Сумський державний університет

Міністерства освіти і науки України

Кваліфікаційна наукова
праця на правах рукопису

БОНДАРЕНКО МИКИТА ОЛЕГОВИЧ

УДК 004.056.55

ДИСЕРТАЦІЯ

МОДЕЛІ ТА МЕТОДИ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ СТВОРЕННЯ КРИПТОСИСТЕМ НА ОСНОВІ ФУНКЦІЙ ДІЙСНИХ ЗМІННИХ

122 – комп’ютерні науки

Подається на здобуття наукового ступеня доктора філософії

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

_____М. О. Бондаренко

Науковий керівник –
Авраменко Віктор Васильович
кандидат технічних наук,
доцент

Суми – 2024

АНОТАЦІЯ

Бондаренко М. О. **Моделі та методи інформаційної технології створення криптосистем на основі функцій дійсних змінних.** – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 122 Комп'ютерні науки. Сумський державний університет, Міністерство освіти і науки України, Суми, 2024.

У дисертаційній роботі розв'язано важливе науково-практичне завдання розробки нових моделей та методів криптографічних систем на основі функцій дійсної змінної.

Обґрунтовано актуальність теми дисертації, зазначено зв'язок роботи з науковими темами, сформульовано мету та задачі дослідження, визначено об'єкт, предмет та методи дослідження, показано наукову новизну та практичне значення отриманих результатів, апробацію результатів та їх висвітлення у публікаціях.

Актуальність даного дослідження зумовлена комплексом факторів, що формують сучасні виклики у сфері інформаційної безпеки та криптографії:

1. Обмеження існуючих криптосистем: більшість сучасних криптографічних систем, таких як AES та RSA, базуються на операціях з цілими числами. Хоча ці системи широко використовуються, вони стикаються з низкою проблем. Зокрема, зі зростанням обчислювальної потужності виникає необхідність постійного збільшення довжини ключів, що призводить до зростання обчислювальних витрат. Крім того, кінцевий набір цілих чисел потенційно обмежує довгострокову стійкість цих систем перед розвитком методів криптоаналізу.

2. Загроза квантових обчислень: розвиток квантових комп'ютерів створює загрозу для багатьох існуючих криптографічних алгоритмів. Зокрема, квантовий алгоритм Шора може ефективно вирішувати проблеми факторизації та дискретного логарифму, на яких базується безпека RSA та ECC. Так, розвиток

квантових комп’ютерів становить загрозу для багатьох криптографічних систем, що підштовхує до принципово інших математичних підходів до шифрування.

3. Потреба в нових підходах: аналіз сучасного стану криптографії показує активні дослідження нових методів на альтернативних засадах, що демонструє потребу в розробці інноваційних способів захисту даних. Однак, більшість з цих нових систем все ще зосереджені на цілих числах і мають свої недоліки.

4. Специфіка захисту зображень: існує окремий напрямок криптографії, спрямований на створення систем для шифрування зображень, що дозволяли б використовувати властивості візуальних даних для покращення стійкості. Це вказує на потребу в спеціалізованих криптографічних рішеннях для різних типів даних.

5. Потенціал систем на основі дійсних чисел: використання криптосистем на основі дійсних чисел представляє перспективний напрямок досліджень. Оскільки потужність множини дійсних чисел вища за потужність множини цілих чисел, це потенційно може забезпечити більший простір ключів та вищу криптографічну стійкість. Однак, дослідження в цьому напрямку є менш розповсюдженими і потребують подальшого розвитку.

6. Інтегральна криптографія: дослідження в області інтегральної криптографії, зокрема використання інтегральних рівнянь Фредгольма, відкривають нові можливості для створення криптосистем з теоретично гарантованою стійкістю. Це вказує на потенціал використання нових математичних підходів у криптографії.

Таким чином, дослідження нових методів криптографічного захисту на основі функцій дійсної змінної та інтегральної непропорційності є актуальним та важливим завданням. Воно має потенціал для створення нових криптографічних примітивів, які могли б подолати обмеження існуючих систем, та запропонувати ефективні рішення для захисту різних типів даних, включаючи зображення. Тема відповідає сучасним тенденціям розвитку криптографії та має потенціал для внеску у підвищення безпеки цифрової інформації в сучасному світі.

Об'єктом дослідження є процеси криптографічного захисту даних.

Предметом досліджень є моделі, методи та алгоритми криптографічних систем на основі функцій дійсної змінної.

Обрані методи дослідження базуються на принципах і методах криптографії, методах розпізнавання сигналів і функціях непропорційності.

Метою дослідження є розробка нових моделей та методів криптосистем на основі функцій дійсної змінної для підвищення стійкості та ефективності шифрування як текстових даних, так і зображень.

У роботі поставлено та вирішено наступні завдання:

1. Проведено аналіз сучасних криптографічних систем, їх переваг та недоліків.
2. Розроблено математичну модель криптосистем на основі функцій дійсної змінної.
3. Створено метод шифрування даних з використанням суми функцій дійсної змінної як симетричних ключів.
4. Розроблено метод дешифрування даних, які зашифровані за допомогою обчислення невідомих коефіцієнтів ключових функцій.
5. Адаптовано розроблені методи для шифрування та дешифрування зображень.
6. Розроблено алгоритм використання зображення як криптографічного ключа для шифрування інших зображень.
7. Створено програмну реалізацію розроблених криптосистем та проведено експериментальні дослідження їх ефективності.

Практичне значення полягає в тому, що отримані результати дозволяють практичну реалізацію запропонованих криптосистем. Усі теоретичні розробки дисертації автором доведено до конкретних інженерних методик, алгоритмів, з використанням запропонованої інформаційної технології шифрування та дешифрування даних за допомогою функцій дійсних змінних. Отримані результати дозволяють практичну реалізацію запропонованих криптосистем. Запропонована криптосистема для захисту зображень з використанням

довільного зображення як ключа може бути застосована для експериментального захисту візуальної інформації в різних сферах. Створене програмне забезпечення для реалізації розроблених криптографічних алгоритмів може бути використане для проведення подальших досліджень та експериментів в області криптографії на основі функцій дійсної змінної. Результати експериментальних досліджень криптостійкості розроблених методів можуть бути використані для порівняльного аналізу різних підходів до шифрування.

Наукова новизна полягає в тому, що у дисертаційній роботі розв'язано важливу науково-практичну задачу створення моделей та методів криптографічних систем на основі функцій дійсної змінної, отримані такі результати:

1. Удосконалено моделі та методи створення криптосистем на основі функцій дійсної змінної, що приводить до збільшення крипостійкість.

2. Уперше розроблено метод використання інтегральних функцій непропорційності для дешифрування даних, що дозволяє використовувати в криптосистемі дискретні функції-ключі.

3. Уперше розроблено криптосистему, що поєднує шифрування за допомогою суми функцій дійсної змінної та шифрування за допомогою інтегральної функції непропорційності. Відбувається двох-етапне шифрування, при якому результат першого етапу шифрується ще раз, що суттєво ускладнює злам криптосистеми.

4. Удосконалено метод шифрування даних шляхом впровадження додаткового елементу перестановки функцій-ключів, що також підвищує криптостійкість системи.

5. Вперше розроблено криптосистему для захисту зображень, де інше довільне зображення використовується в якості криптографічного ключа, шляхом використання функцій інтегральної непропорційності. Це значно спрощує передачу ключа порівняно з передачею функцій-ключів в аналітичному вигляді. Це зображення легше непомітно передати приймальній стороні при використанні симетричних криптосистем. Крім того, зловмиснику складніше

виявити зображення-ключ серед багатьох зображень, до яких він отримав доступ.

6. Експериментально продемонстровано високу криптостійкість розроблених методів шифрування до атак грубої сили через необхідність підбору значень ключа з високою точністю. Також продемонстровано високу здібність до декореляції значень шифротексту.

Дисертаційна робота відповідає пріоритетним напрямкам наукових досліджень Сумського державного університету. Дослідження виконано відповідно до плану науково-дослідних робіт за держбюджетною темою «Методи, математичні моделі та інформаційні технології аналізу і синтезу інфокомунікаційних систем» (ДР № 0118U006971, 2018-2023). Роль автора в цій науково-дослідній роботі полягала в розробці моделей та методів шифрування і дешифрування даних для застосування в інфокомунікаційних системах.

Результати досліджень дисертаційної роботи доповідалися та обговорювалися на міжнародних науково-практичних конференціях. Міжнародна науково-практична конференція «ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ»(м. Одеса, 2021 р.) Міжнародна науково-технічна конференція студентів та молодих учених «Інформатика, математика, автоматика» (Суми-Астана, 2022 р.) Міжнародна науково-технічна конференція студентів та молодих учених «Інформатика, математика, автоматика» (Суми-Астана, 2023 р.) Міжнародна науково-технічна конференція студентів та молодих учених «Інформатика, математика, автоматика» (Суми-Астана, 2024 р.)

За темою дисертаційної роботи опубліковано 10 наукових праць, з них: 4 статті у наукових фахових виданнях України, з яких 2 включені до міжнародних наукометричних баз (у тому числі, одна стаття у виданні, що індексується міжнародною наукометричною базою Scopus), 4 публікації за матеріалами конференцій, 2 патенти на корисну модель.

Ключові слова: інформаційні технології, інформаційні системи, математичні моделі, методи шифрування, методи дешифрування, криптографія, функції

дійсної змінної, функції непропорційності, захист інформації, розпізнавання сигналів, криптостійкість, обчислювальна складність

ABSTRACT

Bondarenko M. O. Models and methods of information technology for creating cryptosystems based on functions of real variables. – Qualifying scientific work on manuscript rights.

Dissertation for the Doctor of Philosophy degree in the specialty 122 Computer Science. Sumy State University, Ministry of Education and Science of Ukraine, Sumy, 2024.

An important scientific and practical task of developing new models and methods of cryptographic systems based on functions of a real variable is solved in the dissertation work.

The relevance of the topic of the dissertation is justified, the connection of the work with scientific topics is indicated, the goal and tasks of the research are formulated, the object, subject and methods of the research are defined, the scientific novelty and practical significance of the obtained results, the approbation of the results and their coverage in publications are shown.

The relevance of this study is determined by a set of factors that shape modern challenges in the field of information security and cryptography:

1. Limitations of existing cryptosystems: Most modern cryptographic systems, such as AES and RSA, are based on integer operations. Although these systems are widely used, they face a number of problems. In particular, with the growth of computing power, there is a need to constantly increase the length of keys, which leads to an increase in computing costs. Furthermore, the finite set of integers potentially limits the long-term sustainability of these systems in the face of the development of cryptanalysis techniques.
2. The threat of quantum computing: The development of quantum computers poses a threat to many existing cryptographic algorithms. In particular, Shor's quantum algorithm can efficiently solve the factorization and discrete logarithm

problems underlying the security of RSA and ECC. Thus, the development of quantum computers poses a threat to many cryptographic systems, which prompts fundamentally different mathematical approaches to encryption.

3. The need for new approaches: the analysis of the current state of cryptography shows the active research of new methods on alternative bases, which demonstrates the need for the development of innovative methods of data protection. However, most of these new systems still focus on integers and have their drawbacks.
4. Specificity of image protection: There is a separate field of cryptography aimed at creating systems for image encryption that would allow using the properties of visual data to improve stability. This indicates the need for specialized cryptographic solutions for different types of data.
5. The potential of systems based on real numbers: the use of cryptosystems based on real numbers represents a promising direction of research. Since the power of the set of real numbers is higher than the power of the set of integers, this can potentially provide a larger key space and higher cryptographic strength. However, research in this direction is less widespread and requires further development.
6. Integral cryptography: research in the field of integral cryptography, in particular the use of integral Fredholm equations, opens up new possibilities for creating cryptosystems with theoretically guaranteed stability. This indicates the potential of using new mathematical approaches in cryptography.

Thus, the research of new methods of cryptographic protection based on functions of real variable and integral disproportionality is a relevant and important task. It has the potential to create new cryptographic primitives that could overcome the limitations of existing systems and offer effective solutions for protecting various types of data, including images. The topic corresponds to the current trends in the development of cryptography and has the potential to contribute to the improvement of the security of digital information in the modern world.

The object of research is the processes of cryptographic data protection.

The subject of research are models, methods and algorithms of cryptographic systems based on functions of a real variable.

The selected research methods are based on the principles and methods of cryptography, signal recognition methods, and disproportionality functions.

The purpose of the research is to develop new models and methods of cryptosystems based on functions of a real variable to increase the stability and efficiency of encryption of both text data and images.

The following tasks were set and solved in the work:

1. An analysis of modern cryptographic systems, their advantages and disadvantages was carried out.
2. A mathematical model of cryptosystems based on functions of a real variable has been developed.
3. A data encryption method was created using the sum of functions of a real variable as symmetric keys.
4. A method of decrypting data encrypted by calculating unknown coefficients of key functions has been developed.
5. Adapted developed methods for encryption and decryption of images.
6. An algorithm for using an image as a cryptographic key for encrypting other images has been developed.
7. The software implementation of the developed cryptosystems was created and experimental studies of their effectiveness were conducted.

The practical significance is the results allow the practical implementation of the proposed cryptosystems. All the theoretical developments of the thesis have been brought to concrete engineering methods and algorithms by the author, using the proposed information technology of encryption and decryption of data using functions of real variables. The obtained results allow the practical implementation of the proposed cryptosystems. The proposed cryptosystem for image protection using an arbitrary image as a key can be applied to the experimental protection of visual information in various fields. The created software for the implementation of the developed cryptographic algorithms can be used for further research and experiments

in the field of cryptography based on the functions of a real variable. The results of experimental studies of cryptoresistance of the developed methods can be used for comparative analysis of different approaches to encryption.

The scientific novelty is that the dissertation solved an important scientific and practical problem of creating models and methods of cryptographic systems based on functions of a real variable, and the following results were obtained:

1. Models and methods of creating cryptosystems based on functions of a real variable have been improved, which leads to an increase in cryptoresistance.

2. For the first time, a method of using integral functions of disproportionality for data decryption was developed, which allows the use of discrete key functions in the cryptosystem.

3. For the first time, a cryptosystem was developed that combines encryption using the sum of functions of a real variable and encryption using the integral function of disproportionality. A two-stage encryption takes place, in which the result of the first stage is encrypted again, which makes it significantly more difficult to crack the cryptosystem.

4. The method of data encryption has been improved by introducing an additional element of permuting key functions, which also increases the crypto-resistance of the system.

5. For the first time, a cryptosystem was developed to protect images, where another arbitrary image is used as a cryptographic key, by using integral disproportionality functions. This greatly simplifies the transfer of the key compared to the transfer of key functions in analytical form. This image is easier to transmit inconspicuously to the receiving party when using symmetric cryptosystems. In addition, it is more difficult for an attacker to identify the key image among the many images he has accessed.

6. The high cryptoresistance of the developed encryption methods to brute force attacks due to the need to select key values with high accuracy was experimentally demonstrated. A high ability to decorrelate ciphertext values has also been demonstrated.

The dissertation corresponds to the priority areas of scientific research of Sumy State University. The study was carried out in accordance with the plan of research works under the state budget topic "Methods, mathematical models and information technologies of analysis and synthesis of information communication systems" (DR No. 0118U006971, 2018-2023). The role of the author in this research work was to develop models and methods of encryption and decryption of data for use in information communication systems.

The research results of the dissertation work were reported and discussed at international scientific and practical conferences. International Scientific and Practical Conference "INFORMATION SECURITY AND INFORMATION TECHNOLOGIES" (Odesa, 2021) International Scientific and Technical Conference of Students and Young Scientists "Informatics, Mathematics, Automation" (Sumy-Astana, 2022) International Scientific and Technical Conference conference of students and young scientists "Informatics, mathematics, automation" (Sumi-Astana, 2023) International scientific and technical conference of students and young scientists "Informatics, mathematics, automation" (Sumi-Astana, 2024)

10 scientific works have been published on the topic of the dissertation, including: 4 articles in scientific specialized publications of Ukraine, of which 2 are included in international scientometric databases (including one article in a publication indexed by the international scientometric database Scopus), 4 publications on materials conferences, 2 patents.

Keywords: information technologies, information systems, mathematical models, encryption methods, decryption methods, cryptography, functions of a real variable, integral disproportionality functions, image encryption, information security, signal recognition, cryptostrength, computational complexity

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації:

Статті у наукових фахових виданнях України

[1] V. Avramenko and M. Bondarenko, “Recognition of reference signals and determination of their weighting coefficients if an additive interference presents,” *Radio Electronics, Computer Science, Control*, p. 73, Oct. 2023, doi: 10.15588/1607-3274-2023-3-8.

(Особистий внесок автора.: Розроблено методи комп’ютерного моделювання системи розпізнавання еталонного сигналу при накладанні завади, проведено аналіз результатів розпізнавання у випадках накладання частот)

(Особистий внесок Авраменко В.В.: Розроблена математична постановка задачі, створена математична модель та методи розпізнавання еталонного сигналу при накладанні завади, проведений аналіз різних випадків накладання завади)

[2] V. Avramenko and M. Bondarenko, “Encryption of messages by the sum of a real variable functions.” *Stuc.intelekt*, vol. 29, pp. 10–19, Jun. 2024, doi: 10.15407/jai2024.02.010.

(Особистий внесок автора: Проведена розробка методу шифрування повідомлень сумою функцій дійсної змінною з застосуванням схеми перестановки функцій-ключів, розроблені методи комп’ютерного моделювання, проведений аналіз результатів на предмет декореляції шифротексту)

(Особистий внесок Авраменко В.В.: Розроблена математична постановка задачі, проведено концептуалізацію підходу, створена математична модель зашифрованого повідомлення)

[3] V. Avramenko and M. Bondarenko, “Encrypting images using the sum of the functions of a real variable,” *Transactions of Kremenchuk Mykhailo Ostrohradskyi National University*, vol. 144, no. 1, pp. 140–147, 2024, doi: 10.32782/1995-0519.2024.1.18. *(Особистий внесок автора: розроблений спосіб застосування*

алгоритму шифрування повідомлень сумою функцій дійсної змінною для захисту візуальних даних, розроблені методи комп'ютерного моделювання)

(Особистий внесок Авраменко В.В.: розроблена математична постановка задачі, створену математична модель зашифрованого повідомлення, проведений аналіз результатів)

[4] V. Avramenko and M. Bondarenko, "Image cryptosystem with image key using integral disproportion," *Radioelectronic and Computer Systems*, vol. 2024, pp. 147–159, Apr. 2024, doi: 10.32620/reks.2024.2.12.

(Особистий внесок автора: розроблені моделі та методи створення криптосистем для захисту зображення використовуючи інше зображення в якості криптографічного ключа, розроблені алгоритми шифрування та дешифрування зображення з використанням інтегральних функцій непропорційності, проаналізовані граничні випадки їх використання, розроблені моделі комп'ютерного моделювання, проведено верифікацію коректності роботи запропонованих методів, проаналізовано результати на предмет стійкості методу до атак грубої сили, проаналізовано здатності запропонованого метода до декореляції шифротексту.)

(Особистий внесок Авраменко В.В.: проведено концептуалізацію підходу, розроблена математична постановка задачі)

Опубліковані праці апробаційного характеру

[5] V. Avramenko and M. Bondarenko, "Using the Sum of Real Type Functions to Encrypt Messages," in *CEUR Workshop Proceedings*, presented at the 3rd International Conference on Information Security and Information Technologies (ISecIT 2021), Odesa, Ukraine, September 13-19, 2021, p. 10-17. Available: https://ceur-ws.org/Vol-3200/paper2.pdf

(Особистий внесок автора: проведена розробка методів дешифрування з використанням функцій інтегральної непропорційності першого порядку,

розроблені методи комп'ютерного моделювання, проведена верифікація коректності роботи та аналіз результатів.)

(Особистий внесок Авраменко В.В.: проведено концептуалізацію підходу, розроблена математична постановка задачі, створено модель зашифрованого повідомлення)

[6] V. Avramenko and M. Bondarenko, "Combined encryption system using the sum of functions of a real variable," presented at the The International Scientific and Technical Conferences of Students and Young scientists "Informatics. Mathematics. Automation," Sumy - Astana, April 18-22, 2022, p. 71. [Online] Available: https://essuir.sumdu.edu.ua/bitstream-download/123456789/87782/1/Conf_IMA_2022.pdf

(Особистий внесок автора: розроблено моделі та методи поєднання шифрування сумою функцій дійсної змінної та функцією інтегральної непропорційності першого порядку.)

(Особистий внесок Авраменко В.В.: розроблена математична постановка задачі, розроблені моделі комп'ютерного моделювання, проведено верифікацію коректності роботи запропонованих методів)

[7] V. Avramenko and M. Bondarenko, "Signal recognition and calculation weighting coefficients in the presence of additive interference," presented at the The International Scientific and Technical Conferences of Students and Young scientists "Informatics. Mathematics. Automation," Sumy - Astana, April 24-28, 2023, p. 81-82. [Online] Available: https://drive.google.com/file/d/1YDGNhbgZY6dfsqwN6P0BcEpcq6CuCKmj/view

(Особистий внесок автора: розроблено методи комп'ютерного моделювання системи розпізнавання еталонного сигналу при накладанні завади, проведено аналіз розпізнавання у випадках накладання частот)

(Особистий внесок Авраменко В.В.: Розроблена математична постановка задачі, створена математична модель та методи розпізнавання еталонного

сигналу при накладанні завади, проведений аналіз різних випадків накладання завади)

[8] V. Avramenko and M. Bondarenko, “Image encryption with key-image using integral disproportion,” presented at the The International Scientific and Technical Conferences of Students and Young scientists “Informatics. Mathematics. Automation,” Sumy - Astana, April 22-29, 2024, p. 38–39. [Online] Available: https://drive.google.com/file/d/1jjUd3KWmCmrPnOXTnZZSGbZIbsWWBPzU/view

(Особистий внесок автора: проведений аналіз існуючих методів шифрування зображень, розроблені моделі та методи створення криптосистем для захисту зображення використовуючи інше зображення в якості криптографічного ключа, розроблені алгоритми шифрування та дешифрування зображення з використанням інтегральних функцій непропорційності, розроблені моделі комп’ютерного моделювання, проведено верифікацію коректності роботи запропонованої криптосистеми, проаналізовано результати на предмет стійкості до атак грубої сили, проаналізовано здатності запропонованого метода до декореляції шифротексту.)

(Особистий внесок Авраменко В.В.: проведено концептуалізацію підходу, розроблена математична постановка задачі)

Наукові праці, які додатково відображають наукові результати дисертаційної роботи

[9] Пат. 153107 U Україна, МПК (2023.01) H04L 9/00. Спосіб шифрування графічних зображень / В. В. Авраменко, М. О. Бондаренко (Україна); заявник та патентовласник Сумський державний університет. - № u202201970; заявл. 10.06.2022; опубл. 24.05.2023, Бюл. № 21. 5 с.

(Особистий внесок автора: розроблений спосіб застосування алгоритму шифрування повідомлень сумою функцій дійсної змінною для захисту візуальних даних, розроблені методи комп’ютерного моделювання)

(Особистий внесок Авраменко В.В.: розроблена математична постановка задачі, створену математична модель зашифрованого повідомлення, проведений аналіз результатів)

[10] Пат. 147560 U Україна, МПК G09C 1/00 H04L 9/16 (2006.01). Спосіб шифрування даних за допомогою суми функцій дійсної змінної / В.В. Авраменко, М.О. Бондаренко, Т.В. Лаврик (Україна); заявник та патентовласник Сумський держ. ун-т. - № u202008363; заявл. 28.12.2020; опубл.19.05.2021, бюл. №20

(Особистий внесок автора: Проведена розробка моделей та методів шифрування та дешифрування)

(Особистий внесок Авраменко В.В.: Проведено концептуалізацію підходу, розроблена математична постановка задачі дешифрування, проведена розробка моделей та методів шифрування та дешифрування)

(Особистий внесок Лаврик Т.В.: розроблені моделі комп'ютерного моделювання, проведено верифікацію коректності роботи запропонованих методів)

ЗМІСТ

ВСТУП

Актуальність теми.

Актуальність даного дослідження зумовлена комплексом факторів, що формують сучасні виклики у сфері інформаційної безпеки та криптографії:

1. Обмеження існуючих криптосистем: Більшість сучасних криптографічних систем, таких як AES та RSA, базуються на операціях з цілими числами. Хоча ці системи широко використовуються, вони стикаються з низкою проблем. Зокрема, зі зростанням обчислювальної потужності виникає необхідність постійного збільшення довжини ключів, що призводить до зростання обчислювальних витрат. Крім того, кінцевий набір цілих чисел потенційно обмежує довгострокову стійкість цих систем перед розвитком методів криптоаналізу.

2. Загроза квантових обчислень: Розвиток квантових комп’ютерів створює загрозу для багатьох існуючих криптографічних алгоритмів. Зокрема, квантовий алгоритм Шора може ефективно вирішувати проблеми факторизації та дискретного логарифму, на яких базується безпека RSA та ECC. Так, розвиток квантових комп’ютерів становить загрозу для багатьох криптографічних систем, що підштовхує до принципово інших математичних підходів до шифрування

3. Потреба в нових підходах: Аналіз сучасного стану криптографії показує активні дослідження нових методів на альтернативних засадах, що демонструє потребу в розробці інноваційних способів захисту даних. Однак, більшість з цих нових систем все ще зосереджені на цілих числах і мають свої недоліки.

4. Специфіка захисту зображень: Існує окремий напрямок криптографії, спрямований на створення систем для шифрування зображень, що дозволяли б використовувати властивості візуальних даних для покращення стійкості. Це вказує на потребу в спеціалізованих криптографічних рішеннях для різних типів даних.

5. Потенціал систем на основі дійсних чисел: Використання криптосистем на основі дійсних чисел представляє перспективний напрямок досліджень. Оскільки потужність множини дійсних чисел вища за потужність множини цілих чисел, це потенційно може забезпечити більший простір ключів та вищу криптографічну стійкість. Однак, дослідження в цьому напрямку є менш розповсюдженими і потребують подальшого розвитку.

6. Інтегральна криптографія: Дослідження в області інтегральної криптографії, зокрема використання інтегральних рівнянь Фредгольма, відкривають нові можливості для створення криптосистем з теоретично гарантованою стійкістю. Це вказує на потенціал використання нових математичних підходів у криптографії.

Таким чином, дослідження нових методів криптографічного захисту на основі функцій дійсної змінної та інтегральної непропорційності є актуальним та важливим завданням. Воно має потенціал для створення нових криптографічних примітивів, які могли б подолати обмеження існуючих систем, та запропонувати ефективні рішення для захисту різних типів даних, включаючи зображення. Тема відповідає сучасним тенденціям розвитку криптографії та має потенціал для внеску у підвищення безпеки цифрової інформації в сучасному світі.

Зв’язок роботи з науковими програмами, планами та темами.

Дисертаційну роботу виконано на кафедрі комп’ютерних наук Сумського державного університету відповідно до плану науково-дослідних робіт за держбюджетними темами: «Методи, математичні моделі та інформаційні технології аналізу і синтезу інфокомунікаційних систем» (ДР № 0118U006971, 2018-2023). Роль автора в цій науково-дослідній роботі полягала в розробці моделей та методів шифрування і дешифрування даних для застосування в інфокомунікаційних системах.

Мета і завдання дослідження.

Метою дослідження є розробка нових моделей та методів криптосистем на основі функцій дійсної змінної для підвищення стійкості та ефективності шифрування як текстових даних, так і зображень.

Для досягнення мети дослідження необхідно вирішити такі **завдання**:

1. Провести аналіз сучасних криптографічних систем, їх переваг та недоліків. Зокрема, звернути увагу на криптосистеми на основі дійсних чисел. Також, дослідити

2. Розробити математичну модель криптосистеми на основі функцій дійсної змінної, яка дозволяє використовувати переваги потужності множини дійсних чисел для підвищення криптостійкості.

3. Створити метод шифрування даних з використанням суми функцій дійсної змінної як симетричних ключів.

4. Розробити метод дешифрування даних, які зашифровані за обчислення невідомих коефіцієнтів ключових функцій.

5. Адаптувати розроблені методи для шифрування та дешифрування зображень, враховуючи специфіку візуальних даних.

6. Розробити алгоритм використання зображення як криптографічного ключа для шифрування інших зображень на основі запропонованих методів.

7. Створити програмну реалізацію розроблених криптосистем

8. Провести експериментальні дослідження їх ефективності.

Об’єктом дослідження є процеси криптографічного захисту даних.

Предметом досліджень є моделі та методи та алгоритми криптографічних систем на основі функцій дійсної змінної.

Методи дослідження базуються на принципах і методах криптографії, розпізнавання сигналів і функціях непропорційності.

Наукова новизна одержаних результатів:

1. Удосконалено моделі та методи створення криптосистем на основі функцій дійсної змінної.

2. Уперше впроваджено метод дешифрування шляхом використання інтегральних функцій непропорційності, що дозволяє визначати невідомі коефіцієнтів в сумі функцій дійсної змінної.

3. Уперше розроблено комбіновану криптосистему, яка поєднує шифрування за допомогою суми функцій дійсної змінної та шифрування за допомогою інтегральної функції непропорційності.

4. Удосконалено метод шифрування даних шляхом впровадження додаткового елементу перестановки функцій-ключів.

5. Уперше розроблено криптосистему для захисту зображень на основі функцій дійсної змінної шляхом використання функцій інтегральної непропорційності, де інше довільне зображення використовується в якості криптографічного ключа.

Практичне значення отриманих результатів.

Усі теоретичні розробки дисертації автором доведено до конкретних інженерних методик, алгоритмів, з використанням запропонованої інформаційної технології шифрування та дешифрування даних за допомогою суми функцій дійсних змінних. Отримані результати дозволяють практичну реалізацію запропонованих криптосистем. Запропонована криптосистема для захисту зображень з використанням довільного зображення як ключа може бути застосована для експериментального захисту візуальної інформації в різних сферах. Створене програмне забезпечення для реалізації розроблених криптографічних алгоритмів може бути використане для проведення подальших досліджень та експериментів в області криптографії на основі функцій дійсної змінної. Результати експериментальних досліджень криптостійкості розроблених методів можуть бути використані для порівняльного аналізу різних підходів до шифрування.

Особистий внесок здобувача. Дисертаційна робота є самостійним завершеним науковим дослідженням. Положення і результати, винесені на захист дисертаційної роботи, отримані здобувачем особисто. [1], [2], [3], [4], [5], [6], [7], [8], [9], [10]

Апробація роботи. Результати досліджень дисертаційної роботи доповідалися та обговорювалися на таких національних та міжнародних конференціях:

Міжнародна науково-практична конференція «ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ»(м. Одеса, 2021 р.) Міжнародна науково-технічна конференція студентів та молодих учених «Інформатика, математика, автоматика» (Суми-Астана, 2022 р.) Міжнародна науково-технічна конференція студентів та молодих учених «Інформатика, математика, автоматика» (Суми-Астана, 2023 р.) Міжнародна науково-технічна конференція студентів та молодих учених «Інформатика, математика, автоматика» (Суми-Астана, 2024 р.)

Публікації. За темою дисертаційної роботи опубліковано 10 наукових праць, з них: статей у наукових фахових виданнях України – 4, з яких 2 включені до міжнародних наукометричних баз; публікацій за матеріалами конференцій – 4.

Структура та обсяг дисертації. Дисертація складається зі вступу, чотирьох розділів, висновків, списку використаних джерел і одного додатку. Загальний обсяг дисертації складає 170 сторінок (6.7 друкованих аркушів), з яких анотація на 5 сторінках (0.22 друкованих аркуша), основна частина на 182 сторінках (4.8 друкованих аркушів), список використаних джерел із 182 найменувань на 20 сторінках (0.9 друкованих аркушів), і додаток на 3 сторінках (0.15 друкованих аркушів).

РОЗДІЛ 1. ЛІТЕРАТУРНИЙ ОГЛЯД КРИПТОСИСТЕМ

1.1. Огляд криптографії

У цьому огляді розглядаються різні типи криптографії, включаючи симетричні та асиметричні системи, методи шифрування тексту, зображень, чи бінарних даних. Досліджується, як квантові обчислення можуть вплинути на поточні методи шифрування, і розглядає нові підходи, які розробляються у відповідь. Особлива увага приділяється методам шифрування зображень, які стають більш важливими, оскільки візуальні дані стають все більшою частиною нашого цифрового життя. Цей огляд закладає основу для впровадження нового криптографічного методу, заснованого на функціях дійсних чисел із використанням інтегральної диспропорції. Цей підхід потенційно можна використовувати як для шифрування тексту, так і для зображення. Досліджуючи сучасні методи та проблеми в криптографії, показується потенціал нових підходів, і те, як вони вписуються в ширшу картину захисту цифрової інформації.

У нашому все більш цифровому світі необхідність захисту даних стала першорядною. Оскільки організації та окремі особи все більше покладаються на цифрові платформи для спілкування, фінансових операцій і зберігання конфіденційної інформації, ризики, пов’язані з витоком даних і несанкціонованим доступом, різко зросли. Відповідно до звіту IBM, середня вартість витоку даних у 2021 році становила 4,24 мільйона доларів США, що підкреслює значні фінансові наслідки неадекватної безпеки даних [11]. Крім того, поширення пристроїв Інтернету речей (IoT) і хмарних обчислень розширило поверхню атак, зробивши надійні заходи захисту даних більш важливими, ніж будь-коли [12].

Одним із підходів до захисту даних є стеганографія, метод приховування самого факту існування прихованої інформації всередині даних, які не викликають підозри - зображення, аудіофайли чи навіть мережеві пакети. У той час як криптографія робить дані недоступними без ключа доступу, стеганографія

має на меті зробити саму присутність конфіденційних даних невиявленою [13]. Наприклад, секретне повідомлення може бути вбудовано в найменш значущі біти файлу зображення, які є візуально непомітними. Також, існують спеціально спроектовані стенографічні файлові системи, такі як StegFS, які дозволяють приховувати дані в невикористаних ділянках секторів чи файлів [14]. Однак поява дедалі складніших алгоритмів стеганоаналізу знизила надійність стеганографічних систем [15]. Отже, хоча стеганографія може забезпечити додатковий рівень безпеки, вона, як правило, не вважається достатньою сама по собі для захисту конфіденційної інформації. Це обмеження підкреслює постійну потребу в надійних криптосистемах, здатних протистояти як спробам виявлення, так і дешифруванню.

Тому, саме криптосистеми є основоположними елементами сучасної безпеки даних, розробленими для захисту інформації шляхом перетворення її в нечитабельний формат для неавторизованих сторін. За своєю суттю криптосистеми складаються з алгоритмів шифрування, алгоритмів дешифрування та ключів. Алгоритм шифрування перетворює відкритий текст (оригінальне повідомлення, plaintext) у зашифрований текст (зашифроване повідомлення, ciphertext) за допомогою ключа, тоді як алгоритм дешифрування повертає цей процес. Ключові поняття в криптографії включають конфіденційність (зберігання даних у таємниці), цілісність (переконання, що дані не були підроблені), автентифікацію (підтвердження особи залучених сторін) і неспростовність (запобігання відмові в надсиланні повідомлення) [16]. Безпека криптосистеми часто залежить від обчислювальної складності певних математичних задач, таких як факторизація цілих чисел або дискретних логарифмів [17].

У міру розвитку технологій криптосистеми змушені розвиватися, щоб підтримувати свою ефективність проти все більш складних атак і нових загроз, таких як квантові обчислення [18].

Традиційно, більшість існуючих криптосистем базуються на множині цілих чисел. Цей підхід отримав перевагу через точну природу цілочисельної

арифметики та добре встановлені математичні теорії щодо вже згаданих задач розкладання на множники та дискретних логарифмів. Однак можливі альтернативні підходи, засновані на різних математичних структурах. Один із таких підходів включає криптосистеми, засновані на дійсних числах або функціях дійсних чисел. Оскільки потужність множини дійсних чисел вища за потужність множини цілих чисел [19], цю властивість можна використати для підвищення стійкості криптосистеми.

Криптосистеми можна розділити на симетричні, які використовують один і той же ключ для шифрування та дешифрування, та асиметричні, які використовують різні ключі для шифрування та дешифрування.

1.2. Симетричні криптосистеми

Симетричні криптосистеми, також відомі як криптосистеми з секретним або закритим ключем, утворюють основу багатьох сучасних рішень для шифрування даних. Спільний ключ шифрування/дешифрування має бути відомим сторонами, які обмінюються інформацією, але зберігатися в секреті від всіх інших. Симетричні алгоритми, як правило, швидші та ефективніші з точки зору обчислень, ніж їхні асиметричні аналоги, що робить їх ідеальними для шифрування великих обсягів даних [20].

Симетричні криптосистеми загалом класифікуються на дві основні категорії: блокові шифри та потокові шифри, кожна з яких має відмінні робочі характеристики. Блокові шифри працюють з блоками даних фіксованого розміру, як правило, 64 або 128 біт, перетворюючи весь блок за раз за допомогою певного ключа. Ці шифри можуть працювати в різних режимах, таких як Electronic Codebook (ECB), Cipher Block Chaining (CBC) або Counter (CTR), кожен з яких пропонує різні властивості безпеки та варіанти використання. Блокові шифри, як правило, є кращими для шифрування великих обсягів даних і широко використовуються в захищених протоколах зв’язку. З іншого боку, потокові шифри генерують псевдовипадковий потік ключів, який

комбінується (зазвичай за допомогою операції XOR) з відкритим текстом біт за бітом або байт за байтом. Потокові шифри зазвичай швидші та мають нижчу апаратну складність, що робить їх придатними для програм, де дані передаються безперервним потоком або де низька затримка є вирішальною. Вони часто використовуються в системах реального часу та середовищах з обмеженими ресурсами. Вибір між блоковим і потоковим шифруванням залежить від конкретних вимог програми.

Загальні приклади симетричних систем включають включають розширений стандарт шифрування (AES), який став стандартом де-факто для симетричного шифрування після раніше широко використовуваного стандарту шифрування даних (DES). Інші відомі алгоритми включають Twofish, Serpent, ChaCha20 та інші. Незважаючи на свою ефективність, симетричні системи стикаються з проблемами розподілу ключів і керування ними. Крім того, безпека симетричних систем часто залежить від довжини ключа, причому довші ключі зазвичай забезпечують сильніший захист, але вимагають більше обчислювальних ресурсів. Так, алгоритмічна складність підбору ключа методом брутфорсу складає $O(2^k)$, де k - довжина ключа в бітах. Щоб усунути деякі з цих обмежень, сучасні криптографічні протоколи часто використовують симетричні та асиметричні методи в парі, використовуючи переваги кожного підходу. Прикладом такого тандему є протокол TLS.

