

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

KHARKIV NATIONAL
UNIVERSITY OF RADIO ELECTRONICS

RADIOTEKHNIKA

**All-Ukrainian
interdepartmental scientific and technical collection**

ISSN 0485-8972
eISSN 2786-5525

Founded in 1965

I S S U E 2 1 5

Kharkiv
Kharkiv National
University of Radio Electronics
2023

UDC 621.3

The collection is included in the List of scientific professional publications of Ukraine, category «Б», technical and physical-mathematical sciences (approved by orders of the Ministry of Education and Science from 17.03.2020 № 409; from 02.07.2020 № 886; from 24.09.2020 № 1188) by specialties: 105 – Applied Physics and Nanomaterials; 125 – Cybersecurity and information protection; 163 – Biomedical Engineering; 171 – Electronics; 172 – Telecommunications and Radio Engineering; 173 – Avionics; 174 –Automation and Computer-Integrated Technologies and Robotics; 175 – Metrology and information-measuring technique; 176 – Micro- and Nanosystem Technology.

Website: rt.nure.ua

Registration certificate KV № 12098-969 PR dated 14. 12. 2006.

The authors are responsible for the content of the article.

Editorial Team

I.V. Svyd, *PhD, Assoc. prof.*, NURE, Ukraine (Chief Editor)
O.G. Avrunin, *Dr. Sc. (Tech.), prof.*, NURE, Ukraine
D.V. Ageiev, *Dr. Sc. (Tech.), prof.*, NURE, Ukraine
V.M. Bezruk, *Dr. Sc. (Tech.), prof.*, NURE, Ukraine
I.M. Bondarenko, *Dr. Sc. (Phys.-Math.), prof.*, NURE, Ukraine
I.D. Gorbenko, *Dr. Sc. (Tech.), prof.*, KhNU V. N. Karazin, Ukraine
D.V. Gretsikh, *Dr. Sc. (Tech.), Assoc. prof.*, NURE, Ukraine
K.Yu. Dergachov, *PhD, Senior Researcher, Sciences, prof.*, NAU «KhAI», Ukraine
V.O. Doroshenko, *Dr. Sc. (Phys.-Math.), prof.*, NURE, Ukraine
I.P. Zakharov, *Dr. Sc. (Tech.), prof.*, NURE, Ukraine
V.M. Kartashov, *Dr. Sc. (Tech.), prof.*, NURE, Ukraine
O.O. Konovalenko, *Dr. Sc. (Phys.-Math.), prof.*, Academician of NASU, IRA NASU, Ukraine
A.S. Kulik, *Dr. Sc. (Tech.), prof.*, NAU «KhAI», Ukraine
L.M. Lytvynenko, *Dr. Sc. (Phys.-Math.), prof.*, Academician of NASU, IRA NASU, Ukraine
A.I. Luchaninov, *Dr. Sc. (Phys.-Math.), prof.*, NURE, Ukraine
K.M. Muzyka, *Dr. Sc. (Tech.), Senior Researcher*, NURE, Ukraine
E.M. Odarenko, *Dr. Sc. (Tech.), prof.*, NURE, Ukraine
O.G. Pashchenko, *PhD, Assoc. prof.*, NURE, Ukraine
V.V. Semenets, *Dr. Sc. (Tech.), prof.*, NURE, Ukraine
S.I. Tarapov, *Dr. Sc. (Phys.-Math.), prof.*, member-cor. NASU, IRE NASU, Ukraine
P.L. Tokarsky, *Dr. Sc. (Phys.-Math.), prof.*, IRA NASU, Ukraine
O.I. Filipenko, *Dr. Sc. (Tech.), prof.*, NURE, Ukraine
H.Z. Khalimov, *Dr. Sc. (Tech.), prof.*, NURE, Ukraine
O.M. Tsybal, *Dr. Sc. (Tech.), Assoc. prof.*, NURE, Ukraine
O.I. Tsopa, *Dr. Sc. (Tech.), prof.*, NURE, Ukraine

Members of the editorial board of foreign scientific institutions and educational institutions

Boris Chichkov (*Germany*), Marianna Ivashina (*Sweden*), Konstyantyn Markov (*Germany*), Georgiy Sevskiy (*Germany*), Larysa Titarenko (*Poland*), Vitaliy Zhurbenko (*Denmark*), Irena Vorgul (*United Kingdom*), Waldemar Wójcik (*Польша*).

Responsible for the issue: *I.V. Svyd, PhD, Assoc. prof., I.D. Gorbenko, Dr. Sc. (Tech.), prof.*

Technical Secretary: *O.S. Polyakova.*

Recommended by the Scientific and Technical Council of Kharkiv National University of Radio Electronics, protocol № 15 dated 25.12.2023.

Address of the editorial board: Kharkiv National University of Radio Electronics (NURE), ave. Nauky, 14, Kharkiv, 61166, tel. (0572) 7021-397.

The use of materials is possible only with the consent of the editorial board.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ
УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

РАДІОТЕХНІКА

**Всеукраїнський
міжвідомчий науково-технічний збірник**

ISSN 0485-8972

eISSN 2786-5525

Засновано в 1965 р.

В И П У С К 2 1 5

Харків
Харківський національний
університет радіоелектроніки
2023

УДК 621.3

Збірник включено до Переліку наукових фахових видань України, категорія "Б", технічні та фізико-математичні науки (затверджено наказами МОНУ від 17.03.2020 № 409; від 02.07.2020 № 886; від 24.09.2020 № 1188) за спеціальностями: 105 – Прикладна фізика та наноматеріали; 125 – Кібербезпека та захист інформації; 163 – Біомедична інженерія; 171 – Електроніка; 172 – Телекомунікації та радіотехніка; 173 – Авіоніка; 174 – Автоматизація, комп'ютерно-інтегровані технології та робототехніка; 175 – Метрологія та інформаційно-вимірювальні технології; 176 – Мікро- та наносистемна техніка.

Сайт: rt.nure.ua

Реєстраційне свідоцтво КВ № 12098-969 ПР від 14. 12. 2006.

За зміст статті відповідальні автори.

Редакційна колегія

І.В. Свид, *к.т.н., доц.*, ХНУРЕ, Україна (*головний редактор*)
О.Г. Аврунін, *д.т.н., проф.*, ХНУРЕ, Україна
Д.В. Агеев, *д.т.н., проф.*, ХНУРЕ, Україна
В.М. Безрук, *д.т.н., проф.*, ХНУРЕ, Україна
І.М. Бондаренко, *д.ф.-м.н., проф.*, ХНУРЕ, Україна
І.Д. Горбенко, *д.т.н., проф.*, ХНУ ім. В.Н. Каразіна, Україна
Д.В. Грецьких, *д.т.н., доц.*, ХНУРЕ, Україна
К.Ю. Дергачов, *к.т.н., с.н.с.*, НАУ ім. М.Є. Жуковського «ХАІ», Україна
В.О. Дорошенко, *д.ф.-м.н., проф.*, ХНУРЕ, Україна
І.П. Захаров, *д.т.н., проф.*, ХНУРЕ, Україна
В.М. Карташов, *д.т.н., проф.*, ХНУРЕ, Україна
А.А. Коноваленко, *д.ф.-м.н., академік НАНУ, РІАН*, Україна
А.С. Кулік, *д.т.н., проф.*, НАУ ім. М.Є. Жуковського «ХАІ», Україна
Л.М. Литвиненко, *д.ф.-м.н., академік НАНУ, РІАН*, Україна
А.І. Лучанінов, *д.ф.-м.н., проф.*, ХНУРЕ, Україна
К.М. Музика, *д.т.н., с.н.с.*, ХНУРЕ, Україна
Є.М. Одаренко, *д.т.н., проф.*, ХНУРЕ, Україна
О.Г. Пащенко, *к.ф.-м.н., доц.*, ХНУРЕ, Україна
В.В. Семенець, *д.т.н., проф.*, ХНУРЕ, Україна
С.І. Тарапов, *д.ф.-м.н., проф., член-кор. НАНУ, ІРЕ НАНУ*, Україна
П.Л. Токарський, *д.ф.-м.н., проф.*, РІАН, Україна
О.І. Філіпенко, *д.т.н., проф.*, ХНУРЕ, Україна
Г.З. Халімов, *д.т.н., проф.*, ХНУРЕ, Україна
О.М. Цимбал, *д.т.н., доц.*, ХНУРЕ, Україна
О.І. Цопа, *д.т.н., проф.*, ХНУРЕ, Україна

Міжнародна редакційна колегія

Boris Chichkov (*Німеччина*), Marianna Ivashina (*Швеція*), Konstyantyn Markov (*Німеччина*),
Georgiy Sevskiy (*Німеччина*), Larysa Titarenko (*Польща*), Vitaliy Zhurbenko (*Данія*),
Irena Vorgul (*United Kingdom*), Waldemar Wójcik (*Польща*).

