def compute_shared_secret(self, other_public_key_bytes):
        other_public_key =
x25519.X25519PublicKey.from_public_bytes(
            other_public_key_bytes
        )
        shared_secret =
self.private_key.exchange(other_public_key)
        return shared_secret
# BD-GKA ПРОТОКОЛ
class BD_GKA:
    def __init__(self, number_of_users):
       self.n = number_of_users
        self.users = [
            Participant(i)
            for i in range(number_of_users)
        ]
    # ФАЗА 1
    # Генерація та обмін відкритими ключами

    def phase1_exchange_public_keys(self):
        public_keys = []
        for user in self.users:
            pk = user.public_bytes()
            public_keys.append(pk)
        return public_keys
```

```
    # ФАЗА 2
    # Обчислення сусідніх секретів
       def phase2_compute_pairwise_secrets(self, public_keys):
        for i in range(self.n):
            left_index = (i - 1) % self.n
            right_index = (i + 1) % self.n
            current_user = self.users[i]
            left_pk = public_keys[left_index]
            right_pk = public_keys[right_index]
            # ECC scalar multiplication
            current_user.left_shared =
current_user.compute_shared_secret(left_pk)
            current_user.right_shared =
current_user.compute_shared_secret(right_pk)
    # ФАЗА 3
    # Обчислення Zi
       def phase3_compute_z_values(self):
        z_values = []
        for user in self.users:
            left_hash = hashlib.sha256(user.left_shared).digest()
            right_hash =
hashlib.sha256(user.right_shared).digest()
            z = bytes(
                a ^ b
                for a, b in zip(left_hash, right_hash)
            )
            user.z_value = z
            z_values.append(z)
        return z_values
    # ФАЗА 4
    # Обчислення фінального групового ключа
    def phase4_compute_group_key(self, z_values):
        for user in self.users:
```

```
            concat_data = b''
            for z in z_values:
                concat_data += z
            hkdf = HKDF(
                algorithm=hashes.SHA256(),
                length=32,
                salt=None,
                info=b'BD-GKA-X25519'
            )
            user.group_key = hkdf.derive(concat_data)
    # ВИКОНАННЯ ПРОТОКОЛУ
    def execute_protocol(self):
        start_time = time.time()
        # Phase 1
        public_keys = self.phase1_exchange_public_keys()
        # Phase 2
        self.phase2_compute_pairwise_secrets(public_keys)
        # Phase 3
        z_values = self.phase3_compute_z_values()
        # Phase 4
        self.phase4_compute_group_key(z_values)
        end_time = time.time()
        execution_time = end_time - start_time
        return execution_time
# ГОЛОВНА ПРОГРАМА
if __name__ == "__main__":
    N = 5
    protocol = BD_GKA(N)
    elapsed = protocol.execute_protocol()
    protocol.print_results()
    print("\nExecution time:", elapsed, "seconds")
# Montgomery Curve Arithmetic
# Including Montgomery Ladder
```

```
# Curve form:
#     B*y^2 = x^3 + A*x^2 + x   (mod p)
from dataclasses import dataclass
# Field arithmetic
def mod_inv(a, p):
    """Inverse modulo p"""
    return pow(a, p - 2, p)
# Point representation
@dataclass
class Point:
    x: int
    y: int
    def is_infinity(self):
        return self.x is None
INF = Point(None, None)
# Montgomery Curve
class MontgomeryCurve:
    def __init__(self, A, B, p):
        self.A = A
        self.B = B
        self.p = p
    def is_on_curve(self, P):
        if P == INF:
            return True
        x = P.x
        y = P.y
        left = (self.B * y * y) % self.p
        right = (
            x * x * x
            + self.A * x * x
            + x
        ) % self.p
        return left == right
```

```
def negate(self, P):
    if P == INF:
        return INF
    return Point(P.x, (-P.y) % self.p)
def add(self, P, Q):
    if P == INF:
        return Q
    if Q == INF:
        return P
    if P.x == Q.x:
        if (P.y + Q.y) % self.p == 0:
            return INF
        return self.double(P)
    p = self.p
    lam = (
        (Q.y - P.y)
        * mod_inv(Q.x - P.x, p)
    ) % p
    x3 = (
        self.B * lam * lam
        - self.A
        - P.x
        - Q.x
    ) % p
    y3 = (
        lam * (P.x - x3)
        - P.y
    ) % p
    return Point(x3, y3)
def double(self, P):
    if P == INF:
        return INF
    p = self.p
```

```
        numerator = (
            3 * P.x * P.x
            + 2 * self.A * P.x
            + 1
        ) % p
        denominator = (
            2 * self.B * P.y
        ) % p
        lam = (
            numerator
            * mod_inv(denominator, p)
        ) % p
        x3 = (
            self.B * lam * lam
            - self.A
            - 2 * P.x
        ) % p
        y3 = (
            lam * (P.x - x3)
            - P.y
        ) % p
        return Point(x3, y3)
        def scalar_mult(self, k, P):
        R = INF
        Q = P
        while k > 0:
            if k & 1:
                R = self.add(R, Q)
            Q = self.double(Q)
            k >>= 1
        return R
# X/Z arithmetic for Montgomery Ladder
def montgomery_ladder(k, u, A, p):
```

```
Curve25519-style Montgomery ladder
Input:
    k  scalar
    u  x-coordinate
Output:
    x([k]P)
A24 = ((A + 2) * mod_inv(4, p)) % p
x1 = u
x2 = 1
z2 = 0
x3 = u
z3 = 1
swap = 0
bits = k.bit_length()
for t in reversed(range(bits)):
    kt = (k >> t) & 1
    swap ^= kt
    if swap:
        x2, x3 = x3, x2
        z2, z3 = z3, z2
    swap = kt
    A_ = (x2 + z2) % p
    AA = (A_ * A_) % p
    B_ = (x2 - z2) % p
    BB = (B_ * B_) % p
    E = (AA - BB) % p
    C = (x3 + z3) % p
    D = (x3 - z3) % p
    DA = (D * A_) % p
    CB = (C * B_) % p
    x3 = ((DA + CB) ** 2) % p
    z3 = (
        x1 *
```

```
            ((DA - CB) ** 2)
        ) % p
        x2 = (AA * BB) % p
        z2 = (
            E *
            (AA + A24 * E)
        ) % p
    if swap:
        x2, x3 = x3, x2
        z2, z3 = z3, z2
    return (x2 * mod_inv(z2, p)) % p
if __name__ == "__main__":
    p = 2**255 - 19
    A = 486662
    B = 1
    curve = MontgomeryCurve(A, B, p)
    # Base point x-coordinate
    u = 9
    # Example private key
    k = 0x123456789ABCDEF123456789ABCDEF
    result_x = montgomery_ladder(
        k,
        u,
        A,
        p
    )
```