1.2.1. Традиційна симетрична криптографія

До традиційних блокових та потокових шифрів можна включити наступні: DES, 3DES, AES, ДСТУ ГОСТ 28147 – 2009, Twofish, ChaCha20, та Інші

DES. Стандарт шифрування даних (DES) [21] — це блочний шифр із симетричним ключем, який колись був наріжним основою криптографічних систем у всьому світі. Розроблений IBM на початку 1970-х років і прийнятий як федеральний стандарт у Сполучених Штатах у 1976 році, DES шифрує дані 64-бітними блоками за допомогою 56-бітного ключа. Алгоритм використовує 16-раундову мережеву структуру Фейстеля, яка була новаторською на момент свого

впровадження [22]. DES швидко став світовим стандартом для комерційних і фінансових програм, захищаючи величезні обсяги конфіденційних даних. Однак із зростанням обчислювальної потужності відносно коротка довжина ключа DES стала значною вразливістю. До кінця 1990-х років спеціалізоване обладнання вже могло зламати DES за допомогою брутфорсу за відносно короткий час. Це призвело до розробки Triple DES (3DES), який пізніше був замінений на AES. Основні недоліки DES включають його коротку довжину ключа, вразливість до диференціального та лінійного криптоаналізу, а також наявність слабких ключів, які створюють легкозламні зашифровані тексти [23]. Незважаючи на це, DES відіграв вирішальну роль у розвитку сучасної криптографії, і його принципи розробки продовжують впливати на сучасні алгоритми шифрування.

3DES. Потрійний DES (3DES), також відомий як TDEA (Triple Data Encryption Algorithm), був розроблений як більш безпечний варіант оригінального алгоритму DES. 3DES, представлений у середині 1990-х років, мав на меті усунути вразливості DES, не вимагаючи абсолютно нового алгоритму . Метод 3DES застосовує алгоритм шифрування DES три рази до кожного блоку даних, використовуючи два або три різні 56-бітні ключі, в результаті чого ефективна довжина ключа становить 112 або 168 біт [24]. Такий підхід значно збільшив стійкість до атак грубою силою порівняно з одним DES. 3DES отримав широке застосування у фінансових послугах та інших галузях, що вимагають високого рівня захисту даних. Однак 3DES значно повільніший за DES, вимагаючи приблизно в три рази більше обчислювальних ресурсів, що обмежує його застосування. Крім того, незважаючи на те, що 3DES є більш безпечним, ніж DES, він все ще вразливий до певних типів атак, таких як атаки зустрічі посередині, які знижують ефективну безпеку нижче теоретичного максимуму [25]. У результаті, хоча 3DES все ще вважався безпечним для застарілих систем, він був витіснений більш сучасними алгоритмами, такими як AES.

AES. Розширений стандарт шифрування (AES) [26] — це симетричний блоковий шифр, який став глобальним стандартом безпечного шифрування

даних. Розроблений бельгійськими криптографами Деменом і Райменом, алгоритм AES був обраний Національним інститутом стандартів і технологій США (NIST) у 2001 році [27]. AES працює з 128-бітними блоками даних і підтримує розміри ключів 128, 192 або 256 біт. На відміну від свого попередника DES, який використовував мережу Фейстеля, AES використовує мережу заміни-перестановки(Substitution Permutation Network, SPN), що підвищує як швидкодію, так і безпеку. Структура алгоритму складається з декількох раундів чотирьох типів перетворень: SubBytes, ShiftRows, MixColumns і AddRoundKey, причому кількість раундів залежить від розміру ключа. Ефективність алгоритму полягає полягає не тільки в розмірі ключа, але й у стійкості до відомих атак, включаючи диференціальний і лінійний криптоаналіз. AES показує свою ефективність як у програмних, так і в апаратних реалізаціях, що робить його придатним для широкого діапазону пристроїв, від високопродуктивних серверів до пристроїв IoT з обмеженими ресурсами. Широке використання AES зробило його наріжним каменем сучасної криптографії, який, ймовірно, залишатиметься актуальним протягом багатьох років.

І хоча Advanced Encryption Standard (AES) широко вважається безпечним і ефективним, він не є досконалим. Однією з першочергових проблем є потенційна вразливість до атак побічного каналу(side-channel attacks), які використовують радше не слабкі місця алгоритму, а інформацію, отриману під час фізичної реалізації шифру,. Аналіз потужності та електромагнітний аналіз успішно використовувалися для отримання ключів із деяких реалізацій AES [28].

Розклад ключів AES, особливо для 256-бітних ключів, піддавався критиці за те, що він не такий надійний, як основний шифр, що потенційно може призвести до атак із пов’язаним ключем [29]. З точки зору продуктивності, незважаючи на те, що AES загалом ефективний, він може бути обчислювально інтенсивним для деяких програм, особливо в середовищах з обмеженими ресурсами або при обробці великих обсягів даних [30]. Найпомітнішою теоретичною атакою на AES є атака biclique, представлена у 2011 році [31]. Ця

атака може зламати повний AES в 4 рази швидше, ніж брутфорс. Втім, з практичною точки зору такий результат все ще не становить реальної загрози.

Нарешті, саму безальтернативність AES можна розглядати як недолік. Якби практичну атаку було виявлено, вона мала б далекосяжні наслідки для багатьох систем і програм по всьому світу.

ДСТУ ГОСТ 28147 – 2009. ГОСТ 28147-89 (адаптований як ДСТУ ГОСТ 28147 - 2009 в Україні [32]) - симетричний блоковим шифр, розробленим ще в СРСР як стандартний алгоритм шифрування. Цей алгоритм працює з 64-бітними блоками з використанням 256-бітного ключа та базується на структурі мережі Фейстеля з 32 раундами . ГОСТ 28147-89 відрізняється простотою конструкції, яка включає залежні від ключа S-блоки, що робить його потенційно більш стійким до певних типів криптоаналізу порівняно з фіксованими конструкціями S-блоків [33].

ГОСТ 28147-89 має здебільшого історичне значення, а у сучасному криптографічному середовищі піддається дедалі більшій критиці. Незважаючи на велику довжину ключа в 256 біт, яка теоретично забезпечує високу безпеку, алгоритм має кілька помітних недоліків і обмежень. Одне з найбільш значних зауважень — низька продуктивність програмної реалізації. У порівнянні з сучасними шифрами, такими як AES, ГОСТ 28147-89 є значно повільнішим, що робить його непрактичним для багатьох сучасних програм. У алгоритму існують серйозні недоліки, пов’язані з розкладом ключів шифрування. Було продемонстровано, що розклад ключів GOST заслабкий, що уможливлює атаки пов’язаних ключів, які можуть зламати систему швидше, ніж брутфорс [34]. Також, хоча залежні від ключа S-блоки спочатку вважалися сильною стороною, вони також були визначені як потенційна вразливість. Було показано, що погано вибрані S-блоки можуть значно послабити шифр [35]. Відсутність стандартизованих S-блоків у різних реалізаціях може призвести до неузгодженості та потенційної вразливості. Ще одним обмеженням є фіксований розмір блоку в 64 біти, які є меншими, ніж сучасні блоки в 128 і більше біт.

Twofish. Twofish — це симетричний блочний шифр, розроблений як кандидат на конкурс cnfylfhne AES. Незважаючи на те, що його не було обрано як алгоритм AES, Twofish залишається дієвим і безпечним алгоритмом. Він працює на 128-бітних блоках і підтримує розміри ключів 128, 192 і 256 біт [36]. Конструкція Twofish включає елементи з різних криптографічних примітивів, включаючи мережі Фейстеля, залежні від ключа S-блоки та матрицю максимальної відстані (MDS) для дифузії. Однією з визначних особливостей Twofish є його гнучкість; його можна оптимізувати для різних цілей, від впровадження смарт-карт до високошвидкісного програмного забезпечення на великих процесорах. Однак варто зазначити, що Twofish повільніше ніж AES, у програмній реалізації, особливо для малих розмірів даних. Незважаючи на це, Twofish залишається привабливим вибором у деяких програмах [37], здебільшого продуктах з відкритим сирцевим кодом.

ChaCha20. Однією з найсучасніших криптосистем можна назвати шифр “ChaCha20”. Це сучасний симетричний потоковий шифр, розроблений у 2008 році як варіант попереднього шифру Salsa20 [38]. Він розроблений для забезпечення високого рівня безпеки з потужною продуктивністю, особливо в програмних реалізаціях.ChaCha20 працює на 512-бітних станах і використовує 32-бітні слова, що робить його ефективним на 32-бітних і 64-бітних процесорах. Використовуються 256-бітний ключ і 96-бітний nonce (вектор ініціалізації), що дозволяє використовувати велику кількість унікальних шифрувань за допомогою одного ключа[39]. Продуктивність ChaCha20 перевершує AES на багатьох платформах без спеціального апаратного прискорення[40]. Також, алгоритм розроблений таким чином, щоб його було просто правильно реалізувати, зменшуючи ризик недоліків безпеки через помилки реалізації. Попри те, де-факто стандартом шифрування є AES, ChaCha20 широко використовується в програмному забезпеченні, а його популярність зростає. Так, поєднання з аутентифікатором Poly1305 стандартизоване з використанням в протоколі TLS 1.3. Також, IETF рекомендує використання ChaCha20-Poly1305 в багатьох інтернет-протоколах. ChaCha20 підтримується в OpenSSH для шифрування на

транспортному рівні. Алгоритм використовується в багатьох програмних продуктах, таких як месенджери Signal та WhatsApp, в сервісах Google та інших.

Основною причиною вибору на користь ChaCha20 є висока швидкість на платформах без апаратного прискорення AES. Іншою перевагою є стійкість до атаки бічних каналів: конструкція робить його більш стійким до атак на синхронізацію порівняно з табличними шифрами. Також, з ChaCha20 немає потреби в таблицях пошуку: це робить його більш придатним для обмежених середовищ.

Проте, варто розуміти, що попри це AES залишається набагато розповсюдженішим, особливо на системах з апаратним прискоренням, де AES є помітно ефективнішим. На відміну від стандартизованого AES, алгоритм ChaCha20 через відносну новизну не був підданий настільки ж ретельному аналізу. Зазначається, що потокова природа шифру може зробити його більш складним для реалізації в певних режимах роботи порівняно з блоковими шифрами. Крім того, висловлюються певні занепокоєння щодо можливості неправильного використання частини nonce, що може поставити під загрозу безпеку. [41].

Інші. Існує також багато інших симетричним криптосистем з традиційними блоковими шифрами, які не отримали настільки широкого розповсюдження з тих чи інших причин. До таких можна включити системи Serpent, Camellia та RC4.

Алгоритм Serpent, розроблений Андерсоном, Біхамом і Кнудсеном, також був фіналістом конкурсу AES. Це 128-бітний блоковий шифр із підтримкою розміру ключа 128, 192 або 256 біт. Serpent відомий своїм високим запасом безпеки, реалізуючи 32 раунди в порівнянні з 10-14 у AES, що робить його, можливо, більш стійким до майбутніх криптоаналітичних атак. Однак цей консервативний дизайн обходиться ціною продуктивності, оскільки Serpent значно повільніший за AES у більшості реалізацій [42].

Camellia, розроблений спільно Mitsubishi Electric і NTT з Японії, має 128-бітний блоковий шифр, який підтримує ключі довжиною 128, 192 і 256 біт.

Камелія поширена в Японії та рекомендована для використання проектом ЄС NESSIE та ISO/IEC 18033-3 [43], але маловідома у решті світу. Дизайн системи багато в чому схожий на AES, але використовує інший розклад ключів раундів (key schedule) та S-бокси.

RC4 - потоковий шифр, який широко використовувався протягом багатьох років, зокрема в таких протоколах, як SSL/TLS і WEP. Відрізняється простотою і швидкістю програмного забезпечення. Проте протягом багатьох років RC4 піддавався численним криптоаналітичним атакам, що виявило значні недоліки [44]. Ці вразливості призвели до того, що IETF припинив його підтримку в TLS. Найсерйозніші проблеми з RC4 включають зміщення вихідного потоку, які можуть призвести до відновлення відкритого тексту в певних сценаріях, особливо коли той самий відкритий текст шифрується кілька разів. Незважаючи на свій застарілий статус, RC4 продовжує використовуватися в деяких застарілих системах.

Інші застарілі, локальні, спеціалізовані або нерозповсюджені симетричні криптосистеми на основі блокових чи потокових шифрів включають: Blowfish, IDEA, RC5, CAST, Skipjack, TEA, Salsa20, HC-128, Rabbit, SEED, ARIA, MISTY1, KASUMI, PRESENT та інші.

1.2.2. Легковагова криптографія

Окремим напрямком є дослідження легковагової (Lightweight) криптографії. Легка криптографія стала важливою через поширення пристроїв з обмеженими ресурсами в епоху IoT. Так, IoT-пристрої стають все більш поширеними, але стикаються з проблемами безпеки, особливо для пристроїв з обмеженими ресурсами, таких як датчики та мітки RFID. Легка криптографія (LWC) пропонується як рішення для захисту зв’язку для цих пристроїв. Галузь зосереджена на розробці криптографічних алгоритмів, придатних для середовищ з обмеженою обчислювальною потужністю, пам’яттю та енергетичними ресурсами, таких як пристрої Інтернету речей, мітки RFID і сенсорні мережі.

Алгоритми LWC використовують різні підходи: мережі заміни-перестановки (SPN), мережа Фейстеля (FN), узагальнена мережа Фейстеля (GFN), додавання-обертання-XOR (ARX), регістр зсуву з нелінійним зворотним зв’язком (NLFSR) і гібридний. [45] Було розроблено кілька помітних легких блокових шифрів. PRESENT, розроблений спеціально для обмежених апаратних середовищ[46], є одним із найвідоміших. Сімейства SIMON і SPECK, розроблені NSA, пропонують оптимізовані рішення для реалізації апаратного та програмного забезпечення відповідно[47]. SKINNY, легкий блоковий шифр із можливістю налаштування, спрямований на досягнення конкурентоспроможної продуктивності як на апаратних, так і на програмних платформах [48]. У категорії потокових шифрів є Trivium [49]] і Grain [50], призначені для ефективної апаратної реалізації. Lizard — ще один легкий потоковий шифр, розроблений для пристроїв з обмеженим живленням [51].

Основні характеристики легких криптографічних алгоритмів включають менші розміри блоків (часто 64 або 80 біт порівняно зі 128 бітами AES), зменшені розміри ключів (зазвичай від 80 до 128 біт) і простіші функції округлення для мінімізації апаратної складності та енергоспоживання. Багато з цих алгоритмів спеціально розроблені для ефективної апаратної реалізації.

Однак ця сфера стикається з декількома проблемами, зокрема тонким балансом між безпекою та продуктивністю, необхідністю стійкості до атак із побічних каналів у вразливих пристроях, а також постійними зусиллями щодо стандартизації [52]. Вказується, що алгоритми легковісної криптографії все ще стикаються зі складностями у вирішенні питань, пов’язаних зі стійкістю IoT-систем ([53]). В роботі Такор та інших [45] надається комплексний аналіз безпеки, який показує, що більшість алгоритмів легковісної криптографії вразливі до різноманітних атак, особливо атак із пов’язаними ключами. Незважаючи на ці виклики, полегшена криптографія продовжує розвиватися.

1.2.3. Нетрадиційна симетрична криптографія

Існує також широкий напрямок дослідження нетрадиційних засад для створення криптографічних систем. Так, існують чисельні пропозиції створення криптосистем на основі динамічного хаосу, біохімії ДНК, квантових операцій, клітинних автоматів, нейронних мереж, вейвлет-трансформації та інших. Нетрадиційні підходи до симетричної криптографії з'явилися як альтернатива звичайним методам, спрямовані на задоволення потреб безпеки та обчислювальних парадигм.

Криптосистеми на основі хаосу, що використовують властивості хаотичних систем, привертають увагу завдяки своєму потенціалу у створенні складних псевдовипадкових послідовностей, придатних для шифрування [54]. Криптосистеми на основі клітинних автоматів (CA) мають цікаві можливості завдяки паралелізму та простим правилам, які можуть створювати складну поведінку [55]. Однак деякі підходи залишаються більш теоретичними або стикаються з проблемами практичного впровадження. Наприклад, криптографія на основі ДНК, незважаючи на інтригуючі властивості, часто має проблеми з застосовністю в реальному світі [56]. Криптографія на основі нейронних мереж є новою областю, якій потрібен час для розвитку та стандартизації [57]. Подібним чином симетричні системи на основі ранців (задача про ранці) стикалися з уразливістю безпеки в минулому [58]. У ході досліджень ці нетрадиційні підходи продовжують розвиватися, причому деякі перспективні для майбутніх криптографічних застосувань, тоді як інші можуть залишатися головним чином академічним інтересом.

Характерною властивістю більшості робот в цих сферах є зосередження на шифруванні конкретних типів даних, таких як зображення чи текст - на відміну від бінарного підходу AES. Так, більшість пропозицій присвячених хаотичній криптографії, сфокусовані на шифруванні зображень, що пояснюється природою самого методу. Деякі автори адаптують алгоритми і для шифрування тексту [59].

Враховуючи ці особливості, детальний огляд нетрадиційних криптосистем буде проведений в наступних розділах.

1.3. Асиметрична криптографія

Огляд. Для симетричних криптосистем систем існує проблема безпечної передачі ключів безпеки у відкритих системах. В асиметричні системах така проблема відсутня. Асиметрична криптографія, також відома як криптографія з відкритим ключем, — це криптографічна система, яка використовує пари ключів: відкритих ключів, які можуть бути відкрито розповсюджені, та закритих ключів, які відомі лише власнику. Це відрізняється від симетричної закритої криптографії, яка використовує той самий ключ як для шифрування, так і для дешифрування. Таким чином, забезпечується безпечна передача даних без попереднього спільного ключа [61]. Такі системи також уможливлюють такі важливі функції, як цифрові підписи та протоколи обміну ключами [62].

Найпоширеніші асиметричні криптосистеми засновані на математичних проблемах з високої обчислювальною складністю: факторизація цілого числа, задача дискретизації логарифмів, задачі еліптичної кривої.

Асиметрична криптографія повільніша за симетричну, тому її часто використовують для обміну симетричними ключами, які потім використовуються для масового шифрування даних. Цей гібридний підхід поєднує в собі переваги безпеки асиметричних систем зі швидкістю симетричного шифрування [16]. Більшість асиметричних криптосистеми належать до одного з наведених класів: RSA, Криптографія еліптичних кривих (Elliptic Curve Cryptography, ECC), Алгоритм Ел-Гамаля та обмін ключами Діффі-Хеллмана

RSA. Rivest-Shamir-Adleman — одна з перших і найбільш широко використовуваних криптосистем із відкритим ключем, винайдена в 1977 році [62]. Його стійкість базується на практичній складності розкладання добутку двох великих простих чисел, відомої як проблема розкладання на множники. У RSA відкритий ключ складається з двох чисел: n, яке є добутком двох великих

простих чисел p і q, і e, публічного показника. Закритий ключ — d, обчислений за допомогою p, q і e. Щоб зашифрувати повідомлення m, його зводять до степеня e за модулем n. Дешифрування передбачає піднесення шифротексту до степеня d за модулем n [16]. RSA підходить як для власне шифрування, так і для цифрових підписів. Незважаючи на свій вік, алгоритм RSA широко використовується в багатьох сферах, наприклад, в протоколі HTTPS, залишаючись стандартом асиметричної криптографії. Однак, RSA має свої недоліки. Так, алгоритм є повільним порівняно за симетричними системами, що особливо помітно на великих обсягах даних[63]. Також, RSA вимагає ретельного впровадження, щоб уникнути атак побічних каналів [64].

ECC. Криптографія еліптичних кривих — це підхід до криптографії з відкритим ключем, який базується на алгебраїчній структурі еліптичних кривих над кінцевими полями. Запропонований у 1985 році, ECC набув значної популярності завдяки своїй здатності забезпечувати еквівалентну безпеку RSA з набагато меншими розмірами ключів [65]. ECC базується на задачі дискретного логарифмування еліптичної кривої, яка навіть важча, ніж факторизація цілих чисел. Це дозволяє ECC запропонувати такий же рівень безпеки, як і RSA, зі значно коротшими ключами. Основні переваги ECC включають менші розміри ключів, швидші обчислення та менші вимоги до пам’яті та пропускної здатності. Так, система придатна для обмежених середовищ, таких як смарт-карти та пристрої IoT. ECC-шифрування широко застосовується в різних протоколах і стандартах, включаючи TLS, SSH, PGP і Bitcoin. Однак реалізація ECC може бути складною, і вирішальне значення має ретельний вибір параметрів. Так, слабкі криві які можуть поставити стійкість системи під загрозу [65].

Алгоритм Ел-Гамаль. Представлений у 1985 році заснований на обміні ключами Діффі-Хеллмана. Його безпека базується на складності обчислення дискретних логарифмів у скінченному полі [66]. Алгоритм має помітні особливості: Так, він пробалістичний (імовірнисний), тобто один і той самий відкритий текст може перетворюватися в різні шифротексти. Ель-Гамаль може

бути адаптований для роботи з ECC і є основою для інших криптографічних схем, таких як алгоритм цифрового підпису DSA.

Недоліком є те, що шифротекст при цьому вдвічі більший за оригінальне повідомлення. Також, Ель-Гамаль повільніший ніж RSA в шифруванні (однак, швидший в дешифруванні).

Недоліки. В цілому, обчислювальна складність атак грубої сили оцінюється в $O(2^k)$, де k - довжина ключа в бітах. Однак, для зламу асиметричних криптосистемах, існують методи криптоаналізу швидші за повний перебор. Цей факт спонукає використовувати все довші ключі шифрування. Враховуючи відносну повільність, це може бути суттєвим недоліком [60]

1.4. Квантові обчислення і криптографія

Поява квантових обчислень створила серйозні виклики традиційним системам безпеки і може бути передвісником повної зміни парадигми. Хоча квантові комп'ютери все ще знаходяться в зародковому стані, їхній потенціал в криптоаналізі викликав значне занепокоєння в сфері кібербезпеки, [67] .

До прикладу, квантовий алгоритм Гровера пропонує квадратичне прискорення для проблем неструктурованого пошуку. Складність брутфорс-атак на симетричні системи, традиційно складає $O(2^k)$, де k — довжина ключа. Алгоритм Гровера зменшує її до $O(2^{k/2})$ [68] . Це становить загрозу для наявних симетричних криптосистем, фактично вдвічі знижуючи безпеку їх ключів. Такі обставини вимагають подвоєння довжини ключа, щоб підтримувати поточний рівень безпеки. Таке рішення може призвести до підвищення обчислювальної складності і понизити пропускну здатність у багатьох системах. [69].

Загроза для асиметричних систем є ще більшою. Квантовий алгоритм Шора [70] може вирішити проблеми факторизація та дискретного логарифму за поліноміальний час $O(n^3)$, різко ослаблюючи надійність систем RSA та ECC [71].

Слабкість традиційної криптографії та фундаментальні концепти квантової криптографії представлені в роботі Шарбаф [72]. Процес стандартизації PQC NIST є свідченням терміновості розробки квантово-стійких алгоритмів [73]. Ці розробки підштовхнули дослідження в області пост-квантової криптографії та квантово-стійких алгоритмів. Пропоновані рішення варіюються від криптографії на основі решітки та багатоваріантної криптографії до підписів на основі хешування та суперсингулярного обміну ізогенними ключами. Кожен із цих підходів пропонує унікальні властивості безпеки та характеристики

В роботі Євсєєва та інших [74] пропонується використання нециклічних завадостійких кодів на еліптичних кривих у модифікованих криптосистемах McEliece, які не вразливі до атаки Сідельнкова. Інша робота включає впровадження модифікацій, таких як OFM S-бокси для усунення потенційних криптографічних бекдорів [75].

Що цікаво, загроза квантових обчислень стимулює інновації в неочікуваних областях. Наприклад, дослідження криптосистем на дійсних числах, представляє новий підхід, який потенційно може запропонувати опір квантовим атакам [76]. Варто зазначити, що терміни розробки великомасштабних квантових комп’ютерів, здатних зламати поточні криптографічні системи, залишаються невизначеними. Оцінки коливаються від 5 до 30 років. Організації та органи зі стандартизації вже рекомендують гібридні підходи, які поєднують традиційні та постквантові алгоритми для забезпечення стійкості проти класичних і квантових атак [77].

1.5. Криптосистеми на основі дійсних чисел

1.5.1. Використання дійсних чисел в криптографії

Невпинний розвиток обчислювальних потужностей в поєднанні з загрозою квантових обчислень створює потребу в постійних інноваціях у криптографії. Оскільки існуючі криптографічні системи піддаються все більшій перевірці на потенційні вразливості, дослідження нових криптосистем є важливим для

забезпечення довгострокової безпеки. Розробка нових криптосистем допомагає урізноманітнити криптографічний ландшафт, зменшуючи залежність від невеликого набору широко використовуваних алгоритмів. Нові системи можуть пропонувати кращу швидкодію або стійкість, вирішувати нові технологічні виклики. Така еволюція гарантує, що якщо старі системи будуть скомпрометовані, нові, надійніші альтернативи будуть доступні, щоб зайняти їх місце. Абсолютна більшість існуючих криптосистем побудована на основі операцій над цілими числами, або ж над кінцевими полями, отриманими з цілих чисел. Історично, такі методи отримали перевагу через обчислювальну ефективність та ретельну вивченість задач, які лежать в їх основі , таких як факторизація та дискретні логарифми.

Проте, цікавою і перспективною є ідея переходу від цілих чисел до дійсних, оскільки відомо, що потужність множини дійсних чисел більша за потужність множини цілих чисел ([19]). Потужність дійсних чисел справді вища, ніж потужність цілих чисел, оскільки вона незліченно нескінченна на відміну від зліченно нескінченної множини цілих чисел. Відповідно, такі системи потенційно можуть мати вищий простір ключа, безпеку відносно атак грубої сили, кращу захищеність від певних типів атак, і вищу стійкість в цілому [90]. Крім того, системи на основі реальних чисел можуть використовувати властивості безперервної математики, на противагу дискретних системам, що може призвести до появи нових криптографічних примітивів.

Можливості створення таких криптосистем і нові підходи розглянуті у ряді робіт. Наприклад, в 2019 автори Грищук запропонували [91] модель криптосистеми інтегральної криптографії. Основа шифрування і дешифрування зводиться до розв’язання прямої та оберненої задачі, яка описується інтегральним рівням Фредгольма першого роду. Автори вказують на гарантовану теоретичну криптостійкість, яка обумовлюється некоректністю оберненої задачі дешифрування. Крім того, наводиться аргумент щодо того, що сучасні алгоритми криптоаналізу не фокусується на інтегральній криптографії, що відповідно є іншим доказом на користь стійкості запропонованої системи і

інтегральної криптографії в цілому. Втім, поза межами статті залишилися аналіз швидкодії та практичний криптоаналізу представленого методу. Попри це, представлена стаття прекрасно ілюструє потенціал і можливості нових напрямках в криптографії.

В 2003 році Косарев та Тазев та група інших авторів пропонували [92] симетричну криптосистему на основі поліномів Чебишева, як потенційну альтернативу традиційним криптосистемам на основі цілих чисел. Представлена система є математично елегантною і обчислювально ефективною. Однак, аналіз Бергамо та інших [90] показує, що така модель має свої вразливості. В цьому дослідженні автори показали атаку, яка дозволяє зловмиснику відновити відкритий текст із даного зашифрованого тексту без знання закритого ключа. Атака використовує властивості поліномів Чебишева та властивості напівгрупи, якою вони володіють. Більш того, показано що ця вразливість стосується всіх систем, заснованих на якобіанських еліптичних раціональних відображеннях Чебишева, а також пов’язаних схем узгодження ключів і автентифікації, що використовують аналогічні принципи.

1.5.2. Методи на основі функцій непропорційності

Цікавим є клас методів, заснованим на використанні математичного апарату непропорційності. Функції непропорційності були запропоновані більше 20 років тому [93], [94] для вирішення задач діагностики, і з тих пір використовуються для вирішення практичних задач в різних сферах. До перших робіт, в яких описано непропорційності як властивості числових функцій, та в яких запропоновано приклади їх використання, належать статті [93] та [94] в 2000 році. Пізніше, було запропоновано використовувати непропорційності для втілення процесів шифрування і дешифрування.

Так, в 2008 році в патенті [95] була описана система, в якій ASCII-символи шифруються за допомогою суми 10 функцій дійсної змінної, що слугують ключами. Вихідне повідомлення представляється у вигляді числа, яке розкладається в m-розрядний бінарний код, який містить більше ніж одну

одиницю. Кожній ключовій функції передує коефіцієнт, який, в залежності від символа, дорівнює нулю або одиниці. Амплітуди цих функцій випадкові для кожного нового символу. Результуюча сума значень функцій є шифротекстом і передається через канал зв'язку. На приймальній стороні розпізнаються фрагменти функції-ключа, представлені в зашифрованому сигналі, використовуючи функції непропорційності по похідній першого порядку[93]. Завдяки їх властивостям, передані символи розшифровуються в залежності від результатів розпізнавання. Водночас, через використання десяти функцій-ключів та методу розпізнавання, процес дешифрування в цьому методі є доволі затратним. Схожі методи розглядається в роботі Калашнікова та інших ([96]), а також в роботі Калашникової та інших ([97]). В цих двох публікаціях запропонований варіант, де символи зашифровані за допомогою лише трьох ключових функцій дійсної змінної. На відміну від попереднього методу, лише чотири символи шифруються - "1", "0", " "(пробіл) та"" (символ нового рядку), всі інші символи розпізнаються як символ нового рядку. Використовуючи властивості функцій непропорційності по похідній ([98]), розпізнаються коефіцієнти в сумі, і шифротекст розшифровується. Для зламу системи, необхідно підібрати тип і параметри ключових функцій.

Очевидний недолік полягає в цьому, що алфавіт вхідного повідомлення в такому випадку дуже обмежений. В згаданих роботах використовуються функції непропорційності першого порядку по похідній [93]. В цьому випадку, є необхідність застосовувати чисельні методи для розрахунку поточних значень першої похідної. Необхідність таких обчислень призводить до значного розширення обсягу шифротексту порівняно з повідомленням, що шифрується. Також зазначено, що оскільки процес дешифрування може включати ділення на малі числа, результатом може бути число близьке до нуля, що породжуватиме похибки. В такому випадку, автори пропонують перевіряти дешифрування перед передачею шифротекста, що значно ускладнює систему. Крім того, використання непропорційності по похідній накладає ряд відповідних обмежень щодо виду функцій-ключів - вони мають бути неперервно диференційованими,

похідні не мають бути константами і так далі. Варто підмітити, що способи на основі непропорційності по похідних в згаданих роботах описані як для аналогових, так і для дискретних систем.

В роботі [99] використовується інший підхід. Одна функція дійсної змінної слугує ключем. Вираховується функція непропорційності чисельного представлення повідомлення по відношенню до ключової функції. Отримані значення функції непропорційності і є шифротекстом, який передається через канал зв'язку. При цьому, окремо розглянуті два випадки - для дискретних та аналогових повідомлень.

У випадку з дискретними системи (текст, зображення, і т.д.), повідомлення представляється у вигляді дискретної функції. Оскільки така функція не має неперервних похідних, для шифрування використовується інтегральна непропорційність першого порядку [94] відносно функції-ключа. У такому випадку, інтегральна непропорційність також дозволяє уникнути інших недоліків непропорційності по похідних, таких як виникнення невизначеностей та близьких до нуля значень при калькуляціях. Дешифрування відбувається оберненою функцією.

У випадку з аналоговими сигналами, коли і сигнал, і ключова функція є неперервними, гладкими, і мають першу похідну, все ще використовується непропорційність по похідній. Дешифрування виконується вирішенням задачі Коші. Втім, зазначено, що приблизне обчислення значень може породжувати похибки і лавиноподібний ефект, коли все подальше повідомлення буде розшифроване невірно. Тому, метод може потребувати застосування більш точних методів чисельного диференціювання, які є обчислювально обтяжувальними.

Розвиток цієї ідеї представлений у наступній статті [100], де використовуються дві функції ключа для реалізації серійного шифрування. Шифрування складається з двох етапів. На першому етапі використовується шифрування за допомогою інтегральної непропорційності відносно першої функції-ключа, так само як і в попередній роботі. Для другого етапу

запропоновано дві варіації. У першому випадку, до отриманого шифротексту додаються значення другої функції-ключа, що слугує як різновид скремблінгу. У другому варіанті, шифротекст першого етапу повторно шифрується, знову використовуючи інтегральну непропорційність, але цього разу вже відносно другої функції ключа. Таким чином, здійснюється “серійне” шифрування. Запропоновані модифікації мають на меті підвищити складність і стійкість системи за рахунок додаткових операцій.

Комп’ютерне моделювання показало високу чутливість до параметрів ключа і загальну стійкість таких систем в [95] та [96].

1.6. Методи шифрування зображень

Захист зображень є особливо критичним в багатьох сферах, наприклад, таких як:

- IoT [101]
- Шифрування військових мап [102]
- Захист медичних зображень [103]
- Захист відсканованих документів [104] [105]

Для шифрування зображень, як і інших видів даних, цілком можна використовувати традиційні алгоритми [106]. Загальний підхід до захисту зображень включає традиційні симетричні та асиметричні криптосистеми, такі як AES, DES та RSA. Оскільки ці підходи працюють безпосередньо на байтовому представленні даних, вони є агностичними відносно контенту, що означає що вони не вимагають специфічних знань щодо типу чи формату даних, які шифруються. Якими б не були данні, до них можна застосувати алгоритми AES, DES або RSA, що дозволяє шифрувати різноманітні типи контенту, включаючи зображення.

Водночас, природа даних значно впливає на надійність та швидкодію шифрування. Візуальні дані мають яскраво виражені характеристики, що відрізняє їх від інших ([107]).

1. Кореляція між сусідніми пікселями (Adjacent Pixels Correlation) - сусідні пікселі довільного зображення мають схожі значення кольору та яскравості, що може бути використано при аналізі, компресії чи шифруванні зображення.

2. Просторова надмірність (Spatial Redundancy) - Через схожість між сусідніми пікселями часто виникає повторювана інформація у зображенні. Цю надмірність можна використовувати для стиснення зображення шляхом видалення зайвих даних без суттєвого впливу на його якість.

3. Висока ємність (High Capacity) - реальні зображення зазвичай зберігають велику кількість інформації. Наприклад, зображення високої якості мають великий розмір файлу, що відрізняє його від тексту, і має бути враховано при розробці алгоритмів шифрування. [103]

4. Візуальні шаблони (Visual patterns) - зображення часто містять повторювані шаблони або передбачувані структури. Ці шаблони можна використовувати в різних методах обробки зображень.

Незважаючи на те, що для шифрування зображень, як і будь-яких інших даних, можна застосовувати традиційні алгоритми, такий підхід має суттєві недоліки. Так, в дослідження Зеґхід та інших, автори проаналізували вади використання таких алгоритмів як AES для шифрування зображень. Вони підкреслюють важливу проблему з безпекою: Одні і ті ж дані будуть відповідати одному і тому ж значенню шифру. Така проблема особливо поширена в зображення з однорідними зонами, де ідентичні блоки залишаються такими же після шифрування, що призводить до текстурних зон в шифротексті і неоптимальній ентропії. [108]. В цій же роботі представлений варіант рішення такої проблеми. Автори пропонують модифікувати алгоритм AES так, щоб вбудувати в нього генератор потоку ключа (keystream generator). Такий підхід

дозволив би уникнути утворення текстурних зон і пов’язаних з ними проблем. Водночас, наведений аналіз фокусується виключно на чорно-білих зображеннях.

Деякі дослідними інкорпорують традиційні алгоритми в нові методології. Наприклад, в роботі Йе та інших представлена асиметрична криптосистема [109], в якій використовується публічний ключ RSA для генерації початкових значень квантової логістичної мапи. Ці значення уможливлюють створення псевдо-випадкової послідовності потоку ключа. Далі, використовуючи хаотичне відображення (chaotic map) та три-розмірне квантове логістичне відображення (quantum logistic map) уможливлюється значно більший простір ключа для захисту від атак грубої сили.

Окрім традиційних підходів та їх модифікацій, широко досліджуються альтернативні засади, на яких можна побудувати криптосистеми, зокрема для захисту зображень або ж першочергово для захисту зображень. До таких методів належать системи з використанням динамічного хаосу [110], [111], [112], [113] , моделі ДНК [114], [115], [116], [117] , комбінованого клітинного автомату та інших, а також їх модифікацій та комбінацій [117] .

Серед різних підходів до шифрування зображень, також існує ідея використовувати інше зображення в якості криптографічного ключа, що привносить відмінний підхід для забезпечення безпеки шифрування. Комплексність та варіативність зображень може зробити позитивний внесок до розміру та різноманітності простору ключа (key space), посилюючи стійкість до криптографічних атак. Цей метод не тільки привносить додатковий рівень безпеки, але також пропонує інтуїтивний та дружній до користувача підхід, в якому можна обирати візуально значущі зображення [104] .

1.6.1. Криптографія динамічного хаосу

Огляд. Окрім варіацій і модифікацій традиційних підходів, існують також інші класи методів, створених спеціально для обробки зображень. Так, однією з популярних тем для досліджень є вже згадані методи на засадах теорії хаосу.

Зокрема, використання динамічних хаотичних відображень дозволяє створити криптосистеми для шифрування зображень.

Хаотичні криптосистеми використовують властиві хаотичним системам непередбачуваність і чутливість до початкових умов для підвищення безпеки алгоритмів шифрування. Концепція використання теорії хаосу в криптографії була вперше запропонована наприкінці 1980-х та на початку 1990-х років, з ранніми основоположними роботами. Робота Меттьюса ([118]), в якій запропоновано “хаотичний алгоритм шифрування”, а також робота Керролла та Пекори про синхронізацію хаотичних систем ([119]) заклали основу для цієї галузі. На відміну від традиційних криптографічних методів, які спираються на алгебраїчні структури та теорію чисел, хаотичні криптосистеми використовують хаотичні відображення та динамічні системи для генерації складних псевдовипадкових послідовностей, які є дуже чутливими до початкових умов. Ця властивість робить хаотичні криптосистеми придатними в шифруванні зображень, де високий вимірний простір та візуальна складність зображень можуть бути використані для створення безпечних та надійних схем шифрування. В публікації 1998 року Баптіста використав ([120]) логістичні відображення для шифрування також і текстових повідомлень. Після цього, було запропоновано ще ряд шифрів подібного класу. Однак, згодом всі вони були зламані. Також виявилося, що подібні хаотичні криптосистеми не підходить для захисту тексту через ряд недоліків, таких як вірогідність помилки при розшифруванні ([121]).

Хаотична криптографія використовує фундаментальні властивості динамічного хаосу для створення криптографічних систем. — чутливість до початкових умов, детерміновану поведінку та псевдовипадковість. Динамічний хаос стосується поведінки певних нелінійних систем, які демонструють непередбачувані та надзвичайно чутливі реакції на незначні зміни початкових умов. Ця непередбачуваність і складність роблять хаотичні системи придатними для генерації безпечних ключів і шифрування даних. У криптосистемах використовуються хаотичні відображення, такі як логістичне відображення,

відображення Хенона та відображення “кота Арнольда” для перемішування та дифузії даних, забезпечуючи, що навіть незначні зміни вхідних даних призводять до сильних змін в вихідних даних.

Зображення, які мають комплексну структуру з декількома атрибутами, добре узгоджується з властивостями хаотичних систем. Так, зображення мають високу розмірність і комплексу структуру, де кожен піксель має декілька атрибутів (наприклад, чотири атрибути при використанні RGBA схеми) ([122]). Інший аспект полягає в тому, що хаотичні системи мають певні накладні витрати, які можуть бути надмірними при роботі з текстом чи бінарними даними, але бути доречними при роботі з зображеннями, особливо зважаючи на можливості паралелізації ([54]).