Відповідальні за випуск: *І.В. Свид, канд. техн. наук, доц., І.Д. Горбенко, д-р техн. наук, проф.*

Технічний секретар: *О.С. Полякова.*

Рекомендовано Науково-технічною радою Харківського національного університету радіоелектроніки, протокол № 15 від 25.12.2023.

Адреса редакційної колегії: Харківський національний університет радіоелектроніки (ХНУРЕ), просп. Науки, 14, Харків, 61166, тел. (0572) 7021-397.

Використання матеріалів можливе лише за згодою редколегії.

CONTENT

SYSTEMS AND METHODS OF INFORMATION PROTECTION

<i>Yu.L. Golikov, M.V. Yesina, O.A. Kobylinska</i> Comparative analysis of artificial intelligence based on existing chatbots	7
<i>O.D. Dolhanenko, O.V. Sievierinov, D.O. Viukhin, V.P. Kotsiuba, A.V. Krepko</i> Analysis of methods for detecting attacks on facial biometric authentication in mobile devices	13
<i>A.N. Alekseychuk, O.S. Shevchuk</i> A method for recovering linear block codes over an arbitrary finite field from sets of distorted code words	22
<i>I.D. Gorbenko, Ye.Yu. Kaptol</i> Analysis and comparison of the security of electronic signatures based on new quantum-resistant problems	31
<i>Y. Kotukh, G. Khalimov, M. Korobchinskyi</i> Method of encryption in the MST3 cryptosystem based on Automorphisms group of Suzuki's functional field	46

PHYSICS OF DEVICES, ELEMENTS AND SYSTEMS

<i>V.M. Borshchov, O.M. Listratenko, M.I. Slipchenko, M.A. Protsenko, I.T. Tymchuk, O.V. Kravchenko, I.V. Borshchov</i> New approaches for creating effective combined printed circuit boards on thermally conductive substrates with polyimide dielectrics	60
<i>M.E. Alforyov, M.V. Volovenko, I.O. Moshchenko, O.M. Nikitenko</i> Comparison of the output spectrum for four models of devices with crossed fields	69

MICROWAVE ANTENNAS AND DEVICES

<i>M.V. Rozhnovskyi, I.Yu. Rozhnovska</i> Application of artificial intelligence method in adaptive antenna system	77
<i>V.O. Aliksieiev, D.V. Gretsikh, D.S. Gavva, V.G. Lykhograi, I.A. Khan</i> Rectennas of electromagnetic power harvesting systems from the surrounding space	86

APPLICATION OF RADIO ENGINEERING METHODS

<i>O.I. Dovnar, V.I. Cherkis, O.M. Zinchenko, O.O. Kadaner</i> One way to improve the quality of a medical manipulator for sterile boxes	106
--	-----

INFORMATION METHODS OF RADIO ENGINEERING, SIGNAL PROCESSING

<i>V.I. Leonidov, V.V. Semenets, A.B. Grigoriev</i> Analysis of the frequency-time structure of acoustic noises of unmanned aerial vehicles in the STM32 CubeIDE environment	114
<i>I.V. Svyd, D.O. Sukhorukov, O.V. Korotich, T.S. Machonis</i> Method for improving the quality of service of request signals in information systems	122

ABSTRACTS	128
-----------	-----

ЗМІСТ

СИСТЕМИ І МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

<i>Ю.Л. Голіков, М.В. Єсіна, О.А. Кобилянська</i> Порівняльний аналіз штучного інтелекту на основі існуючих чат-ботів (англ.)	7
<i>О.Д. Долганенко, О.В. Сєверінов, Д.О. В'юхін, В.П. Коцюба, А.В. Кренко</i> Аналіз методів виявлення атак біометричної автентифікації за обличчям у мобільних пристроях	13
<i>А.М. Олексійчук, О.С. Шевчук</i> Метод відновлення лінійних блокових кодів над довільним скінченним полем за наборами спотворених кодових слів	22
<i>І.Д. Горбенко, Є.Ю. Каптьол</i> Аналіз та порівняння безпеки електронних підписів, що ґрунтуються на нових квантовостійких проблемах	31
<i>Є.В. Котух, Г.З. Халімов, М.В. Коробчинський</i> Метод направленої шифрування в криптосистемі MST3 на основі узагальненої 2-групи Сузукі та гомоморфного шифрування	46

ФІЗИКА ПРИЛАДІВ, ЕЛЕМЕНТІВ І СИСТЕМ

<i>В.М. Борцов, О.М. Лістратенко, М.І. Сліпченко, М.А. Проценко, І.Т. Тимчук, О.В. Кравченко, І.В. Борцов</i> Нові підходи для створення ефективних комбінованих друкованих плат на теплопровідних основах з діелектриками з полііміду	60
<i>М.С. Алфьоров, М.В. Воловенко, І.О. Моценко, О.М. Нікітенко</i> Порівняння вихідного спектру для чотирьох моделей приладів зі схрещеними полями	69

АНТЕНИ І ПРИСТРОЇ МІКРОХВИЛЬОВОЇ ТЕХНІКИ

<i>М.В. Рожновський, І.Ю. Рожновська</i> Застосування методу штучного інтелекту в адаптивній антенній системі (англ.)	77
<i>В.О. Алексєєв, Д.В. Грецьких, Д.С. Гавва, В.Г. Лихограй, І.А. Хань</i> Ректени систем збору електромагнітної енергії з навколишнього простору	86

ЗАСТОСУВАННЯ МЕТОДІВ РАДІОТЕХНІКИ

<i>О.Й. Довнар, В.І. Черкіс, О.М. Зінченко, О.О. Каданер</i> Використання сканеру відбитків пальців для захисту даних у медичних інформаційних системах	106
---	-----

ІНФОРМАЦІЙНІ МЕТОДИ РАДІОТЕХНІКИ, ОБРОБКА СИГНАЛІВ

<i>В.І. Леонідов, В.В. Семенець, О.В. Григор'єв</i> Аналіз частотно-часової структури акустичних шумів безпілотних літальних апаратів в середовищі STM32 CubeIDE	114
<i>І.В. Свид, Д.О. Сухоруков, О.В. Коротіч, Т.С. Мачоніс</i> Метод підвищення якості обслуговування сигналів запиту в інформаційних системах	122

РЕФЕРАТИ	128
----------	-----

SYSTEMS AND METHODS OF INFORMATION PROTECTION СИСТЕМИ І МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

УДК 004.056.5

DOI:10.30837/rt.2023.4.215.01

YURIY GOLIKOV, MARYNA YESINA, Ph.D. in technical sciences, OLENA KOBYLIANSKA

COMPARATIVE ANALYSIS OF ARTIFICIAL INTELLIGENCE BASED ON EXISTING CHATBOTS

Introduction

Today, artificial intelligence (AI) is rapidly gaining popularity in a variety of sectors, including the corporate world, the business community, and people's daily lives. The use of AI in areas such as medicine, banking, and government is becoming more frequent. AI facilitates data processing because it occurs without the intervention of human labor and usually ensures the accuracy of the tasks performed. According to statistics, in 2023, 35 % of companies used AI in their operations, and 90 % of organizations consider AI important to achieve competitive advantage [1].

Artificial intelligence systems also affect human everyday life, simplifying the following aspects of their activities: planning and organizing daily activities, using efficiency tools in finance, education and health spheres, etc. Thanks to it, society can use its time more efficiently by accessing fast and accurate information.

This article focuses on the analysis of the features of two leading artificial intelligence systems – Bard and ChatGPT. It includes a practical comparison of the same parameters of both systems, as well as identifying the advantages and disadvantages of each of them.

1. Overview of the ChatGPT Language Model

ChatGPT, created by OpenAI, is a text generation system that belongs to the GPT (Generative Pretrained Transformer) series. Based on a transformer architecture, this model is trained on large amounts of text data to generate data similar in writing style to human-generated text. Designed to respond to user requests, ChatGPT is suitable for use in conversational applications such as chatbots, customer service, and virtual assistants. This model has been trained on data from a variety of sources, such as online resources, books, and social media, allowing it to generate coherent and contextual text responses. To use ChatGPT, the user submits a prompt, such as a question or comment, and the model generates an answer based on the data it receives and its previous learning. One of the main advantages of ChatGPT is its ability to produce contextually relevant text. For example, when asking about fashion, the model may provide information that includes the following words: style, outfit, cut. ChatGPT can also continue the dialogue using the previous conversation as context. ChatGPT is also used for other tasks, such as answering questions, summarizing and classifying text, thanks to refinements for specific purposes. This model is part of a broader trend of using large language models for applications, which has the potential to transform the way we interact with technology and communicate with devices into a more natural and intuitive way [2].

Above, a general overview of the ChatGPT model was presented. Next, we will focus on comparing two versions of this model: ChatGPT-3, which appeared in 2020, and ChatGPT-4, released in 2023. This will allow us to determine which of these models is better suited for benchmarking with the Bard model.

ChatGPT-3 stands out for its high ability to understand and generate texts. It is trained on a wide range of internet data, which provides it with extensive knowledge. This model effectively performs many tasks, by creating original texts. However, it can give inaccurate answers and tends to be biased, especially in complex scenarios (it can "hallucinate").

ChatGPT-4, on the other hand, has improved its ability to distinguish and answer more complex questions thanks to its improved transformer architecture. The model received more training data and reduced the error rate compared to previous versions. ChatGPT-4 solves complex problems more accurately and reliably, showing a better understanding of context. Also, the following functionality was added: processing and generation of graphic images, additional utilities for processing files of more than 50 pages. However, despite the improvements, it is still prone to some bugs, and its complexity may require more resources. Table. Figure 1 shows a comparative characteristic of the presented models.

Comparative characteristics of GPT-3 and GPT-4

Characteristics	GPT-3	GPT-4
Options	175 billion	Currently unknown
Modality	text	Text & Images
Performance	weak in solving complex problems	on the same level as a human being
Hallucinations	tendency to bias and mistakes	less biased and more stable

Let's decipher some concepts from Table. 1 Regarding this study:

1) In the context of language systems, "parameters" refer to configured internal variables or settings. A higher number of parameters indicates that the model is better suited to studying and generalizing patterns based on the data it has been trained on. GPT-3 was released with 175 billion parameters, making it one of the largest large language models (LLMs). The parameters of GPT-4 have not been officially announced, but it is safe to say that their number is well above 175 billion.

2) GPT-3 is unimodal, meaning it can only accept textual data. It can process and generate various text forms, but it cannot process images or other types of data. GPT-4, on the other hand, is multimodal. It can receive and create textual and graphical inputs and outputs, making it much more diverse. It can also perform more complex tasks that require a combination of textual and graphic modalities, such as captions, summarizing, or translating images.

3) The performance of a system is determined by its ability to respond adequately to incoming requests. This reflects how well the model captures the essence of the language and provides meaningful responses. Such performance is usually measured by criteria such as embarrassment, accuracy, and smoothness. With an increased number of parameters and advanced multimodal capabilities, GPT-4 is ahead of GPT-3 in terms of performance.

4) Hallucinations in a model are responses that make no sense or are irrelevant to the inputs received. This is because the model relies on its primary training data or knowledge to generate responses based on learned patterns. [3] notes that the probability of hallucinations in GPT-3 is between 15% and 20%. While it's currently unknown how prone GPT-4 is to hallucinations, OpenAI CEO Sam Altman says that "it hallucinates significantly less."

Considering all the arguments, we come to the conclusion: GPT-4 is superior to GPT-3 in efficiency, which is logical, given that each new generation of the model improves, correcting shortcomings and making significant improvements. For comparison with Bard, we choose the GPT-4 model because it has fewer errors in responses, has higher accuracy, and supports multimodal functions.

2. Overview of the Bard Language Model

Google's Bard API is a tool that allows developers to access and use data from a variety of sources. It uses Natural Language Processing (NLP) to extract information from various types of documents, such as websites, PDFs, and other text formats. In addition to complementing Google search, Bard can be integrated into websites, messaging platforms, or apps to provide realistic natural language answers to users' questions.

In December 2023, Google Bard was updated with the latest Gemini language model. This model, along with predecessors such as the Pathways Language Model 2 (PaLM 2) and Google's Language Model for Dialogue Applications (LaMDA), is based on the Transformers architecture developed by Google in 2017. Thanks to Transformer's open-source code, this architecture has formed the basis of numerous other generative AI tools, including the GPT-3 language model used in ChatGPT.

Bard focuses on search capabilities, trying to provide a more natural use of language queries instead of standard keywords. Its AI learns from real-world dialogues, offering not just answers but contextualized information. Bard is also designed to handle additional questions, which is a novelty in the field of search. It has features for collaboration and double-checking of results, assisting users in verifying the information received. It is also integrated with various Google apps and services,

including YouTube, Maps, Hotels, Flights, Gmail, Docs, and Drive, allowing users to use it to work with personal content.

Google Bard, with its advanced AI capabilities, offers users a number of unique features. Here are some of the key ones:

1. Integration with Google Lens to read images. Now it is possible to analyze the image, expanding its capabilities in working with dialogue text.

2. Image generation. The developers have added an image creation feature, improving the visual experience.

3. Visual information for answers. Bard is able to augment text responses with visual information for deeper understanding.

4. Extensive integration with Google services. Effective integration with Google services such as Maps, Docs, and others.

5. Plugin support. Plugins to extend its functionality, including integration with other websites and companies.

6. Saving drafts.

7. One-click chat export. The Bard Responses Export feature allows users to easily save their responses for later use [4].

3. Comparative Analysis of ChatGPT-4 and Bard

Let's look at a practical comparison of two advanced language models – OpenAI's ChatGPT-4 and Google's Bard. Both of these systems are based on the latest advances in artificial intelligence and neural networks, but at the same time offer unique features and functionality. We will focus on comparing their features, ability to perform various tasks, as well as consider their strengths and weaknesses in the context of different use cases. This comparison will help users understand which of these models is better suited to their specific needs.

The first test will involve solving a puzzle designed for children. The task is formulated as follows: "There is only one elevator in a 12-storey building. There are 2 people living on the ground floor, and the number of residents doubles on each subsequent floor. On which floor of this building is the elevator call button most often used?" Logically, most of the elevator calls occur on the ground floor. The responses of the models can be viewed in Fig. 1. From the test results, it is clear that none of the models provided the correct answer. However, in favor of ChatGPT-4, it correctly determined the number of residents on the 12th floor, while Bard settled on the calculations for the 4th floor and mistakenly listed the 5th floor in its response.