Також, передача візуальної інформації дозволяє виконувати часткове (partial) та перцептуальне (perceptual) шифрування, при якому розшифрований об’єкт візуально схожий, але не є повністю ідентичним оригінальному ([123]). Шифрування досягається за допомогою перетворення пікселів зображення обраною хаотичною динамічною системою. Ці процеси знищують внутрішні шаблони в зображенні, роблячи його невпізнаваним без правильного ключа дешифрування. ([124]).

В роботі [110] Вонґ пропонує архітектуру хаотичних криптосистем для шифрування зображень, акцентуючи увагу на процесі заміщення-дифузії, де пікселі зображення перемішуються і їхні значення послідовно змінюються. В [111] Ханчінамані та Кулакарні пропонують нову схему шифрування зображень, використовуючи 2-D хаотичну карту Заславського та псевдо-Гадамардове перетворення, що підвищує безпеку через етапи перестановки та дифузії. В [112] Чен та інші описують нову схему шифрування зображень, яка поєднує перестановку та дифузію в один етап, уникаючи трудомісткого перетворення з плаваючої коми в цілі числа. Використовуючи таблицю пошуку та S-Box AES, схема генерує псевдовипадкові послідовності для дифузії та застосовує комбіновану архітектуру перестановки/дифузії для перемішування та зміни значень пікселів.

Чжан та інші [113] пропонують схему шифрування зображень, використовуючи 4D гіперхаотичну систему в поєднанні з глобальним циклічним зсувом бітів та SHA-256 для генерації початкового ключа. Цей метод підвищує безпеку за рахунок виконання перестановки та дифузії на рівні бітів, змінюючи розподіли пікселів і протидіючи різним атакам. В цьому класу методів також існують варіації і комбіновані системи. В роботі Чоі та інших описана криптосистема, яка поєднує використання хаотичних відображення з алгоритмом комбінованого клітинного автомату (Combined Cellular Automata). [125] Останні роботи в цій сфері включають [126] , [127] і [128].

Хусейн та Ходер в публікації 2023 року[128]. представляє метод шифрування медичних зображень, що використовує мультихаотичні відображення в поєднанні з Triple Data Encryption Standard (3DES). Метод використовує логістичні відображення, а також відображення Арнольда та відображення Бейкера для покращення криптостійкості системи.

Лі та інші в статті 2023 року [127] пропонують метод шифрування кольорових зображень, заснований на динамічній вибірці хаотичної системи та сингулярному розкладі матриць (SVD). Використовуючи нелінійну комбінацію логістичних і синусових хаотичних відображень, у поєднанні з SVD і нейронними мережами, автори представляють нову схему шифрування, яка виконує перемішування та дифузію значень пікселів, створюючи шифровані чорно-білі зображення.

Немах та Шукур в роботі теж 2023 року ([126]) представляють нову тривимірну консервативну хаотичну систему, яка використовує гіперболічні функції для шифрування зображень. Запропонована система використовує модифікований протокол обміну ключами Діффі-Хеллмана та самозворотну матрицю для етапу дифузії. Теоретичний аналіз та симуляція вказує, що метод ефективно протистоїть статистичним атакам та атакам шуму. Водночас, використання гіперболічних функцій та консервативної хаотичної системи може призвести до значних обчислювальних витрат, що потенційно обмежує швидкість та ефективність процесу шифрування. На жаль, аналіз швидкодії

алгоритму в цій та попередній статтях не наведений. Також, складність реалізації нової хаотичної системи та забезпечення точних параметрів може бути проблемним при практичному застосуванні.

Як вказано в оглядовій роботі Жанга та Лю [107], криптосистеми для захисту зображень на основі динамічного хаосу пропонуються використовувати для сфери захисту медичних зображень, для IoT систем та мікроконтролерів, для потенційних мереж 6G, а також для супутникових знімків.

Недоліки. Водночас, як вказано в цій же роботі [107], практичне застосування всього класу хаотичних криптосистем має багато викликів. Через ці недоліки, таки методи поки не отримали широкого застосування. Хоча за останні десятиліття була запропонована велика кількість різних алгоритмів, на даний момент не існує затверджених стандартів, протоколів, та криптографічних фреймворків на основі динамічного хаосу. Комерційне застосування цих методів дуже обмежене (в основному, аналоговими системами) та експериментальне. В багатьох запропонованих системах цього класу після кропіткого криптоаналізу були виявлені проблеми з безпекою. Так, в праці, що оглядає методи атак на хаотичні криптосистеми [129] було замічено, що всі хаотичні системи шифрування зображень, які використовують константні ключи безпеки, є вразливими до криптоатак.

Рума та Сафія [130] проаналізували алгоритми шифрування засновані на гіпер-хаосі. Було виявлено, що вони є вразливими до атак CCA (Chosen-ciphertext attack) та CPA (chosen-plaintext attack). Всього трьох пар тексту і шифротексту (тобто оригінального і зашифрованого зображення) було достатньо для зламу шифрування.

Цілий ряд робіт по криптоаналіз хаотичних систем належить Ченцін Лі. В 2008, він та інші проаналізували [131] симетричний блоковий шифр Паріка з використання одновимірних хаотичних відображень. Було виявлено, що системі притаманна наявність слабких ключей та низька випадковість проміжних даних шифру. Вся система була зламана використовуючи атаку відомого тексту, де

всього лише 120 послідовних байт в оригінальному зображені були відомі. Повідомляється, що модифіковані версії системи мали такі ж самі недоліки.

В роботі 2018 року було проаналізовано [132] хаотичні алгоритми шифрування зображень, заснування на інформаційний ентропії. Результати показують, що такі алгоритми доволі не стійкі до різноманітних типів атак.

В роботі 2019 Лю та Жанґ проаналізували вразливості гіпер-хаотичних систем шифрування на прикладі алгоритму Лі [133] . Було виявлено два моменти - в процесі дифузії не було змін в сірих значень певних пікселів, а також зворотність процесу перестановки.

В цілому, в хаотичних системах виділяють такі недоліки:

1. Чутливість до початкових умов [122], яка може бути як сильною, так і слабкою стороною. Чутливість вимагає дуже високою точності до початкових параметрів, якої може бути складно дотримуватись в цифрових системах, де точність є скінченною.

2. Обмежений простір ключа (key space) - забезпечення достатнього великого простору є критичним для безпеки і напряму впливає на вразливість до атак брутфорсу. Втім, як підмічено в роботі Карі та інших [134], шифрування зображень за допомогою гібридних паралельних хаотичних відображень часто страждає від обмеженого простору ключа.

3. Алгоритми хаотичного шифрування можуть вимагати більших обчислювальних ресурсів, особливо для високо-розмірних хаотичних відображень. Накладні видатки можуть бути значними порівняно з традиційними алгоритмами. В роботі Грищук [91] вказано, що такі системи мають низьку продуктивність шифрування, складну процедуру та задовгий час дешифрування. В дослідженні [135] порівняно швидкодію традиційних систем, зокрема AES, з хаотичними - не на користь останніх.

4. Хаотичні системи є неперервними, але їх цифрові імплементації дискретні - тому дискретизація може призвести до деградації хаотичних властивостей [136].

5. Як було вже наведено [129], [130] , [131], [132] , [133] хаотичні системи можуть бути вразливими до різних видів криптоатак.

6. На відміну від широко визнаних алгоритмів AES та RSA, хаотичним криптосистемам бракує стандартизації. Недостача стандартизації означає відсутність порівнянного рівня ретельного аналізу та тестування, що може означати наявність вразливостей на різних рівнях безпеки [131].

7. Хаотичні системи вимагають точних і зазвичай комплексних ключів. Управління і безпечне розповсюдження таких ключів може бути ускладненим порівняно з ключами традиційних криптосистем [54] .

8. Реалізація хаотичних систем в апаратному забезпеченні може бути проблемною, що ілюструє робота Савед та інших [137].

Через це, динамічний хаос на даний момент не має широкого застосування як повноцінна основа для роботи криптосистем. Однак, він вже застосовується в суміжних сферах - для генераторів псевдовипадкових чисел в модулях апаратної безпеки (HSM), а також для систем управління цифровими правами (DRM) ([138]).

1.6.2. Криптографія на основі ДНК

Огляд. Іншим класом методів нетрадиційних підходів є криптографія на основі ДНК (DNA cryptography). Це спосіб принципово відрізняється від всіх інших, оскільки пропонує використовувати реальні молекули ДНК як сховище даних [139] (на противагу до цифрових носіїв), та хімічні процеси для здійснення операції над ними. Тому, для такого підходу бінарні дані спочатку перетворюються в послідовність ДНК за допомогою спеціально обладнання. Після цього, молекула ДНК шифрується визначеним біохімічним “алгоритмом” і зберігається у відповідних умовах. Для отримання даних назад в цифровому форматі потрібно зробити зворотній процес, декодуючи ДНК. Конкретно, бінарні дані кодуються у послідовності ДНК шляхом відображення дво-бітних бінарних значень (00, 01, 10, 11) на чотири нуклеотиди: Аденін (А), Цитозин (Ц),

Гуанін (Г) і Тимін (Т). Ці закодовані дані зберігаються у фізичних молекулах ДНК та шифруються за допомогою методів, таких як підстановка, де бінарні дані замінюються послідовностями ДНК, і транспозиція, де сегменти ДНК перемішуються. Додаткові специфічні для ДНК операції, такі як сплайсинг, гібридизація, і ампліфікація ПЛР підвищують безпеку ([140], [141]) . Варто зазначити, що незважаючи на переваги високої щільності зберігання, ДНК-криптографія стикається з технічними та вартісними викликами при практичному впровадженні.

Піонерною роботою, що поклала початок обчисленням на основі ДНК, була стаття Адлмана 1994 року [142], в якій він запропонував вирішення проблеми Гамільтонового шлях. Вершини і ребра графу кодувалися в ДНК, і за допомогою біохімічних процесів створювалися ті ДНК молекули, які відповідають вірним гамільтоновим шляхам в графі. Здатності ДНК-операцій до паралелізації дозволяли вирішувати цю задачу набагато швидше, ніж класичні комп’ютерні алгоритми.

В 2003 році, на основі подальших досягнень в сфері ДНК-обчислень Чен запропонував модель біомолекулярної криптосистеми [114]. В ній описується метод шифрування за допомогою перетворень повідомлень карбонових нанотрубок, а також приводяться результати його використання для зображень. Водночас, обсяг даних, який може бути зашифрований цим методом, дуже обмежений.

В роботі 2012 року, Праманік та Сетуа [115] проводять огляд і пропонують новий метод паралелізації шифрування, використовуючи молекулярну структуру ДНК, схему одноразових блокнотів і техніку гібридизації ДНК для оптимізації швидкодії.

В роботі Юнпенга та інших [143] представляється метод шифрування який комбінує ДНК криптографію з блоковими шифрами і теорією хаосу. Алгоритм перетворює текст в ASCII коди, які потім перетворює в послідовність ДНК, використовуючи спеціально техніку відображення. Потім, ці послідовності шифрується індексним методом, який використовує хаотичний генератор ключа

на логістичному відображенні. Варто зазначити, що хоча цей метод комбінує і підсилює переваги означених систем, він також поєднує і їх недоліки. Так, автори вказують на необхідність подальших вдосконалень в використанні ДНК-обчислень і їх біологічних властивостей для подолання недоліків блокових шифрів.

В публікації [144] Мандґе та Чударі презентують метод шифрування на основі ДНК, матричних операцій та надійної генерації ключа. Однак, як зазначено в [116] в роботі описані лише базові операції, а вся надійність системи повністю залежить від ключа.

Серед більш новітніх робіт, є стаття Крішнамурті 2023 року - [145], де надається поєднання ДНК-шифрування з матричною алгеброю. Процес шифрування включає перетворення тексту в ДНК послідовності, використовуючи правила компліментарності, використання транспозиції або XOR операцій з випадково згенерованим ключем-матрицею. Водночас, роботі не вистачає аналізу швидкодії та криптостійкості. Робота Пандей та Чанда [146] представляє нову криптографічну систему ДНК, яка поєднує численні інноваційні методи, такі як ICFM (Index Comparison Flip Mutation), BFM (Bit Flip Mutation), RFS (Rail Fence Straightening), OMB (One-to-Many Breeding), SM (Swap Mutation). Ці методи застосовуються до двійкової форми відкритого текстового повідомлення з наступним кодуванням у бази ДНК, що має підвищувати безпеку та ефективність обчислень. Водночас, аналіз швидкодії та безпеки не наведений, так само як і аналіз стійкості до різноманітних крипто-атак, тоді як багаторівневість алгоритми може збільшувати обчислювальну складність.

Недоліки. Порівняльний аналіз Анвар та інших [116] вказує, що незважаючи на високу ємність ДНК та масивні здатності до паралелізації, цей клас методів має суттєві недоліки. Так, більшість з оглянутих алгоритмів мають зависоку обчислювальну складність по часу, що також підтверджує дослідження Іліясу та інших [147]. Ті ж самі висновки роблять Сінг і Ядай [148], Хазра та інші [149]. Найбільшою проблемою залишається необхідність складного і

високовартісного лабораторного обладнання для роботи з ДНК і її інтеграції зі звичайними цифровими системами [149]. Окремо стоїть необхідність надати теоретичне обґрунтування валідності криптосистем на основі ДНК, а також необхідність в стандартизованих методах оцінки і порівняння таких систем ([143]). Багато з оглянутих методів все ще знаходяться на ранніх етапах розробки - так, для частини ДНК-криптосистем є проблемою сама можливість шифрувати повний набір ASCII-символів. Аналогічно, існує проблема колізій під час дешифрування. [150]. Незважаючи на перспективність та інноваційність, методам криптографії на основі ДНК бракує потужностей для реального використання.

Можна виділити наступні недоліки:

1. Складність імплементації - ДНК-системи вимагають спеціального лабораторного обладнання, що ускладнює їх включення в традиційне обчислювальне оточення.

2. Моделям ДНК-шифрування сильно бракує стандартизації для реального користування, а також детального теоретичного та практичного аналізу.

3. Управління та передача ДНК-ключів набагато складніша, ніж у випадку з цифровми даними.

4. Унікальним для ДНК-криптосистем є також питання біологічної безпеки. Довільні синтетичні ДНК можуть потенційно породжувати біологічну небезпеку.

5. Незважаючи на високу ємність даних при використання ДНК, процеси кодування та декодування інформації біологічними методами зазвичай набагато повільніше електронних систем.

6. Реплікація ДНК та операції над ними можуть природнім чином вносити помилки, що створює загрозу для цілісності даних. Алгоритми та схеми зберігання мають місити механізми корекції таких помилок, що привносить додаткову складність.

7. Молекули ДНК чутливі до умова зберігання, таких як температура та кислотність, що впливає на їх надійність як способу зберігання даних.

8. Ціна матеріалів та обладнання набагато перевищує звичайні електронні компоненти, роблячи такі системи високовартісними.

На даний момент, існує певний інтерес до сфери ДНК-обчислень та використання ДНК для зберігання даних, існує певне експериментальне програмне та апаратне забезпечення. Однак, через означені недоліки та незрілість поточного стану, наразі методи ДНК не використовуються для криптографії, залишаючись теоретичною та експериментальною сферою. На даний момент не існує стандартів, протоколів, чи комерційних продуктів з використанням ДНК-криптографії.

1.6.3. Криптографія на основі Комбінованого Клітинного Автомату

Огляд. Наступним класом методів для шифрування є використання Комбінованого Клітинного Автомату(Combined Cellular Automata, CCA) для побудови криптосистем. Клітинний автомат представляє собою дискретну модель сітки клітин, кожна з яких може знаходиться в кінцевому наборі станів. Ці стани змінюються через певний проміжок часу в залежності від набору правил, які базуються на стані сусідніх клітин. Ця властивість може бути використана для побудови комплексної псевдо-випадкової послідовності, яка підходить для шифрування. Стани клітинного автомату можна використовувати для генерації клітин безпеки, генерування псевдо-випадкових чисел, або для безпосередніх маніпуляцій з текстом.

Концепція клітинного автомату була винайдена ще в 1940х Джоном Фон Нейманом та Станіславом Уламом, однак її застосування в криптографії відносно недавнє [151]. Робота Вольфрама над клітинними автоматами в 1980-х роках заклала основу для їх застосування в криптографії. Його книга [152] досліджує обчислювальну потужність клітинних автоматів . Подальший

потенціал клітинних автоматів розкривається в роботі Менезеса та інших [16]. Комбіновані клітинні автомати можуть генерувати комплексу поведінку з простих заданих правил([153]), що може бути адаптовано для різноманітних криптографічних примітивів (генератори псевдовипадкових чисел, хеш функції, шифри)[154] . Перевагами таких систем є те, що вони можуть бути ефективно реалізовані на апаратному рівні ([55]).

В роботі Серединскі [55] та інших клітинні автомати використовуються для створення симетричної криптосистеми, заснованої на шифрі Вернама. Клітинні автомати використовуються для створення псевдовипадкових послідновностей. Зазначається, що якість цих послідовностей сильно залежить від обраного набору правил. За допомогою техніки клітинного програмування було виявлено новий набір правил, який демонструє кращу стійкість. Однак, роботі не вистачає аналізу складності і швидкодії.

В статті Джон та інших [155] досліджується створення нового потокового шифру “CARPenter”, який використовує лінійне та нелінійне правило для клітинного автомату з 5 сусідами, також відоме як п’ятивалентне правило. Автори демонструють покращення таких криптографічних показників, як дифузія та випадковість. Разом з тим, підвищується обчислювальна складність та вимоги для апаратного забезпечення.

В своїй дисертації Омран [156] досліджує новітню схему шифрування зображень, запроектовану для комунікаційних систем V2X, де одним з прошарків використовується кінцевий автомат. Алгоритм функціонує на трьох рівнях. На першому з них, клітинний автомат з правилом 30 використовується для генерації початково ключа шифрування. Далі, використовуються класичні S-бокси, а після цього використовується ДНК кодування для генерації другого ключа шифрування. Втім, трьохрівневий підхід, хоч теоретично і підвищує надійність, також збільшує обчислювальну складність. Інтеграція прошарку ДНК також привносить в алгоритм всі недоліки, властиві ДНК-криптографії. Крім того, складне управління ключами та можливі накладні витрати можуть вплинути на загальну продуктивність системи.

Робота Сбайтрі та інших пропонує криптосистему спеціально для обмежених в ресурсах вбудованих систем [157]. Метод включає обернені та необернені клітинні автомати для генерації під-ключей. Алгоритм підтримує розмір блоку в 64 біти і довжину ключа в 128 біти, що структуровані в 10 раундів. Обернений двовимірний клітинний автомат використовується для основного процесу шифрування та дешифрування, коли необернений елементарний клітинний автомат використовується для генерації під-ключей. Алгоритм демонструє високий показник дифузії, а також лавинного ефекту. Достатня швидкодія дозволяє використовувати цей метод у вбудованих системах. Серед недоліків можна виділити складність управління ключами - в даному випадку, мова йде про 10 під-ключей замість одного. Також, задовільна продуктивність алгоритм все ще залежить від конкретного апаратного забезпечення вбудованих систем, і може підходити не всім з них.

Робота Дас та інших [158] досліджує новітню криптосистему на основі клітинних автоматів. Метод використовує особливі правила клітинних автоматів, такі як правило 32 і правило 2, які комбінуються з операціями XOR для підсилення безпеки. Система підтримує розмір блоків в 128 біт та розмір ключа в 128, 192, та 256 біт, що виконуються у восьми раундах. Метод показує гарну продуктивність, а також достатньо високі показники дифузії. Як і в попередній роботі, використання декількох ключей, які використовуються в різних раундах, може викликати складності з їх управлінням та передачею.

Станіка та Ангелеску (2024) [159] представляють криптосистему на основі оборотних клітинних автоматів (Reversible Cellular Automata, RCA), використовуючи одномірні клітинні автомати зі спеціально розробленими оборотними правилами. Ця криптосистема забезпечує збереження інформації за допомогою прямої та зворотної ітерації для шифрування та дешифрування. Реалізація на FPGA демонструє її ефективність та надійність, придатну для практичного застосування. Однак складність проектування оборотних правил, проблеми з управлінням ключами, вимоги до апаратного забезпечення, проблеми масштабованості та потенційні вразливості є суттєвими недоліками.

Недоліки. Як можна бачити, CCA-криптосистеми стикаються з наступними проблемами:

1. Швидкодія. При тому, що апаратна реалізація може бути ефективною, програмна імплементація таких систем може мати вищу обчислювальну складність порівняно з традиційними шифрами. Також, ітеративна природа клітинних автоматів може приводити до проблем з затримкою в системах реального часу.

2. Складність аналізу безпеки. Нелінійна та комплексна поведінка криптосистем на основі комбінованих клітинних автоматів робить її складною для застосування традиційних способів криптоаналізі. До того ж, формальні докази безпеки таких систем проти всіх можливих видів атак є складними через широкий простір можливих станів.

3. Управління ключами. Генерація та передача початкових станів та наборів правил для клітинних автоматів може бути комплексною. Крім того, взаємозв'язок між розміром ключа та стійкістю не настільки стійка як в традиційних криптосистемах, які вже є ретельно дослідженими.

4. Відсутність стандартизації попри широку варіативність запропонованих варіантів.

Потенційно, криптосистеми на комбінованих клітинних автоматах можуть бути використані для легковаговою криптографії в IoT-системах та модулях апаратної безпеки [55], а також для генерації псевдовипадкових чисел. Попри це, зважаючи на недоліки та поточний стан розвитку, наразі CCA-криптосистеми мають лише експериментальне застосування.

1.6.4. Комбінація різних підходів

Огляд. Існує також ідея поєднання елементів попередньо описаних підходів. Так, робляться дослідження в області комбінації хаотичної криптографії, ДНК-криптографії та криптографії на основі комбінованих клітинних автоматів.

Мондаль [160] та ін. (2019) пропонують безпечну схему шифрування зображень, яка поєднує клітинні автомати (CA) з хаотичним відображенням “skew tent”. Цей метод використовує хаотичну мапу для генерації початкового вектора для CA, яка створює псевдовипадкові послідовності чисел (PRNS) ефективніше, ніж традиційні хаотичні генератори псевдовипадкових чисел (PRNG). Процес шифрування включає перестановку пікселів за допомогою PRNS, а потім дифузію на основі випадкового числа з хаотичного відображення.

Чай та інші [161] комбінують хаотичний підхід з ДНК. Метод включає використання ДНК-кодування, двовимірних логістичних відображень, хвильову схему перестановки, строкову дифузію на ДНК-рівні, а також хеш SHA-256 для задання початкових значень. Аналіз продуктивності показує рівномірні гістограми, високу ентропію та низьку кореляцію між сусідніми пікселями

В роботі [162] Ву та інші поєднують ДНК та хаотичну криптографію. Метод поєднує операції з ДНК-послідовностями з кількома покращеними одномірними хаотичними картами, використовує кодування ДНК і хаотичні послідовності для заміни та перестановки пікселів. Сема демонструє високу чутливість до початкових умов і ключів. Однак складність реалізації, обчислювальні витрати, проблеми масштабованості та інтенсивність використання ресурсів створюють значні виклики. Як новий підхід, він також потребує подальшого тестування для виявлення потенційних вразливостей. Стаття Жанг та інших [163] комбінує хаотичний та ДНК підхід до шифрування. Автори пропонують нову схему шифрування зображень, що поєднує систему змішаних лінійно-нелінійних сполучених відображень решіток (Mixed Linear-Nonlinear Coupled Map Lattices, MLNCML) з операціями ДНК-послідовностей. Система MLNCML генерує псевдовипадкові послідовності через просторово-часовий хаос, тоді як операції з ДНК забезпечують високу складність і безпеку. Метод використовує механізм одноразового шифру для підвищення чутливості та стійкості до різних атак. Аналіз продуктивності показує великий простір ключів, високу ентропію та сильну стійкість до диференціальних і статистичних атак. Попри високі показники безпеки, алгоритм має виклики у вигляді

складності реалізації, обчислювальних витрат, проблем масштабованості та вимог до ресурсів.

В роботі Ґуесмі та інших [117] поєднуються елементи хаотичного шифрування та шифрування ДНК. Пропонується метод шифрування зображення, що комбінує операції над ДНК-послідовностями, хаотичну систему Лоренца, та хешування SHA-2. Вхідні дані кодуються в ДНК-послідовність, з подальшим застосування операції XOR. Система Лоренца генерує хаотичні послідовності які змінюють позиції пікселів в зображенні, забезпечуючи показники дифузії та конфузії. SHA-2 створює 256-бітний ключ безпеки. Алгоритм демонструє великий простір ключів, високу чутливість до змін ключа, стійкість до диференціальних і статистичних атак, а також високі значення ентропії. Однак складність реалізації, обчислювальні витрати, проблеми масштабованості, інтенсивність використання ресурсів і потенційні вразливості становлять значні виклики.

В роботі Чоі та інших описана криптосистема [125] , яка поєднує використання трьохвимірного генералізованого хаотичного відображення з комбінованим клітинним автоматом. Алгоритм має два етапи. На першому використовуються комбіновані нелінійний та лінійний клітинний автомат для створення ключа і маніпуляцій значень пікселів. На другому етапі, трьохвимірне генералізоване хаотичне відображення використовується для перемішування позицій пікселів. Описана система може покращувати показники безпеки, але також може бути затратної в ресурсах. Надійність системи проілюстрована лише статистичними тестами.

В публікації Пенг та інших ([150]) поєднуються методи ДНК-криптографії та хаотичні відображення. Так, описується спосіб одноразового шифрування, в якому використовуються, з однієї сторони, хаотичні відображення, таблиці кодування конфузії та відображення кодування, а з іншої, ДНК-сховище. Така комбінація забезпечує високі показники простору ключа. Аналіз продуктивності алгоритму демонструє порівняну або кращу швидкодію в порівнянні з іншими

хаотичними та ДНК-криптосистемами як в асимптотичній оцінці, так і на окремих прикладах. Втім, метод все ще поступається традиційним алгоритмам.

Недоліки. В цілому, хоча комбінація методів і може приводити до покращення стійкості з точки зору статистичного аналізу, вона також може призводити до пропорційного підвищення обчислювальної складності. Введення багаторівневих компонентів також може збільшувати кількість слабких точок, придатних для проведення атак. Поєднання різних методів також означає, що комбінованій системі притаманні недоліки обох складових. В цілому, комбіновані методи так само не мають реального широкого застосування на практиці

1.6.5. Нейронна криптографія

Огляд. В зв’язку з швидким розвитком штучного інтелекту та нейромереж в останні десятиліття, дослідники експериментують з застосуванням цих технологій в різноманітних сферах. Виникло питання, як здатності нейромереж до адаптації та навчання можна застосувати для застосування в криптосистемах. Вперше таким питанням задалися Кінзел та Кантер в 2002 році [57]. Стаття вводить концепцію синхронізації між двома нейронними мережами (Tree Parity Machines) через взаємне навчання. Пропонується використовувати цей процес синхронізації для безпечного обміну ключами через публічний канал. У документі висвітлюються переваги цього підходу перед традиційними криптографічними методами, такі як простота, швидкість і можливість генерувати нові ключі для кожного зв’язку. При цьому автори визнають потенційну вразливість, аргументуючи безпеку системи на основі різниці між часом синхронізації та часом навчання для зловмисника. Стаття заклала основу для подальших досліджень нейронної криптографії, включаючи більш просунуті атаки та механізми захисту. Окрім використання нейромереж для обміну ключами, запропоновано також використовувати їх безпосередньо для процесів шифрування та дешифрування. Суть цих систем полягає у використанні здатності нейронних мереж вивчати складні, нелінійні зв’язки між входами та

виходами, що ускладнює для зловмисників зворотне проектування процесу, не знаючи точної структури мережі та вагових коефіцієнтів[164].

Бігделі та інші [165] запропонував інноваційну схему шифрування зображень на основі хаотичних нейронних мереж. Їхній підхід поєднує численні хаотичні системи з двошаровою структурою нейронної мережі. Запропонована CNN складається з двох 3-нейронних шарів: хаотичного нейронного шару (CNL) і пермутаційного нейронного шару (PNL). CNL використовує три хаотичні системи (Chua, Lorenz і Lü) для генерування ваг і упереджень. PNL застосовує лінійну перестановку з наступною 2D нелінійною перестановкою для 3D перестановки. Алгоритм використовує 160-бітний код автентифікації та може бути розширений до 224 бітів. Процес шифрування є ітеративним, із кількома раундами. Однак це також створює проблеми з точки зору обчислювальної складності та потенційної вразливості передовими криптоаналітичними методами. Ця робота є прикладом потенціалу нейронних мереж у криптографії в поєднанні з хаотичними системами, і висвітлює поточні проблеми щодо розробки методів шифрування з використанням архітектури нейронних мереж.

Недоліки. Незважаючи на те, що нейронна криптографія є інноваційною, вона стикається з численними проблемами, які обмежують її широке практичне впровадження. Складність і обчислювальні витрати систем на основі нейронних мереж часто роблять їх непрактичними для пристроїв з обмеженими ресурсами або програм реального часу. На відміну від традиційних криптографічних методів, нейронна криптографія не має офіційних доказів безпеки, що ускладнює гарантію надійності проти всіх можливих атак. Використання нейронних мереж також вводить нові вектори атак, специфічні для машинного навчання, такі як змагальні атаки або вилучення моделі. Управління та розподіл ключів створює значні перешкоди, особливо для підтримки синхронізації між сторонами, що спілкуються. Поле страждає від відсутності стандартизації та визнання в ширшій криптографічній спільноті, що перешкоджає його прийняттю в реальних сценаріях. Хоча нейронна криптографія може забезпечувати певний опір загрозам квантових обчислень, її точна стійкість проти квантових алгоритмів

залишається невизначеною. Стохастичний характер навчання нейронної мережі може призвести до проблем із відтворюваністю, потенційно підриваючи послідовність процесів шифрування. Більше того, порівняно з традиційними криптографічними методами, нейронна криптографія зазнала менш ретельного вивчення з боку криптографічної спільноти, потенційно залишаючи невиявленими вразливості.

1.6.6. Інші альтернативні підходи

Окрім підходів з використанням динамічного хаосу, ДНК, та комбінованих клітинних автоматів є ще менш розповсюджені пропозиції. До них можна віднести наступні:

- Фрактальна криптографія [166]
- Квантова криптографія [167]
- Компресивна криптографія [168]
- Візуальна криптографія [169]
- Нейронна [170]
- Оптична [171]
- Тензорна [[172]

Підходи на основі фракталів використовують властивості самоподібності, але часто мають проблеми з високою обчислювальною складністю та чутливістю до початкових умов. Криптосистеми квантового зображення, хоча теоретично багатообіцяючі, стикаються з проблемами практичного впровадження через апаратні обмеження та вразливість до шуму. Методи, засновані на стисненні, пропонують інтригуючу комбінацію стиснення та шифрування, але мають збалансувати рівні безпеки та коефіцієнти стиснення та можуть бути сприйнятливими до атак із вибраним відкритим текстом. Візуальна криптографія, хоча й концептуально проста, обмежена у своєму застосуванні до складних зображень і стикається з проблемами розширення та вирівнювання пікселів. Системи на основі нейронних мереж демонструють потенціал для

адаптивного шифрування, але викликають занепокоєння щодо змагальних атак та інтерпретації. Оптичні криптосистеми використовують різноманітні перетворення, але чутливі до шуму та неузгодженості, а практичні реалізації часто виявляються складними та дорогими. Методи на основі тензорів, хоча й пропонують багатовимірні можливості шифрування, борються з високими обчислювальними вимогами та відносно обмеженою дослідницькою базою. У цих різноманітних підходах зберігаються спільні проблеми, зокрема постійний компроміс між безпекою та продуктивністю, складність керування ключами та відсутність стандартизованих показників оцінки. Крім того, загроза квантових обчислень, що насувається, кидає тінь на багато класичних криптографічних систем, тоді як атаки на бічних каналах використовують уразливості у фізичних реалізаціях. Оскільки розміри та роздільна здатність зображень продовжують збільшуватися, масштабованість залишається актуальною проблемою, так само як і забезпечення стійкості до стандартних операцій обробки зображень.

1.6.7. Криптосистеми з використання XOR

В роботі Давуд та інших проведено вичерпний аналіз та класифікацію порівнюваних методів шифрувань кольорових зображень [173]. У цьому дослідженні описані загальні операції, які використовуються для шифрування зображення, включаючи скремблінг, дифузію, перетасування, обертання, заміну, перемішування та транспозицію. Дифузія та перестановка особливо популярні через їх ефективність і простоту. Алгоритми шифрування зображень зазвичай класифікуються на алгоритми повного шифрування та алгоритми часткового шифрування, які класифікуються відповідно до їхньої орієнтації домену, чи то просторової, частотної чи гібридної. Крім того, це дослідження забезпечує глибокий аналіз різних сучасних методів з використанням конкретних показників безпеки.

Окрім згаданих підходів, існує також цікава ідея використовувати інше зображення в якості ключа. Так, можна використовувати зображення для генерації ключа або використовувати зображення як ключ безпосередньо. Одним

із перших такий концепт був запропонований в статі Чжоу та інших [174] . Тут запропоновані два нових алгоритми, які використовують довільне зображення для отримання або бітової площини(bit plane), або мапу ребер (edge map) в якості ключа. Ці алгоритми розкладають оригінальне зображення на бінарні бітові площини, які потім шифруються використовуючи бітову операцію XOR для зображення-ключа. Порядок всіх бітових площин обернений, і зашифроване зображення отримується застосування алгоритму скремблінгу.

Подібний принцип з додатковими ускладненням продемонстрований в іншій роботі [175] , де представлена гнучкість в кількох складових процесу шифруваня. Як і в попередній версії, довільно обране зображення розкладається на бітові площини, що слугують ключем безпеки. Метод шифрування зображень також включає в себе вибір способу декомпозиції бітової площини, застосовування алгоритм скремблінгу для бітової перестановки та комбінацію всіх оброблених бітових площин. Таким чином, при цьому методі ключ безпеки складається не тільки лише з зображення-ключа, але також з обраного алгоритму декомпозиції, обраних бітових площин та методу скрамблінгу. Хоча це може підвищити стійкість системи, це також значно ускладнює процес керування ключами. В цілому, використання XOR-операцій над бітових площинами є ключовим принципом у всіх наявних роботах, де використовується зображення в якості ключа. Цей клас методів відомий своїми досить великими просторами ключів безпеки, що виникають із численних можливих зображень, які можуть бути використані для генерації образу ключа, тим самим підвищуючи стійкість до брутфорс атак. Наступні роботи [104], [176], [177] ,[105] в цілому описують три варіанти: шифрування бітової площини ключа (KBE), шифрування SCAN ключа (KSE) і зміщення ключа RGB (KRDE). KSE модифікує оригінальні та ключові зображення у просторовій області за допомогою алгоритмів, написаних мовою SCAN. У KRDE оригінальне зображення та ключове зображення розбиваються на базові компоненти RGB, після чого виконуються операції XOR та скремблінг для створення зашифрованого зображення. Різні показники безпеки для таких методів наведено в [104], [105], [178]. Однак у порівнянні з

алгоритмами, розглянутими в [173], дані значення ентропії, середнього значення, піксельної кореляції та UACI є неоптимальними. Хоча їхні значення NPCR порівнянні, це вказує на область потенційного покращення безпеки в криптосистемах із ключами зображень. Слід зазначити, що всі розглянуті методи призводять до отримання зашифрованого зображення - тобто, сам шифротекст є зображенням. Однак так званий метод KRDE в [105] створює бінарний блоб. Цей метод передбачає виконання операцій XOR над кожним RGB-компонентом вихідного та ключового зображення з наступними різними обчисленнями для створення 3D-масиву як зашифрованого виводу. На жаль, цьому методу не вистачає детального аналізу безпеки. Тим не менш, можна припустити, що відмова від підтримки властивостей зображення в зашифрованому об’єкті може мати переваг у сфері безпеки.

1.6.8. Форматно-специфічні підходи

В той час як всі оглянуті криптосистеми є агностичними до цифрового формату зображень, тобто розглядають лише візуальні дані, деякі роботи сфокусовані на конкретних бінарних форматах і їх нюансах. Наприклад, існують криптосистеми для шифрування зображень у форматі JPEG. В 1996 році Тан представив [179] одну з найбільш ранніх схем шифрування для даних JPEG і MPEG, запропонувавши інтегрувати шифрування в процес стиснення. Метод використовує скрамблінг коефіцієнтів DCT на основі перестановки та вибіркове шифрування значень DC для досягнення ефективного шифрування з мінімальними витратами. Забезпечуючи прийнятну безпеку для комерційних програм, автор відзначає потенційну вразливість криптоаналізу через відому структуру стиснених даних. Робота висвітлила ключові проблеми шифрування мультимедіа, включаючи баланс безпеки, ефективності та продуктивності стиснення. Це також продемонструвало потенціал підходів до шифрування, що стосуються певного формату, які використовують структуру стандартів стиснення мультимедійних даних, створюючи основу для численних подальших робіт у цій галузі.

Хе та інші в роботі 2018 року [180] запропонував метод шифрування зображень JPEG на основі бітового потоку, який вирішує кілька проблем існуючих методів. Їхній підхід спрямований на збереження розміру файлу та покращення сумісності форматів із збереженням безпеки. Він використовує ключ шифрування пов’язаний з наповненням зображення для більшої безпеки. Зазначається, що розмір шифротексту майже не перевищує розмір оригінального зображення. Автори підкреслюють, що багато попередніх методів шифрування JPEG страждають від таких проблем, як значне збільшення розміру файлу, несумісність формату та вразливість до структурних атак. Їхній метод намагається подолати ці проблеми за допомогою нових методів шифрування коефіцієнтів DC і AC. Однак підхід все ще має деякі обмеження. Обчислювальна складність зростає із збільшенням кількості ітерацій у процесі шифрування коефіцієнта постійного струму, що потенційно може вплинути на продуктивність для вимог високого рівня безпеки. Крім того, незважаючи на те, що цей метод зберігає розмір файлу краще, ніж багато існуючих методів, все ж існують невеликі варіації через вирівнювання байтів. Автори також відзначають, що їхній підхід, як і інші методи шифрування, повинен збалансувати безпеку з обчислювальною продуктивністю.

Кобаяші та Кія в 2018 [181] запропонували метод шифрування JPEG на основі бітового потоку, який унікально вирішує проблему збереження точного розміру файлу під час шифрування. Хоча попередні методи часто призводили до незначних змін розміру файлу через створення або втрату кодів маркерів, цей підхід підтримує точний розмір файлу шляхом вибіркового шифрування лише певних додаткових бітів у бітовому потоці JPEG. Однак цей метод має деякі обмеження. Шифрування обмежено певними частинами бітового потоку, щоб уникнути впливу на коди маркерів, потенційно знижуючи загальну безпеку порівняно з більш комплексними схемами шифрування. Крім того, ефективність методу знижується при вищих показниках якості JPEG, оскільки менше байтів можна безпечно зашифрувати без ризику зміни розміру файлу. Автори також відзначають, що деяка візуальна інформація все ще може бути видимою в

зашифрованих зображеннях, особливо коли зашифровані лише компоненти DC, що вказує на компроміс між збереженням розміру файлу та візуальною безпекою. Незважаючи на ці труднощі, цей метод пропонує унікальне рішення для сценаріїв, де підтримка точного розміру файлу є критичною, наприклад, у певних процесах передачі зображень. Основним недоліком таких систем, звісно, є їх обмеженість одним форматом даних.