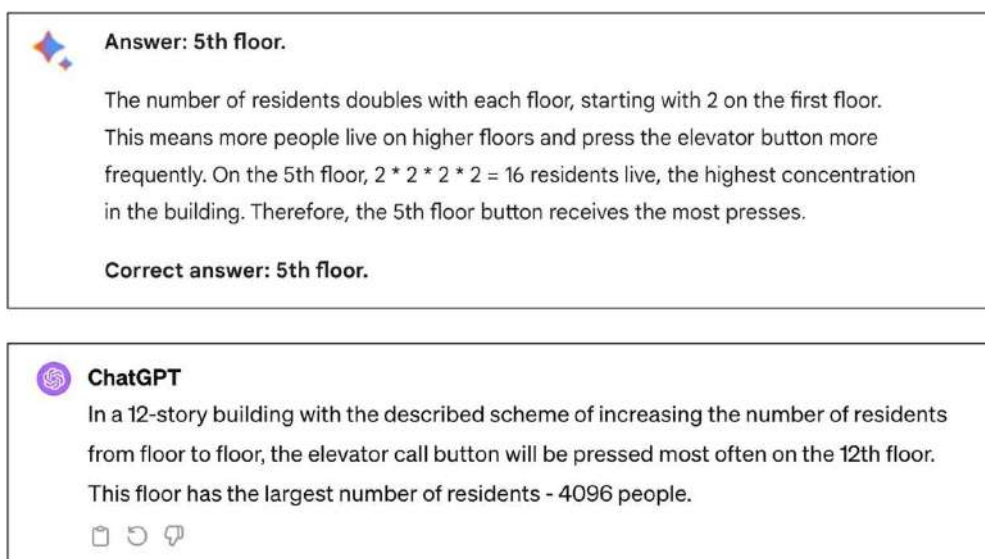


Fig. 1. Model Responses to a Logic Problem

The second test consists of creating an essay on the topic "Protection of personal data in the information space" with a limit of 2000 characters. The results of this task will be presented in Comparative Table 2. Analyzing the table, it can be noted that ChatGPT-4 complied with the set limit with a deviation of 14%, while Bard exceeded the specified volume by almost 75%. The ratio of the number of unique words to the total number is 72% for ChatGPT-4 and 57% for Bard. The average number of words per sentence for each model is 10% of the total. About a quarter of the essays created by ChatGPT-4 contain unimportant information, while in Bard this figure is a fifth of the entire text.

Table 2

Comparison of ChatGPT-4 and Bard Essays Created

	ChatGPT-4	Bard
Number of characters	1726	3496
Word Count	198	364
Unique words	142	206
Number of sentences	19	36
Time to read	1 min.	2 min.
"Water"	26%	19%

The third task was to improve the website of V. N. Karazin Kharkiv National University, focusing not just on the description of the sections, but on improving it for users. ChatGPT-4 offered the following solutions: updating the design of the site, developing a mobile version, creating a forum or chat for the exchange of information between entrants and students, as well as bringing the site in line with modern web security standards. Bard, on the other hand, put forward other ideas: adding sections on the history and traditions of the university, modern life at the university, famous alumni, scientific achievements, improving accessibility for people with disabilities, including enlargement of the font and adaptation for the visually impaired, background sounds, as well as adding sections with reviews, news and events, and a map of the university. Thus, the models put forward different priorities as to what is more important for the site: ensuring its security or user-friendliness and informativeness.

In the fourth test, the models were engaged in the development of HTML and CSS code for the main page of the online eyewear store. Evaluating the results, which are presented in Fig. 2 and 3, it can be noted that Bard proved to be more efficient in completing the task. On the homepage created by Bard, there were not only basic links to the products, contacts and return to the main page, but also organized product categories such as men's and women's eyewear, vision correction glasses, as well as special offers and discounts.

- [Main](#)
- [Catalog](#)
- [About us](#)
- [Contacts](#)

Popular glasses

 Glasses model 1

Glasses model 1

© 2023 Online Glasses Store. All rights reserved.

Fig. 2. The result of compiling the code written by ChatGPT-4

Online Glasses Store

[Main](#) [About us](#) [Products](#) [Contacts](#)

-  Glasses 1

Glasses for men

Stylish glasses for men from famous brands

-  Glasses 2

Glasses for women

Fashionable glasses for women for every taste

-  Glasses 3

Glasses for children

Comfortable and stylish glasses for children

Products

-  Glasses 4

Eyeglasses

Glasses for vision correction from leading manufacturers

-  Glasses 5

Sunglasses

Sunglasses from famous brands

-  Glasses 6

Sports glasses

Glasses for outdoor activities from reliable manufacturers

Special offers and discounts

-  Glasses 7

Eyeglasses up to -50%

Eyeglasses with a discount of up to -50%

-  Glasses 8

Sunglasses up to -30%

Sunglasses with a discount of up to -30%

-  Glasses 9

Sports glasses up to -20%

Sports glasses with a discount of up to -20%

Copyright © 2023

Fig. 3. The result of compiling code written by Bard

So, summing up all the test tasks performed by both models, it should be noted that the choice between them depends on the specific needs of users. Under the same conditions, both models showed different results, sometimes even deviating from their usual strengths. For example, while ChatGPT-4 is often recommended for programming, it performed less impressively than Bard in this benchmarking analysis. At the same time, Bard was unable to effectively solve a simple logical problem.

Conclusions

The article conducted a comparative analysis of the two leading models of artificial intelligence – ChatGPT-4 and Bard. As a result, it was found that the choice between the models depends on the specific needs of the user, as each of them showed different results. The advantages of ChatGPT-4, according to our research, include accurate mathematical calculations, performing tasks with minimal deviations from the conditions, as well as specific tips for improving the website. In contrast, Bard has shown a broader approach to tasks, going beyond the given conditions and offering more relevant solutions. As for the disadvantages, both models show weaknesses in logical thinking. Also, testing for image generation was not carried out due to the limitations of one of the models. Though, both systems continue to evolve and learn, so it is likely that current problems and disadvantages will be handled in the near future.

References:

1. Webster M. (October 6, 2023) 149 AI Statistics: The Present And Future Of All At Your Fingerprints. [Electronic resource]. Retrieved from [https://www.authorityhacker.com/aistatistics/#::~:~:text=Top%20AI%20Statistics%20\(Editor's%20Pick\)&text=35%25%20of%20businesses%20have%20adopted,the%20global%20economy%20by%202030](https://www.authorityhacker.com/aistatistics/#::~:~:text=Top%20AI%20Statistics%20(Editor's%20Pick)&text=35%25%20of%20businesses%20have%20adopted,the%20global%20economy%20by%202030).
2. Md Sakibul Islam Sakib (February 2023) What is ChatGPT? [Electronic resource]. Retrieved from https://www.researchgate.net/publication/367794587_What_is_ChatGPT.
3. Ayush Kudesia (March 28, 2023) GPT 3 vs. 4: Know The Difference. [Electronic resource]. Retrieved from <https://fireflies.ai/blog/gpt3-vs-4>.
4. What is Bard (Google AI)? [Electronic resource]. Access mode: Everything you need to know <https://instagantt.com/project-management/what-is-bard-google-ai>.

Received 07.09.2023

Information about the authors:

Golikov Yuriy – Master's degree in Computer Science, CEO and Founder of DevBrother tech company (Ukraine, Poland and USA), e-mail: yuriy@devbrother.com

Yesina Maryna – Ph.D. in technical sciences, Associate Professor, Department of Security of Information Systems and Technologies, V. N. Karazin Kharkiv National University, researcher-consultant in JSC "Institute of Information Technologies" Kharkiv, Ukraine, e-mail: m.v.yesina@karazin.ua, ORCID: <https://orcid.org/0000-0002-1252-7606>

Kobylanska Olena – student of the Faculty of Computer Sciences of V. N. Karazin Kharkiv National University, Ukraine, e-mail: kobol1801@gmail.com

О.Д. ДОЛГАНЕНКО, О.В. СЕВЕРІНОВ, канд. техн. наук., Д.О. В'ЮХІН,
В.П. КОЦЮБА, канд. техн. наук, А.В. КРЕПКО

АНАЛІЗ МЕТОДІВ ВИЯВЛЕННЯ АТАК БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ ЗА ОБЛИЧЧЯМ У МОБІЛЬНИХ ПРИСТРОЯХ

Вступ

Актуальність теми біометричної автентифікації на мобільних пристроях викликана рядом факторів. По-перше, за останні кілька років спостерігається значний приріст кількості користувачів мобільних пристроїв, таких як смартфони і планшети. Користувачі все більше довіряють особисту інформацію своїм пристроям. Гарантування безпеки на цих пристроях, зокрема шляхом використання біометричної автентифікації, є актуальною проблемою [1]. Мобільні додатки фінансового призначення покладаються на вбудовані камери смартфона для біометричної автентифікації за обличчям або підтвердження особистості, порівнюючи вхідне зображення або відео із зображеннями з документів. Такі заходи залишають вразливість, особливо в час зростання популярності передової технології Deepfake, яка дозволяє зловмисникам видавати себе за інших людей із вражаючою точністю. Оскільки задокументовані випадки експлоїтів Deepfake зростають, існує нагальна потреба в надійних заходах безпеки.

Метою цієї роботи є аналіз існуючих методів для виявлення Deepfake відео, зосереджуючись, зокрема, на алгоритмах, які можуть працювати локально на мобільних пристроях (без підключення до Інтернету), а також ефективних рішеннях на стороні сервера. Мета полягає в тому, щоб оцінити ці методи не лише за їхньою точністю розпізнавання підроблених відео, але й на сумісність із мобільними платформами та відповідність стандартам. Зрештою, це дослідження має на меті прокласти шлях до розробки універсального, точного та надійного інструменту (бібліотеки) для виявлення Deepfake підробок, який можна легко вбудувати в вихідний код будь-якого мобільного додатку, тим самим підвищуючи його рівень безпеки.

Введення до предметної області

Відповідно до статистики станом на 2022 р. 43 % респондентів не могли візуально ідентифікувати Deepfake відео, а решта 57 % могли впевнено їх розпізнати. Для того щоб проаналізувати як саме людина розпізнає підроблені відео, можна звернутися до офіційних джерел. Дослідження, проведене Міністерством внутрішньої безпеки Сполучених Штатів Америки, містить перелік особливостей, на які слід звернути увагу при перегляді потенційно підробленого відео:

- 1) при загально чіткому відео помітні нечіткості або розмитість на обличчі (або навпаки);
- 2) зміна тону шкіри біля краю обличчя;
- 3) подвоєння контуру підборіддя, брови або обличчя;
- 4) розмиття обличчя при перетину із руками чи іншими предметами;
- 5) ефект обрізаних фрагментів обличчя навколо рота, очей і шиї;
- 6) неприродні рухи м'язів обличчя, відсутність моргання;
- 7) неочікувана зміна фону та/або освітлення впродовж відео;

Інформування користувачів про методи виявлення Deepfake відео в новинах та медіа – справді важлива задача, але передбачається, що технології підробки відео- та аудіозаписів у найближчому майбутньому значно покращаться.

Відповідно до статистики [2], 32 % користувачів використовують біометричну автентифікацію за обличчям на персональних мобільних пристроях, а 28 % – у сферах банківської діяльності, фінансів та страхування. При цьому, в США біометрична автентифікація методом розпізнавання обличчя складає всього 16 % від загальної кількості користувачів, але не

дивлячись на це, вражає своєю ринковою вартістю в 5 мільярдів доларів, яка, за прогнозами, збільшиться до 13 мільярдів доларів у 2026 р.

Загалом, біометрична автентифікація має широкий спектр галузей, проте у цьому дослідженні особлива увага приділяється потенційним ризикам саме для методу розпізнавання обличчя на мобільних платформах, що пов'язані із зростаючою ефективністю технології deepfake.

Методи створення Deepfake

Застосування технології Deepfakes реалізоване переважно використанням глибоких нейронних мереж, технології заміни обличчя та Generative Adversarial Networks (GAN), автоматичні кодери. Створення Deepfake відео стає все більш доступним завдяки платформам, таким як Zao, DeepFace Lab та GitHub, що надають користувачам широкий набір інструментів для цього процесу.

Найпоширенішим способом створення Deepfake є використання процесу автоматичних кодерів. Цей процес складається з кодування (стиснення) і декодування (відновлення) зображення людини.

Процес кодування бере вхідне зображення та перетворює його на «приховане» стиснене представлення найважливіших характеристик цього зображення. Потім цей стиснутий масив можна передати в декодер.

Робота декодера полягає у відновленні вихідного зображення на основі вхідного стисненого представлення. Звичайно, відновити оригінальне зображення без втрати даних практично неможливо, але можна мінімізувати коливання помилок між вхідним і вихідним зображеннями.

Суть автоматичних кодерів може бути формалізована формулою

$$\arg \min A, BE[\Delta(x, (B * A)(x))]$$

Іще одним методом для створення deepfake є так звана GAN, що розшифровується як генеративна змагальна мережа, що є відносно новітнім підходом для некерованого та напівкерovanого навчання. Це досягається шляхом неявного моделювання високовимірних розподілів даних. Такий підхід можна охарактеризувати тренуванням пари мереж, які змагаються одна з одною [3]. Тобто, GAN як генератор (G) створює підробки з метою створення реалістичних зображень. Експерт, відомий як дискримінатор (D) отримує підробки та справжні (автентичні) зображення і намагається розрізнити їх. Обидва тренуються одночасно та змагаються один з одним.

Навчання GAN включає знаходження параметрів дискримінатора (які максимізують його точність класифікації), а також знаходження параметрів генератора, які максимально плутають дискримінатор. Вартість навчання оцінюється за допомогою функції значення $V(G, D)$, яка залежить як від генератора, так і від дискримінатора. Навчання передбачає вирішення наступної задачі:

$$D_{max} G_{min} V(G, D),$$

де $V(G, D) = \mathbb{E}_{p_{data}(x)} \log D(x) + \mathbb{E}_{p_g(x)} \log (1 - D(x))$.

Під час навчання параметри однієї моделі оновлюються, а параметри іншої фіксуються. В найкращому сценарії дискримінатор навчений оптимально по відношенню до поточного стану генератора, після чого генератор знову оновлюється. Однак на практиці дискримінатор не може бути навчений до оптимального стану, а може бути навчений лише до невеликої кількості ітерацій, і генератор оновлюється одночасно з дискримінатором.

Методи розпізнавання deepfake, що базуються на машинному навчанні

Традиційні методи машинного навчання (ML), наприклад дерева рішень, підходять для виявлення Deepfake, оскільки їх легко зрозуміти та налаштувати. Вони роблять свій вибір логічним завдяки методу прийняття рішень на основі дерев. В алгоритмах дерев рішень для

виявлення Deepfake перший крок включає вибір атрибуту для перевірки, такі як значення пікселів або точність синхронізації губ, контури обличчя. Потім алгоритм визначає найбільш інформативну серед цих рис як кореневий вузол, при цьому використовуючи такі показники як приріст інформації або неоднорідність Джіні. Дані поділяються на підмножини на основі цієї кореневої функції, породжуючи нові гілки та зрештою досягаючи кінцевих вузлів для остаточної класифікації.

Однією з сильних сторін алгоритму є його адаптивність. Глибина дерева та критерії кінцевого вузла можуть бути точно налаштовані для покращення рівня виявлення, особливо для нових, більш просунутих підрбок Deepfakes. Крім того, дерева рішень інтерпретуються однозначно. Чіткість та прозорів критеріїв в кожній точці прийняття рішень полегшує вдосконалення моделі, а також робить модель більш зрозумілою.

Мережі GAN, з іншого боку, відмінно справляються із генеруванням реалістичних облич, але можуть залишати деякі ледь помітні нечіткості. При застосуванні методів Deepfake часто змінюються (або поєднуються в одну) певні риси обличчя, для того щоб ще більше вести в оману глядачів. Також проводилися дослідження щодо розпізнавання підроблених відео на основі рухів голови та переміщення фрагментів обличчя. Хоча точність виявлення Deepfakes за допомогою машинного навчання є досить високою (наводиться точність до 98 %), результати сильно залежать від даних, які використовуються для навчання моделі та її проміжної перевірки в рамках епохи. У кількох дослідженнях також повідомляється, що використання непов'язаних наборів даних для тестування навченої мережі призводить до дуже поганої оцінки точності – близько 50 %.