1.7. Постановка задачі

Враховуючи наведений аналіз, постає наступна задача:

1. Дослідити можливості створення криптосистем на основі дійсних змінних, які б дозволяли використати переваги дійсних чисел та уникнути описані недоліки наявних криптосистем на основі цілих чисел.

2. Створити нові криптографічні моделі та методи на основі дійсних чисел, розробити криптосистему з алгоритмами шифрування та дешифрування, що використовують функції дійсної змінної в якості ключа, і розробити симетричну криптосистему на їх основі. Створити як системи загального призначення, так і спеціалізовані варіанти для захисту зображень.

3. Розробити програмну реалізацію симетричної криптосистеми на основі створених методів. Перевірити та проаналізувати результати її роботи.

1.8. Висновки до першого розділу

Аналітичний огляд сучасного стану та тенденцій розвитку систем захисту даних дозволяє зробити такі висновки:

1. Криптосистеми на основі цілих чисел утворюють основу сучасної цифрової безпеки, де основне місце займають AES та RSA. Ці системи покладаються на обчислювальну складність відповідних математичних задач, однак із зростанням обчислювальної потужності вони стикаються з дедалі складнішими проблемами. Такі системи потребують все довших ключів для

підтримки безпеки призводить до збільшення обчислювальних витрат. Крім того, ці системи можуть бути вразливими до певних типів атак, а кінцевий набір цілих чисел потенційно обмежує їх довгострокову життєздатність перед розвитком методів криптоаналізу.

2. Окрім основних типів криптосистем, активно досліджуються нові методи на альтернативних засадах, що демонструє потребу в розробці нових способів захисту даних. Більшість з цих систем також зосереджені на цілих числах. Однак, такі системи не є поширеними і мають відповідні недоліки.

3. Одним з напрямком криптографії є створення систем для шифрування зображень, що дозволяли б використовувати властивості візуальних даних для покращення стійкості. Серед них, існує ідея використовувати інше зображення в якості ключа.

4. Розвиток квантових комп’ютерів становить значну загрозу для багатьох сучасних криптографічних систем, як симетричних, так і асиметричних. Ця загроза підштовхує дослідження квантово-стійкої криптографії, включаючи дослідження принципово інших математичних підходів до шифрування.

5. Одним з альтернативних підходів є використання систем на основі дійсних чисел, оскільки вище потужність дійсних чисел потенційно підвищує простір ключа і криптографічну стійкість. Однак, дослідження криптосистем на основі дійсних чисел є менш розповсюдженим, а наявні методи потребують подальшого розвитку.

6. Відповідно до приведеного аналізу, означена необхідність та поставлена задача розробити нові моделі та методи шифрування та дешифрування, які б дозволяли використати переваги дійсних чисел, та уникнути описані недоліки наявних криптосистем.

Основні наукові результати, наведені у першому розділі, опубліковано у працях автора: [1], [2], [3], [4], [5], [6], [7], [8], [9], [10].

РОЗДІЛ 2.
МОДЕЛІ ТА МЕТОДИ КРИПТОГРАФІЧНОЇ СИСТЕМИ НА ОСНОВІ ФУНКЦІЙ ДІЙСНОЇ ЗМІННОЇ

2.1. Математична модель повідомлення, зашифрованого за допомогою функцій дійсної змінної

На відміну від методів, які були розглянуті, пропонується метод шифрування даних за допомогою суми функцій дійсної змінної.

Дані з повідомлення, що шифрується, представляються у вигляді послідовності значень довжиною T.

В якості ключа шифрування задаються m функцій дійсної змінної f(x), які називаються функціями-ключами. Кожна функція має порядковий номер q. Ці функції представляються у дискретному вигляді. Для цього, обчислюються N значень кожної функції-ключа, використовуючи один і той же крок h для зміни аргументу. Результатом обчислень є m одновимірних масивів дійсних чисел довжиною N, за допомогою яких і шифрується символ повідомлення.

Шифротекст елементу повідомлення являє собою суму ключових функцій з невідомими коефіцієнтами.

Для шифрування, кожен j-й елемент повідомлення спочатку представляється в бітовому вигляді. Кожному q-му біту ставиться у відповідність q-та функція-ключ. В залежності від значення біту, обчислюється коефіцієнт k для цієї функції-ключа. Для нульового біту коефіцієнт також дорівнює нулю, але для одиничного біту коефіцієнт представляє собою випадково згенероване число дійсного типу. Сума функцій з відповідними коефіцієнтами є шифром y для j-го елементу повідомлення. Таким чином, суму утворюють лише ті функції, чий порядковий номер відповідає одиничному біту елементу повідомлення.

Оскільки y також є масивом довжиною N, шифротекст даних довжиною T представляє собою матрицю y(T,N).

Отже, математична модель шифрування описується наступним чином:

$$y(j,i) = \sum_{q=1}^{m} k_{qj}\, f_q(i) \qquad (2.1)$$

Де y - шифротекст повідомлення, матриця дійсних чисел розміром T на N ;

y(j,i) - значення елементів матриці шифротексту;

T - довжина масиву елементів повідомлення;

j - порядковий номер елементу повідомлення, j=1,2,...T;

N - довжина масиву кожної функції-ключа, N > m;

i - порядковий номер значень масиву функції-ключа, i=1,2,...N;

f(i) - функції-ключі, одновимірні масиви дійсних чисел довжиною N, обчислені шляхом зміни аргументу від xmin до xmax з кроком h.

xmin та xmax - мінімальне та максимальне значення аргументу функції-ключа.

h - крок зміни аргументу при обчисленні функції-ключа.

f_q (i) - q-та функція-ключ.

q - порядковий номер функції-ключа, q=1,2,...m;

m - кількість функцій-ключів;

k - коефіцієнти дійсного типу, що генеруються в залежності від значення біту елементу повідомлення. Якщо біт нульовий, то k=0. Якщо біт одиничний, то k дорівнює випадково згенерованому дійсному числу.

k_{qj} - значення коефіцієнту q-го біту j-го елементу повідомлення.

Задача розшифрування полягає в розпізнаванні того, які з ключових функцій були включені в (2.1). Для цього необхідно дешифрувати значення коефіцієнтів k і порівняти їх з нулем, або з числом близьким до нього. Якщо коефіцієнт k не дорівнює нулю, це свідчить, що відповідна функція-ключ входить в суму (2.1). Таким чином стає відомим бінарний код поточного елементу зашифрованого повідомлення. Для розв’язання цієї задачі пропонується метод, який базується на використанні функцій непропорційності. Для розв’язання цієї задачі пропонується метод, який базується на використанні функцій непропорційності.

2.2. Функції непропорційності

Пропорційною називають функцію, в якій відношення двох складових є константою:

$$y = kx \tag{2.2}$$

Для вирішення ряду задач виникає необхідність перевірки заданої функції на пропорційність - в тому числі на окремих інтервалах або в заданих точках. Якщо ж пропорційність відсутня, необхідно кількісно виміряти, наскільки задане відношення відхиляється від пропорційного. Задля вирішення таких задач, було введено [93], [94] концепцію непропорційності як характеристику чисельних функцій. Однак, властивості функцій непропорційності відкривають можливості для використання в інших сферах - таких як розпізнавання сигналів та захисту даних.

Існують такі функції непропорційності:

1. Функції непропорційності по похідним;
2. Функції непропорційності по значенням;
3. Відносна функція непропорційності;
4. Інтегральна функція непропорційності по похідній;
5. Інтегральна функція непропорційності по значенню.

В рамках пропонованої моделі застосовуються функція непропорційності по похідній першого порядку та інтегральна функція непропорційності по похідній першого порядку.

В рамках пропонованої моделі застосовуються непропорційність по похідній та інтегральна непропорційність по похідній.

Відомо, що для функції y = f(x), $\frac{dy}{dx}$ є лімітом відношення $\frac{\Delta y}{\Delta x}$при $\Delta x \to 0$. Відповідно, відношення x і y є пропорційним, якщо при заданому x виконується рівність:

$$\frac{y}{x} = \frac{dy}{dx} \tag{2.3}$$

Так, різниця між $\frac{y}{x}$ і $\frac{dy}{dx}$ є непропорційністю по похідній першого порядку функції y=f(x) по x:

$$@d_x^{(1)} y = \frac{y}{x} - \frac{dy}{dx} \tag{2.4}$$

Символ @ означає операцію непропорційності, d - похідну, нотація @d в цілому означує непропорційність по похідній. Ліва частина читається як “ет d один у по x”. В загальному вигляді, непропорційність по похідній порядку n описується так:

$$@d_x^{(n)} y = \frac{y}{x^n} - \frac{1}{n!}\frac{d^n y}{dx^n} \tag{2.5}$$

Якщо функція y(x) має вид $y=kx^n$, для всіх x непропорційність дорівнює нулю незалежно від значення коефіцієнта k. Завдяки цьому, функції непропорційності дозволяють обчислювати невідомі коефіцієнти при функціях, в тому числі у випадку, коли y(x) є сумою функцій з невідомими коефіцієнтами:

$$y(x) = k_1 f_1(x) + k_2 f_2(x) + \cdots + k_m f_m(x) \tag{2.6}$$

Ця властивість розпізнавання коефіцієнтів є ключовою і відкриває можливості до створення як систем розпізнавання, так і криптосистем.

Однак, непропорційність по похідній має певні обмеження. Можливі такі випадки: - Не для всіх точок в області визначення існує похідна. - При обчислені значень похідної можуть виникати невизначеності 0/0 або ∞/∞ - Похідні не існують для дискретних функцій.

Тому, у ситуаціях, де використання непропорційності по похідній (2.4) не є можливим, використовується інтегральна непропорційність по похідній. В цьому випадку, непропорційність обчислюється для інтегралів функцій y(t) і x(t). Так, інтегральна непропорційність по похідній першого порядку функції y(t) відносно x(t) має вигляд:

$$@I_{x(t)}^{(1)} y(t) = \frac{\int_{t-h}^{t} y\,(t)dx}{\int_{t-h}^{t} x\,(t)dx} - \frac{y(t)}{x(t)} \tag{2.7}$$

Де нотація @I позначає інтегральну непропорційність. В подальшому під інтегральною непропорційністю матиметься на увазі саме Інтегральна непропорційність по похідній першого порядку.

Якщо функції є дискретними і представлені одновимірними масивами, необхідні чисельні методи для обчислення непропорційності. Після обчислення апроксимованих значень інтегралів методом трапеції з кроком h для y(t) та x(t), інтегральна непропорційність отримує наступний вигляд:

$$@I_{x_i}^{(1)} y_i = \frac{y_{i-1} + y_i}{x_{i-1} + x_i} - \frac{y_i}{x_i} \tag{2.8}$$

Крім цього, в подальшому використовуватиметься обернена операція, коли із (2.8) треба знайти y_i :

$$y_i = \frac{\left(y_{i-1} - I_i(x_{i-1} + x_i)\right)x_i}{x_{i-1}} \tag{2.9}$$

Властивості інтегральної функції непропорційності є ключовим елементом для обчислення коефіцієнтів і розпізнавання сигналів, а також є наріжним принципом шифрування та дешифрування в запропонованих криптосистемах.

2.3. Метод дешифрування за допомогою інтегральної функції непропорційності

Для спрощення описання методу дешифрування, розглянемо випадок, коли сума (2.1) представлена п’ятьма дискретно заданими функціями. Тоді, сума має наступний вигляд:

$$y(j) = k_1 f(1,j) + k_2 f(2,j) + k_3 f(3,j) + k_4 f(4,j) + k_5 f(5,j) \qquad (2.10)$$

Алгоритм обчислення коефіцієнтів k складається з m=5 рівнів, на кожному з яких обчислюється непропорційність $D_{(l,n)}(j)$, де - l рівень, а n - номер обчислення непропорційності на цьому рівні.

Перший рівень.

Обчислимо непропорційність (2.8) y(j) по будь-якій функції із правої частини (2.10). Нехай це f(1,j):

$$\begin{aligned} D_{1,1}(j) &= @I_{f_1}^{(1)} y \\ &= \frac{y(j-1)+y(j)}{f(1,j-1)+f(1,j)} - \frac{y(j)}{f(1,j)} \\ &= k_1\left[\frac{f(1,j-1)+f(1,j)}{f(1,j-1)+f(1,j)} - \frac{f(1,j)}{f(1,j)}\right] \\ &+k_2\left[\frac{f(2,j-1)+f(2,j)}{f(1,j-1)+f(1,j)} - \frac{f(2,j)}{f(1,j)}\right] \\ &+\cdots \\ &+k_{M+1}\left[\frac{f(M+1,j-1)+f(M+1,j)}{f(1,j-1)+f(1,j)} - \frac{f(M+1,j)}{f(1,j)}\right] \end{aligned} \qquad (2.11)$$

Також обчислимо непропорційності інших функцій f(r,j) із (2.10) по f(1,j):

$$D_{1,r}(j) = @I_{f_1}^{(1)} f_r = \frac{f(r,j-1)+f(r,j)}{f(1,j-1)+f(1,j)} - \frac{f(r,j)}{f(1,j)} \qquad (2.12)$$

де j=0, 1, ...N-1; r = 2, 3, 4, 5.

Підставимо (2.12) в (2.11) і врахуємо, що перша складова в (2.12) дорівнює нулю.

В результаті отримаємо:

$$D_{1,1}(j) = k_2 D_{1,2}(j) + k_3 D_{1,3}(j) + k_4 D_{1,4}(j) + k_5 D_{1,5}(j) \qquad (2.13)$$

Другий рівень.

В (2.13) вибираємо, наприклад, $D_{1,2}$ (j) і обчислюємо непропорційність (2.8) $D_{1,1}$ (j) по $D_{1,2}$ (j):

$$\begin{aligned} D_{2,1}(j) &= @I^{(1)}_{D_{1,2}} D_{1,1} \\ &= \frac{D_{1,1}(j-1) + D_{1,1}(j)}{D_{1,2}(j-1) + D_{1,2}(j)} - \frac{D_{1,1}(j)}{D_{1,2}(j)} \\ &= k_2 \left[\frac{D_{1,2}(j-1) + D_{1,2}(j)}{D_{1,2}(j-1) + D_{1,2}(j)} - \frac{D_{1,2}(j)}{D_{1,2}(j)}\right] \\ &+ k_3 \left[\frac{D_{1,3}(j-1) + D_{1,3}(j)}{D_{1,2}(j-1) + D_{1,2}(j)} - \frac{D_{1,3}(j)}{D_{1,2}(j)}\right] \\ &+ k_4 \left[\frac{D_{1,4}(j-1) + D_{1,4}(j)}{D_{1,2}(j-1) + D_{1,2}(j)} - \frac{D_{1,4}(j)}{D_{1,2}(j)}\right] \\ &+ k_5 \left[\frac{D_{1,5}(j-1) + D_{1,5}(j)}{D_{1,2}(j-1) + D_{1,2}(j)} - \frac{D_{1,5}(j)}{D_{1,2}(j)}\right] \end{aligned} \qquad (2.14)$$

Також обчислимо:

$$D_{2,r}(j) = @I^{(1)}_{D_{1,2}} D_{1,r} = \frac{D_{1,r}(j-1) + D_{1,r}(j)}{D_{1,2}(j-1) + D_{1,2}(j)} - \frac{D_{1,r}(j)}{D_{1,2}(j)} \qquad (2.15)$$

де j=0,1,...N-1; r=3,4,5.

Після підстановки (2.15) в (2.14) із врахуванням, що перша складова нульова, отримаємо:

$$D_{2,1}(j) = k_3 D_{2,3}(j) + k_4 D_{2,4}(j) + k_5 D_{2,5}(j) \qquad (2.16)$$

Третій рівень.

Знову обираємо в (2.16) будь-яку із складових, наприклад, $D_{2,3}(j)$. Обчислимо непропорційність (2.8) $D_{2,1}(j)$ по $D_{2,3}(j)$:

$$\begin{aligned} D_{3,1}(j) &= @I^{(1)}_{D_{2,3}} D_{2,1} \\ &= \frac{D_{2,1}(j-1)+D_{2,1}(j)}{D_{2,3}(j-1)+D_{2,3}(j)} - \frac{D_{2,1}(j)}{D_{2,3}(j)} \\ &= k_3\left[\frac{D_{2,3}(j-1)+D_{2,3}(j)}{D_{2,3}(j-1)+D_{2,3}(j)} - \frac{D_{2,3}(j)}{D_{2,3}(j)}\right] \\ &+k_4\left[\frac{D_{2,4}(j-1)+D_{2,4}(j)}{D_{2,3}(j-1)+D_{2,3}(j)} - \frac{D_{2,4}(j)}{D_{2,3}(j)}\right] \\ &+k_5\left[\frac{D_{2,5}(j-1)+D_{2,5}(j)}{D_{2,3}(j-1)+D_{2,3}(j)} - \frac{D_{2,5}(j)}{D_{2,3}(j)}\right] \end{aligned} \tag{2.17}$$

Також обчислимо

$$D_{3,r}(j) = @I^{(1)}_{D_{2,3}} D_{2,r} = \frac{D_{2,r}(j-1)+D_{2,r}(j)}{D_{2,3}(j-1)+D_{2,3}(j)} - \frac{D_{2,r}(j)}{D_{2,3}(j)} \tag{2.18}$$

де j=0,1,...N-1;r=4,5.

Підстановка (2.18) в (2.17) дає:

$$D_{3,1}(j) = k_4 D_{3,2}(j) + k_5 D_{3,3}(j) \tag{2.19}$$

Четвертий рівень.

Обираємо в (2.19) $D_{3,2}$ (j) і обчислимо по ній непропорційності (2.8):

$$\begin{aligned} D_{4,1}(j) &= @I^{(1)}_{D_{3,2}} D_{3,1} \\ &= \frac{D_{3,1}(j-1)+D_{3,1}(j)}{D_{3,2}(j-1)+D_{3,2}(j)} - \frac{D_{3,1}(j)}{D_{3,2}(j)} \\ &= k_4\left[\frac{D_{3,2}(j-1)+D_{3,2}(j)}{D_{3,2}(j-1)+D_{3,2}(j)} - \frac{D_{3,2}(j)}{D_{3,2}(j)}\right] \\ &+k_5\left[\frac{D_{3,3}(j-1)+D_{3,3}(j)}{D_{3,2}(j-1)+D_{3,2}(j)} - \frac{D_{3,3}(j)}{D_{3,2}(j)}\right] \end{aligned} \tag{2.20}$$

$$D_{4,2}(j) = @I^{(1)}_{D_{3,2}} D_{3,3} = \frac{D_{3,3}(j-1) + D_{3,3}(j)}{D_{3,2}(j-1) + D_{3,2}(j)} - \frac{D_{3,3}(j)}{D_{3,2}(j)} \quad (2.21)$$

Після підстановки (2.21) в (2.20) отримуємо:

$$D_{4,1}(j) = k_5 D_{4,2}(j) \quad (2.22)$$

П’ятий рівень.

Обчислимо непропорційність (2.8) $D_{4,1}(j)$ по $D_{4,2}(j)$:

$$\begin{aligned} D_{5,1}(j) &= @I^{(1)}_{D_{4,2}} D_{4,1} \\ &= \frac{D_{4,1}(j-1) + D_{4,1}(j)}{D_{4,2}(j-1) + D_{4,2}(j)} - \frac{D_{4,1}(j)}{D_{4,2}(j)} \\ &= k_5 \left[\frac{D_{4,2}(j-1) + D_{4,2}(j)}{D_{4,2}(j-1) + D_{4,2}(j)} - \frac{D_{4,2}(j)}{D_{4,2}(j)} \right] = 0 \end{aligned} \quad (2.23)$$

Рівність нулю $D_{5,1}(j)$ пояснюється наявністю пропорціонального зв’язку між $D_{4,1}(j)$ і $D_{4,2}(j)$, як це видно із (2.23). Із цього рівняння обчислюється k_5:

$$k_5 = \frac{D_{4,1}(j)}{D_{4,2}(j)} \quad (2.24)$$

Із (2.19, 2.16, 2.13, 2.10) знаходимо k_4, k_3, k_2, k_1:

$$k_4 = \frac{D_{3,1}(j) - k_5 D_{3,3}(j)}{D_{3,2}(j)} \quad (2.25)$$

$$k_3 = \frac{D_{2,1}(j) - k_4 D_{2,4}(j) - k_5 D_{2,5}(j)}{D_{2,3}(j)} \quad (2.26)$$

$$k_2 = \frac{D_{1,1}(j) - k_3 D_{1,3}(j) - k_4 D_{1,4}(j) - k_5 D_{1,5}(j)}{D_{1,2}(j)} \quad (2.27)$$

$$k_1 = \frac{y(j) - k_2 f(2,j) - k_3 f(3,j) - k_4 f(4,j) - k_5 f(5,j)}{f(1,j)} \quad (2.28)$$

Таким чином, послідовне застосування інтегральної непропорційності описаним способом дозволяє визначити всі коефіцієнти k_i в сумі (2.10). Це робить метод придатним для дешифрування повідомлень.

2.4. Приклад визначення невідомих коефіцієнтів при функціях, які утворюють суму

Визначення невідомих коефіцієнтів при функціях, які утворюють суму, є основою криптографічних систем, які пропонуються. Тому важливо окремо перевірити наскільки точно розв'язується ця задача із застосуванням функції непропорційності.

З цією метою розглянута задача розпізнавання еталонного сигналу при наявності адитивної завади на невідомих частотах. Як буде показано нижче, в цьому випадку математична постановка задачі також має вид (2.1) і для її розв'язання потрібно знайти значення невідомих коефіцієнтів.

Еталонним є сигнал з корисною інформацією, який передається відправником, і який потрібно розпізнати приймаючою стороною. Проблема полягає в тому, що на еталонний сигнал при передачі може накладатися завада з завчасно невідомими характеристиками на невідомих частотах спектру.

При розв'язанні цієї задачі доводиться досліджувати різні умови, яким відповідають корисний (еталонний) сигнал і завада. Відповідно багато раз доводиться обчислювати невідомі коефіцієнти при функціях. Це дозволяє більш надійно перевірити метод обчислення невідомих коефіцієнтів за допомогою інтегральної функції непропорційності.

Адитивна завада може складатися з двох частин:

1. Невідомий періодичний сигнал у випадковому спектрі.
2. Сума детерміністичних сигналів з заданого набору який передається разом з еталонним сигналом.

У першому випадку, завада у вигляді періодичного сигналу може бути наслідком природних явищ або навмисно накладатися третьої стороною. Вона може бути апроксимована кінцевою сумую базисних функцій - наприклад, представлена кінцевим рядом Фур'є.

У другому випадку, маються на увазі сигнали, які передаються відправником разом з еталонним сигналом. Приймаючій стороні відомі їх характеристики, але невідомо, які з них присутні у сумі, і з якими коефіцієнтами.

Як можна бачити, цільовий сигнал разом з описаними накладеними завадами демонструють схожість з шифротекстом, який ускладнює доступ до даних, а процес розпізнавання сигналів - з дешифруванням і відтворенням корисних даних.

На приймаючу сторону надходить вхідний сигнал y(t):

$$y(t) = k_1 g(t) + k_2 \eta(t) \tag{2.29}$$

Де g(t) - еталонний сигнал,

η(t) - завада,

k_1 та k_2 - вагові коефіцієнти відповідно еталонного сигналу та завади. Значення коефіцієнтів невідомі.

Розглянемо перший випадок, де завада у вигляді випадкового періодичного сигналу розкладена на кінцеву суму базисних функцій f_i (t):

$$\eta(t) = \sum_{i=1}^{M} e_i f_i(t) \tag{2.30}$$

Де

M - кількість базисних функцій,

e_i - відповідні коефіцієнти базисних функцій,

i=1, 2, ... M - порядковий номер базисних функцій.

Таким чином, вся завада представляється у вигляді суми M функцій з невідомими коефіцієнтами.

Тут можна бачити схожість моделі завади в (2.30) з моделлю (2.1).

Після підстановки (2.30) в (2.29), вхідний сигнал має вигляд:

$$y(t) = k_1 g(t) + k_2 \sum_{i=1}^{M} e_i f_i(t) \quad (2.31)$$

Необхідно визначити значення коефіцієнту k_1 еталонного сигналу g(t), використовуючи дані функції f_i (t) та поточне значення y(t). Якщо цей коефіцієнт не дорівнює нулю, це означає що еталонний g(t) сигнал успішно розпізнаний в вхідному сигналі y(t). Його значення є вагою еталонного сигналу. Якщо ж $k_1=0$, то еталонний сигнал відсутній.

Щоб вирішити цю задачу, необхідно вказати множину базисних функцій f_i (t). Їхня кількість M має бути не меншою, ніж потрібно для апроксимації завади.

Розглянемо другий випадок, коли до завади η(t) додається множина детермінованих сигналів. Легко бачити, що цей випадок зводиться до попереднього. В такому випадку, до вже наявної множини M базисних функцій просто додаються r нових функцій. Вони представляють накладені детерміновані сигнали з заданого набору. Таким чином, в сумі беруть участь додаткові функції $f_{(M+2)}$,$f_{(M+3)}$, ... $f_{(M+r)}$.

Якщо функція y(t) може бути представлена сумою відомих функцій $r_i(t)$ з невідомими коефіцієнтами q_i як:

$$y(t) = q_1 r_1(t) + q_2 r_2(t) + \cdots + q_M r_M(t) \quad (2.32)$$

То послідовна калькуляцію непропорційності (2.8) дозволяє визначити невідомі коефіцієнти в (2.32). Для того щоб можна було використовувати цю властивість для вирішення проблеми, необхідно привести вхідний сигнал y(t) з (2.31) до вигляду (2.32). Для цього, введемо нове означення. Нехай $c_i = k_2 e_i$.

Тоді:

$$f_{M+1}(t) = g(t) \tag{2.33}$$

$$c_{M+1} = k_1 \tag{2.34}$$

Підставляючи (2.33) та (2.34) в (2.30), отримаємо суму функцій:

$$y(t) = \sum_{i=1}^{M+1} c_i \, f_i(t) \tag{2.35}$$

Розглянемо випадок, коли вхідний сигнал y(t) виміряний дискретно в часі з кроком h і представлений у вигляді масиву y_j=y(jh). Тут j = 0,1,2,..N-1.

Кількість N визначається загальною кількістю функцій, що використовуються в системі розпізнавання. На додачу до кількості функцій M, еталонна функція $f_{(M+1)}$ (t) та y(t) повинні бути взяті до уваги. В цьому випадку: N≥(M+1+1)+1.

Представимо (2.35) в дискретній формі. При f(i,j)=f_i (jh), отримаємо:

$$y(i) = \sum_{i=1}^{M+1} c_i \, f(i,j) \tag{2.36}$$

Задача розпізнавання сигналів зводиться до обчислення невідомих коефіцієнтів $c_{(M+1)}$ для визначення того, які саме функції сигналів беруть участь в результуючій сумі.

Як і при шифруванні в (2.1), вираз являє собою суму відомих функцій з невідомими коефіцієнтами, де функції представлені в дискретній формі у вигляді одновимірних масивів заданої довжини.

Таким чином, і задача розпізнавання сигналів в сумі функцій(2.36), і задача розшифрування з суми (2.1) вирішується спільними методами з застосуванням інтегральних функцій непропорційності описаними.

Застосування непропорційності (2.8) відповідно до алгоритму [182] дозволяє обчислити невідомі значення коефіцієнтів $c_{(M+1)}$ в (2.36). При цьому, також обчислюються коефіцієнти c_1, c_2, ... c_M які визначають заваду η(t). Для цього, достатньо лише поточних значень y(t).

Однак, оскільки дискретні функції не мають першої похідної, замість функцій непропорційності по похідній першого порядку необхідно використовувати інтегральну функцію непропорційності першого порядку (2.8) і метод, описаний в (2.10-2.28) Розглянемо декілька прикладів розпізнавання сигналів з метою перевірки описаного методу.

Розглянемо випадок, коли завада періодична із обмеженою зверху частотою. В (2.16) вона представлена сумою гармонічних функцій:

$$y(t) = c_1\cos(\omega t) + c_2\sin(\omega t) + c_3\cos(2\omega t) + c_4\sin(2\omega t) + \cdots + c_{M-1}\cos\left(\frac{M}{2}\omega t\right) + c_M\sin\left(\frac{M}{2}\omega t\right) + c_{M+1}f_{M+1}(t) \quad (2.38)$$

де ω - кругова частота.

В цьому випадку коефіцієнти c_1 і c_2 представляють першу гармоніку, c_3 і c_4 - другу і т.д.

Щоб можна було представити періодичну заваду, треба знати її період і, хоча б наближено, максимальну частотну складову. Це дозволить визначити частоту першої і найвищої гармоніки з номером $\frac{M}{2}$ в (2.38). При цьому частота найвищої гармоніки з номером $\frac{M}{2}$ може бути або рівною, або більшою від максимальної частоти, з якою контролюється завада. Розглянемо декілька прикладів.

Приклад 1. При розв'язання задачі вважається, що завада η(t) має вид (2.11). Необхідно перевірити, що при відомих f_i (t) запропонований алгоритм дозволяє отримати правильні значення коефіцієнтів e_i, i=1,2,...,M в (2.11). Для цього візьмемо y(t) (2.38) і прирівняємо до нуля коефіцієнт $c_{(M+1)}$ при еталонній функції $f_{(M+1)}$ (t). В результаті отримаємо

$$y(t) = \eta(t) = c_1\cos(\omega t) + c_2\sin(\omega t) + c_3\cos(2\omega t) + c_4\sin(2\omega t) + \ldots + c_M\sin\left(\frac{M}{2}\omega t\right) \quad 2.39$$

Необхідно знайти коефіцієнти $c_1, c_2, \ldots, c_M$.

Нехай завада має вид:

$$\eta(t) = 0.5\cos(\mathrm{t}) - 7.25\cos(2\mathrm{t}) + 1.25\sin(2\mathrm{t}) - 2.5\sin(5\mathrm{t}) + 0.12\cos(7\mathrm{t}) + 2\cos(9\mathrm{t}) + 0.625\sin(10\mathrm{t}) - 3\sin(11\mathrm{t}) + 6.75\cos(20\mathrm{t}) - 10\sin(20\mathrm{t})$$
$$= 0.5\mathrm{f}_1(\mathrm{t}) - 7.25\mathrm{f}_3(\mathrm{t}) + 1.25\mathrm{f}_4(\mathrm{t}) - 2.5\mathrm{f}_{10}(\mathrm{t}) + 0.12\mathrm{f}_{13}(\mathrm{t}) + 2\mathrm{f}_{17}(\mathrm{t}) + 0{,}625\mathrm{f}_{20}(\mathrm{t}) - 3\mathrm{f}_{22}(\mathrm{t}) + 6{,}75\mathrm{f}_{39}(\mathrm{t}) - 10\mathrm{f}_{40}(\mathrm{t}) \quad (2.40)$$

За умовою лише наближено відома смуга частот, в яку входить завада. Тому допустимо, що її найвища гармоніка дорівнює 25, хоча в дійсності вона дорівнює тільки 20. Таким чином кількість функцій, які визначають заваду, M=50. Всього кількість функцій, які залучені для визначення коефіцієнтів в (2.40), з врахуванням y(t) дорівнює 51. Враховуючи відсутність еталонної функції, кількість елементів в дискретних представленнях функцій N≥(M+1)+1=52. Приймемо N=52. Крок зміни аргументу h=1.

Результати приведені в колонці Приклад 1 Таблиці 2.1.

Таблиця 2.1 — Результати тестування методу розпізнавання за допомогою інтегральної непропорційності

c_i	Приклад 1	Приклад 2	Приклад 3	Приклад 4	Приклад 5	Приклад 6
1	0,5	0.5218	2,74225	500	500	500
2	8,18E-12	-0.0135554	4,48451	-4,54E-09	-2,24E-07	5,42E-07
3	-7,25	-7.47506	-7,25	-7250	-7250	-7250
4	1,25	1.18038	8,35047	1250	1250	1250
5	2,28E-12	-0.0234714	-7,28E-11	7,61E-09	9,74E-09	1,33E-08

c_i	Приклад 1	Приклад 2	Приклад 3	Приклад 4	Приклад 5	Приклад 6
6	2,05E-12	-0.0409719	1,84E-10	-1,47E-08	8,01E-09	-2,31E-08
7	7,18E-12	0.0184056	-2,61E-10	1,64E-08	-7,16E-09	6,26E-08
8	8,20E-12	-0.083213	-2,00E-10	1,44E-08	8,69E-09	-1,27E-08
9	-1,14E-12	-0.0356034	6,49E-11	8,18E-09	9,16E-08	-2,18E-07
10	-2,5	-2.47883	-6,23709	-2500	-2500	-2500
11	1,45E-13	-0.0093848	1,07E-11	3,81E-09	-1,47E-08	4,57E-08
12	-1,00E-14	-0.00439558	-3,48E-12	2,97E-09	-2,63E-08	7,40E-08
13	0,12	0.119222	15,0684	120	120	120
14	3,98E-12	-0.00837845	7,12E-11	4,66E-09	5,40E-09	-1,81E-09
15	-6,86E-12	0.0635089	2,37E-10	-9,62E-09	-6,14E-09	-2,65E-08
16	2,59E-13	-0.0605521	-1,13E-10	-4,24E-09	-1,88E-08	4,52E-08
17	2	1.97527	2	2000	2000	2000
18	-1,01E-11	-0.000225677	3,16E-10	-2,30E-08	6,30E-09	-2,41E-08
19	1,29E-11	-0.0203486	-3,55E-10	2,67E-08	3,51E-09	4,24E-08
20	0,625	0.606359	-3,55481E-10	625	625	625
21	2,57E-12	0.0018544	8,31E-11	8,39E-10	-3,10E-08	6,40E-08
22	-3	-2.95846	-3	-3000	-3000	-3000
23	-4,11E-13	-0.00546663	-1,33E-11	3,02E-09	1,13E-08	-2,58E-08
24	1,93E-13	0.00449403	-1,62E-11	-4,15E-10	9,07E-09	-2,47E-08
25	8,18E-14	-0.00684171	1,97E-11	3,44E-09	9,65E-09	-1,89E-08
26	-1,20E-12	-0.00255814	6,26E-12	-7,02E-10	-1,71E-08	4,44E-08
27	4,86E-12	-0.00866345	2,80E-11	-1,94E-08	-3,73E-07	8,90E-07
28	1,04E-12	-0.0321576	-8,87E-11	-1,61E-08	-1,92E-07	4,48E-07
29	4,14E-12	-0.0195644	5,23193	-1,67E-08	-3,08E-07	7,35E-07
30	2,35E-12	0.0329743	-1,11E-10	3,56E-09	-1,26E-09	3,11E-08
31	-1,98E-12	-0.0267472	6,45E-11	-1,09E-09	1,31E-08	-8,37E-09
32	-3,30E-12	0.00830763	2,51E-11	3,24E-09	-3,65E-09	-1,07E-08
33	1,34E-12	0.84833	1,57E-11	6,85E-10	5,96E-09	-2,16E-08
34	-4,15E-12	0.419396	1,53E-10	-4,37E-09	1,33E-08	-5,11E-08
35	3,09E-12	0.00274051	3,38E-11	5,73E-09	1,75E-08	-3,30E-08
36	-1,71E-12	0.0116143	-6,31E-11	-5,41E-09	-1,13E-08	1,98E-08
37	2,38E-12	-0.0428529	6,87E-11	1,83E-08	-3,11E-07	8,62E-07
38	-9,99E-12	0.0417336	-3,31E-11	-2,65E-08	-3,44E-07	8,72E-07
39	6,75	6.49839	-3,31312E-11	6750	6750	6750
40	-10	-10.0569	-10	-10000	-10000	-10000
41	6,36E-11	0.460666	-2,02E-09	1,07E-07	-9,08E-08	5,03E-07
42	-5,45E-11	0.815869	3,96E-10	-4,83E-08	-2,88E-08	1,65E-07
43	5,52E-12	-0.0841818	2,11E-10	-1,51E-08	1,86E-08	-3,67E-08
44	-3,16E-11	0.361305	-7,62E-10	6,28E-08	-6,19E-08	1,50E-07
45	-3,70E-11	-0.81944	1,67E-09	-7,63E-08	1,03E-07	-5,27E-07
46	-7,89E-11	0.558422	1,26E-09	-8,78E-08	1,60E-08	-7,45E-08
47	1,21E-11	0.243344	1,67E-10	3,71E-09	-1,02E-07	2,75E-07
48	-2,46E-11	0.0592147	-1,08E-09	-1,04E-07	-3,90E-07	8,61E-07
49	1,39E-12	0.0183457	-4,05E-11	-5,06E-09	4,58E-07	-1,23E-06
50	-9,09E-12	0.0526963	-14,9484	3,30E-08	7,11E-07	-1,66E-06
51	-	-	-0,49484	-1,256	-1,256	-2,08E-07
52	-	-	-	-	0,725	0,725

Отримані значення коефіцієнтів c_1=0,5; c_3=-7,25; c_4=1,25; c_{10}=-2,5; c_{13}=0,12; c_{17}=2; c_{22}=-3; c_{40}=-10. Усі інші коефіцієнти дорівнюють нулю. Очевидно, що отримані результати співпадають із значеннями відповідних коефіцієнтів в (2.40). Алгоритм працює правильно.

Приклад 2. Досліджується випадок, коли неправильно визначений діапазон частот, в яких знаходиться завада. Наприклад, коли до виразу (2.40), яким визначається завада, додається cos(27t):

$$\eta(t) = 0.5\cos(t) - 7{,}25\cos(2t) + 1.25\sin(2t) - 2{,}5\sin(5t) + 0.12\cos(7t) + 2\cos(9t) + 0{,}625\sin(10t) - 3\sin(11t) + 6{,}75\cos(20t) - 10\sin(20t) + \cos(27t) \quad (2.41)$$

Як видно із колонки Приклад 2 Таблиці 2.1, усі коефіцієнти не дорівнюють нулю і відрізняються від значень в (2.41). Тобто в цьому випадку алгоритм не працює.

Приклад 3. Розглядається розкладання суми еталонної функції g(t) і завади η(t).

$$y(t) = g(t) + \eta(t) \quad (2.42)$$

де завада η(t) має вид (2.40), а еталонна функція описана виразом:

$$\mathrm{g(t)} = 1.5\cos(\mathrm{t}) + 3\sin(\mathrm{t}) + 4.75\sin(2\mathrm{t}) - 2.5\sin(5\mathrm{t}) + 10\cos(7\mathrm{t}) + 2.15\sin(10\mathrm{t})) + 3.5\cos(15\mathrm{t}) + 4\cos(20\mathrm{t}) - 10\sin(25\mathrm{t}) = 1.5f_{1(t)} + 3\mathrm{f}_2(\mathrm{t}) + 4{,}75\mathrm{f}_4(\mathrm{t}) - 2{,}5\mathrm{f}_{10}(\mathrm{t}) + 10\mathrm{f}_{13}(\mathrm{t}) + 2{,}15\mathrm{f}_{20}(\mathrm{t}) + 3{,}5\mathrm{f}_{29}(\mathrm{t}) + 4\mathrm{f}_{39}(\mathrm{t}) - 10\mathrm{f}_{50}(\mathrm{t}) \quad (2.43)$$

В цьому прикладі еталонна функція (2.43) знаходиться в тому ж діапазоні частот, що і завада. При цьому відбувається накладання завади на еталонній сигнал, бо шість функцій входять як в g(t), так і в η(t). При цьому базисних

функцій $f_1(t),...,f_{50}(t)$ достатньо також для представлення еталонного сигналу(2.43).