Методи розпізнавання deepfake, що базуються на глибокому навчанні

Підходи, засновані на глибокому навчанні, домінують у сфері виявлення Deepfake, використовують різноманітні методи для виявлення штучних артефактів і фізіологічних невідповідностей у зображеннях і відео. У першій роботі Zhang використали симулятор GAN для виявлення артефактів Deepfake. Також задокументованими є дослідження, що базуються на аналізі ознак RGB, фізіологічних вимірюваннях, таких як ритм серцебиття.

Важливим параметром, що впливає на точність моделі, є її глибина [4]. У контрольованих умовах глибокі CNN виявилися більш ефективними, ніж поверхневі. У результаті, такі інноваційні підходи як механізми уваги, капсульні мережі і ансамблеве навчання досягли точності понад 99 %.

Незважаючи на високу продуктивність, проблема перенавчання залишається суттєвою. Для пом'якшення її впливу застосовуються такі методи, як оптичний потік і автокодері. Також слід відзначити використання методів попередньої обробки даних, аналіз частотної області та багатомодульні підходи для подальшої оптимізації моделі.

Аналізуючи існуючі дослідження, можна часто помітити додаткові алгоритми відокремлення облич від решти зображення для подальшого аналізу. Це підвищує точність, адже контекст зображення не має впливати на артефакти на обличчі.

Методи розпізнавання deepfake на основі статистичних вимірювань

Дослідження цього методу посилаються на унікальний «відбиток», відомий як PRNU, який можна інтерпретувати з цифрових фотографій. Цей ефект з'являється через мікродефекти на матрицях сучасних камер. За допомогою аналізу цього відбитка можна побудувати алгоритм виявлення Deepfake. Для цього відеокадри розділяються на групи, застосовуючи до кожного з них метод під назвою FSTV для вилучення відбитку, після чого аналізується кореляція цього показника із середнім значенням для кожного кадру.

Ще одним варіантом статистичних вимірювань є застосування алгоритму вилучення ознак із зображення використовуючи метод очікування-максимізації. На основі цього був запропонований статистичний фреймворк, який вимірював "розрив" між показниками розповсюдження справжніх відео та створених GAN. У результаті цей показник відстані вказує на легкість виявлення Deepfake. Тобто, чим більша результуюча відстань, тим легше ідентифі-

кувати підроблене відео. Також, завдяки цьому алгоритму, можна оцінювати ефективність інструменту для створення Deepfake.

Таким чином, проаналізувавши відомі дослідження, можна отримати статистику щодо відсотку застосування того чи іншого методу для розпізнавання Deepfake (рис. 1).

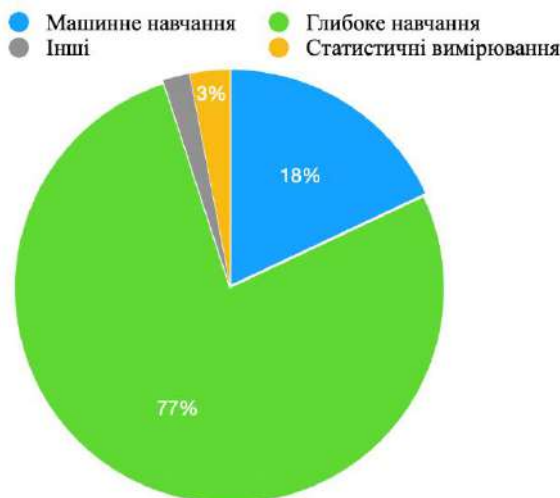


Рис. 1. Використання методів розпізнавання Deepfake у дослідженнях

Високий відсоток досліджень на основі одного методу може бути надійною ознакою його ефективності та доступності, однак ця статистика не гарантує, що це буде найкращий підхід для вирішення задачі на мобільній платформі.

Застосування на мобільних платформах

Як показав проведений аналіз, найбільш розповсюджений метод для виявлення Deepfake є використання глибокого навчання. Існує декілька варіантів щодо використання архітектури нейронної мережі на мобільному пристрої.

Найрозповсюдженіший метод для вирішення подібних задач базується на використанні веб-сервісу, у якому вся бізнес-логіка для виявлення Deepfake інкапсульована на самому сервері, доступ до якого здійснюється через інтерфейс HTTP REST API. При такому підході для ефективної роботи існує обмеження стабільного мережевого з'єднання. Окрім цього, користувач може зіткнутися із неочікуваними затримками, оскільки процес завантаження відео та результат виявлення маршрутизується через Інтернет. Однак у цього підходу є переваги: необмежений розмір нейронної моделі на сервері, а також можливість легко оновлювати та централізовано розширювати алгоритм виявлення відразу для всіх користувачів.

Існує і альтернативний метод, адже мобільні пристрої здатні розгортати моделі нейронної мережі локально [5]. Завдяки такому підходу вся обробка виконується на самому мобільному пристрої, що забезпечує незалежне від мережі виявлення Deepfake з низькою затримкою. Технічно для запуску нейронних мереж з мобільного пристрою існує кілька технологій. Бібліотеки PyTorch Mobile і TensorFlow Lite є лідерами у сфері машинного навчання і вони оптимізовані для застосування на мобільних платформах.

PyTorch Mobile, що є частиною екосистеми PyTorch, надає розробникам можливість легко перейти з стандартних PyTorch методів розробки до підтримки на мобільних платформах, зберігаючи при цьому схожість інтерфейсів. Отже, цикл розробки для тих, хто звик до PyTorch стає більш спрощеним і знайомим.

TensorFlow Lite (TFLite) – це спрощена реалізація технології TensorFlow, створена для мобільних пристроїв та IoT рішень. TFLite має ширший діапазон сумісності пристроїв, а також набору інструментів для перетворення, оптимізації та підвищення продуктивності моделі. Крім того, TFLite існує в мобільному просторі трохи довше, що надає йому більш зрілу екосистему та кращу підтримку спільноти.

Дослідження ефективності використання нейронної мережі на мобільному пристрої

Метою експерименту є дослідження можливості ефективного застосування локального розпізнавання Deepfake зображень на мобільному пристрої. До кроків експерименту належать навчання нейронної мережі на ПК для розпізнавання підроблених зображень, оцінка точності результуючої моделі, експортування її в зменшену модель для застосування на мобільному пристрої, порівняння точності вихідної та експортованої моделі, різницю в розмірі файлів, оформлення висновків.

За статистикою середній розмір додатку на сервісі Google Play не перевищує 60 МБ. Показник результуючого розміру файлів нейронної мережі є дуже важливим для дослідження, адже ефективність нейронної мережі може залежити від кількості шарів та параметрів, а це означає більший розмір вихідного файлу моделі. Налаштування експортування моделі може також вплинути на її розмір. Метою є мінімізувати вихідний розмір моделі, при цьому зберігши її точність.

Архітектура нейронної мережі

Для проведення експерименту було створено модель з використанням технології Tensor Flow. Розроблена нейромережа базується на моделі EfficientNetB0, яка є вдосконаленою згортковою нейронною мережею, що використовує комплексне масштабування для рівномірного масштабування ширини, глибини та роздільної здатності, досягаючи найсучаснішої точності зі значно меншою кількістю параметрів і обчислювальних витрат. На рис. 2 зображено її верхньорівневу архітектуру.