Фактично розкладається сума завади і еталонної функції (2.43) але уже по M=51 функціям внаслідок додавання $f_{(M+1)}$ (t). З врахуванням y(t) всього в розпізнаванні беруть участь 52 функції. Тому, береться N=53.

Результати приведені в Прикладі 3 таблиці 2.1. Отримано $c_{(M+1)}=c_{51}=$-0.49484 замість одиниці.

Тобто в цьому випадку метод не працює.

Із приведених трьох прикладів слідують дві важливі умови:

Кінцева кількість базисних функцій повинна бути достатньою для представлення завади.

Базисних функцій, які визначають заваду, повинно бути недостатньо для представлення еталонного сигналу.

Виходячи із цього, розглянемо наступні приклади.

Приклад 4. Завада має вид (2.41). Еталонна функція відрізняється від (2.43) за рахунок додавання cos(30t) і таким чином відповідає другій умові:

$$g(t)=1,5\cos(t)+3\sin(t)+4,75\sin(2t)-2,5\sin(5t)+10\cos(7t)$$
$$+2,15\sin(10t)+3,5\cos(15t)+4\cos(20t)-10\sin(25t)+5\cos(30t) \qquad 2.44$$

Нехай

$$y(t)=-1,256g(t)+1000\eta(t) \qquad 2.45$$

Тобто треба знайти ваговий коефіцієнт при еталонному сигналі, який практично в 1000 раз менший від коефіцієнта при заваді. Як і в попередньому випадку, в процесі розпізнавання приймають участь 52 функції і N=53.

Результати приведені в колонці Приклад 4 Таблиці 2.1.

Слід звернути увагу, що відбулося розкладання завади. Тому в таблиці приведені її коефіцієнти із (2.39), помножені на 1000. Еталонний сигнал не

розклався. Коефіцієнт $c_{M+1}(t) = c_{51}(t) = -1{,}256$ співпадає із коефіцієнтом при g(t) в (2.45).

Таким чином, установлено, що в y(t) входить еталонній сигнал g(t) із коефіцієнтом -1,256. Відбулося розпізнавання сигналу при наявності адитивної завади і визначення його вагового коефіцієнта.

Приклад 5. Розглянемо випадок, коли до періодичної завади (2.45) додається сигнал g_1 (t):

$$g_1(t) = 5\sin(6t) - 2.5\exp(-t) + 4.5 \qquad (2.46)$$

Він містить постійну складову. Спектр сигналу $g_1(t)$ виходить за межі смуги частот, в якій знаходиться завада.

Нехай

$$y(t) = -1{,}256g(t) + 1000\eta(t) + 0{,}725g\_1\ (t) \qquad (2.47)$$

Крім заданих 50 функцій і y(t) додаються ще дві функції. Тому береться N=54.

Результати показані в “Приклад 5” таблиці 2.1. Для завади отримані такі ж самі результати, як і в попередньому випадку. Відповідно для g(t) і $g_1(t)$ отримані коефіцієнти c_{51}=-1.256 і c_{52}=0.725, які співпадають із коефіцієнтами в (2.47). Тобто відбулося розпізнавання еталонного сигналу g(t), обчислення його вагового коефіцієнта і коефіцієнта при сигналові, який додається до періодичної складової завади. При цьому завада практично має вагу в 1000 раз більшу порівняно із еталонним сигналом.

Приклад 6. Від попереднього відрізняється лише відсутністю g(t) в складі y(t):

$$y(t) = 1000\eta(t) + 0{,}725g_1(t) \qquad (2.48)$$

Як видно із колонки “Приклад 6” таблиці 2.1, коефіцієнт при g(t) $c_{51}=0$, що свідчить про відсутність еталонного сигналу в складі y(t).

Також відомо, що в склад завади входить g_1 (t) з коефіцієнтом $c_{52}=0.725$.

Результати, отримані для випадків 5 і 6 свідчать, що запропонований метод дозволяє розпізнати еталонний сигнал і визначити його ваговий коефіцієнт при наявності комбінованої адитивної завади.

Наведені приклади показують, що задачі розпізнавання сигналів і створення криптосистем можуть бути описані спільними моделями, які зводяться до опису суми функцій з невідомими коефіцієнтами. В обох випадках, поставлена задача може бути вирішена шляхом застосування методу послідовного обчислення інтегральної непропорційності.

Метод демонструє властивості функцій інтегральної непропорційності, застосування яких дозволяє визначати значення невідомих коефіцієнтів при функціях в їх сумі.

На прикладах перевірено, що метод дозволяє правильно визначити значення коефіцієнтів для різних комбінацій між корисним сигналом і завадою. Це демонструє, що описаний метод працює коректно і є придатним до застосування при дешифруванні.

Використовуючи представлені моделі та методи на основі функцій непропорційності, далі пропонується криптосистема на основі функцій дійсних чисел, яка описана в наступному розділі.

2.5. Висновки до другого розділу

1. Представлена математична модель повідомлення, зашифрованого за допомогою суми функцій дійсної змінної. Ці функції представлені у вигляді одновимірних масивів. Для дешифрування повідомлення необхідно обчислювати невідомі коефіцієнти в сумі функції.

2. Описаний метод дешифрування шляхом використання функцій інтегральної непропорційності, який дозволяє обчислити невідомі коефіцієнти при відомих функціях в їх сумі.

3. Перевірено коректність роботи методу на прикладі вирішення прикладної задачі розпізнавання еталонного сигналу при наявності адитивної завади. Продемонстровано, що метод працює коректно і є придатним для використання в криптосистемах.

Основні наукові результати, наведені у другому розділі, опубліковано у працях автора: [2], [9].

РОЗДІЛ 3.
ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ СТВОРЕННЯ КРИПТОГРАФІЧНИХ СИСТЕМ НА ОСНОВІ СУМИ ФУНКЦІЙ ДІЙСНОЇ ЗМІННОЇ

Пропонуються симетричні криптосистеми на основі суми функцій дійсної змінної. При їх реалізації використовуються описані раніше властивості функцій непропорційності.

3.1. Огляд криптографічних систем на основі функцій непропорційності

Відомі декілька варіантів криптосистем, в яких застосовуються функції непропорційності. Так, в 2008 році в патенті [95] була описана система, в якій ASCII-символи шифруються за допомогою суми 10 функцій дійсної змінної, що слугують ключами. Вихідне повідомлення представляється у вигляді числа. Воно розкладається в m-розрядний бінарний код, який містить більше ніж одну одиницю. Кожній ключовій функції передує коефіцієнт, який, в залежності від символу, дорівнює нулю або одиниці. Амплітуди цих функцій випадкові для кожного нового символу. Результуюча сума значень функцій є шифротекстом і передається через канал зв’язку. На приймальній стороні розпізнаються фрагменти функції-ключа, представлені в зашифрованому сигналі, використовуючи функції непропорційності по похідній першого порядку[93]. Завдяки їх властивостям, передані символи розшифровуються в залежності від результатів розпізнавання. Водночас, через використання десяти функцій-ключів та специфіки методу розпізнавання, процес дешифрування в цьому методі є доволі затратним.

Схожі методи розглядається в роботі Калашнікова та інших ([96]), а також в роботі Калашникової та інших ([97]). В цих двох публікаціях запропонований варіант, де символи зашифровані за допомогою лише трьох ключових функцій дійсної змінної. На відміну від попереднього методу, лише чотири символи

шифруються - “1”, “0”, ” “(пробіл) та”” (символ нового рядку), всі інші символи розпізнаються як символ нового рядку. Використовуючи властивості функцій непропорційності по похідній ([98]), розпізнаються коефіцієнти в сумі, і шифротекст розшифровується. Очевидний недолік полягає в цьому, що алфавіт вхідного повідомлення в такому випадку дуже обмежений.

В згаданих роботах використовуються функції непропорційності по похідній першого порядку [93]. В цьому випадку, є необхідність застосовувати чисельні методи для розрахунку поточних значень першої похідної. Необхідність таких обчислень призводить до значного розширення обсягу шифротексту порівняно з повідомленням, що шифрується. Також зазначено, що оскільки процес дешифрування може включати ділення на малі числа, результатом може бути число, яке близьке до нуля, що породжуватиме похибки. Крім того, використання функцій непропорційності по похідній накладає ряд відповідних обмежень щодо виду функцій-ключів - вони мають бути неперервно диференційованими, а їх похідні не мають бути константами.

В роботі [99] , використовується інший підхід. Одна функція дійсної змінної слугує ключем. Вираховується функція непропорційності чисельного представлення повідомлення по відношенню до ключової функції. Отримані значення функції непропорційності і є шифротекстом, який передається через канал зв’язку. При цьому, окремо розглянуті два випадки - для дискретних та аналогових повідомлень.

У випадку з дискретними системи (текст, зображення, і т.д.), повідомлення представляється у вигляді дискретної функції. Оскільки така функція не має неперервних похідних, для шифрування використовується інтегральна непропорційність першого порядку [94] відносно функції-ключа. Дешифрування відбувається операцією, оберненою до обчислення непропорційності.

У випадку з аналоговими сигналами, коли і сигнал, і ключова функція є неперервними, гладкими, і мають першу похідну, використовується непропорційність по похідній першого порядку. Дешифрування виконується шляхом розв’язанням задачі Коші. Втім, зазначено, що приблизне обчислення

значень може породжувати похибки і лавиноподібний ефект, коли все подальше повідомлення буде розшифроване невірно. Тому, метод може потребувати застосування більш точних методів чисельного диференціювання, які є обчислювально обтяжувальними.

Розвиток цієї ідеї представлений у наступній статті [100], де використовуються дві функції-ключі для реалізації послідовного шифрування. Шифрування складається з двох етапів. На першому етапі використовується шифрування за допомогою інтегральної непропорційності відносно першої функції-ключа, так само як і в попередній роботі. Для другого етапу запропоновано дві варіації. У першому випадку, до отриманого шифротексту додаються значення другої функції-ключа, що слугує як різновид скремблінгу. У другому варіанті, шифротекст першого етапу повторно шифрується, знову використовуючи інтегральну непропорційність, але цього разу вже відносно другої функції ключа. Таким чином, здійснюється “serial” шифрування. Запропоновані модифікації мають на меті підвищити складність і стійкість системи за рахунок додаткових операцій.

3.2. Базовий варіант криптографічної системи на основі суми функцій дійсної змінної

Виникає необхідність створити алгоритми шифрування та дешифрування для аналогових та дискретних повідомлень, використовуючи функції дійсної змінної в якості ключа, які були б позбавлені необхідності обчислювати похідні, та поєднували переваги обох класів систем - [97] та [99].

Представлена криптосистема базується на моделі, представленій в Розділі 2.

Повідомлення, що шифрується, представляє собою послідовність одно-байтових цілих чисел довжиною T. У випадку з текстом, це послідовність однобайтових цілих значень, кожне з яких відповідає представленню символу в таблиці ASCII. У випадку з зображенням, це може бути послідовність значень

компонентів пікселів. Також, це може бути просто байтова послідовність, наприклад, у випадку шифрування бінарних об’єктів.

Відповідно до моделі (2.1), ключ складається з системи m функцій дійсної змінної f(x), що задані аналітично або дискретно. Оскільки число функцій має бути достатнім, щоб відповідати кількості бітів елементу, задається m=8 функцій-ключів. Функції-ключі обчислюються у вигляді одновимірних масивів цілих чисел довжиною N. Через вимогу N > m, кількість значень цих масивів має бути не менше 9.

Текстове повідомлення шифрується за допомогою формули (2.1), і результуючий шифротекст у вигляді матриці дійсних чисел y(T,N) передається через канал зв’язку.

Як було показано, задача розшифрування полягає в визначенні, які з заданих функцій-ключів брали участь у шифруванні чергового символу. Іншими словами, задача дешифрування зводиться до визначення коефіцієнтів при ключових функціях. Для цього, використовується метод обчислення за допомогою інтегральної функції непропорційності (2.8), що був перевірений в Розділі 2.

Розглянемо детальніше складові представленої криптосистеми.

3.2.1. Ключ шифрування

Ключ шифрування описує систему з m функцій-ключів. Вони можуть передаватися як в неперервному, так і в дискретному вигляді. Однак, якщо функції-ключі задані неперервно, необхідно, відповідно до (2.1), привести їх до дискретного вигляду.

Для цього треба, щоб обидві сторони знали також і параметри, з якими обчислюються масиви функцій-ключів. Відтак, ці параметри також мають бути частиною ключа шифрування.

Ключ шифрування в неперервному вигляді повинен містити наступні частини:

1. Система з m ключових функцій дійсної змінної f_i, що задані неперервно.
2. Ціле число N, що описує кількість елементів масиву значень ключових функцій.
3. Ціле число h - крок, з яким вираховуються значення функції ключа.
4. x_{min} - початкове значення аргументу, з якого обчислюється значення функції ключа.
5. x_{max} - кінцеве значення аргументу, до якого обчислюється значення функції ключа.
6. Дійсне число ε - точність порівняння, допустиме відхилення від нуля при аналізу значень коефіцієнтів при ключових функціях.

Однак, для шифрування бінарних даних на практиці, крок h дорівнює одиниці. Також, діапазон обчислення аргументу починається з одиниці $x_{min}=1$, а кількість обчислених елементів описується числом N, тому x_{max} можна опустити. Тому, за замовчанням, ключ в неперервному вигляді складається з наступник елементів:

1. Система з m ключових функцій дійсної змінної f_q, що задані неперервно.
2. Ціле число N, що описує кількість елементів масиву значень ключових функцій.
3. Дійсне число ε - точність порівняння, допустиме відхилення від нуля при аналізу значень коефіцієнтів при ключових функціях.

Ключ шифрування в дискретному вигляді являє собою ті ж m ключових функцій дійсної змінної, але заданих дискретно, тобто обчислених відповідно до параметрів N, h, x_{min}, x_{max}.

Таким чином, дискретний ключ представляє собою m одновимірних масивів дійсних чисел довжиною N, тобто матрицю дійсних чисел розмірністю $m \times N$.

Як можна бачити, природа ключа є складеною. При передачі ключа в неперервному вигляді це дозволяє при необхідності змінювати лише його певні складові, не компрометуючи безпеку - наприклад, змінювати нумерацію ключових функцій, їх параметри та складові, не змінюючи вид функцій.

Незалежно від форми ключа при передачі, на початку процесів шифрування/дешифрування, ключ має бути приведений до дискретного вигляду матриці дійсних чисел m×N .

3.2.2. Алгоритм шифрування і шифротекст

Алгоритм шифрування полягає в представлені елементу повідомлення у вигляді суми дійсних чисел з випадковими коефіцієнтами.

Алгоритм шифрування повідомлення довжиною T:

1. Передумови: Для кожної з m функцій-ключів f_q (i), обчислити масив їх N значень, де f_q (i)=f_q (ih), i=1,2,...N - аргумент, q=1,2,..m - порядковий номер функції, при цьому N>m.
2. Для кожного j-го елементу повідомлення довжиною T:
   2.1 Представити елемент повідомлення у бітовому вигляді.
   2.2 Обчислити коефіцієнт k для кожного біту:
      2.2.1 Якщо біт дорівнює нулю, відповідному коефіцієнту k теж присвоїти нуль.
      2.2.2 Якщо біт дорівнює одиниці, відповідному коефіцієнту k присвоїти випадково згенероване значення дійсного типу.
   2.3 Обчислити суму функцій з (2.1).

Масив дійсних чисел довжиною N є представленням елементу в шифротексті. Послідовність із T таких масивів є шифротекстом повідомлення, яке передається через відкритий канал зв’язку. Таким чином, шифротекст представляє собою матрицю дійсних чисел розмірністю N на T.

3.2.3. Алгоритм дешифрування

Задача дешифрування полягає у визначеності коефіцієнтів при ключових функціях, які описують елемент повідомлення. Для розв'язання цієї задачі використовуються метод, продемонстрований в (2.10-2.28) на основі інтегральних функцій непропорційності першого порядку(2.8).

Як і при шифруванні, якщо функції-ключі задані неперервно, необхідно привести їх до дискретного виду, вичисливши їх значення відповідно до заданих параметрів, тобто обчислити масиви $f_q(i) = f_q(ih)$ при i=1,2,...N та q=1,2,..m, де N>m.

Отриманий шифротекст представляється у вигляді T одновимірних масивів y(j,i), де j=1,2,...T, а i=1,2,...N.

Оскільки для шифрування одно-байтового символу використовуються m=8 ключових функцій, j-й символ описується так:

$$y(j,i) = k_1 f_1(x) + k_2 f_2(x) + k_3 f_3(x) + k_4 f_4(x) + k_5 f_5(x) + k_6 f_6(x) + k_7 f_7(x) + k_8 f_8(x) \quad (3.1)$$

Алгоритм дешифрування:

1. Передумови: Для кожної з m функцій-ключів f_q (i), обчислити масив їх N значень, де f_q (i)=f_q (ih), i=1,2,...N - аргумент, q=1,2,..m - порядковий номер функції, при цьому N>m.
2. Для кожного елементу шифротексту y(j,i) застосувати Багаторівневий алгоритм розпізнавання коефіцієнтів, який отримує значення k.
3. По-бітово відтворити елемент шифротексту шляхом порівняння k з нулем з точністю ε.

Для розпізнавання коефіцієнтів використовується багаторівневий алгоритм розпізнавання, який використовує властивості непропорційностей. Він містить

стільки же рівнів, скільки і ключових функцій. Відповідно, розглядається вісім рівнів обчислень.

Функції непропорційності означаються нотацією $F_{\ln(j,i)}$, де l - рівень, n - порядковий номер для обчислення непропорційності на поточному рівні. Число обчислень на кожному рівні варіюється від восьми на першому рівні до одного на останньому. Повний опис обчислень восьми рівнів наводиться нижче.

3.2.4. Багаторівневий алгоритм розпізнавання коефіцієнтів для восьми ключових функцій

Перший рівень Спочатку необхідно вибрати будь-яку функцію з набору функцій-ключів. Наприклад, виберемо f_1 (i). Далі, обчислимо функцію непропорційності y(j,i) відносно f_1 (i). Це позначається як F_{11}(j,i-1).

$$\left(F_{11}(j,i-1)\& = @I^{(1)}_{f_1(i)} y(j,i)@\& = \frac{y(j,i-1)+y(j,i)}{f_1(i-1)+f_1(i)} - \frac{y(j,i)}{f_1(i)}\right.$$
$$= k_{1j}\left[\frac{f_1(i-1)+f_1(i)}{f_1(i-1)+f_1(i)} - \frac{f_1(i)}{f_1(i)}\right] + k_{2j}\left[\frac{f_2(i-1)+f_2(i)}{f_1(i-1)+f_1(i)} - \frac{f_2(i)}{f_1(i)}\right] + \cdots$$
$$\left. + k_{8j}\left[\frac{f_8(i-1)+f_8(i)}{f_1(i-1)+f_1(i)} - \frac{f_8(i)}{f_1(i)}\right]\right) \tag{3.2}$$

де i=1,2,…,N-1.

Непропорційності (4.17) повинні також бути обчислені для інших ключових функцій відносно f_1(i). Вони позначаються як F_{1r} (j,i-1), де r=2,3,…,8.

$$F_{1r}(j,i-1) = @I^{(1)}_{f_1(i)} f_r(i) = \frac{f_r(i-1)+f_r(i)}{f_1(i-1)+f_1(i)} - \frac{f_r(i)}{f_1(i)} \tag{3.3}$$

У (3.2) непропорційність f_1 (j,i) обчислюється відносно самої себе, де вона дорівнює нулю. Після підстановки (3.3) в (3.2) отримуємо

$$F\_11\ (j,i) = k\_2j\ F\_12\ (j,i) + k\_3j\ F\_13\ (j,i) + \cdots + k\_8j\ F\_18\ (j,i) \tag{3.4}$$

де i=0,1,…,N-1.

Другий рівень. Оберемо будь-яку непропорційність з (3.4), наприклад F_{12} (j,i). Тоді обчислимо непропорційність (4.17) F_{11} (j,i) відносно F_{12} (j,i):

$$\begin{array}{ll} F_{21}(j,i-1) & = \\ I^{(1)}_{F_{12}(j,i)} F_{11}(j,i) & \square \\ \square & = \dfrac{F_{11}(j,i-1)+F_{11}(j,i)}{F_{12}(j,i-1)+F_{12}(j,i)} - \dfrac{F_{11}(j,i)}{F_{12}(i)} \\ \square & = k_{2j}\left[\dfrac{F_{12}(j,i-1)+F_{12}(j,i)}{F_{12}(j,i-1)+F_{12}(j,i)} - \dfrac{F_{12}(j,i)}{F_{12}(i)}\right] \\ \square & + k_{3j}\left[\dfrac{F_{13}(j,i-1)+F_{13}(j,i)}{F_{12}(j,i-1)+F_{12}(j,i)} - \dfrac{F_{13}(j,i)}{F_{12}(i)}\right] \\ \square & + \cdots + \\ \square & + k_{8j}\left[\dfrac{F_{18}(j,i-1)+F_{18}(j,i)}{F_{12}(j,i-1)+F_{12}(j,i)} - \dfrac{F_{18}(j,i)}{F_{12}(i)}\right] \end{array} \tag{3.5}$$

де i=1,2,…,N-2.

Також необхідно обчислити непропорційності (2.8) для решти функцій непропорційності, які були обчислені на першому рівні, відносно F_{12} (i). Позначимо їх як F_{2r} (j,i), r=2,3,…,7.

$$F_{2r}(j,i-1) = @I^{(1)}_{F_{12}(j,i)} F_{1r}(j,i) = \frac{F_{1r}(j,i-1)+F_{1r}(j,i)}{F_{12}(j,i-1)+F_{12}(j,i)} - \frac{F_{1r}(j,i)}{F_{12}(i)} \tag{3.6}$$

де i=1,2,…,N-2.

Непропорційність F_{12} (j,i) відносно себе дорівнює нулю. Таким чином, з рівняння (3.5) отримуємо наступний вираз:

$$F_{21}(j,i) = k_{3j}F_{22}(j,i) + k_{3j}F_{23}(j,i) + \cdots + k_{8j}F_{27}(j,i) \tag{3.7}$$

де i=0,1,…,N-2.

Третій рівень. Виберемо будь-яку непропорційність з правої частини рівняння (3.7). Нехай це буде F_{22} (j,i). Тоді обчислимо непропорційність F_{21} (j,i) відносно F_{22} (j,i), яка позначається як F_{31}.

$$\begin{array}{c} F_{31}(j,i-1) \\ I^{(1)}_{F_{22}(j,i)}F_{21}(j,i) \end{array} = \frac{F_{21}(j,i-1)+F_{21}(j,i)}{F_{22}(j,i-1)+F_{22}(j,i)} - \frac{F_{21}(j,i)}{F_{22}(i)}$$

$$= k_{3j}\left[\frac{F_{22}(j,i-1)+F_{22}(j,i)}{F_{22}(j,i-1)+F_{22}(j,i)} - \frac{F_{22}(j,i)}{F_{22}(i)}\right]$$

$$+k_{4j}\left[\frac{F_{23}(j,i-1)+F_{23}(j,i)}{F_{22}(j,i-1)+F_{22}(j,i)} - \frac{F_{23}(j,i)}{F_{22}(i)}\right]$$

$$+\cdots+$$

$$+k_{8j}\left[\frac{F_{27}(j,i-1)+F_{27}(j,i)}{F_{22}(j,i-1)+F_{22}(j,i)} - \frac{F_{27}(j,i)}{F_{22}(i)}\right] \quad (3.8)$$

де i=1,2,…,N-3.

Непропорційності F_{3r} (j,i-1) теж повинні бути обчислені, де r=2,3,…,6.

$$F_{3r}(j,i-1) = @I^{(1)}_{F_{22}(j,i)}F_{2r}(j,i) = \frac{F_{2r}(j,i-1)+F_{2r}(j,i)}{F_{22}(j,i-1)+F_{22}(j,i)} - \frac{F_{2r}(j,i)}{F_{22}(i)} \quad (3.9)$$

З формули (3.8), враховуючи (3.9), отримуємо:

$$F_{31}(j,i) = k_{4j}F_{32}(j,i) + k_{5j}F_{33}(j,i) + \cdots + k_{8j}F_{36}(j,i) \quad (3.10)$$

де i=0,1,…,N-3.

Четвертий рівень

Виберемо будь-яку непропорційність з (3.10), наприклад F_{32}(j,i), і обчислимо непропорційність F_{41}(j,i-1) функції F_{31}(j,i) відносно F_{32} (j,i):

$$\left(F_{41}(j,i-1) = @I^{(1)}_{F_{32}(j,i)} F_{31}(j,i) = \frac{F_{31}(j,i-1)+F_{31}(j,i)}{F_{32}(j,i-1)+F_{32}(j,i)} - \frac{F_{31}(j,i)}{F_{32}(i)}\right.$$
$$= k_{4j}\left[\frac{F_{32}(j,i-1)+F_{32}(j,i)}{F_{32}(j,i-1)+F_{32}(j,i)} - \frac{F_{32}(j,i)}{F_{32}(i)}\right]$$
$$+ k_{5j}\left[\frac{F_{33}(j,i-1)+F_{33}(j,i)}{F_{32}(j,i-1)+F_{32}(j,i)} - \frac{F_{33}(j,i)}{F_{32}(i)}\right] + \cdots$$
$$\left. + k_{8j}\left[\frac{F_{36}(j,i-1)+F_{36}(j,i)}{F_{32}(j,i-1)+F_{32}(j,i)} - \frac{F_{36}(j,i)}{F_{32}(i)}\right]\right) \tag{3.11}$$

де i=1,2...N-4.

Обчислимо непропорційність F_{4r} (j,i-1), при r=2,3,4, та 5.

$$F_{4r}(j,i-1) = @I^{(1)}_{F_{32}(j,i)} F_{3r}(j,i) = \frac{F_{3r}(j,i-1)+F_{3r}(j,i)}{F_{32}(j,i-1)+F_{32}(j,i)} - \frac{F_{3r}(j,i)}{F_{32}(i)} \tag{3.12}$$

Якщо ми враховуємо, що (3.11) включає нульову непропорційність, то з (3.11) та (3.12) випливає, що

$$F_{41}(j,i) = k_{5j}F_{42}(j,i) + k_{6j}F_{43}(j,i) + k_{7j}F_{44}(j,i) + k_{8j}F_{45}(j,i) \tag{3.13}$$

де i=0,1,…,N-4.

П'ятий рівень. Наприклад, оберемо F_{42} (j,i) з (3.13) для наступних обчислень і обчислимо непропорційність F_{51} (j,i-1) функції F_{41} (j,i) відносно F_{42} (j,i):

$$\begin{aligned} F_{51}(j,i-1) &= @I^{(1)}_{F_{42}(j,i)} F_{41}(j,i) \\ &= \frac{F_{41}(j,i-1)+F_{41}(j,i)}{F_{42}(j,i-1)+F_{42}(j,i)} - \frac{F_{41}(j,i)}{F_{42}(i)} \\ &= k_{5j}\left[\frac{F_{42}(j,i-1)+F_{42}(j,i)}{F_{42}(j,i-1)+F_{42}(j,i)} - \frac{F_{42}(j,i)}{F_{42}}\right] \\ &+k_{6j}\left[\frac{F_{43}(j,i-1)+F_{43}(j,i)}{F_{42}(j,i-1)+F_{42}(j,i)} - \frac{F_{43}(j,i)}{F_{42}(i)}\right] \\ &+k_{7j}\left[\frac{F_{44}(j,i-1)+F_{44}(j,i)}{F_{42}(j,i-1)+F_{42}(j,i)} - \frac{F_{44}(j,i)}{F_{42}(i)}\right] \\ &+k_{8j}\left[\frac{F_{45}(j,i-1)+F_{45}(j,i)}{F_{42}(j,i-1)+F_{42}(j,i)} - \frac{F_{45}(j,i)}{F_{42}(i)}\right] \end{aligned} \quad 3.14$$

де i=1,2,…,N-5. Також слід обчислити непропорційність F_{5r} (j,i).

$$F_{5r}(j,i-1) = @I^{(1)}_{F_{42}(j,i)} F_{4r}(j,i) = \frac{F_{4r}(j,i-1)+F_{4r}(j,i)}{F_{42}(j,i-1)+F_{42}(j,i)} - \frac{F_{4r}(j,i)}{F_{42}(i)} \qquad (3.15)$$

Використовуючи (3.14) та (3.15), отримуємо:

$$F_{51}(j,i) = k_{6j}F_{52}(j,i) + k_{7j}F_{53}(j,i) + k_{8j}F_{54}(j,i) \qquad (3.16)$$

де i=0,1,…,N-5.

Шостий рівень. Нехай непропорційність F_{52} (j,i) вибрана з (3.16). Тоді обчислимо непропорційність F_{61} (j,i-1) функції F_{51} (j,i) відносно F_{52} (j,i):

$$\begin{aligned} F_{61}(j,i-1) &= @I^{(1)}_{F_{52}(j,i)} F_{51}(j,i) \\ &= \frac{F_{51}(j,i-1)+F_{51}(j,i)}{F_{52}(j,i-1)+F_{52}(j,i)} - \frac{F_{51}(j,i)}{F_{52}(i)} \\ &= k_{6j}\left[\frac{F_{52}(j,i-1)+F_{52}(j,i)}{F_{52}(j,i-1)+F_{52}(j,i)} - \frac{F_{52}(j,i)}{F_{52}(i)}\right] \\ &+k_{7j}\left[\frac{F_{53}(j,i-1)+F_{53}(j,i)}{F_{52}(j,i-1)+F_{52}(j,i)} - \frac{F_{53}(j,i)}{F_{52}(i)}\right] \\ &+k_{8j}\left[\frac{F_{54}(j,i-1)+F_{54}(j,i)}{F_{52}(j,i-1)+F_{52}(j,i)} - \frac{F_{54}(j,i)}{F_{52}(i)}\right] \end{aligned} \qquad (3.17)$$

де i=1,2,…,N-6.

Також обчислені непропорційності F_{6r} (j,i-1), r=2,3.

$$F_{6r}(j,i-1) = @I^{(1)}_{F_{52}(j,i)} F_{5r}(j,i) = \frac{F_{5r}(j,i-1)+F_{5r}(j,i)}{F_{52}(j,i-1)+F_{52}(j,i)} - \frac{F_{5r}(j,i)}{F_{52}(i)} \qquad (3.18)$$

Після підстановки (3.18) в (3.17) і враховуючи, що перший член в (3.17) дорівнює нулю, отримуємо:

$$F_{61}(j,i) = k_{7j}F_{62}(j,i) + k_{8j}F_{63}(j,i) \qquad (3.19)$$

де i=0,1,…,N-6.

Сьомий рівень. Виберемо F_{62} (j,i) з рівняння (3.19) і обчислимо наступні непропорційності:

$$\begin{aligned} F_{71}(j,i-1) &= @I^{(1)}_{F_{62}(j,i)} F_{61}(j,i) \\ &= \frac{F_{61}(j,i-1)+F_{61}(j,i)}{F_{62}(j,i-1)+F_{62}(j,i)} - \frac{F_{61}(j,i)}{F_{62}(i)} \\ &= k_{7j}\left[\frac{F_{62}(j,i-1)+F_{62}(j,i)}{F_{62}(j,i-1)+F_{62}(j,i)} - \frac{F_{62}(j,i)}{F_{62}(i)}\right] \\ &+k_{8j}\left[\frac{F_{63}(j,i-1)+F_{63}(j,i)}{F_{62}(j,i-1)+F_{62}(j,i)} - \frac{F_{63}(j,i)}{F_{62}(i)}\right] \end{aligned} \tag{3.20}$$

де i=1,2,…,N-7.

$$F_{72}(j,i-1) = @I^{(1)}_{F_{62}(j,i)} F_{63}(j,i) = \frac{F_{63}(j,i-1)+F_{63}(j,i)}{F_{62}(j,i-1)+F_{62}(j,i)} - \frac{F_{63}(j,i)}{F_{62}(i)} \tag{3.21}$$

Після підстановки (3.21) в (3.20) отримуємо наступний вираз:

$$F_{71}(j,i) = k_{8j} F_{72}(j,i) \tag{3.22}$$

де i=0,1,…N-7.

Восьмий рівень. На останньому, восьмому рівні залишається одна непропорційність, яка обчислюється наступним чином:

$$\begin{aligned} F_{81}(j,i-1) &= @I^{(1)}_{F_{72}(j,i)} F_{71}(j,i) \\ &= \frac{F_{71}(j,i-1)+F_{71}(j,i)}{F_{72}(j,i-1)+F_{72}(j,i)} - \frac{F_{71}(j,i)}{F_{72}(i)} \\ &= k_{8j}\left[\frac{F_{72}(j,i-1)+F_{72}(j,i)}{F_{72}(j,i-1)+F_{72}(j,i)} - \frac{F_{72}(j,i)}{F_{72}(i)}\right] \\ &= 0 \end{aligned} \tag{3.23}$$

Як видно з (3.22), непропорційності F_{71} (j,i) та F_{72} (j,i) пропорційно пов'язані. Цей результат дозволяє обчислити невідомі коефіцієнти k_{1j}, k_{2j}, …, та k_{8j} в (3.1).

Нагадаємо, що ці коефіцієнти є випадковими амплітудами ключових функцій, що і містять інформацію про передане повідомлення.

Так, з (3.22) обчислюємо:

$$k_{8j} = \frac{F_{71}(j,i)}{F_{72}(j,i)} \tag{3.24}$$

Решта коефіцієнтів були обчислені за допомогою формул (3.19, 3.16, 3.13, 3.10, 3.7, 3.4, 3.1).

$$k_{7j} = \frac{F_{61}(j,i) - k_{8j}F_{63}(j,i)}{F_{62}(j,i)} \tag{3.25}$$

$$k_{6j} = \frac{F_{51}(j,i) - k_{7j}F_{53}(j,i) - k_{8j}F_{54}(j,i)}{F_{52}(j,i)} \tag{3.26}$$

$$k_{5j} = \frac{F_{41}(j,i) - k_{6j}F_{43}(j,i) - k_{7j}F_{44}(j,i) - k_{8j}F_{45}(j,i)}{F_{42}(j,i)} \tag{3.27}$$

$$k_{4j} = \frac{F_{31}(j,i) - k_{5j}F_{33}(j,i) - k_{6j}F_{34}(j,i) - k_{7j}F_{35}(j,i) - k_{8j}F_{36}(j,i)}{F_{32}(j,i)} \tag{3.28}$$

$$k_{3j} = \frac{F_{21}(j,i) - k_{4j}F_{23}(j,i) - k_{5j}F_{24}(j,i) - k_{6j}F_{25}(j,i) - k_{7j}F_{26}(j,i)) - k_{8j}F_{27}(j,i)}{F_{22}(j,i)} \tag{3.29}$$

$$k_{2j} = \frac{F_{11}(j,i) - k_{3j}F_{13}(j,i) - k_{4j}F_{14}(j,i) - k_{5j}F_{15}(j,i) - k_{6j}F_{16}(j,i)) - k_{7j}F_{17}(j,i) - k_{8j}F_{18}(j,i)}{F_{12}(j,i)} \tag{3.30}$$

$$k_{1j} = \frac{y(j,i) - k_{2j}f_2(i) - k_{3j}f_3(i) - k_{4j}f_4(i) - k_{5j}f_5(i) - k_{6j}f_6(i) - k_{7j}f_7(i) - k_{8j}f_8(i)}{f_1(i)} \tag{3.31}$$

В залежності від того, які з цих коефіцієнтів дорівнюють нулю, а які ні, відтворюється і розшифровується j-й символ повідомлення. Нульовий коефіцієнт означає нульовий біт у відповідний позиції, не нульовий коефіцієнт означає одиничний біт у відповідній позиції.

На практиці, при обчисленні непропорційності відносно інших непропорційностей можуть накопичуватися похибки. На останньому рівні результат може не бути строго рівним нулю, але наближатися до нього. Тому, необхідно порівнювати непропорційність (3.23), обчислену на останньому рівню, не строго з нулем, а по модулю з точністю ε . Якщо модуль коефіцієнта на останньому рівні менший або рівний ε, вважається, що між розглянутими функціями існує пропорційний зв'язок. Наприклад, якщо задано $\varepsilon=10^{-4}$, то при $|F_{81}(j,i)| \le \varepsilon$, значення вважається рівним нулю.

Значення, ε визначається при тестуванні криптосистеми. Теоретично, ця непропорційність дорівнює нулю для всіх i=2,3,...N, але, враховуючи похибки обчислення, рекомендується виконувати обчислення за допомогою формул (3.25-3.31) для і, при якому модуль непропорційності (3.23) мінімальний.

3.2.5. Вимоги до функцій-ключів

1. Ключові функції мають бути дійсного типу.

2. Вони не можуть бути константними і не повинні приймати нульових значень.

3. При використанні ключової функції не повинно виникати ситуації, коли ділення на число, близьке до нуля, призводить до неприпустимої помилки обчислення. Для цього рекомендується перевірити криптосистему на весь алфавіт символів, які будуть використовуватися в повідомленнях.

4. Необхідно перевірте, щоб сума двох або більше ключових функцій не збігалася з будь-якою іншою з ключових функцій.

5. Рекомендується включати всі параметри у вираз для кожної ключової функції. У цьому випадку зміна значення будь-якого параметра призводить до зміни всіх ключових функцій, а не однієї або декількох з них.

6. Перш ніж надсилати зашифроване повідомлення, треба зробити тестове розшифрування, щоб уникнути помилок, які можуть виникнути в результаті недотримання попередніх пунктів.

3.2.6 Приклад шифрування тексту і аналіз результатів

Розглянемо приклад шифрування і дешифрування символів з таблиці ASCII-кодів.

Задана система з m=8 наступних функцій-ключів:

$$f_1(x) = 1000\sin\big((\alpha_1 - \beta_1)x\big)\cos(w\beta_1 x)$$
$$f_2(x) = 1000\exp(0.1\alpha_2 x)\sin(w\beta_2 x)\cos\big((\alpha_2 + \beta_2)x\big)$$
$$f_3(x) = 1000\exp(-\alpha_3 x)\sin(w\beta_3 x)$$
$$f_4(x) = 1000\cos\big((\alpha_1 x - \beta_1)x\big)\sin(w\beta_1 x)$$
$$f_5(x) = 1000\exp(0.1\sin(\alpha_2 x))\sin\big(wcos(\beta x)\big)\cos\big((\alpha_2 + \beta_2)x\big)$$
$$f_6(x) = 1000\sin(-\cos(\alpha_3 x))\cos\big(wsin(\beta_3 x)\big)$$
$$f_7(x) = 1000\sin(wx + \alpha_1)\exp(-\beta_1 x^2)$$
$$f_8(x) = 1000\cos(w\gamma x^2)$$

(3.32)

Де значення констант наступні:

α_1 =1, α_2=0.12, α_3=0.5, β_1=0.1, β_2=1.5, β_3=0.7, γ=0.5, w=400.