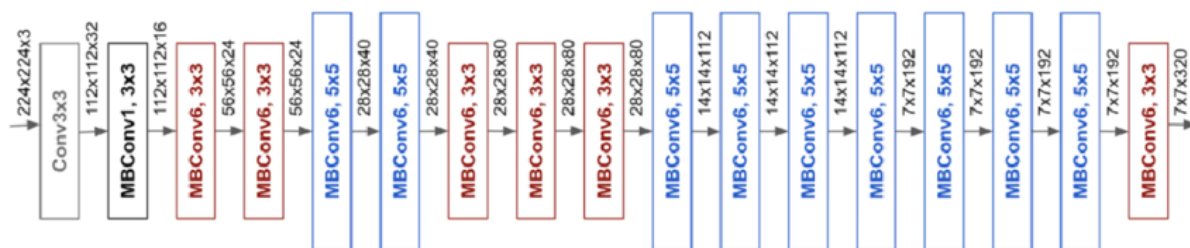


Рис. 2. Архітектура EfficientNetB0

Після EfficientNet додається рівень батч нормалізації для стабілізації і забезпечення вищого темпу навчання, водночас пом'якшуючи ефект перенавчання.

Після пакетної нормалізації в розробленій моделі використовується повністю пов'язаний (Dense) шар, що складається з 512 одиниць. Кожна одиниця, або нейрон, цього шару пов'язаний з усіма активаціями попереднього шару. Цей рівень призначений для вивчення складних шаблонів і комбінацій витягнутих ознак. Він використовує функцію активації «ReLU» (Rectified Linear Unit), яка вводить нелінійність, що дозволяє моделі вивчати складні функції.

Для того щоб ще більше підвищити здатність моделі до узагальнення, було введено шар Dropout після першого шару Dense. Таким чином, при кожному оновленні під час навчання, у частину одиниць введення встановлюється 0, що надалі допомагає запобігти ефекту перенавчання.

Далі йде ще один повністю зв'язаний щільний шар із 128 одиницями та активацією «ReLU», що збільшує глибину моделі та її здатність вивчати більш абстрактні уявлення.

На рис. 3 зображено повну схематичну архітектуру розробленої моделі.

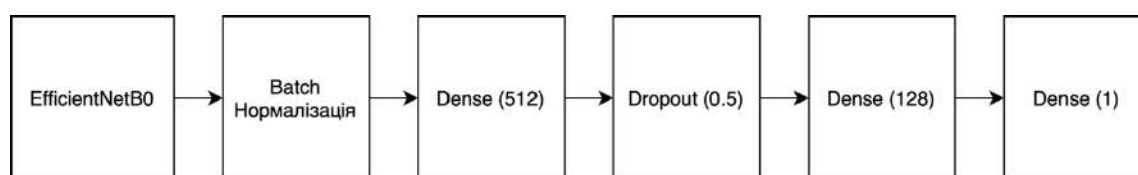


Рис. 3 Повна архітектура розробленої моделі

Архітектура моделі була описана мовою програмування Python з використанням бібліотеки "tensorflow.keras.models", " tensorflow.keras.layers" та інших.

Вхідні дані експерименту

Для навчання та перевірки роботи нейромережі було застосовано датасет FaceForensics++. Цей датасет включає 1000 оригінальних відео, довжиною 2-3 секунди, а також три окремих категорії підробок: FaceSwap, Face2Face та Deepfake. На рис. 4 зображено приклади вирізаних ділянок із обличчями з відео різних датасетів (оригінального та підробок).



Рис. 4. Приклад оригінального, Deepfakes, Face2Face та FaceSwap зображення

Відео всіх категорій було автоматично оброблено: з кожного окремого відео було обрано 2-3 випадкових фрейми, із яких було вирізано ділянки з обличчями. Таким чином, було отримано готовий датасет, який було поділено на дані для навчання, оцінювання та перевірки.

Повний перелік вхідних даних та налаштувань можна побачити в табл. 1. Можна побачити розміри датасетів для двох класів навчання (оригінальні та підроблені зображення). Слід зазначити, що датасет підроблених зображень складається з приблизно однакової кількості зображень отриманих, при цьому застосовуються три технології: Deepfakes, Face2Face та FaceSwap. Також слід додати, що зображення для оцінки та перевірки є унікальними по відношенню до тих, що використовуються для навчання.

Таблиця 1

Вхідні дані та налаштування навчання

Назва параметру	Значення
Оригінальних зображень для навчання	2945 зобр.
Підроблених зображень для навчання	6008 зобр.
Оригінальних зображень для оцінювання	150 зобр.
Підроблених зображень для оцінювання	150 зобр.
Оригінальних зображень для перевірки	82 зобр.
Підроблених зображень для перевірки	83 зобр.
Розмір пакету навчання	34 зобр.
Кількість епох навчання (максимум)	20 епох
Допустима кількість епох із незмінним значенням втрати	5 епох

Слід додати, що розмір пакету навчання був підібраний після декількох попередніх спроб навчання. При розмірі пакету 34 було досягнуто найвищу точність моделі.

Вихідні дані навчання моделі

Після проведення навчання було отримано результати, що наведені в табл. 2.

Результати навчання моделі

Назва параметру	Значення
Кількість епох (результуюча)	11 епох
Кількість епох (ефективна)	6 епох
Втрата кроку навчання (step loss)	0.2027 од.
Втрата оцінювання	0.1436 од.
Точність оцінювання	0.9455 од.
Загальна точність (поріг 0.21)	95%
Розмір файлу моделі	57.9 МБ

З результатів навчання, що наведено в табл. 2, можна побачити, що результуюча кількість епох відрізняється від ефективної. Через те, що було встановлено параметр "терпіння незмінного значення втрати" у 5 епох, зупинка навчання фактично виникла після 6 епохи, а останні 5 епох було проігноровано.

Слід звернути увагу, що загальна точність моделі при встановленому порозі 0,21 (тобто, зображення із вихідним показником моделі менше за 0,21 вважаються підробленими) – 95 %, що є досить високим показником, враховуючи різноманітність датасету для навчання та перевірки.

Не менш важливим є розмір вихідного файлу моделі у 57,9 МБ. Порівнюючи це значення із середнім загальним розміром додатків на GooglePlay (60 МБ) можна дійти висновку, що модель такого розміру не може бути оптимальною для використання у додатку на мобільному пристрої.

Дослідження методів зменшення моделі

Наступним кроком експерименту є експортування моделі в сумісний з мобільними платформами формат. Експортування проводилося за допомогою скрипта мовою програмування Python із використанням бібліотеки "tensorflow.lite". Наведемо приклад коду, який перетворює файл проміжного етапу навчання (розширенням ".h5") у файл розширенням ".tflite", що є сумісним із мобільними пристроями:

```
epoch_result.save('/path/to/dir', save_format='tf')
loaded_model = tf.keras.models.load_model('/path/to/dir ', custom_objects=None,
compile=True)
converter = tf.lite.TFLiteConverter.from_keras_model(loaded_model)
tflite_model = converter.convert()
```

У результаті було отримано файл експортованої моделі розміром 18,9 МБ. Це приблизно в три рази менше за оригінальний файл. Необхідно перевірити точність роботи експортованої моделі на мобільному пристрої.

Для експериментальної перевірки точності роботи моделі було створено додаток під операційну систему Android мовою програмування Kotlin. Бібліотека, що застосовувалась для завантаження моделі, – "org.tensorflow:tensorflow-lite-support:0.2.0". Кроки підготовки зображень перед потраплянням до нейромережі та інші налаштування – ідентичні до тих, що застосовувалися на ПК. Окрім цього, було завантажено ідентичний набір підроблених та оригінальних зображень, які застосовувалися для перевірки моделі на ПК. Таким чином, середовища проведення експерименту максимально схожі та відрізняються тільки платформою виконання та файлом моделі.

У результаті було отримано точність моделі – 94,3 %. Бачимо зменшення показнику, по відношенню до 95 % на оригінальній моделі.

Основним методом зменшення розміру моделі при експорті є квантизація:

```
converter = tf.lite.TFLiteConverter.from_keras_model(loaded_model)
converter.target_spec.supported_types = [tf.float16]
```

При додаванні налаштування квантування float16, розмір моделі залишився незмінним – 18,9 МБ, при цьому точність залишилася 94,3 %.