Зашифруємо послідовність чисел, що відповідають ASCII-символам. Кожен символ представлений сумою (3.1) восьми ключових функцій (3.32):

Враховуючи вимогу, що довжина масиву шифру N має бути більшою за кількість функцій m, задано N=16.

В таблиці 3.1 у верхньому горизонтальному рядку показані символи переданого повідомлення “Hello”. Відповідні шифри подані у вигляді масивів, розташовані вертикально. Розшифровані символи розташовані горизонтально в нижньому рядку.

Очевидно, що отримане повідомлення збігається з переданим. Слід зазначити, що шифри-масиви сусідніх символів літери ‘l’ абсолютно різні. Коди інших суміжних однакових символів у повідомленні наведені в таблиці 3.2.

Таблиця 3.1 – Шифротекст повідомлення “Hello”

y	‘H’	‘e’	‘l’	‘l’	‘o’
0	-323.36050	-1096.0141	-872.47149	37.134528	-112.93721
1	257.702939	167.391848	1051.01033	532.400561	427.740614
2	57.298613	175.907791	-408.37541	-216.26334	-116.65218
3	-165.32821	126.358160	-324.75198	-162.19800	-197.22270
4	-186.82906	-394.77504	-929.02530	-439.94548	-449.01146
5	-163.70378	-392.33753	-1059.2853	-385.85981	-170.75848
6	37.446166	299.880685	370.310135	74.675455	44.746439
7	-110.70494	426.787248	-218.90900	-238.68403	-314.75860
8	-2.714026	-59.278796	115.564604	-2.371129	-165.23427
9	9.436954	152.916970	116.697501	-23.361501	281.220083
10	42.465400	-412.02347	-203.82595	84.424717	150.029168
11	-24.295297	615.002251	349.117675	-42.371452	-231.55086
12	101.570285	95.754178	543.764259	227.452661	-122.68102
13	195.422364	132.219196	855.514365	432.359247	754.345004
14	-11.067358	-507.14921	-252.27430	-29.696351	228.457327
15	214.445079	264.682389	659.731238	467.369970	-63.039751

Таблиця 3.2 – Шифротекст повідомлення “AAAAA”

y	‘A’	‘A’	‘A’	‘A’	‘A’
0	-597.135343	-762.540347	-609.489179	-1245.052456	-917.400855
1	9.473961	-6.667141	-2.760240	-37.310266	-17.407304
2	274.695430	368.229254	291.933312	625.796927	451.736269
3	15.193014	87.216540	60.428145	237.898008	138.849052
4	-123.497929	-217.377766	-165.579209	-438.953490	-291.370618
5	-58.830278	-107.584825	-81.548078	-221.367775	-145.669069
6	-8.280530	-11.911812	-9.337867	-21.332769	-14.999968
7	199.488556	342.700766	261.876769	683.403833	456.291669
8	-76.316724	-131.227388	-100.265637	-261.818697	-174.769533
9	-60.158608	103.377062	78.993047	-206.183725	137.653657
10	-125.104506	-215.011307	-164.292499	-428.868345	-286.313719
11	214.641127	368.892513	281.874942	735.803375	491.224813
12	-14.047252	24.142272	18.447384	-48.154847	-32.148341
13	6.530344	11.223364	8.575899	22.386440	14.945262
14	-223.052958	-383.349601	-292.921754	-764.640006	-510.476209
15	169.891087	291.983039	223.107534	582.397666	388.810617

Наведені вище результати вказують на те, що шифри суміжних ідентичних символів у повідомленні відрізняються один від одного. Ця властивість значно ускладнює злам криптосистеми методом грубої сили. Щоб зламати шифр,

необхідно підібрати як форму восьми ключових функцій, так і значення їх параметрів.

Наведено приклад, який ілюструє стійкість системи до отримання ключів, навіть якщо якимось чином вдалося дізнатися форми ключових функцій. Припустимо, що наведена вище послідовність символів зашифрована за допомогою функцій (3.32) і розшифрована за допомогою тих самих функцій, але константа w була визначена неправильно. Замість w = 400 було використано w = 399.999 під час дешифрування. У цьому випадку непропорційність на останньому восьмому рівні за абсолютною величиною перевищує допустиме відхилення ε від нуля. Тобто розшифровка неможлива. Тільки якщо w = 399.9999, повідомлення може бути розшифровано. Цей результат показує, що навіть таке незначне відхилення одного з параметрів ключових функцій не дозволяє розшифрувати переданий символ.

3.2.7.Приклад шифрування зображення і аналіз результатів

Представлення даних. Приведемо приклад роботи алгоритму для шифрування зображення замість текстових повідомлень. Розглядається шифрування візуальних даних зображення з кольоровою схемою RGBA.

Позаяк представлені методи є криптосистемою загального призначення, модифікації алгоритм не потребує. Однак, так як в зазначеному варіанті шифрується саме візуальна інформація, а не весь бінарний файл, потрібно представити зображення у вигляді масивів y.

В кольоровій схемі RGBA, кожен піксель зображення представлений у вигляді чотирьох однобайтових компонентів, значення яких варіюються від 0 до 255. Кожне значення відповідає яскравості відповідного компоненту - червоного R, зеленого G, та синього B. Останній компонент альфа A описує прозорість.

Так, зображення представляється у вигляді чотирьох масивів одно-байтових значень R, G, B, A довжиною яких дорівнює кількості пікселів в зображенні. Послідовність цих масивів є повідомленням, що передається на вхід

в алгоритм шифрування. Таким чином, шифротекст у складається з чотирьох частин y_r, y_g, y_b, y_a кожного компоненту відповідно. Їх можна передавати через канал зв'язку послідовно або паралельно.

Після дешифрування, з розшифрованих значень компонентів відтворюється візуальна інформація зображення.

Приклади. Розглянемо приклад шифрування зображення (Рис. 3.1), яке має формат PNG, та розмір 300×300 пікселів. В якості ключа знову використана система функцій (3.32) з такими значеннями констант: $\alpha_1=1$, $\alpha_2=0.12$, $\alpha_3=0.5$, $\beta_1=0.1$, $\beta_2=1.5$, $\beta_3=0.7$, $\gamma=0.5$, $w=100$

В результаті шифрування та дешифрування отримано зображення (Рис. 3.2), яке є по-піксельно ідентичним оригінальному.

Рис. 3.1 – Оригінальне зображення

Рис. 3.2 – Дешифроване зображення

В цьому прикладі, зображення є непрозорим, тобто компонент прозорості A для всіх пікселів незмінний і дорівнює 255. Тим не менш, шифротекст y_a кожного значення цього компоненту відрізняються і є випадковим, що ілюструє Таблиця 3.3. По горизонталі, таблиця показує значення значення A перших чотирьох пікселів зображення. По вертикалі, показані відповідний шифротекст кожного значення - одновимірні масиви дійсних чисел y_a.

Таблиця 3.3 – Шифротекст однакових компонентів непрозорості

y_a	$A_0 = 255$	$A_1 = 255$	$A_2 = 255$	$A_3 = 255$
0	-7.90961	-2.27316	-0.03674	-5.54336
1	1.10056	-6.28811	-3.46288	0.16009
2	7.28851	15.6825	9.01487	1.11380
3	0.59911	-7.33486	-5.80853	3.12199
4	-2.29156	-7.97004	-6.38325	-1.34180
5	-2.54780	-5.40779	-5.46397	-5.23169
6	-3.35284	-14.3582	-11.5202	2.28306
7	-0.92275	2.96268	-0.09732	-6.35736
8	-1.91578	-1.74340	-2.99941	-3.37424
9	5.33770	14.6850	10.2739	0.560757
10	-5.42285	-2.67856	-3.92203	-5.13982
11	2.83398	2.71203	1.68157	4.87892
12	1.02335	0.18559	0.42701	-0.72213
13	4.80636	4.68834	4.42991	3.74912
14	1.82292	-7.24611	-2.16100	12.4323
15	4.16886	6.44373	2.90908	-5.54336

Для зламу методом грубої сили, необхідно вгадати функції-ключі, так само як і значення їх параметрів.

Зображення 3 показує зображення, дешифроване з невірним ключом. А саме, параметр w=100.1 замість коректного значення w=100, при правильно підібраних ключових функціях та значень інших параметрів. Як можна бачити, навіть найменше відхилення значення лише одного параметру породжує цілком невірне зображення.

Рис. 3.3 – Невірно дешифроване зображення

Варто зазначити, що структура описаної криптосистеми дозволяє робити подальші модифікації та комбінування з іншими підходами.

Для ще більшого підвищення криптостійкості, запропоновані декілька варіантів ускладнень представленою криптосистеми

3.3. Модифікація криптографічної системи з додатковим етапом шифрування

Для ще більшого ускладнення задачі криптоаналізу, пропонується поєднати створену криптосистему з методом шифрування за допомогою інтегральної непропорційності, розглянутим в [99].

Таким чином, пропонується комбінована криптосистема з двох-етапними алгоритмом шифрування та дешифрування.

Перший етап шифрування полягає у вже описаному методі шифрування сумою функцій дійсної змінної. На другому етапі, кожен з масивів шифротексту додатково шифрується шляхом обчислення інтегральної непропорційності відносно додаткової функції-ключа. В якості функції-ключа другого етапу можна використовувати як одну з набору вже наявних, або задати нову відмінну від них. Дешифрування також складається з двох етапів. На першому етапі, розшифровується проміжний шифротекст за допомогою функції-ключа, отримуючи суму функцій з невідомими коефіцієнтами. Це відбувається за

допомогою застосування зворотної формули інтегральної непропорційності (2.9):

На другому етапі, коефіцієнти розпізнаються вже описаним багаторівневим алгоритмом, розшифровуючи передане повідомлення.

Ключ шифрування

Як і в основній версії, ключ шифрування містить набір з m ключових функцій дійсної змінної f_i, які використовуються для шифрування першого етапу. До складу ключа додається ще одна додаткова функція дійсної змінної P, що використовується на другому етапі. Ця функція може співпадати з однією з вже наявних функцій-ключів fi, хоча може бути і окремо заданою. Як завжди, функції мають бути узгодженими між сторонами, вони можуть бути задані як дискретно, так і неперервно. В другому випадку, сторони мають узгодити інтервал дискретизації, крок h та кількість елементів N масиву, що представляють кожну функцію.

Перед початком процесу шифрування/дешифрування, відповідна сторона має попередньо обчислити N елементів одновимірних масивів як функцій-ключів f_i, так і P.

Отже, складові ключа:

1. Система з m ключових функцій дійсної змінної f_q, що задані неперервно або дискретно.
2. Функція-ключ другого етапу P.
3. Ціле число N, що описує кількість елементів масиву значень ключових функцій.
4. Дійсне число ε - точність порівняння.

Алгоритм шифрування

Алгоритм шифрування складається з двох етапів.

1. Передумови:
    a. Для кожної з m функцій-ключів $f_q(i)$, обчислити масив їх N значень, де $f_q(i) = f_q(ih)$, $i = 1,2,\dots N$ - аргумент, $q = 1,2,..m$ - порядковий номер функції, при цьому $N > m$.

b. Обчислити масив з N значень функції-ключа $P(i)$, де $P(i) = P(ih)$, $i = 1,2,\dots N$ - аргумент.

2. Перший етап Обрахувати суму функцій (2.1) за вже описаним алгоритмом шифрування 1. Результуючий масив $y(i,j)$ слугує проміжним шифротекстом.
3. Другий етап: Обчислити інтегральну непропорційність (2.8) масиву $y(j,i)$ відносно $P(i)$, отримуючи шифротекст $z(j,i)$:

$$z(j,i) = @I_{P_i}^{(1)} y_i = \frac{y(j,i-1) + y(j,i)}{P(i-1) + P(i)} - \frac{y(j,i)}{P(i)} \tag{3.33}$$

Алгоритм дешифрування

Алгоритм дешифрування також складається з двох етапів.

1. Передумови:
   a. Для кожної з m функцій-ключів $f_q(i)$, обчислити масив їх N значень, де $f_q(i) = f_q(ih)$, $i = 1,2,\dots N$ - аргумент, $q = 1,2,..m$ - порядковий номер функції, при цьому $N > m$.
   b. Обчислити масив з N значень функції-ключа $P(i)$, де $P(i) = P(ih)$, $i = 1,2,\dots N$ - аргумент.
2. Перший етап: Розшифрувати проміжний шифротекст $y(j,i)$, використовуючи ключ P та обернену формулу інтегральної непропорційності (2.9) з $y(j,0) = z(j,0)$:

$$y(j,i) = \frac{\Big(y(j,i-1) - z(j,i)\big(P(i-1) + P(i)\big)\Big)P(i)}{P(i-1)} \tag{3.34}$$

3. Другий етап: Розшифрувати текст, за допомогою багаторівневого алгоритму розпізнавання коефіцієнтів.

Приклад роботи та результати

Наведемо приклад роботи криптосистеми для символів з таблиці ASCII та проаналізуємо отримані результати. Знову використаємо систему ключових функцій (3.32), де значення констант наступні: $\alpha_1 = 1$, $\alpha_2 = 0.12$, $\alpha_3 = 0.5$, $\beta_1 = 0.1$, $\beta_2 = 1.5$, $\beta_3 = 0.7$, $\gamma = 0.5$, $w = 400$

Так само, на першому етапі кожен символ представляється масивом $y(x)$. Крок зміни аргументу $h = 1$, аргумент $x = (i + 1)h$, $i = 0,1,2,\dots,N-1$, а кількість елементів кожного одновимірного масиву $N = 16$. В якості ключової функції P другого етапу шифрування обрана восьма функція $f_8(x)$ з (3.32) .

Так, для j-го символу була обчислена інтегральна непропорційність шифротексту $z(j,i)$ (2.8) масиву проміжного шифротексту $y(j,i)$ (3.1) відносно $f_8(i)$.

У цьому випадку $z(j,0) = y(j,0)$. Відповідно, на першому етапі розшифрування (3.34), замість $P(i)$, підставляється функція $f_8(i)$, $i = 0,1,\dots,N-1$.

$$y(j,i) = \Big(y(j,i-1) - z(j,i)\big(f_8(i-1) + f_8(i)\big)\Big)\frac{f_8(i)}{f_8(i-1)} \quad 3.35$$

Таблиця 3.4 - Шифротекст повідомлення “AAAA”

z_i	‘A’	‘A’	‘A’	‘A’
0	-25.880200	-125.805000	-92.610000	-21.659500
1	-7.66861	-33.344300	-22.500700	0.165706
2	0.075565	0.227887	0.095248	0.323851
3	0.305706	0.190868	-0.532981	3.217130
4	1.424380	4.493130	2.043540	-0.318421
5	-0.165401	-0.405383	-0.091127	-0.375667
6	-0.189447	-0.487427	-0.133403	1.191490
7	0.616723	1.520420	0.350949	8.221220
8	4.210650	10.562800	2.624890	-0.642164
9	-0.329225	-0.824535	-0.203537	3.319930
10	1.701620	4.263480	1.054290	0.962753
11	0.493473	1.236350	0.305660	-0.424024
12	-0.217339	-0.544524	-0.134622	0.067951
13	0.034829	0.087261	0.021573	0.270130
14	0.138459	0.346895	0.085762	4.245270
15	2.175970	5.451700	1.347810	-96.106300
z[i]	‘A’	‘A’	‘A’	‘A’

Таблиця 3.4 показує шифри $z(j,i)$ символу ‘A’, переданого багато разів поспіль.

Нижня горизонтальна лінія показує розшифровані символи, які співпадають з оригінальними символами. Очевидно, що кожного разу той самий символ шифрується реалізаціями випадкового масиву, кожен з яких відрізняється один від одного.

Таблиця 3.5 ілюструє шифрування повідомлення “The secret document”. Результати, представлені в Таблиці 3.5, демонструють складність зламу системи методом брутфорсу. Припускається, що ключові функції стали відомі криптоаналітику, але один з коефіцієнтів, включених у ці функції, залишився невідомим. При правильному значенні коефіцієнта $w = 400$ повідомлення розшифровується правильно. Однак при $w = 399.99995$ розпізнавання повідомлення неможливе. Для деяких символів в результаті невірного дешифрування не існує текстового відображення. У цьому випадку замість спотвореного символу стоїть “empty”.

Таблиця 3.6 показує, як відтворюються літери латинського алфавіту, якщо коефіцієнт становить $w = 399.99995$ замість $w = 400$.

Таким чином, невелика похибка 0.00005 лише в одному коефіцієнті робить неможливим злам системи. Якщо врахувати, що є кілька коефіцієнтів, а також необхідність підбору ключових функцій, то “силовий” злам системи стає неможливим.

Важливо не лише вгадати ключові функції, але й знати їх порядкові номери, за якими вони використовувалися при шифруванні. Якщо ці функції використовуються з іншими номерами під час шифрування, передане повідомлення буде спотворене.

Таблиця 3.7 показує результати, коли друга та сьома ключові функції були поміняні місцями під час розшифрування.

Таблиця 3.5 – Дешифрування повідомлення “The secret document” з неправильним параметром *w*

Оригінальне повідомлення	Дешифроване з вірним параметром w = 400	Дешифроване з неправильним параметром w = 399.99995
T	T	V
h	h	n
e	e	n
whitespace	whitespace	empty
s	s	s
e	e	g
c	c	c
r	r	r
e	e	g
t	t	v
whitespace	whitespace	f
d	d	d
o	o	o
c	c	c
u	u	w
m	m	o
e	e	g
n	n	n
t	t	v

Таблиця 3.6 – Дешифрування латинського алфавіту з неправильним параметром w

Оригінальне повідомлення	Дешифроване з вірним параметром w = 400	Дешифроване з неправильним параметром w = 399.99995
A	A	empty
B	B	empty
C	C	empty
D	D	empty
E	E	empty
F	F	empty
G	G	empty
H	H	empty
I	I	G
J	J	F
K	K	G
L	L	D
M	M	E
N	N	F
O	O	G
P	P	H
Q	Q	O
R	R	O
S	S	L
T	T	O
U	U	n
W	W	O
X	X	empty
Y	Y	S
Z	Z	^

Таблиця 3.7 – Дешифрування повідомлення з некоректною нумерацією функцій

Оригінальне повідомлення	Коректна нумерація функцій	Некоректна нумерація функцій
T	T	empty
h	h	*
e	e	’
whitespace	whitespace	empty
s	s	s
e	e	’
c	c	c
r	r	r
e	e	’
t	t	6
whitespace	whitespace	empty
d	d	&
o	o	o
c	c	c
u	u	7
m	m	/
e	e	’
n	n	n
t	t	6

Таблиця 3.8 представляє результати перестановки цих ключових функцій для літер в алфавіті. У цій таблиці “ps” позначає псевдографічний символ.

Таблиці 3.7 і 3.8 показують, що така перестановка унеможливлює розпізнавання переданого повідомлення. Результат розшифрування ще гірший, якщо форма хоча б однієї ключової функції спотворена. Наприклад, якщо в ключовій функції $f_2(x)$ під час розшифрування замість $sin(w\beta_2 x)$ стоїть $cos(w\beta_2 x)$, то повідомлення “The secret document” розшифровується як “Tle we’”.

Наведені вище приклади показують, що перехід від натуральних чисел до функцій дійсної змінної ефективно захищає від зламу шляхом перебору , а додатковий етап шифрування ще більш ускладнює криптоаналіз.

Таблиця 3.8 – Дешифрування латинського алфавіту з некоректною нумерацією функцій.

Оригінальне повідомлення	Коректна нумерація функцій	Некоректна нумерація функцій
A	A	B
B	B	G
C	C	B
D	D	empty
E	E	P
F	F	G
G	G	ps
H	H	ps
I	I	G
J	J	K
K	K	ps
L	L	N
M	M	O
N	N	ps
O	O	ps
P	P	R
Q	Q	S
R	R	ps
S	S	ps
T	T	V
U	U	W
W	W	+
X	X	empty
Y	Y	Z
Z	Z	H

3.4. Модифікація криптографічної системи з перестановкою ключових функцій

Запропоновано ще одну модифікацію до криптосистеми на основі суми функцій дійсної змінної.

Відомо, що для коректного дешифрування необхідно не лише знати форму та значення ключових функцій, але також і їх порядок. Тобто, необхідно дотримуватись того факту, що перша функція відповідає першому біту, друга - другому, і т.д. Як показано в попередніх прикладах, при відомих функціях, але їх неправильній нумерації, правильне розшифрування шифротексту неможливо.

З метою використання цієї властивості, запропоновано додаткову модифікацію, що полягає в перестановці ключових функцій за узгодженою схемою. Таким чином, в цій версії до вже описаного складу ключа шифрування також додається інформація про схему перестановки.

Перестановка ключів відповідно до схеми може виконуватися через задану кількість циклів шифрування або ж через узгоджені проміжку часу. Найпростішим варіантом схеми може бути зсув по колу порядкового номеру ключів при шифруванні кожного нового повідомлення.

Алгоритми шифрування та дешифрування при цьому не змінюються.

Така модифікація дозволяє додатково ускладнювати процес зламу, у випадку коли третя сторона якимось чином отримала доступ до функцій-ключів, але схема перестановки залишається невідомою. Також це дозволяє пере-використовувати один ключ (набір функцій-ключів) декілька разів протягом довшого проміжку часу не компрометуючи безпеку.

Приведемо ще один приклад результатів шифрування з заданою модифікацію.

Розглядається випадок зі схемою з шести перестановками ключових функцій, кожна з яких відбувається для кожного нового повідомлення. Моделюється ситуація, коли зловмисник отримав доступ до ключових функцій, але схема перестановок залишається невідомою. Повідомлення складається з латинського алфавіту.

Задамо новий ключ шифрування, що складається з інших 8 ключових функцій:

1. $f_1(x) = 1000\left(\alpha_1 \sin\left(\text{pow}(\cos(w\beta_1 x), 2)\right) + \alpha_2 \cos\left(\sin(\beta_2 x)\right) + \exp\left(\sin\left(\alpha_3 x + \cos(\beta_3 x^2)\right)\right)\right)$
2. $f_2(x) = 1000\left(\beta_3 \cos\left(w\beta_1 \sin(\alpha_2 x)\right) + \beta_2 w \sin\left(\exp\left(\alpha_3 \cos(\alpha_1 x)\right)\right)\right)$
3. $f_3(x) = 1000(\beta_3 \cos\left(\alpha_1 \exp(0.01\alpha_3 x)\right) + \beta_2 \sin\left(w\alpha_2 \sin(\beta_1 x)\right)$
4. $f_4(x) = 1000\left(\alpha_2 \sin\left(w\beta_1 \exp(-0.03\alpha_3 x)\right)\right)\alpha_1 \sin(\beta_2 \beta_3 x)))$
5. $f_5(x) = 1000\left((\alpha_2 - 10x)\beta_2 \cos(\sin(\beta_1 x)x) + \beta_3 w \sin(\alpha_1 x + \alpha_3)\right))$
6. $f_6(x) = 1000\left((100 - \beta_3 x)\exp\left(\alpha_3 \sin(\alpha_1 x)\right) + (\beta_1 + 20x)\sin\left(w\beta_2 \cos(\alpha_2 x)\right)\right)$
7. $f_7(x) = 1000\left(\alpha_3 \sin(\beta_1 x)\left(\sin(\beta_2 x) + \cos(w\alpha_2 x)\beta_3(-\alpha x^2)\right)\right)$
8. $f_8(x) = 1000\left((\alpha_1 + \beta_3)\cos\left(\alpha_3 w \sin(\beta_1 x)\alpha_2 \cos(\beta_2 x)\right)\right)$

(3.36)

Константи мають значення α_1=10, α_2=0.12, α_3=0.5, β_1=0.1, β_2=12, β_3=0.7, w=500. Таблиця 3.9 ілюструє спробу дешифрування, використовуючи невірний порядок застосування ключових функцій.

Результати показують, що така спроба є невдалою, і схема перестановок складає додатковий прошарок безпеки для криптосистеми.

Таблиця 3.9 – Дешифрування зі схемою перестановки

Оригінальне повідомлення	Дешифроване з вірною перестановкою	Дешифроване без перестановки
A	A	A
B	B	B
C	C	C
D	D	€
E	E	(Пробіл)
F	F	(Пробіл)
G	G	…
H	H	(Пробіл)
I	I	%
J	J	%
K	K	-
L	L	1
M	L	1
N	N	5
O	O	v

Оригінальне повідомлення	Дешифроване з вірною перестановкою	Дешифроване без перестановки
P	P	…
Q	Q	)
R	R	(Пробіл)
S	S	9
T	T	I
U	U	Y
V	V	Y
W	W	№
X	X	I
Y	Y	Y
Z	Z	‡

3.5. Висновки до третього розділу

У третьому розділі досліджено криптосистему на основі функцій дійсної змінної, з чого слідують наступні висновки:

1. Описані методи вирішення поставленої задачі. Запропонований метод розшифрування повідомлення, зашифрованого сумою функцій дійсної змінної, для якого використовуються властивості функцій інтегральної непропорційності до розпізнавання невідомих коефіцієнтів.

2. Розроблені алгоритми шифрування та дешифрування повідомлень, спроектована криптосистема на основі суми функцій дійсної змінної. Ключ криптосистеми являє собою систему функцій-ключів дійсної змінної, що можуть бути задані як аналітично, так і дискретно. Визначені і надані обмеження, які накладаються на ключові функції. Описано метод шифрування елементу повідомлення одновимірним масивом, елементи якого являють собою суму ключових функцій із випадковими коефіцієнтами. Ця сума включає ті ключові функції, для яких відповідний біт елементу дорівнює одиниці. Описаний алгоритм дешифрування, в якому послідовне застосування інтегральної непропорційності дозволяє обчислити коефіцієнти, розпізнати які з функції-ключів включені в суму, і відтворити зашифроване повідомлення. Описано структуру шифротексту.

3. Створена програмна реалізація симетричної криптосистеми, в якій система функцій дійсної змінної використовується в якості ключа. Розроблені і запропоновані модифікації для подальшого посилення криптостійкості.

РОЗДІЛ 4. ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ СТВОРЕННЯ КРИПТОГРАФІЧНОЇ СИСТЕМ ДЛЯ ЗАХИСТУ ЗОБРАЖЕНЬ З ВИКОРИСТАННЯМ ІНШОГО ЗОБРАЖЕННЯ В ЯКОСТІ КЛЮЧА

4.1. Опис криптосистеми

Враховуючи придатність методів , які використовують інтегральні функції непропорційності для створення криптографічних систем на основі дійсних чисел, пропонується також створити спеціалізовану криптосистему для роботи з зображеннями.

Відомо, що характер даних може впливати на надійність і ефективність шифрування. Візуальні дані демонструють відмінні характеристики, включаючи сильну кореляцію між сусідніми пікселями, високу ємність, просторову надмірність і візуальні шаблони. Крім того, більший розмір даних зображень, особливо у форматах з високою роздільною здатністю, вимагає ефективних методів шифрування для забезпечення безпеки та продуктивності. Ці характеристики підкреслюють необхідність створення та вдосконалення криптосистем, призначених для роботи з зображеннями.

Розглядається новітній підхід до шифрування зображень, в якому інше довільне зображення використовується як ключ. Ключем може слугувати зображення різного розміру, формату або вмісту. Для цього, вміст зображення представляється як функція, задана дискретно.

Для вирішення цієї задачі також використовуються функції непропорційності. Так, інтегральна непропорційність (2.8) і обернена до неї операція (2.9) є основою для процесів шифрування та дешифрування в запропонованій системі.

4.1.1 Шифрування

Як вже відомо, рівняння (2.10) описує інтегральну непропорційність функції y(x) відносно функції f(x), кожна з яких задана дискретно і представлена одновимірним масивом чисел. У випадку обробки зображень, і зображення, яке шифрується, і зображення-ключ представляються у вигляді одновимірних масивів значень компонентів пікселів.

Для спрощення, спочатку розглянемо випадок з чорно-білим зображенням. У таких схемах кольорова палітра представлена лише 1 байтом, де значення 0 - чорний, а 255 - білий. Це означає, що кожен піксель представлений одним значенням, і все зображення можна представити як одновимірний масив цілих чисел. Це дозволяє нам застосувати інтегральну непропорційність для шифрування зображення. Враховуючи, що f - це зображення-ключ E, а y - зображення, що шифрується I, то рівняння (2.10) набуває вигляду:

$$C_i = \frac{I_{i-1} + I_i}{E_{i-1} + E_i} - \frac{I_i}{E_i} \tag{4.1}$$

де C - масив шифротексту;

I - масив зображення;

E - масив зображення-ключа;

i - порядковий номер елементу масиву.

Результатом обчислення інтегральної непропорційності є також одновимірний масив, але дійсних чисел. Цей масив і є зашифрованим зображенням (шифротекст), яке може бути передане через канал як бінарний об’єкт.

Як видно з формули (4.1), i-й піксель шифрується з використанням значення попереднього пікселя i-1, тому необхідно мати початкове опорне значення для початку обчислень. Таким чином, шифрування (4.1) починається з другого пікселя (i=1), тоді як перший піксель (i=0) не шифрується і залишається

як є. Цей так званий відкритий піксель передається відкрито. Хоча потенційно це може виглядати як слабке місце, один піксель не розкриває будь-яку значущу інформацію про вміст всього зображення.

Для кольорових зображень використовуються інші схеми, де найпопулярнішою є RGBA. Кожен піксель зображення характеризується чотирма компонентами - червоним (R), зеленим (G), синім (B) та альфа (A). Альфа-компонент представляє непрозорість пікселя.

Таким чином, кольорове зображення можна представити як 4 одновимірні масиви цілих чисел.

Оскільки кожен компонент все ще є 1-байтовим цілочисельним значенням, ми можемо застосувати той самий метод (4.1) до них:

$$R_{C_i} = \frac{R_{I_{i-1}} + R_{I_i}}{R_{E_{i-1}} + R_{E_i}} - \frac{R_{I_i}}{R_{E_i}} \tag{4.2}$$

$$G_{C_i} = \frac{G_{I_{i-1}} + G_{I_i}}{G_{E_{i-1}} + G_{E_i}} - \frac{G_{I_i}}{G_{E_i}} \tag{4.3}$$

$$B_{C_i} = \frac{B_{I_{i-1}} + B_{I_i}}{B_{E_{i-1}} + B_{E_i}} - \frac{B_{I_i}}{B_{E_i}} \tag{4.4}$$

$$A_{C_i} = \frac{A_{I_{i-1}} + A_{I_i}}{A_{E_{i-1}} + A_{E_i}} - \frac{A_{I_i}}{A_{E_i}} \tag{4.5}$$

де R, G, B, A - відповідні компоненти;

C - масив зашифрованого зображення відповідних компонентів;

I - масив зображення відповідних компонентів;

E - масив зображення-ключа відповідних компонентів;

i - порядковий номер елементу масиву.

Тут ми маємо чотири одновимірні масиви уже дійсних чисел, кожен з яких представляє відповідні зашифровані компоненти зображення. Разом вони є шифротекстом кольорового зображення, який готовий до передачі через канал зв’язку. З технічної сторони, вони можуть бути передані окремо або одночасно.

Слід зазначити, що зашифрована послідовність містить інформацію про значення пікселів, але не про їхні координати. Приймаюча сторона повинна мати можливість правильно розмістити пікселі після дешифрування та забезпечити оригінальні пропорції зображення. Таким чином, ширина вхідного зображення також передається разом із шифротекстом.

Загалом, основний алгоритм шифрування виглядає наступним чином:

1. Прочитати вхідне зображення піксель за пікселем та визначити значення компонент RGBA.
2. Прочитати зображення-ключ піксель за пікселем та визначити значення компонент RGBA.
3. Взяти перший піксель входу. Залишити його як є. Він не шифрується і передається відкрито.
4. Починаючи з другого, кожен компонент пікселя обробляється за допомогою інтегральної непропорційності (формули 4.2-4.5). Результатом такого обчислення є дійсне число, що представляє зашифрований RGBA-компонент пікселя. Таким чином, зашифрований піксель - це послідовність з 4 дійсних чисел. Зашифроване зображення - це послідовність зашифрованих пікселів.
5. Отримана послідовність передається через канал зв’язку разом із шириною оригінального зображення.

4.1.2. Шифротекст

На відміну від інших криптосистем для зображень, шифротекст не є зображенням сам по собі. Натомість, він являє собою масиви дійсних чисел, що передаються як бінарний об’єкт.

У випадку чорно-білого зображення це один одновимірний масив дійсного типу, де розмір масиву дорівнює кількості пікселів у зображенні. Кожне значення представляє зашифроване значення пікселя чорно-білого зображення.

У випадку RGBA-зображення це чотири одновимірні масиви дійсного типу. Їхні розміри однакові і також дорівнюють кількості пікселів у зображенні. Кожне значення представляє зашифроване значення пікселя відповідного RGBA-компонента.

Вони можуть передаватися послідовно або окремо. (Таблиця 4.1) та (Таблиця 4.2) показують, як може оброблятися послідовність після шифрування.

У першому випадку (Таблиця 4.1) результуюча послідовність передається піксель за пікселем, тобто зашифровані значення RGBA для першого пікселя, потім зашифровані значення RGBA для другого пікселя. Цей випадок є прямолінійним і простим для реалізації.

У другому випадку (Таблиця 4.2) передаються чотири масиви, тобто всі зашифровані значення R, а потім всі значення G, B та A. Це дозволяє розділити шифротекст і передавати його окремо у разі необхідності, наприклад, з зсувом у часі або використовуючи різні канали зв’язку.

Таблиця 4.1 Послідовно передана послідовність

Вхід	Шифротекст	Передана послідовність
R_0 R_1 R_i …	R_0 R_1 R_i …	R_0 G_0 B_0 A_0 R_1 G_1 B_1 A_1 … R_i G_i B_i A_i
G_0 G_1 G_i …	G_0 G_1 G_i …	
B_0 B_1 B_i …	B_0 B_1 B_i …	
A_0 A_1 A_i …	A_0 A_1 A_i …	

Таблиця 4.2 Окремо передана послідовність

Вхід	Шифротекст	Передана послідовність
R_0 R_1 R_i …	R_0 R_1 R_i …	R_0 R_1 R_i … G_0 G_1 G_i … B_0 B_1 B_i … A_0 A_1 A_i …
G_0 G_1 G_i …	G_0 G_1 G_i …	
B_0 B_1 B_i …	B_0 B_1 B_i …	
A_0 A_1 A_i …	A_0 A_1 A_i …	

4.1.3. Дешифрування

Основою процесу дешифрування є вже описане обернене перетворення інтегральної непропорційності (2.9).

Знову ж таки, розглянемо спочатку чорно-біле зображення. У цьому випадку кожен піксель зображення описується одним байтом, а шифротекст - це масив дійсних чисел, отриманий шляхом обчислення інтегральної непропорційності зображення-ключа відносно вхідного зображення за формулою (4.1). Таким чином, обернене перетворення (2.9) дозволяє відновити значення пікселів вхідного зображення за допомогою зображення-ключа та шифротексту:

$$D_i = \frac{E_i\big((E_{i-1} + E_i)C_i + E_{i-1}\big)}{E_{i-1}} \tag{4.6}$$

де D - масив дешифрованого зображення;

C - масив зашифрованого зображення відповідних компонентів;

E - масив зображення-ключа відповідних компонентів;

i - порядковий номер елементу масиву.

Подібно до шифрування (4.1), обчислення дешифрування (4.6) починається з другого пікселя (i=1), оскільки перший не зашифрований. Шифротекст для кольорового RGBA-зображення складається з чотирьох масивів дійсних чисел, обчислених таким же чином, по одному для кожного компонента. Застосування формули (4.6) до кожного з них породжує наступні формул дешифрування:

$$R_{D_i} = \frac{R_{E_i}\left(\left(R_{E_{i-1}} + R_{E_i}\right)R_{C_i} + R_{E_{i-1}}\right)}{R_{E_{i-1}}} \tag{4.7}$$

$$G_{D_i} = \frac{G_{E_i}\left(\left(G_{E_{i-1}} + G_{E_i}\right)G_{C_i} + G_{E_{i-1}}\right)}{G_{E_{i-1}}} \tag{4.8}$$

$$B_{D_i} = \frac{B_{E_i}\left(\left(B_{E_{i-1}} + B_{E_i}\right)B_{C_i} + B_{E_{i-1}}\right)}{B_{E_{i-1}}} \tag{4.9}$$

$$A_{D_i} = \frac{A_{E_i}\left(\left(A_{E_{i-1}} + A_{E_i}\right)A_{C_i} + A_{E_{i-1}}\right)}{A_{E_{i-1}}} \tag{4.10}$$

де R, G, B, A - відповідні компоненти;

D - масив дешифрованого зображення відповідних компонентів;

C - масив зашифрованого зображення відповідних компонентів;

E - масив зображення-ключа відповідних компонентів;

i - індекс.

Результатом такого обчислення є чотири масиви, де кожне значення представляє декодоване значення RGBA вхідного зображення. Зауважимо, що оскільки результуючий масив рівнянь (4.7) - (4.10) все ще має тип дійсних чисел, необхідно округлити кожне значення до найближчого цілого, щоб отримати правильне ціле значення компонентів RGBA:

$$x := round(v) \tag{4.11}$$

де v - елемент масиву дійсних чисел;

round - функція округлення до найближчого цілого.

Останнім кроком є збір цих значень для відновлення зображення. Оскільки параметр ширини також був переданий, позиція кожного пікселя обчислюється наступним чином:

$$x = i \bmod w \tag{4.12}$$

де x - x-координата відновленого пікселя;

i - індекс поточного пікселя;

w - ширина зображення.

$$y = \left\lfloor \frac{i}{w} \right\rfloor \tag{4.13}$$

де y - y-координата відновленого пікселя;

i - індекс поточного пікселя;

w - ширина зображення.

Основний алгоритм дешифрування наступний:

1. Зчитати зображення-ключ піксель за пікселем.
2. Отримати шифротекст - зашифровану послідовність та параметр ширини.
3. Перший отриманий піксель не зашифрований, залишити його як є.
4. Обробити кожне дійсне значення шифротексту за допомогою оберненого перетворення (Рівняння (4.7) - (4.10)) для дешифрування: Результатом цього обчислення є дійсне число, яке представляє зашифрований компонент RGBA пікселя.
5. Округлити це число до найближчого цілого (Рівняння (4.11)). Результатом є розшифрований компонент RGBA пікселя.
6. Обчислити координати кожного розшифрованого пікселя за допомогою рівнянь (4.12) та (4.13).
7. Зібрати пікселі для відновлення зображення.

4.1.4. Особливості та граничні випадки

Зображення-ключ може бути будь-яким довільним зображенням, без специфічних вимог до розміру чи формату. Оскільки воно є ключем для шифрування та дешифрування, важливо, щоб і передавач, і приймач мали ідентичну копію цього зображення-ключа. Зображення-ключ слід обирати або передавати через захищений канал.

За умовою, кількість пікселів у зображенні-ключі повинна збігатися з кількістю пікселів у вхідному зображенні. Таким чином, зображення іншого розміру (ширини та висоти), але з тією ж кількістю пікселів можна використовувати без змін.

Однак, оскільки вказано, що довільне зображення може бути використано як ключ, перед початком процесів шифрування/дешифрування необхідно привести обране зображення-ключ до потрібної кількості пікселів.

Запропоноване рішення за замовчанням полягає в наступному:

Якщо зображення-ключ більше за вхідне зображення, обрізати пікселі ключа до розміру вхідного зображення.

Якщо зображення-ключ менше за вхідне зображення, доповнити пікселі ключа до розміру вхідного зображення, шляхом повторення пікселів з початку.

Втім, конкретний спосіб зміни розміру може бути налаштовуваним і складати частину ключа. Наприклад, візуальне розтягування є іншим варіантом, але при цьому конкретний алгоритм розтягування має бути узгоджений.

Використання неправильного зображення-ключа (навіть незначно відмінного) для дешифрування призведе до повністю спотвореного зображення, схожого на випадковий шум. Це підкреслює важливість точного управління ключами.

Оскільки RGBA є цілими числами від 0 до 255, під час шифрування в рівнянні (4.1) може виникнути ділення на 0. Це граничний випадок, який слід обробляти. Запропоноване рішення полягає в тимчасовому збільшенні кожного значення RGBA перед шифруванням і зменшенні їх після дешифрування для отримання оригінального значення. Іншими словами, діапазон пікселів умовно зміщується з (0…255) до (1…256).

Оскільки алгоритм працює безпосередньо зі значеннями пікселів, він застосовний до будь-якого формату зображень (JPG, PNG, BMP тощо) і може використовуватися для різних схем кольору, таких як чорно-біла, RGB, RGBA, HSV та LUN. З іншого боку, це означає, що алгоритм не обробляє метадані, специфічні для формату, що призводить до того, що файл розшифрованого

зображення менший за оригінальний, незважаючи на те, що саме зображення однакове.

4.1.5. Обчислювальна складність та використання пам’яті

Обчислювальна складність алгоритму є лінійною, O(N), де N - кількість пікселів у зображенні.

Хоча зашифроване зображення вимагає в чотири рази більше місця, ніж оригінальне, варто зазначити, що для представлення зашифрованих даних використовується 32-бітна точність з плаваючою комою замість 64-бітної. Цей вибір не лише зменшує вимоги до пам’яті, але й забезпечує, після ретельного тестування, збереження візуальної точності розшифрованого зображення, роблячи його ідентичним оригіналу на рівні пікселів.

Щоб запобігти діленню на нуль під час шифрування, кожне значення RGBA (спочатку в діапазоні від 0 до 255) збільшується на 1. Оскільки значення 256 не вміщується в u8 (однобайтовий беззнаковий цілочисельний тип), для уникнення переповнення під час цієї операції використовується тимчасовий тип u16. Після розшифрування значення зменшуються на 1, щоб отримати оригінальні значення зображення.

Загальна просторова складність алгоритму становить O(N), де N - розмір вхідного зображення в пікселях. Допоміжна просторова складність становить O(1), оскільки алгоритм вимагає лише фіксованого набору тимчасових змінних, окрім вхідних даних. Ці змінні включають вищезгаданий тимчасовий контейнер u16, значення першого пікселя, ширину зображення тощо - жодні з яких не залежить від розміру вхідних даних.

Крім того, алгоритм може бути легко розпаралелений шляхом незалежної обробки різних значень RGBA.

4.2. Дослідження криптосистеми

Для ілюстрації роботи алгоритму наводиться покрокова демонстрація мінімального прикладу. Зашифруємо “input.PNG” (Рис. 4.1) використовуючи “key.PNG” (Рис. 4.2) як ключ. Обидва зображення - прості зображення розміром 2x2 (4 пікселі та 16 цілих значень), з кольоровою схемою RGBA у форматі PNG. Значення пікселів для вхідного зображення описані в (Таблиця 4.3), а значення зображення-ключа - в (Таблиця 4.4). Вони згенеровані випадковим чином, включаючи випадкову непрозорість, для демонстрації роботи. Формат PNG було обрано для підтримки непрозорості.

Рис. 4.1. “input.PNG”

Рис. 4.2. “key.PNG”

Рис. 4.3. “output.PNG”

Таблиця 4.3 - Пікселі вхідного зображення

	Піксель 1	Піксель 2	Піксель 3	Піксель 4
R	204	62	215	218
G	107	151	132	211
B	1	76	124	196
A	254	210	234	218

Таблиця 4.4 - Пікселі зображення-ключа

	Піксель 1	Піксель 2	Піксель 3	Піксель 4
R	71	5	151	0
G	155	175	131	0
B	34	165	10	0
A	207	249	240	251

Після застосування алгоритму шифрування, генерується шифротекст. Хоча це не зображення, воно все ще складається з 16 значень, але дійсного типу. Вони наведені в (Таблиця 4.5). Як згадувалося раніше, відкритий піксель в колонці 1 не зашифрований, і його значення просто приведені до дійсного типу. Решта значень виглядають як випадкові дійсні числа без виявлення кореляцій з оригінальним зображенням. Зауважимо, що діапазон значень шифротексту не обмежений початковим значенням (від 0 до 255). Після дешифрування результатом є “output.PNG” (Рис. 4.3), значення якого описані в (Таблиця 4.6). Як можна побачити, (Таблиця 4.3) і (Таблиця 4.6) однакові, отже дешифрування працює коректно.

Таблиця 4.5 – Шифротекст

	Піксель 1	Піксель 2	Піксель 3	Піксель 4
R	204.0	-9.229857	0.344770	-216.156860
G	107.0	0.051857	-0.082251	-209.406020
B	1.0	0.006383	-10.222393	-170.166670
A	254.0	0.078772	-0.066753	0.051845

Таблиця 4.6 - Дешифроване зображення

	Піксель 1	Піксель 2	Піксель 3	Піксель 4
R	204	62	215	218
G	107	151	132	211
B	1	76	124	196
A	254	210	234	218

Продемонструємо, як криптосистема оброблює кореляції. Розглянемо граничний випадок, де шифрується зображення “red.PNG” розміром 2x2, що складається з однакових пікселів. Кожен піксель цього зображення має значення RGBA (255, 0, 0, 255), тобто є червоним і непрозорим.

Знову використовуючи як ключ “key.PNG” (Рис. 4.2 та Таблиця 4.4), процес шифрування породжує шифротекст, детально описаний у (Таблиці 4.7).

Примітно, що хоча пікселі відкритого тексту однакові, отримані значення шифротексту для відповідних пікселів значно відрізняються, демонструючи ефективну здатність алгоритму до декореляції.

Таблиця 4.7 - Шифротекст червоних пікселів

	Піксель 1	Піксель 2	Піксель 3	Піксель 4
R	255.0	-40.712470	1.556296	-252.653600
G	0.0	0.0056176167	-0.0010822513	-0.9849624
B	0.0	0.005951952	-0.07960966	-0.8333333
A	255.0	-0.012142301	-0.01947081	0.022666454

Щоб підкреслити важливість використання правильного ключа для дешифрування, розглянемо сценарій, в якому змінено значення одного пікселя в зображенні-ключі. Наприклад, змінимо перший піксель “key.PNG” (Рис. 4.2) з його початкового значення (5, 175, 165, 249) на (0, 0, 0, 0), тобто на повністю чорний і непрозорий.

Дешифрування шифротексту з (Таблиці 4.5) з цим модифікованим зображенням-ключем призводить до спотвореного результату, представленого в (Таблиці 4.8) та візуалізованого на (Рис. 4.4). Змінене зображення показує, що, крім першого пікселя, решта даних некоректна і не має подібності до оригінального зображення, підкреслюючи чутливість алгоритму до точності ключа.

Таблиця 4.8 - Неправильне дешифрування

	Піксель 1	Піксель 2	Піксель 3	Піксель 4
R	204	9	255	174
G	107	0	32	222
B	1	0	79	52
A	254	0	18	179

Рис. 4.4. Неправильне дешифрування

Надійність алгоритму була ретельно перевірена на різноманітному наборі зображень, що відрізняються як розміром, так і форматом. Це було проілюстровано з використанням як стандартних, так і користувацьких зображень. “Cat.JPG” (Рис. 4.5) - це фото кішки розміром 408x36 у форматі JPG. Фото бабуїна “baboon.png” (Рис. 4.6) - приклад стандартного зображення з бази даних зображень USC SIPI, має розміри 512x512 у форматі PNG. Шифрування зображення кота (Рис. 4.5) з використанням зображення бабуїна (Рис. 4.6) як ключа призвело до дешифрованого зображення (Рис. 4.7), яке ідеально відображає оригінальне зображення, таким чином підтверджуючи точність процесу дешифрування.

Рис. 4.5. “Cat.JPG” як вхідне зображення

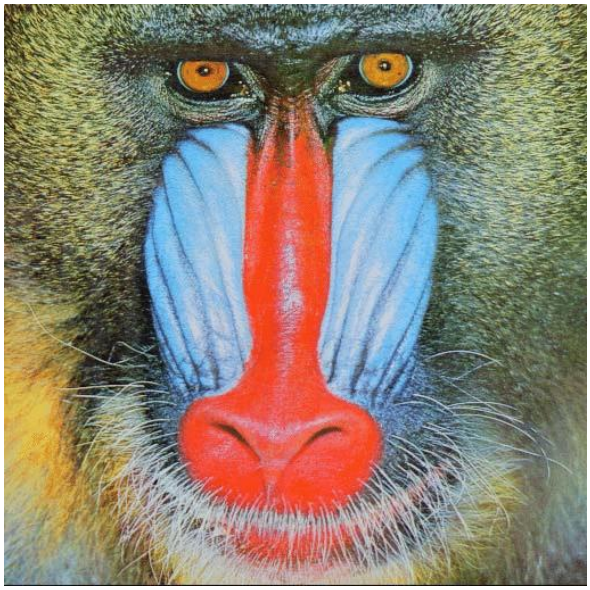


Рис. 4.6. “Baboon.PNG” як зображення-ключ

Рис. 4.7. Дешифроване “Cat.JPG”

Зауважимо, що дешифроване зображення (Рис. 4.7) ідентичне оригінальному зображенню (Рис. 4.5); тут всі 124848 пікселів мають однакові значення RGBA. Це було перевірено програмно в цьому випадку та багатьох інших.

Методологія тестування спирається на по-піксельне порівняння, де кожен компонент RGBA пікселя в оригінальному зображенні порівнюється з відповідним компонентом RGBA пікселя в дешифрованому зображенні. Таким

чином, зображення повністю ідентичні. Будь-які втрати якості зображення відсутні, що демонструє надійність алгоритму.

Щоб вирішити потенційні проблеми щодо випадковості даних у мінімальних прикладах, був проведений більш складний тест. “Cat.JPG” (Рис. 4.5) було зашифровано з використанням “baboon.PNG” (Рис. 4.6) як зображення-ключа. Після цього другий піксель зображення-ключа було змінено на (0, 0, 0, 0), і шифротекст було дешифровано з цим модифікованим ключем. Як видно з результату (Рис. 4.8), дешифроване зображення пошкоджене. Це підтверджує на реальних прикладах, що навіть незначно змінений ключ (неправильний 1 піксель) призводить до невдалого дешифрування, демонструючи безпеку запропонованого алгоритму.

Рис. 4.8. Дешифроване “Cat.JPG” з пошкодженим зображенням-ключем

(Рис. 4.8) було порівняно з оригінальним зображенням, використовуючи той самий попіксельний метод. Це показує, що 124847 з 124848 пікселів відрізняються. Єдиний незмінений піксель - перший, який не шифрується і передається відкрито навмисно. Більше того, 373441 з 374544 RGB-компонентів відрізняються. Це означає, що, за винятком першого, немає пікселів, де хоча б одне з RGB-значень збігається з оригінальним. Однак значення A зображень залишаються незмінними, оскільки обидва вхідне та ключове зображення непрозорі, і значення A завжди дорівнює 255.

Крім того, виміряємо показники якості дешифрованих зображень. Середня нормалізована квадратична помилка (Mean Normalized Square Error, MNSE) - це

метрика, що використовується для кількісної оцінки подібності між двома зображеннями. MNSE обчислюється шляхом порівняння значень пікселів оригінального зображення I та дешифрованого зображення D:

$$M = \frac{1}{N}\sum_{i=1}^{N}\left(\frac{I_i - D_i}{I_i}\right)^2 \tag{4.14}$$

де N - загальна кількість пікселів;

I - значення пікселя оригінального зображення;

співвідношення залежить від формату та стиснення. У наведеному прикладі розмір зображення (Рис. 4.5) становить 240.2 кБ, розмір об’єкта шифротексту - 1.9 МБ, а розмір дешифрованого зображення (Рис. 4.7) - 254.6 кБ.

На додаток до наведених прикладів, алгоритм також був протестований на інших зображеннях. Серед них знімки екрану веб-сторінок (Рис. 4.9), скани особистих документів автора (Рис. 4.10) та зображення кота-хакера, згенероване штучним інтелектом ChatGPT (Рис. 4.11). Їхні значення MNSE також дорівнюють 0.00. Зменшені версії цих зображень наведені з міркувань економії місця.

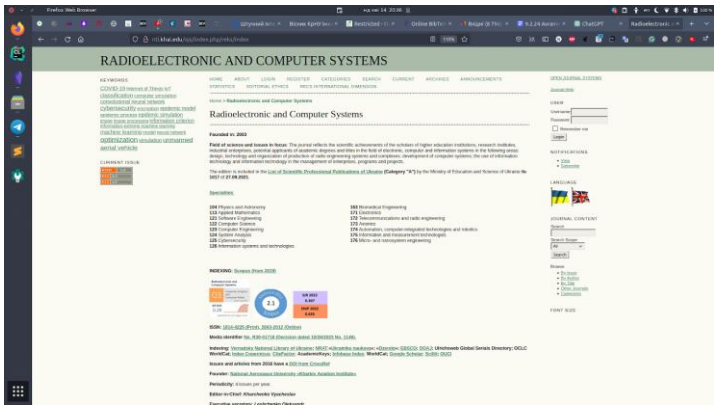
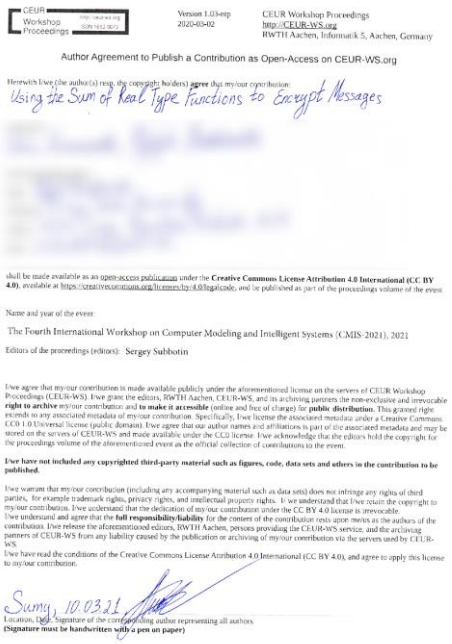


Рис. 4.9. Протестований знімок екрану



CEUR Workshop Proceedings

Version 1.03-emp
2020-03-02

CEUR Workshop Proceedings
http://CEUR-WS.org
RWTH Aachen, Informatik 5, Aachen, Germany

Author Agreement to Publish a Contribution as Open-Access on CEUR-WS.org

Herewith I/we (the author(s) resp. the copyright holders) **agree** that my/our contribution:

Using the Sum of Real Type Functions to Encrypt Messages

[redacted]

shall be made available as an open-access publication under the **Creative Commons License Attribution 4.0 International (CC BY 4.0)**, available at https://creativecommons.org/licenses/by/4.0/legalcode, and be published as part of the proceedings volume of the event.

Name and year of the event:

The Fourth International Workshop on Computer Modeling and Intelligent Systems (CMIS-2021), 2021

Editors of the proceedings (editors): Sergey Subbotin

I/we agree that my/our contribution is made available publicly under the aforementioned license on the servers of CEUR Workshop Proceedings (CEUR-WS). I/we grant the editors, RWTH Aachen, CEUR-WS, and its archiving partners the non-exclusive and irrevocable **right to archive** my/our contribution and **to make it accessible** (online and free of charge) for **public distribution**. This granted right extends to any associated metadata of my/our contribution. Specifically, I/we license the associated metadata under a Creative Commons CC0 1.0 Universal license (public domain). I/we agree that our author names and affiliations is part of the associated metadata and may be stored on the servers of CEUR-WS and made available under the CC0 license. I/we acknowledge that the editors hold the copyright for the proceedings volume of the aforementioned event as the official collection of contributions to the event.

I/we have not included any copyrighted third-party material such as figures, code, data sets and others in the contribution to be published.

I/we warrant that my/our contribution (including any accompanying material such as data sets) does not infringe any rights of third parties, for example trademark rights, privacy rights, and intellectual property rights. If we understand that I/we retain the copyright to my/our contribution. I/we understand that the dedication of my/our contribution under the CC BY 4.0 license is irrevocable.
I/we understand and agree that the **full responsibility/liability** for the content of the contribution rests upon me/us as the authors of the contribution. I/we release the aforementioned editors, RWTH Aachen, persons providing the CEUR-WS service, and the archiving partners of CEUR-WS from any liability caused by the publication or archiving of my/our contribution via the servers used by CEUR-WS.
I/we have read the conditions of the Creative Commons License Attribution 4.0 International (CC BY 4.0), and agree to apply this license to my/our contribution.

Sumy, 10.03.21,
Location, Date, Signature of the corresponding author representing all authors
(Signature must be handwritten with a pen on paper)

Рис. 4.10. Протестований відсканований документ

Рис. 4.11. Протестоване зображення, згенероване ШІ

4.3. Аналіз результатів

Експерименти, зокрема шифрування та дешифрування стандартних зображень, демонструють надійність запропонованого алгоритму шифрування

зображень. Метод використання довільного зображення в якості ключа виявився ефективним, незважаючи на малопоширеність в традиційних методах шифрування. В експериментах з з модифікацією зображення-ключа продемонстрована чутливість алгоритму до змін ключа. Показана здатність алгоритму обробляти зображення з рівномірним розподілом кольорів та зберігати цілісність зашифрованих даних.

Запропонована система має певні обмеження. Так, загальною проблемою в симетричних криптосистемах є задача безпечного обміну ключем шифрування. Хоча це не є прямим недоліком запропонованого алгоритму, таку проблему треба брати до уваги при практичному впровадженні.

Варто зазначити, що показана криптосистема зосереджена лише на вмісті зображення. Це означає, що метадані специфічні для певного формату не шифруються і не передаються. Тому розмір дешифрованого зображення менший за оригінальний, і вони мають різні бінарні представлення. З практичної точки зору це означає, наприклад, різні результати хешування, що слід враховувати в практичному застосуванні.

Дослідження також виявляє окремі області для подальшого вдосконалення. Найбільш помітним недоліком є збільшення розміру шифротексту в байтах, який приблизно в чотири рази більший за розмір вхідного зображення. Така особливість може бути неоптимальної для передачі великих файлів. В граничних випадках можливі підвищені вимоги до пропускною здатності каналу. Альтернативно, необхідно застосування методів стиснення даних або кодування для зменшення розміру шифротексту без порушення його цілісності.

Асимптотична часова та просторова складність алгоритму порівнянна з відомими альтернативами і достатня для використання в програмному забезпеченні загального застосування, в тому числі на клієнтській стороні на стороні клієнта, у мобільних та веб-додатках. Однак збільшення розміру шифротексту може вимагати збільшення пропускної здатності. Також криптосистема може не підходити для вбудованих систем з обмеженими ресурсами.

Іншою можливою проблемою є передача відкритого пікселя, який залишається відкритим у шифротексті, теоретично створюючи потенційну вразливість.

4.4. Висновки до четвертого розділу

У четвертому розділі досліджено можливості створення спеціалізованих криптосистем для захисту зображень, використовуючи інше зображення в якості ключа і одержано такі результати:

Запропонований новий підхід до захисту зображень, в якому інше довільне зображення використовується в якості ключа. Для цього спроектована криптосистема на основі дійсних чисел, розроблені алгоритми шифрування та дешифрування, які використовують властивості інтегральної непропорційності.

Розроблена програмна реалізація симетричної криптосистеми для зображень, в якій довільне зображення різного розміру, формату або вмісту слугує ключем шифрування. Запропонована система працює як з чорно-білими, так і з кольоровими зображеннями в будь-яких форматах. Використовується підхід, що впливає безпосередньо на пікселі зображення, тому система придатна для шифрування візуальних даних в будь-яких форматах.

Продемонстровано роботу криптосистеми та проведені експерименти, що демонструють надійність і безпеку запропонованого підходу. Зокрема, показана чутливість алгоритму до змін ключа, складність зламу системи методом брутфорсу, та здатність до декореляції шифротексту. Показано, що просторова та часова асимптотична складність методу є оптимальною і не перевищує відповідні показники інших відомих систем. Описані наявні вимоги та обмеження.

Основні наукові результати, наведені у четвертому розділі, опубліковано у основних працях автора: [10], [3].

ВИСНОВКИ

У дисертаційній роботі розв'язано важливу науково-практичну задачу створення моделей та методів криптографічних систем на основі функцій дійсної змінної. У результаті проведених досліджень одержано такі результати:

1. Проаналізовано сучасний стан розвитку криптографічних систем і встановлено, що більшість розглянутих методів базуються на використанні множини цілих чисел. Розглянуті та підкреслені недоліки таких систем. Встановлено, що розвиток квантових комп'ютерів становить загрозу для багатьох криптографічних систем, що підштовхує до принципово інших математичних підходів до шифрування. За результатами аналізу аргументовано доцільність переходу від цілих до дійсних значень для побудови криптосистем, обґрунтовано вибір методу на основі використання функцій дійсної змінної в якості криптографічних ключів.

2. Удосконалено моделі та методи створення криптосистем на основі функцій дійсної змінної, що повинно збільшити крипостійкість.

3. Уперше впроваджено метод використання інтегральних функцій непропорційності для дешифрування даних, що дозволяє використовувати в криптосистемі дискретні функції-ключі.

4. Уперше розроблено криптосистему, що поєднує шифрування за допомогою суми функцій дійсної змінної та шифрування за допомогою інтегральної функції непропорційності. Відбувається двох-етапне шифрування, при якому результат першого етапу шифрується ще раз, що суттєво ускладнює злам криптосистеми.

5. Удосконалено метод шифрування даних шляхом впровадження додаткового елементу перестановки функцій-ключів, що також підвищує криптостійкість системи.

6. Вперше розроблено криптосистему для захисту зображень, де інше довільне зображення використовується в якості криптографічного ключа, шляхом використання функцій інтегральної непропорційності. Це значно спрощує передачу ключа порівняно з передачею функцій-ключів в аналітичному

вигляді. Це зображення легше непомітно передати приймальній стороні при використанні симетричних криптосистем. Крім того, зловмиснику складніше виявити зображення-ключ серед багатьох зображень, до яких він отримав доступ.

7. Експериментально продемонстровано високу криптостійкість розроблених методів шифрування до атак грубої сили через необхідність підбору значень ключа з високою точністю. Також продемонстровано високу здібність до декореляції значень шифротексту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] V. Avramenko and M. Bondarenko, “Using the Sum of Real Type Functions to Encrypt Messages,” in *CEUR Workshop Proceedings*, 2021. Available: *https://ceur-ws.org/Vol-3200/paper2.pdf*

[2] V. Avramenko and M. Bondarenko, “Recognition of reference signals and determination of their weighting coefficients if an additive interference presents” *Radio Electronics, Computer Science, Control*, p. 73, Oct. 2023, doi: *10.15588/1607-3274-2023-3-8*.

[3] V. Avramenko and M. Bondarenko, “Image cryptosystem with image key using integral disproportion,” *Radioelectronic and Computer Systems*, vol. 2024, pp. 147–159, Apr. 2024, doi: *10.32620/reks.2024.2.12*.

[4] V. Avramenko and M. Bondarenko, “Encrypting images using the sum of the functions of a real variable,” *Transactions of Kremenchuk Mykhailo Ostrohradskyi National University*, vol. 144, no. 1, pp. 140–147, 2024, doi: *10.32782/1995-0519.2024.1.18*.

[5] V. Avramenko and M. Bondarenko, “Encryption of messages by the sum of a real variable functions.” *Stuc.intelekt*, vol. 29, pp. 10–19, Jun. 2024, doi: *10.15407/jai2024.02.010*.

[6] V. Avramenko, M. Bondarenko, and T. Lavryk, “Спосіб шифрування даних за допомогою суми функцій дійсної змінної,” 147560, Sep. 05, 2021 Available: *https://essuir.sumdu.edu.ua/handle/123456789/85897*

[7] В. В. Авраменко and М. О. Бондаренко, “Спосіб шифрування графічних зображень,” 153107, May 24, 2023 Accessed: Sep. 04, 2024. [Online]. Available: *https://essuir.sumdu.edu.ua/handle/123456789/92703*

[8] V. Avramenko and M. Bondarenko, “Combined encryption system using the sum of functions of a real variable,” presented at the The International Scientific and Technical Conferences of Students and Young scientists “Informatics. Mathematics. Automation,” 2022, p. 71. Available: *https://essuir.sumdu.edu.ua/bitstream-download/123456789/87782/1/Conf_IMA_2022.pdf*

[9] V. Avramenko and M. Bondarenko, “Signal recognition and calculation weighting coefficients in the presence of additive interference,” presented at the The International Scientific and Technical Conferences of Students and Young scientists “Informatics. Mathematics. Automation,” Sumy-Astana, 2023. Available: https://drive.google.com/file/d/1YDGNhbgZY6dfsqwN6P0BcEpcq6CuCKmj/view

[10] V. Avramenko and M. Bondarenko, “Image encryption with key-image using integral disproportion,” presented at the The International Scientific and Technical Conferences of Students and Young scientists “Informatics. Mathematics. Automation,” 2024, pp. 38–39. Available: https://drive.google.com/file/d/1jjUd3KWmCmrPnOXTnZZSGbZIbsWWBPzU/view

[11] I. Security, “Cost of a Data Breach Report 2021,” *Risk quantification*, 2021.

[12] M. Haralambos and G. Paolo, *Integrating Security and Software Engineering: Advances and Future Visions: Advances and Future Visions*. Idea Group Inc (IGI), 2006. Available: https://books.google.com?id=Ohn31ygnrNkC

[13] N. F. Johnson and S. Jajodia, “Exploring steganography: Seeing the unseen,” *Computer*, vol. 31, no. 2, pp. 26–34, Feb. 1998, doi: 10.1109/MC.1998.4655281.

[14] V. Kolenko, V. Nakonechna, and Y. Anosova, “Commercial secret of the enterprise protection based on steganographic algorithms,” *Visnyk KrNU*, vol. 1, pp. 59–65, Feb. 2021, doi: 10.30929/1995-0519.2021.1.59-65.

[15] J. Fridrich, M. Goljan, and R. Du, “Detecting LSB steganography in color, and gray-scale images,” *IEEE MultiMedia*, vol. 8, no. 4, pp. 22–28, Oct. 2001, doi: 10.1109/93.959097.

[16] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton: CRC Press, 2020. doi: 10.1201/9780429466335.

[17] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 0th ed. Chapman and Hall/CRC, 2014. doi: 10.1201/b17668.

[18] D. J. Bernstein and T. Lange, “Post-quantum cryptography,” *Nature*, vol. 549, no. 7671, pp. 188–194, Sep. 2017, doi: 10.1038/nature23461.

[19] J. Bagaria, “Set theory,” in *The Princeton Companion to Mathematics*, 2010. doi: *10.4324/9781315167749-28*.

[20] W. Stallings, *Cryptography and network security: Principles and practice*, Seventh edition. Boston Munich: Pearson, 2017.

[21] N. I. of S. and Technology, “Data Encryption Standard (DES),” U.S. Department of Commerce, Federal Information Processing Standard (FIPS) 46 (Withdrawn), Jan. 1977. Accessed: Aug. 03, 2024. [Online]. Available: *https://csrc.nist.gov/pubs/fips/46/final*

[22] D. Coppersmith, “The Data Encryption Standard (DES) and its strength against attacks,” *IBM Journal of Research and Development*, vol. 38, no. 3, pp. 243–250, May 1994, doi: *10.1147/rd.383.0243*.

[23] E. Biham and A. Shamir, “Differential cryptanalysis of DES-like cryptosystems,” *J. Cryptology*, vol. 4, no. 1, pp. 3–72, Jan. 1991, doi: *10.1007/BF00630563*.

[24] E. Barker and N. Mouha, “Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher,” National Institute of Standards and Technology, NIST Special Publication (SP) 800-67 Rev. 2 (Withdrawn), Nov. 2017. doi: *10.6028/NIST.SP.800-67r2*.

[25] P. C. van Oorschot and M. J. Wiener, “Parallel Collision Search with Cryptanalytic Applications,” *J. Cryptology*, vol. 12, no. 1, pp. 1–28, Jan. 1999, doi: *10.1007/PL00003816*.

[26] FIPS, “Specification for the ADVANCED ENCRYPTION STANDARD (AES),” *Federal Information Processing Standards Publication*. 2001.

[27] M. J. Dworkin, “Advanced Encryption Standard (AES),” National Institute of Standards and Technology (U.S.), Gaithersburg, MD, NIST FIPS 197-upd1, May 2023. doi: *10.6028/NIST.FIPS.197-upd1*.

[28] S. Mangard, E. Oswald, and T. Popp, Eds., “Differential Power Analysis,” in *Power Analysis Attacks: Revealing the Secrets of Smart Cards*, Boston, MA: Springer US, 2007, pp. 119–165. doi: *10.1007/978-0-387-38162-6_6*.

[29] A. Biryukov and D. Khovratovich, “Related-Key Cryptanalysis of the Full AES-192 and AES-256,” in *Advances in Cryptology – ASIACRYPT 2009*, M. Matsui, Ed., Berlin, Heidelberg: Springer, 2009, pp. 1–18. doi: *10.1007/978-3-642-10366-7_1*.

[30] T. Eisenbarth and S. Kumar, “A Survey of Lightweight-Cryptography Implementations,” *Design & Test of Computers, IEEE*, vol. 24, pp. 522–533, Dec. 2007, doi: *10.1109/MDT.2007.178*.

[31] A. Bogdanov, D. Khovratovich, and C. Rechberger, “Biclique Cryptanalysis of the Full AES,” in *Advances in Cryptology – ASIACRYPT 2011*, D. H. Lee and X. Wang, Eds., Berlin, Heidelberg: Springer, 2011, pp. 344–371. doi: *10.1007/978-3-642-25385-0_19*.

[32] DSTU, *ДСТУ ГОСТ 28147:2009 Система обробки інформації. Захист криптографічний. Алгоритм криптографічного перетворення (ГОСТ 28147-89)*. d, 2009. Accessed: Jun. 17, 2024. [Online]. Available: *https://usts.kiev.ua/wp-content/uploads/2020/07/dstu-host-28147-2009.pdf*

[33] А. Н. Лебедев, “Криптография с «открытым ключом» и возможности его практического применения,” *Защита информации. Конфидент*, no. 2, p. 25, 1992, Accessed: Jun. 17, 2024. [Online]. Available: *https://scholar.google.com/scholar?cluster=2514084716895768662&hl=en&oi=scholarr*

[34] N. T. Courtois, “Security Evaluation of GOST 28147-89 in View of International Standardisation,” *Cryptologia*, vol. 36. 2012. doi: *10.1080/01611194.2011.632807*.

[35] M.-J. O. Saarinen, “A chosen key attack against the secret S-boxes of GOST.” Accessed: Aug. 03, 2024. [Online]. Available: *https://eprint.iacr.org/2019/540*

[36] B. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson, “Twofish: A 128Bit Block Cipher,” Jan. 1998.

[37] B. Schneier, “Schneier on Security: Products that Use Twofish.” Accessed: Aug. 03, 2024. [Online]. Available: *https://www.schneier.com/academic/twofish/products/*

[38] D. Bernstein, “ChaCha, a variant of Salsa20,” Jan. 2008.

[39] Y. Nir and A. Langley, “ChaCha20 and Poly1305 for IETF Protocols,” Internet Engineering Task Force, Request for Comments RFC 8439, Jun. 2018. doi: *10.17487/RFC8439*.

[40] D. J. Bernstein and P. Schwabe, “New AES software speed records.” Accessed: Aug. 03, 2024. [Online]. Available: *https://eprint.iacr.org/2008/381*

[41] H. Böck, A. Zauner, S. Devlin, J. Somorovsky, and P. Jovanovic, “Nonce-Disrespecting Adversaries: Practical Forgery Attacks on GCM in TLS,” presented at the 10th USENIX Workshop on Offensive Technologies (WOOT 16), 2016. Accessed: Aug. 03, 2024. [Online]. Available: *https://www.usenix.org/conference/woot16/workshop-program/presentation/bock*

[42] A. Biryukov and L. Perrin, “State of the Art in Lightweight Symmetric Cryptography,” *IACR Cryptol. ePrint Arch.*, Jun. 2017, Accessed: Aug. 03, 2024. [Online]. Available: *https://www.semanticscholar.org/paper/State-of-the-Art-in-Lightweight-Symmetric-Biryukov-Perrin/532441547d905feae7a65f635594585c96d2987b*

[43] K. Aoki *et al.*, “Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms - Design and Analysis,” presented at the LNCS, Aug. 2000, pp. 39–56. doi: *10.1007/3-540-44983-3_4*.

[44] N. AlFardan, D. J. Bernstein, K. G. Paterson, B. Poettering, and J. C. N. Schuldt, “On the Security of RC4 in TLS,” presented at the 22nd USENIX Security Symposium (USENIX Security 13), 2013, pp. 305–320. Accessed: Aug. 03, 2024. [Online]. Available: *https://www.usenix.org/conference/usenixsecurity13/technical-sessions/paper/alFardan*

[45] V. A. Thakor, M. A. Razzaque, and M. R. A. Khandaker, “Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review,

Comparison and Research Opportunities," *IEEE Access*, vol. 9, pp. 28177–28193, 2021, doi: *10.1109/ACCESS.2021.3052867*.

[46] A. Bogdanov *et al.*, "PRESENT: An Ultra-Lightweight Block Cipher," in *Cryptographic Hardware and Embedded Systems - CHES 2007*, P. Paillier and I. Verbauwhede, Eds., Berlin, Heidelberg: Springer, 2007, pp. 450–466. doi: *10.1007/978-3-540-74735-2_31*.

[47] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, "The SIMON and SPECK lightweight block ciphers," in *Proceedings of the 52nd Annual Design Automation Conference*, in DAC '15. New York, NY, USA: Association for Computing Machinery, Jun. 2015, pp. 1–6. doi: *10.1145/2744769.2747946*.

[48] C. Beierle *et al.*, "The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS," in *Advances in Cryptology – CRYPTO 2016*, M. Robshaw and J. Katz, Eds., Berlin, Heidelberg: Springer, 2016, pp. 123–153. doi: *10.1007/978-3-662-53008-5_5*.

[49] C. De Cannière, "Trivium: A Stream Cipher Construction Inspired by Block Cipher Design Principles," in *Information Security*, S. K. Katsikas, J. López, M. Backes, S. Gritzalis, and B. Preneel, Eds., Berlin, Heidelberg: Springer, 2006, pp. 171–186. doi: *10.1007/11836810_13*.

[50] M. Hell, T. Johansson, and W. Meier, "Grain: A stream cipher for constrained environments," *IJWMC*, vol. 2, pp. 86–93, Jan. 2007, doi: *10.1504/IJWMC.2007.013798*.

[51] M. Hamann, M. Krause, and W. Meier, "LIZARD – A Lightweight Stream Cipher for Power-constrained Devices," *IACR Transactions on Symmetric Cryptology*, pp. 45–79, Mar. 2017, doi: *10.13154/tosc.v2017.i1.45-79*.

[52] I. T. L. Computer Security Division, "Lightweight Cryptography | CSRC | CSRC." Accessed: Aug. 03, 2024. [Online]. Available: *https://csrc.nist.gov/Projects/Lightweight-Cryptography*

[53] N. A. Gunathilake, A. Al-Dubai, and W. J. Buchana, "Recent Advances and Trends in Lightweight Cryptography for IoT Security," in *2020 16th International*

Conference on Network and Service Management (CNSM), Izmir, Turkey: IEEE, Nov. 2020, pp. 1–5. doi: *10.23919/CNSM50824.2020.9269083*.

[54] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International Journal of Bifurcation and Chaos*, vol. 16, pp. 2129–2151, Aug. 2006, doi: *10.1142/S0218127406015970*.

[55] F. Seredynski, P. Bouvry, and A. Y. Zomaya, "Cellular automata computations and secret key cryptography," *Parallel Computing*, vol. 30, no. 5, pp. 753–766, May 2004, doi: *10.1016/j.parco.2003.12.014*.

[56] Y. Zhang, B. Fu, and X. Zhang, "DNA cryptography based on DNA Fragment assembly," in *2012 8th International Conference on Information Science and Digital Content Technology (ICIDT2012)*, Jun. 2012, pp. 179–182. Accessed: Jul. 29, 2024. [Online]. Available: *https://ieeexplore.ieee.org/document/6269252*

[57] W. Kinzel and I. Kanter, "Neural cryptography," in *Proceedings of the 9th International Conference on Neural Information Processing, 2002. ICONIP '02.*, Nov. 2002, pp. 1351–1354 vol.3. doi: *10.1109/ICONIP.2002.1202841*.

[58] G. Herold and A. Meurer, "New Attacks for Knapsack Based Cryptosystems," in *Security and Cryptography for Networks*, I. Visconti and R. De Prisco, Eds., Berlin, Heidelberg: Springer, 2012, pp. 326–342. doi: *10.1007/978-3-642-32928-9_18*.

[59] M. Lawnik, L. Moysis, and C. Volos, "Chaos-Based Cryptography: Text Encryption Using Image Algorithms," *Electronics*, vol. 11, no. 19, p. 3156, Oct. 2022, doi: *10.3390/electronics11193156*.

[60] C. Paar and J. Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners*. Berlin, Heidelberg: Springer, 2010. doi: *10.1007/978-3-642-04101-3*.

[61] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, Nov. 1976, doi: *10.1109/TIT.1976.1055638*.

[62] R. L. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” *Communications of the ACM*, vol. 21, no. 2, 1978, doi: *10.1145/359340.359342*.

[63] І. Д. Горбенко and Ю. І. Горбенко, *КРИПТОЛОГІЯ. ТЕОРІЯ. ПРАКТИКА. ЗАСТОСУВАННЯ*. Харків, 2012. Available: *https://duikt.edu.ua/uploads/l_1886_59996057.pdf*

[64] P. C. Kocher, “Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems,” in *Advances in Cryptology — CRYPTO ’96*, N. Koblitz, Ed., Berlin, Heidelberg: Springer, 1996, pp. 104–113. doi: *10.1007/3-540-68697-5_9*.

[65] D. Hankerson and A. Menezes, “Elliptic Curve Cryptography,” in *Encyclopedia of Cryptography and Security*, H. C. A. van Tilborg and S. Jajodia, Eds., Boston, MA: Springer US, 2011, pp. 397–397. doi: *10.1007/978-1-4419-5906-5_245*.

[66] T. Elgamal, “A public key cryptosystem and a signature scheme based on discrete logarithms,” *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469–472, Jul. 1985, doi: *10.1109/TIT.1985.1057074*.

[67] Y. V. Ostrianska, M. V. Yesina, and I. D. Gorbenko, “Analysis of views of the European Union on quantum-post-quantum limitations,” *Radiotekhnika*, no. 210, 2022, doi: *10.30837/rt.2022.3.210.06*.

[68] L. K. Grover, “Quantum mechanics helps in searching for a needle in a haystack,” *Physical Review Letters*, vol. 79, no. 2, 1997, doi: *10.1103/PhysRevLett.79.325*.

[69] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. O’Brien, “Quantum computers,” *Nature*, vol. 464, no. 7285, pp. 45–53, Mar. 2010, doi: *10.1038/nature08812*.

[70] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” *SIAM Journal on Computing*, vol. 26, no. 5, 1997, doi: *10.1137/S0097539795293172*.

[71] J. Proos and C. Zalka, “Shor’s discrete logarithm quantum algorithm for elliptic curves,” *Quantum Information and Computation*, vol. 3, no. 4, 2003, doi: 10.26421/qic3.4-3.

[72] M. S. Sharbaf, “Quantum cryptography: An emerging technology in network security,” in *2011 IEEE International Conference on Technologies for Homeland Security (HST)*, Waltham, MA, USA: IEEE, Nov. 2011, pp. 13–19. doi: 10.1109/THS.2011.6107841.

[73] I. T. L. Computer Security Division, “Post-Quantum Cryptography | CSRC | CSRC.” Accessed: Aug. 03, 2024. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography

[74] S. Yevseiev, O. Korol, O. Veselska, S. Pohasii, and V. Khvostenko, “Evaluation of Cryptographic Strength and Energy Intensity of Design of Modified Crypto-Code Structure of McEliece with Modified Elliptic Codes,” 2021, pp. 144–157.

[75] S. Yevseiev, R. Korolyov, A. Tkachov, O. Laptiev, I. Opirskyy, and O. Soloviova, “Modification of the algorithm (OFM) S-box, which provides increasing crypto resistance in the post-quantum period,” *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, no. 5, pp. 8725–8729, Oct. 2020, doi: 10.30534/ijatcse/2020/261952020.

[76] D. Grigoriev and I. Ponomarenko, “Homomorphic public-key cryptosystems over groups and rings,” *Quaderni di Mathematica*, vol. 13, pp. 305–325, Jan. 2004.

[77] N. Bindel, U. Herath, M. McKague, and D. Stebila, “Transitioning to a Quantum-Resistant Public Key Infrastructure.” Accessed: Aug. 03, 2024. [Online]. Available: https://eprint.iacr.org/2017/460

[78] O. Barabash, “The Indirect method of obtaining Estimates of the Parameters of Radio Signals of covert means of obtaining Information,” *IJETER*, vol. 8, no. 8, pp. 4133–4139, Aug. 2020, doi: 10.30534/ijeter/2020/17882020.

[79] S. Zhang, J. Pan, Z. Han, and L. Guo, “Recognition of noisy radar emitter signals using a one-dimensional deep residual shrinkage network,” *Sensors*, vol. 21, no. 23, 2021, doi: *10.3390/s21237973*.

[80] Y. Wang, W. Cai, T. Gu, W. Shao, Y. Li, and Y. Yu, “Secure Your Voice: An Oral Airflow-Based Continuous Liveness Detection for Voice Assistants,” *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, vol. 3, no. 4, pp. 1–28, Dec. 2019, doi: *10.1145/3369811*.

[81] X. Zhang, L. Tianyun, P. Gong, R. Lui, and Z. Xiong, “Modulation Recognition of Communication Signals Based on Multimodal Feature Fusion,” *Sensors*, vol. 22, no. 17, 2022, doi: *10.3390/s22176539*.

[82] R. S. Fathalla and W. S. Alshehri, “Emotions Recognition and Signal Classification,” *International Journal of Synthetic Emotions*, vol. 11, no. 1, pp. 1–16, 2020, doi: *10.4018/ijse.2020010101*.

[83] S. Sabut, O. Pandey, B. S. P. Mishra, and M. Mohanty, “Detection of ventricular arrhythmia using hybrid time–frequency-based features and deep neural network,” *Phys Eng Sci Med*, vol. 44, no. 1, pp. 135–145, Mar. 2021, doi: *10.1007/s13246-020-00964-2*.

[84] H. Chen, C. Guo, Z. Wang, and J. Wang, “Research on recognition and classification of pulse signal features based on EPNCC,” *Scientific Reports*, vol. 12, no. 6731, 2022, doi: *10.1038/s41598-022-10808-6*.

[85] A. S. Dovbysh, V. Y. Piatachenko, J. V. Simonovskiy, and O. A. Shkuropat, “Information-extreme hierarchical machine learning of the hand brush prosthesis control system with a non-invasive bio signal reading system,” *RIC*, vol. 0, no. 4, pp. 178–187, Dec. 2020, doi: *10.15588/1607-3274-2020-4-17*.

[86] A. Dovbysh and V. Piatachenko, “Hierarchical clustering approach for information-extreme machine learning ofhand brush prosthesis,” in *CEUR Workshop Proceedings*, 2021, pp. 1706–1715. Available: *https://ceur-ws.org/Vol-2870/paper123.pdf*

[87] F. K. Jondral, “Software-Defined Radio—Basics and Evolution to Cognitive Radio,” *J Wireless Com Network*, vol. 2005, no. 3, p. 652784, Dec. 2005, doi: *10.1155/WCN.2005.275*.

[88] V. M. Bezruk and S. A. Ivanenko, “Detection and recognition of signals under conditions of high a priori uncertainty in the tasks of radio monitoring,” *Control, Navigation and Communication Systems. Academic Journal*, vol. 2, no. 48, pp. 135–141, 2018, doi: *10.26906/SUNZ.2018.2.135.*

[89] V. M. Bezruk and S. A. Ivanenko, “Vyyavlennya ta rozpiznavannya syhnaliv v kohnytyvnykh radiomerezhakh [Detection and recognition of signals in cognitive radio networks],” in *MADRYD*, Kharkiv, 2019. Available: *http://openarchive.nure.ua/handle/document/10877*

[90] P. Bergamo, P. D’Arco, A. Santis, and L. Kocarev, “Security of public-key cryptosystems based on Chebyshev polynomials,” *Circuits and Systems I: Regular Papers, IEEE Transactions on*, vol. 52, pp. 1382–1393, Aug. 2005, doi: *10.1109/TCSI.2005.851701*.

[91] R. Hryshchuk and O. Hryshchuk, “A generalized model of Fredholm’s cryptosystem,” *Cybersecurity: Education Science Technique*, no. 4, pp. 14–23, 2019, doi: *10.28925/2663-4023.2019.4.1423*.

[92] L. Kocarev and Z. Tasev, “Public-key encryption based on Chebyshev maps,” presented at the Circuits and Systems, 2003. ISCAS ’03. Proceedings of the 2003 International Symposium on, Jun. 2003, pp. III–28. doi: *10.1109/ISCAS.2003.1204947*.

[93] V. V. Avramenko, “Характеристики непропорциональности числовых функций и их применение при решении задач диагностики,” *Вісник Сумського державного університету. Серія Технічні науки.*, vol. 16, pp. 12–20, 2000, Available: *https://essuir.sumdu.edu.ua/handle/123456789/1824*

[94] A. P. Karpenko, “Integral’nye kharakteristiki neproportsional’nosti chislovykh funktsii i ikh primenenie v diagnostike [Integral characteristics of the disproportionality of numerical functions and their application in diagnostics],” *Visnik of the Sumy State University. Series: Technical Sciences*, vol. 16, pp. 20–25, 2000,

Accessed: Dec. 02, 2021. [Online]. Available: https://essuir.sumdu.edu.ua/bitstream-download/123456789/10931/1/4_Karpenko.pdf

[95] V. Avramenko and M. Zabolotny, “A Way of Data Coding.” Державне підприємство "Український інститут промислової власності" (УКРПАТЕНТ), 2009. Available: https://essuir.sumdu.edu.ua/handle/123456789/9879

[96] V. V. Kalashnikov, V. V. Avramenko, N. I. Kalashnykova, and V. V. Kalashnikov, “A Cryptosystem Based Upon Sums of Key Functions,” *International Journal of Combinatorial Optimization Problems and Informatics*, vol. 8, no. 1, pp. 31–38, 2017, Available: https://www.redalyc.org/articulo.oa?id=265253895005

[97] N. Kalashnykova, V. V. Avramenko, and V. Kalashnikov, “Sums of Key Functions Generating Cryptosystems,” 2019, pp. 293–302. doi: 10.1007/978-3-030-22750-0_23.

[98] В. В. Авраменко and А. П. Карпенко, “Распознавание фрагментов заданных эталонов в анализируемом сигнале с помощью функций непропорциональности,” *Вісник Сумського державного університету*, vol. 34, no. 1, pp. 96–101, 2002, Accessed: Jun. 20, 2024. [Online]. Available: https://scholar.google.com/scholar?cluster=5088282024681642268&hl=en&oi=scholarr

[99] V. Avramenko and V. Demianenko, “Cryptosystem based on a key function of a real variable,” in *CEUR Workshop Proceedings*, 2020. doi: 10.46932/sfjdv2n2-113.

[100] V. Avramenko and V. Demianenko, “Serial encryption using the functions of real variable,” *reks*, no. 2, pp. 39–50, Jun. 2021, doi: 10.32620/reks.2021.2.04.

[101] V. Makarichev, V. Lukin, O. Illiashenko, and V. Kharchenko, “Digital Image Representation by Atomic Functions: The Compression and Protection of Data for Edge Computing in IoT Systems,” *Sensors*, vol. 22, no. 10, p. 3751, May 2022, doi: 10.3390/s22103751.

[102] H. K. Albahadily, A. A. J. Altaay, and I. A. Jabbar, “Encryption of Military Maps ImagesUsing Peter De Jong Chaotic Maps and Lightwaght Encryption,”

in *2022 Fifth College of Science International Conference of Recent Trends in Information Technology (CSCTIT)*, Baghdad, Iraq: IEEE, Nov. 2022, pp. 137–142. doi: *10.1109/CSCTIT56299.2022.10145728*.

[103] S. Madhu and M. Ali Hussain, "Securing Medical Images by Image Encryption using Key Image," *IJCA*, vol. 104, no. 3, pp. 30–34, Oct. 2014, doi: *10.5120/18184-9079*.

[104] S. Madhu, M. A. Hussain, N. Leelavathy, and B. Sujatha, "Development of Secure and Novel Methods of Image Encryption Using an Image as Key," in *Research Highlights in Mathematics and Computer Science Vol. 7*, Prof. Q.-W. Wang, Ed., B P International (a part of SCIENCEDOMAIN International), 2023, pp. 89–102. doi: *10.9734/bpi/rhmcs/v7/4297E*.

[105] N. Archana, S. Manogna, Dr. M. A. Hussain, and Dr. Sk. Razia, "Secure Sharing of Documents using Image Encryption and Key Image," *IJRTE*, vol. 8, no. 4, pp. 9415–9419, Nov. 2019, doi: *10.35940/ijrte.D9724.118419*.

[106] A. G. Phatak, "A Non-format Compliant Scalable RSA-based JPEG Encryption Algorithm," *International Journal of Image, Graphics and Signal Processing*, vol. 8, no. 6, pp. 64–71, Jun. 2016, doi: *10.5815/ijigsp.2016.06.08*.

[107] B. Zhang and L. Liu, "Chaos-Based Image Encryption: Review, Application, and Challenges," *Mathematics*, vol. 11, no. 11, p. 2585, Jun. 2023, doi: *10.3390/math11112585*.

[108] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, "A Modified AES Based Algorithm for Image Encryption," *International Journal on Computer Science and Engineering*, vol. 1, no. 1, 2007.

[109] G. Ye, K. Jiao, X. Huang, B.-M. Goi, and W.-S. Yap, "An image encryption scheme based on public key cryptosystem and quantum logistic map," *Scientific Reports*, vol. 10, no. 1, p. 21044, Dec. 2020, doi: *10.1038/s41598-020-78127-2*.

[110] K.-W. Wong, "Image Encryption Using Chaotic Maps," *Intelligent Computing Based on Chaos*, pp. 333–354, Jan. 2009, doi: *10.1007/978-3-540-95972-4_16*.

[111] G. Hanchinamani and L. Kulakarni, “Image Encryption Based on 2-D Zaslavskii Chaotic Map and Pseudo Hadmard Transform,” *International Journal of Hybrid Information Technology*, vol. 7, no. 4, 2014, doi: 10.14257/ijhit.2014.7.4.16.

[112] P. Cheng, H. Yang, P. Wei, and W. Zhang, “A fast image encryption algorithm based on chaotic map and lookup table,” *Nonlinear Dynamics*, vol. 79, no. 3, pp. 2121–2131, Feb. 2015, doi: 10.1007/s11071-014-1798-y.

[113] J. Zhang, Z. Lu, and M. Li, “Study on an efficient hyper-chaos-based image encryption scheme using global bit permutation,” *Technology and Health Care*, vol. 28, pp. 303–309, Jun. 2020, doi: 10.3233/THC-209030.

[114] J. Chen, “A DNA-based, biomolecular cryptography design,” in *Proceedings of the 2003 International Symposium on Circuits and Systems, 2003. ISCAS ’03.*, IEEE, 2003, pp. 822–825. doi: 10.1109/ISCAS.2003.1205146.

[115] S. Pramanik and S. K. Setua, “DNA cryptography,” in *2012 7th International Conference on Electrical and Computer Engineering*, IEEE, Dec. 2012, pp. 551–554. doi: 10.1109/ICECE.2012.6471609.

[116] T. Anwar, S. Paul, and S. K. Singh, “Message Transmission Based on DNA Cryptography: Review,” *International Journal of Bio-Science and Bio-Technology*, vol. 6, no. 5, pp. 215–222, Oct. 2014, doi: 10.14257/ijbsbt.2014.6.5.22.

[117] R. Guesmi, M. A. B. Farah, A. Kachouri, and M. Samet, “A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2,” *Nonlinear Dynamics*, vol. 83, no. 3, pp. 1123–1136, Feb. 2016, doi: 10.1007/s11071-015-2392-7.

[118] R. Matthews, “ON THE DERIVATION OF A ‘CHAOTIC’ ENCRYPTION ALGORITHM,” *Cryptologia*, vol. 13, no. 1, pp. 29–42, Jan. 1989, doi: 10.1080/0161-118991863745.

[119] L. M. Pecora and T. L. Carroll, “Synchronization in chaotic systems,” *Phys. Rev. Lett.*, vol. 64, no. 8, pp. 821–824, Feb. 1990, doi: 10.1103/PhysRevLett.64.821.

[120] M. S. Baptista, “Cryptography with chaos,” *Physics Letters A*, vol. 240, no. 1–2, pp. 50–54, Mar. 1998, doi: 10.1016/S0375-9601(98)00086-3.

[121] S. Li, G. Chen, K.-W. Wong, X. Mou, and Y. Cai, “Baptista-type chaotic cryptosystems: Problems and countermeasures,” *Physics Letters A*, vol. 332, no. 5–6, pp. 368–375, Nov. 2004, doi: *10.1016/j.physleta.2004.09.028*.

[122] L. Y. Zhang *et al.*, “On the Security of a Class of Diffusion Mechanisms for Image Encryption,” *IEEE Transactions on Cybernetics*, vol. 48, no. 4, pp. 1163–1175, Apr. 2018, doi: *10.1109/TCYB.2017.2682561*.

[123] R. Lukac, *Perceptual Digital Imaging*, 1st edition. CRC Press, 2012.

[124] L. Kocarev and S. Lian, Eds., *Chaos-Based Cryptography: Theory,Algorithms and Applications*, vol. 354. in Studies in Computational Intelligence, vol. 354. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011. doi: *10.1007/978-3-642-20542-2*.

[125] U. S. Choi, S. J. Cho, and S. W. Kang, “New Color Image Encryption for Medical Images Based on Three Dimensional Generalized Chaotic Cat Map and Combined Cellular Automata,” *Advances in Science, Technology and Engineering Systems Journal*, vol. 5, no. 2, pp. 104–110, 2020, doi: *10.25046/aj050213*.

[126] A. A. Neamah and A. A. Shukur, “A Novel Conservative Chaotic System Involved in Hyperbolic Functions and Its Application to Design an Efficient Colour Image Encryption Scheme,” *Symmetry*, vol. 15, no. 8, p. 1511, Jul. 2023, doi: *10.3390/sym15081511*.

[127] M. Li, X. Fang, and A. Ernest, “A Color Image Encryption Method Based on Dynamic Selection Chaotic System and Singular Value Decomposition,” *Mathematics*, vol. 11, no. 15, p. 3274, Jul. 2023, doi: *10.3390/math11153274*.

[128] A. Z. Hussain and M. A. A. Khodher, “Medical image encryption using multi chaotic maps,” *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 21, no. 3, p. 556, Jun. 2023, doi: *10.12928/telkomnika.v21i3.24324*.

[129] M. I. Sobhy and A.-E. R. Shehata, “Methods of attacking chaotic encryption and countermeasures,” in *2001 IEEE International Conference on Acoustics, Speech, and Signal Processing. Proceedings (Cat. No.01CH37221)*, May 2001, pp. 1001–1004 vol.2. doi: *10.1109/ICASSP.2001.941086*.

[130] R. Rhouma and S. Belghith, “Cryptanalysis of a new image encryption algorithm based on hyper-chaos,” *Physics Letters A*, vol. 372, no. 38, pp. 5973–5978, Sep. 2008, doi: *10.1016/j.physleta.2008.07.057*.

[131] C. Li, S. Li, G. Alvarez, G. Chen, and K.-T. Lo, “Cryptanalysis of a chaotic block cipher with external key and its improved version,” *Chaos, Solitons & Fractals*, vol. 37, no. 1, pp. 299–307, Jul. 2008, doi: *10.1016/j.chaos.2006.08.025*.

[132] C. Li, D. Lin, B. Feng, J. Lu, and F. Hao, “Cryptanalysis of a Chaotic Image Encryption Algorithm Based on Information Entropy,” *IEEE Access*, vol. 6, pp. 75834–75842, 2018, doi: *10.1109/ACCESS.2018.2883690*.

[133] L. Liu, Z. Zhang, and R. Chen, “Cryptanalysis and Improvement in a Plaintext-Related Image Encryption Scheme Based on Hyper Chaos,” *IEEE Access*, vol. 7, pp. 126450–126463, 2019, doi: *10.1109/ACCESS.2019.2938181*.

[134] A. P. Kari, A. H. Navin, A. M. Bidgoli, and M. Mirnia, “A new image encryption scheme based on hybrid chaotic maps,” *Multimedia Tools and Applications*, vol. 80, no. 2, pp. 2753–2772, Jan. 2021, doi: *10.1007/s11042-020-09648-1*.

[135] N. Thein, H. A. Nugroho, T. B. Adji, and I. W. Mustika, “Comparative Performance Study on Ordinary and Chaos Image Encryption Schemes,” presented at the 2017 International Conference on Advanced Computing and Applications (ACOMP), IEEE Computer Society, Nov. 2017, pp. 122–126. doi: *10.1109/ACOMP.2017.25*.

[136] Z. Qiao, *Nonlinear Dynamics, Applications to Chaos-based Encryption*. 2021. Available: *https://books.google.com?id=eBgj0AEACAAJ*

[137] W. S. Sayed, A. G. Radwan, H. A. H. Fahmy, and A. El-Sedeek, “Software and Hardware Implementation Sensitivity of Chaotic Systems and Impact on Encryption Applications,” *Circuits Syst Signal Process*, vol. 39, no. 11, pp. 5638–5655, Nov. 2020, doi: *10.1007/s00034-020-01424-8*.

[138] D. Mishra, M. Obaidat, S. Rana, D. Dharminder, A. Mishra, and B. Sadoun, “Chaos-Based Content Distribution Framework for Digital Rights

Management System," *IEEE Systems Journal*, vol. PP, pp. 1–7, Mar. 2020, doi: *10.1109/JSYST.2020.2977929*.

[139] G. M. Church, Y. Gao, and S. Kosuri, "Next-generation digital information storage in DNA," *Science*, vol. 337, no. 6102, p. 1628, Sep. 2012, doi: *10.1126/science.1226355*.

[140] M. Mondal and K. S. Ray, "Review on DNA Cryptography." Accessed: Jul. 26, 2024. [Online]. Available: *http://arxiv.org/abs/1904.05528*

[141] Y. Niu, K. Zhao, X. Zhang, and G. Cui, "Review on DNA Cryptography," in *Bio-inspired Computing: Theories and Applications*, L. Pan, J. Liang, and B. Qu, Eds., Singapore: Springer, 2020, pp. 134–148. doi: *10.1007/978-981-15-3415-7_11*.

[142] L. M. Adleman, "Molecular computation of solutions to combinatorial problems," *Science*, vol. 266, no. 5187, pp. 1021–1024, Nov. 1994, doi: *10.1126/science.7973651*.

[143] Z. Yunpeng, Zhu Yu, W. Zhong, and R. O. Sinnott, "Index-based symmetric DNA encryption algorithm," in *2011 4th International Congress on Image and Signal Processing*, Shanghai, China: IEEE, Oct. 2011, pp. 2290–2294. doi: *10.1109/CISP.2011.6100690*.

[144] T. Mandge and V. Choudhary, "A DNA encryption technique based on matrix manipulation and secure key generation scheme," in *2013 International Conference on Information Communication and Embedded Systems (ICICES)*, Feb. 2013, pp. 47–52. doi: *10.1109/ICICES.2013.6508181*.

[145] M. Krishnamurthy, "Encrypting information using DNA sequences with matrix algebra," vol. 6, pp. 1586–1590, Nov. 2023.

[146] A. Pandey and S. Chanda, "Implementation of DNA Cryptography using IBROS Cypher," *International Research Journal of Innovations in Engineering and Technology*, vol. 7, pp. 72–82, Aug. 2023, doi: *10.47001/IRJIET/2023.708010*.

[147] M. A. Iliyasu, O. A. Abisoye, S. A. Bashir, and J. A. Ojeniyi, "A Review of Dna Cryptograhic Approaches," in *2020 IEEE 2nd International Conference on*

Cyberspac (CYBER NIGERIA), Feb. 2021, pp. 66–72. doi: *10.1109/CYBERNIGERIA51635.2021.9428855*.

[148] G. Singh and Dr. R. Yadav, "DNA Based Cryptography Techniques with Applications and Limitations," *International Journal of Engineering and Advanced Technology*, vol. 8, pp. 3997–4004, Aug. 2019, doi: *10.35940/ijeat.F9285.088619*.

[149] A. Hazra, S. Ghosh, and S. Jash, "A Review on DNA Based Cryptographic Techniques," *International Journal of Network Security*, vol. 20, pp. 1093–1104, Nov. 2018, doi: *10.6633/IJNS.201811_20(6).10*.

[150] W. Peng, S. Cui, and C. Song, "One-time-pad cipher algorithm based on confusion mapping and DNA storage technology," *PLOS ONE*, vol. 16, p. e0245506, Jan. 2021, doi: *10.1371/journal.pone.0245506*.

[151] A. R. Smith, "Introduction to and Survey of Cellular Automata or Polyautomata Theory," *bioinformatics.bio.uu.nl*, 2001, Accessed: Jul. 31, 2024. [Online]. Available: *https://www.academia.edu/53141843/Introduction_to_and_Survey_of_Cellular_Automata_or_Polyautomata_Theory*

[152] S. Wolfram, "Cryptography with Cellular Automata," in *Advances in Cryptology — CRYPTO '85 Proceedings*, vol. 218, H. C. Williams, Ed., Berlin, Heidelberg: Springer Berlin Heidelberg, 1986, pp. 429–432. doi: *10.1007/3-540-39799-X_32*.

[153] E. Formenti, K. Imai, B. Martin, and J.-B. Yunès, *Advances on Random Sequence Generation by Uniform Cellular Automata*, vol. 8808. 2014. doi: *10.1007/978-3-319-13350-8_5*.

[154] S. Bilan, M. Bilan, and S. Bilan, "Novel pseudo-random sequence of numbers generator based cellular automata," *Collection Information technology and security*, vol. 3, pp. 38–50, Jun. 2015, doi: *10.20535/2411-1031.2015.3.1.57710*.

[155] A. John, R. Lakra, and J. Jose, "On the design of stream ciphers with Cellular Automata having radius = 2," *IACR Cryptol. ePrint Arch.*, p. 327, 2020, Available:

https://scholar.google.com/citations?view_op=view_citation&hl=en&user=tqxzB5IAAAAJ&citation_for_view=tqxzB5IAAAAJ:WF5omc3nYNoC

[156] O. Omran, “Cellular Automata Based Image Encryption,” 2022.

[157] Y. Sbaytri, S. Lazaar, H. Benaboud, and S. Bouchkaren, “A New Secure Cellular Automata Cryptosystem for Embedded Devices,” 2019, pp. 259–267. doi: 10.1007/978-3-030-22885-9_22.

[158] M. Das, K. Das, M. Sahu, and R. Dash, “Application of Cellular Automata for an Efficient Symmetric Key Cryptosystem,” May 2019, pp. 21–26. doi: 10.1109/ICAML48257.2019.00012.

[159] G. Stanica and P. Anghelescu, “Reversible Cellular Automata Based Cryptosystem,” *Electronics*, vol. 13, p. 2515, Jun. 2024, doi: 10.3390/electronics13132515.

[160] B. Mondal, S. Singh, and P. Kumar, “A secure image encryption scheme based on cellular automata and chaotic skew tent map,” *Journal of Information Security and Applications*, vol. 45, pp. 117–130, Apr. 2019, doi: 10.1016/j.jisa.2019.01.010.

[161] X. Chai, Y. Chen, and L. Broyde, “A novel chaos-based image encryption algorithm using DNA sequence operations,” *Optics and Lasers in Engineering*, vol. 88, pp. 197–213, Jan. 2017, doi: 10.1016/optlaseng.2016.08.009.

[162] X. Wu, H. Kan, and J. Kurths, “A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps,” *Applied Soft Computing*, vol. 37, Aug. 2015, doi: 10.1016/j.asoc.2015.08.008.

[163] Y.-Q. Zhang, X.-Y. Wang, J. Liu, and Z.-L. Chi, “An image encryption scheme based on the MLNCML system using DNA sequences,” *Optics and Lasers in Engineering*, vol. 82, pp. 95–103, Jul. 2016, doi: 10.1016/j.optlaseng.2016.02.002.

[164] E. Volna, M. Kotyrba, V. Kocian, and M. Janosek, “Cryptography Based On Neural Network,” May 2012, doi: 10.7148/2012-0386-0391.

[165] N. Bigdeli, Y. Farid, and K. Afshar, “A novel image encryption/decryption scheme based on chaotic neural networks,” *Engineering*

Applications of Artificial Intelligence, vol. 25, pp. 753–765, Jun. 2012, doi: *10.1016/j.engappai.2012.01.007*.

[166] N. Al-Saidi, "Using fractal as an Encryption Method," Apr. 2009.

[167] N. R. Zhou, T. X. Hua, L. H. Gong, D. J. Pei, and Q. H. Liao, "Quantum image encryption based on generalized Arnold transform and double random-phase encoding," *Quantum Inf Process*, vol. 14, no. 4, pp. 1193–1213, Apr. 2015, doi: *10.1007/s11128-015-0926-z*.

[168] M. Zhang *et al.*, "Image Compression and Encryption Scheme Based on Compressive Sensing and Fourier Transform," *IEEE Access*, vol. PP, pp. 1–1, Feb. 2020, doi: *10.1109/ACCESS.2020.2976798*.

[169] M. Naor and A. Shamir, "Visual cryptography," in *Advances in Cryptology — EUROCRYPT'94*, vol. 950, A. De Santis, Ed., Berlin, Heidelberg: Springer Berlin Heidelberg, 1995, pp. 1–12. doi: *10.1007/BFb0053419*.

[170] A. K. Panigrahi *et al.*, "A Faster and Robust Artificial Neural Network Based Image Encryption Technique With Improved SSIM," *IEEE Access*, vol. PP, pp. 1–1, Jan. 2024, doi: *10.1109/ACCESS.2024.3353294*.

[171] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Opt. Lett., OL*, vol. 20, no. 7, pp. 767–769, Apr. 1995, doi: *10.1364/OL.20.000767*.

[172] R. Fischlin and J.-P. Seifert, "Tensor-based Trapdoors for CVP and their Application to Public Key Cryptography," Feb. 2000. doi: *10.1007/3-540-46665-7_29*.

[173] A. Dawood, Q. Thabit, and T. Fahad, "A Comprehensive Review of Color Image Encryption Technology," *Basrah journal for engineering science*, vol. 23, no. 1, pp. 56–63, Jul. 2023, doi: *10.33971/bjes.23.1.8*.

[174] Y. Zhou, K. Panetta, and S. Agaian, "Image encryption using binary key-images," in *2009 IEEE International Conference on Systems, Man and Cybernetics*, IEEE, Oct. 2009, pp. 4569–4574. doi: *10.1109/ICSMC.2009.5346780*.

[175] Y. Zhou, W. Cao, and C. L. P. Chen, "Image encryption using binary bitplane," *Signal Processing*, vol. 100, pp. 197–207, Jul. 2014, doi: *10.1016/j.sigpro.2014.01.020*.

[176] S. Somaraj and M. AliHussain, “An Image Encryption Technique Using Scan Based Approach and Image as Key,” in *Advances in Intelligent Systems and Computing*, vol. 507, Springer Verlag, 2017, pp. 645–653. doi: *10.1007/978-981-10-2471-9_62*.

[177] S. Somaraj and M. A. Hussain, “A Novel Image Encryption Technique Using RGB Pixel Displacement for Color Images,” in *2016 IEEE 6th International Conference on Advanced Computing (IACC)*, IEEE, Feb. 2016, pp. 275–279. doi: *10.1109/IACC.2016.59*.

[178] S. Somaraj and M. A. Hussain, “Performance and Security Analysis for Image Encryption using Key Image,” *Indian Journal of Science and Technology*, vol. 8, no. 35, Dec. 2015, doi: *10.17485/ijst/2015/v8i35/73141*.

[179] L. Tang, “Methods for encrypting and decrypting MPEG video data efficiently,” in *Proceedings of the fourth ACM international conference on Multimedia*, in MULTIMEDIA ’96. New York, NY, USA: Association for Computing Machinery, Feb. 1997, pp. 219–229. doi: *10.1145/244130.244209*.

[180] J. He, S. Huang, S. Tang, and J. Huang, “JPEG Image Encryption With Improved Format Compatibility and File Size Preservation,” *IEEE Transactions on Multimedia*, vol. 20, no. 10, pp. 2645–2658, Oct. 2018, doi: *10.1109/TMM.2018.2817065*.

[181] H. Kobayashi and H. Kiya, “Bitstream-Based JPEG Image Encryption with File-Size Preserving,” in *2018 IEEE 7th Global Conference on Consumer Electronics (GCCE)*, IEEE, Oct. 2018, pp. 384–387. doi: *10.1109/GCCE.2018.8574605*.

[182] V. V. Avramenko and Y. I. Prohnenko, “Raspoznavanie periodicheskikh etalonnykh signalov pri nalozhenii periodicheskikh pomekh [Recognition of periodic reference signals with the imposition of periodic interference],” *Eastern-European Journal of Enterprise Technologies*, vol. 6/4, no. 60, pp. 64–67, 2012, Available: *https://cyberleninka.ru/article/n/raspoznavanie-periodicheskih-etalonnyh-signalov-pri-nalozhenii-periodicheskih-pomeh*

ДОДАТОК А

Список опублікованих праць за темою дисертації

Наукові праці, в яких опубліковані основні наукові результати дисертації:

Статті у наукових фахових виданнях України

[1] V. Avramenko and M. Bondarenko, “Recognition of reference signals and determination of their weighting coefficients if an additive interference presents,” *Radio Electronics, Computer Science, Control*, p. 73, Oct. 2023, doi: 10.15588/1607-3274-2023-3-8.

(Особистий внесок автора.: Розроблено методи комп’ютерного моделювання системи розпізнавання еталонного сигналу при накладанні завади, проведено аналіз результатів розпізнавання у випадках накладання частот)

(Особистий внесок Авраменко В.В.: Розроблена математична постановка задачі, створена математична модель та методи розпізнавання еталонного сигналу при накладанні завади, проведений аналіз різних випадків накладання завади)

[2] V. Avramenko and M. Bondarenko, “Encryption of messages by the sum of a real variable functions.” *Stuc.intelekt*, vol. 29, pp. 10–19, Jun. 2024, doi: 10.15407/jai2024.02.010.

(Особистий внесок автора: Проведена розробка методу шифрування повідомлень сумою функцій дійсної змінною з застосуванням схеми перестановки функцій-ключів, розроблені методи комп’ютерного моделювання, проведений аналіз результатів на предмет декореляції шифротексту)

(Особистий внесок Авраменко В.В.: Розроблена математична постановка задачі, проведено концептуалізацію підходу, створена математична модель зашифрованого повідомлення)

[3] V. Avramenko and M. Bondarenko, “Encrypting images using the sum of the functions of a real variable,” *Transactions of Kremenchuk Mykhailo Ostrohradskyi National University*, vol. 144, no. 1, pp. 140–147, 2024, doi: 10.32782/1995-

0519.2024.1.18. *(Особистий внесок автора: розроблений спосіб застосування алгоритму шифрування повідомлень сумою функцій дійсної змінною для захисту візуальних даних, розроблені методи комп'ютерного моделювання)*

(Особистий внесок Авраменко В.В.: розроблена математична постановка задачі, створену математична модель зашифрованого повідомлення, проведений аналіз результатів)

[4] V. Avramenko and M. Bondarenko, "Image cryptosystem with image key using integral disproportion," *Radioelectronic and Computer Systems*, vol. 2024, pp. 147–159, Apr. 2024, doi: 10.32620/reks.2024.2.12.

(Особистий внесок автора: розроблені моделі та методи створення криптосистем для захисту зображення використовуючи інше зображення в якості криптографічного ключа, розроблені алгоритми шифрування та дешифрування зображення з використанням інтегральних функцій непропорційності, проаналізовані граничні випадки їх використання, розроблені моделі комп'ютерного моделювання, проведено верифікацію коректності роботи запропонованих методів, проаналізовано результати на предмет стійкості методу до атак грубої сили, проаналізовано здатності запропонованого метода до декореляції шифротексту.)

(Особистий внесок Авраменко В.В.: проведено концептуалізацію підходу, розроблена математична постановка задачі)

Опубліковані праці апробаційного характеру

[5] V. Avramenko and M. Bondarenko, "Using the Sum of Real Type Functions to Encrypt Messages," in *CEUR Workshop Proceedings*, presented at the 3rd International Conference on Information Security and Information Technologies (ISecIT 2021), Odesa, Ukraine, September 13-19, 2021, p. 10-17. Available: https://ceur-ws.org/Vol-3200/paper2.pdf

(Особистий внесок автора: проведена розробка методів дешифрування з використанням функцій інтегральної непропорційності першого порядку,

розроблені методи комп'ютерного моделювання, проведена верифікація коректності роботи та аналіз результатів.)

(Особистий внесок Авраменко В.В.: проведено концептуалізацію підходу, розроблена математична постановка задачі, створено модель зашифрованого повідомлення)

[6] V. Avramenko and M. Bondarenko, "Combined encryption system using the sum of functions of a real variable," presented at the The International Scientific and Technical Conferences of Students and Young scientists "Informatics. Mathematics. Automation," Sumy - Astana, April 18-22, 2022, p. 71. [Online] Available: https://essuir.sumdu.edu.ua/bitstream-download/123456789/87782/1/Conf_IMA_2022.pdf

(Особистий внесок автора: розроблено моделі та методи поєднання шифрування сумою функцій дійсної змінної та функцією інтегральної непропорційності першого порядку.)

(Особистий внесок Авраменко В.В.: розроблена математична постановка задачі, розроблені моделі комп'ютерного моделювання, проведено верифікацію коректності роботи запропонованих методів)

[7] V. Avramenko and M. Bondarenko, "Signal recognition and calculation weighting coefficients in the presence of additive interference," presented at the The International Scientific and Technical Conferences of Students and Young scientists "Informatics. Mathematics. Automation," Sumy - Astana, April 24-28, 2023, p. 81-82. [Online] Available: https://drive.google.com/file/d/1YDGNhbgZY6dfsqwN6P0BcEpcq6CuCKmj/view

(Особистий внесок автора: розроблено методи комп'ютерного моделювання системи розпізнавання еталонного сигналу при накладанні завади, проведено аналіз розпізнавання у випадках накладання частот)

(Особистий внесок Авраменко В.В.: Розроблена математична постановка задачі, створена математична модель та методи розпізнавання еталонного

сигналу при накладанні завади, проведений аналіз різних випадків накладання завади)

[8] V. Avramenko and M. Bondarenko, “Image encryption with key-image using integral disproportion,” presented at the The International Scientific and Technical Conferences of Students and Young scientists “Informatics. Mathematics. Automation,” Sumy - Astana, April 22-29, 2024, p. 38–39. [Online] Available: https://drive.google.com/file/d/1jjUd3KWmCmrPnOXTnZZSGbZIbsWWBPzU/view

(Особистий внесок автора: проведений аналіз існуючих методів шифрування зображень, розроблені моделі та методи створення криптосистем для захисту зображення використовуючи інше зображення в якості криптографічного ключа, розроблені алгоритми шифрування та дешифрування зображення з використанням інтегральних функцій непропорційності, розроблені моделі комп’ютерного моделювання, проведено верифікацію коректності роботи запропонованої криптосистеми, проаналізовано результати на предмет стійкості до атак грубої сили, проаналізовано здатності запропонованого метода до декореляції шифротексту.)

(Особистий внесок Авраменко В.В.: проведено концептуалізацію підходу, розроблена математична постановка задачі)

Наукові праці, які додатково відображають наукові результати дисертаційної роботи

[9] Пат. 153107 U Україна, МПК (2023.01) H04L 9/00. Спосіб шифрування графічних зображень / В. В. Авраменко, М. О. Бондаренко (Україна); заявник та патентовласник Сумський державний університет. - № u202201970; заявл. 10.06.2022; опубл. 24.05.2023, Бюл. № 21. 5 с.

(Особистий внесок автора: розроблений спосіб застосування алгоритму шифрування повідомлень сумою функцій дійсної змінною для захисту візуальних даних, розроблені методи комп’ютерного моделювання)

(Особистий внесок Авраменко В.В.: розроблена математична постановка задачі, створену математична модель зашифрованого повідомлення, проведений аналіз результатів)

[10] Пат. 147560 U Україна, МПК G09C 1/00 H04L 9/16 (2006.01). Спосіб шифрування даних за допомогою суми функцій дійсної змінної / В.В. Авраменко, М.О. Бондаренко, Т.В. Лаврик (Україна); заявник та патентовласник Сумський держ. ун-т. - № u202008363; заявл. 28.12.2020; опубл.19.05.2021, бюл. №20

(Особистий внесок автора: Проведена розробка моделей та методів шифрування та дешифрування)

(Особистий внесок Авраменко В.В.: Проведено концептуалізацію підходу, розроблена математична постановка задачі дешифрування, проведена розробка моделей та методів шифрування та дешифрування)

(Особистий внесок Лаврик Т.В.: розроблені моделі комп'ютерного моделювання, проведено верифікацію коректності роботи запропонованих методів)