Наступним кроком було прибрано квантування float16 та додано вбудований флаг `tf.lite.Optimize.DEFAULT`. Цей тип квантування під час перетворення статично квантує лише ваги моделі від числа з плаваючою комою до цілого, що забезпечує 8-бітну точність:

```
converter = tf.lite.TFLiteConverter.from_keras_model(loaded_model)
converter.optimizations = [tf.lite.Optimize.DEFAULT]
```

Застосувавши цей метод квантування, розмір моделі зменшився до 5,3 МБ, що є дуже гарним показником для застосування в мобільному додатку, порівняно з оригінальними 57,9 МБ. Однак точність при цьому зменшилася до 93,6 %.

Останнім кроком було поєднано обидва налаштування квантування з метою підвищити точність:

```
converter = tf.lite.TFLiteConverter.from_keras_model(loaded_model)
converter.optimizations = [tf.lite.Optimize.DEFAULT]
converter.target_spec.supported_types = [tf.float16]
```

Такий комбінований підхід досягнув розміру моделі в 9,5 МБ, при цьому точність повернулася до оригінальної – 94,3 %. Таким чином, було збережено точність, при цьому мінімізувавши розмір файлу. На рис. 5 можна побачити співвідношення моделі до вихідного розміру.

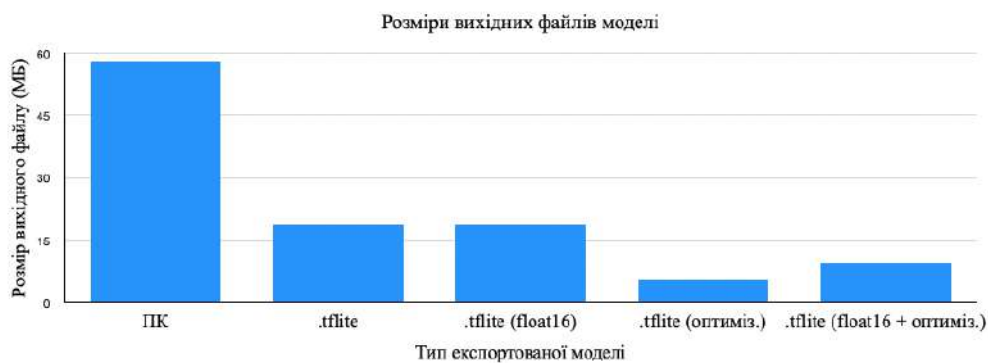


Рис. 5. Відношення типу вихідної моделі до розміру файлу

Схожим чином можна наглядно продемонструвати залежність точності моделі від її типу (рис. 6).

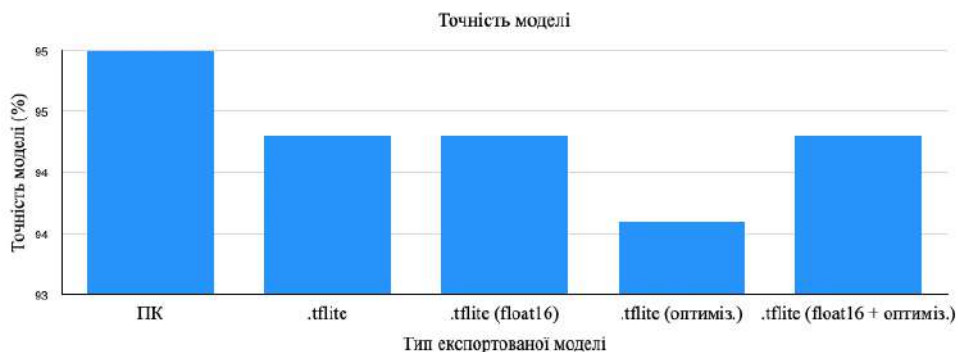


Рис. 6. Відношення типу вихідної моделі до її точності

Виходячи з цих даних, можна зробити висновок, що при застосуванні на мобільній платформі можливий варіант експортування моделі з мінімальною втратою її точності, при цьому застосовується квантування зменшення розміру вихідного файлу в 6-11 разів. Втрата

точності при цьому може погано вплинути на надійність розпізнавання deepfake, але максимальне зменшення розміру вихідного файлу надасть можливість створювати ансамблі з декількох моделей різної архітектури, що значно підвищить надійність системи.

Висновки

Проаналізовано основні методи створення Deepfake, до яких належать автокодери та мережі GAN, а також методи їх виявлення, такі як глибоке навчання, машинне навчання та методи, що базуються на статистичних вимірюваннях. Завдяки існуючим дослідженням було знайдено оптимальний підхід до створення моделі розпізнавання Deepfake.

Експериментально досліджено ефективність та доцільність локального розпізнавання Deepfake у системах біометричної автентифікації за обличчям на мобільних пристроях – отримано оптимістичні результати щодо точності та фізичного розміру файлу моделі. У результаті можна сказати, що застосування локальних методів розпізнавання Deepfake на мобільному пристрої є цілком реальним та надійним методом протидії атакам на системи біометричної автентифікації та загалом перевірки відображеного матеріалу на предмет підробки.

Список літератури:

1. Мироненко Є.В., Северінов О.В. Біометрична ідентифікація і автентифікація особи за геометрією обличчя. Харків : НТУ «ХПІ», 2020.
2. Passport-Photo-Biometric-Statistics [Електронний ресурс]. Режим доступу: <https://passport-photo.online/blog/biometric-statistics/#gref>
3. Creswell, Antonia; White, Tom; Dumoulin, Vincent; Arulkumaran, Kai; Sengupta, Biswa; Bharath, Anil A. (2018). Generative Adversarial Networks: An Overview // IEEE Signal Processing Magazine, 35(1), 53–65. DOI: 10.1109/MSP.2017.2765202
4. Hady A. Khalil; Shady A. Maged; (2021). Deepfakes Creation and Detection Using Deep Learning // International Mobile, Intelligent, and Ubiquitous Computing Conference. 2021. DOI: 10.1109/MIUCC52538.2021.9447642
5. Zainab Zahid, Ammar Haider, Nosheen Sabahat, Asim Tanwir. Vulnerabilities in Biometric Authentication of Smartphones // 2020 IEEE 23rd International Multitopic Conference (INMIC). 2020. DOI: 10.1109/inmic50486.2020.9318094

Надійшла до редколегії 10.09.2023

Відомості про авторів:

Долганенко Олександр Денисович – студент кафедри безпеки інформаційних технологій; Харківський національний університет радіоелектроніки; Україна; e-mail: sasha.dolganenko@gmail.com; ORCID: <http://orcid.org/0000-0002-3996-6940>

Северінов Олександр Васильович – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, професор кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління, Україна; e-mail: oleksandr.sievierinov@nure.ua; ORCID: <https://orcid.org/0000-0002-6327-6405>

В'юхін Данііл Олександрович – старший викладач кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління; Харківський національний університет радіоелектроніки, Україна; e-mail: daniil.viukhin@nure.ua; ORCID: <https://orcid.org/0009-0009-8442-9587>

Коцюба Василь Петрович – канд. техн. наук, доцент, викладач кафедри радіоелектронних систем пунктів управління Повітряних Сил, факультет автоматизованих систем управління та наземного забезпечення польотів авіації; Харківський національний університет Повітряних Сил імені Івана Кожедуба, Україна; e-mail: vasyl.kotsyuba@gmail.com; ORCID: <https://orcid.org/0000-0001-6336-8193>

Крепко Алла Василівна – молодший науковий співробітник науково-дослідної лабораторії, факультет автоматизованих систем управління та наземного забезпечення польотів авіації; Харківський національний університет Повітряних Сил імені Івана Кожедуба Україна; e-mail: krepkoalla@ukr.net; ORCID: <https://orcid.org/0009-0005-1659-4944>

МЕТОД ВІДНОВЛЕННЯ ЛІНІЙНИХ БЛОКОВИХ КОДІВ НАД ДОВІЛЬНИМ СКІНЧЕННИМ ПОЛЕМ ЗА НАБОРАМИ СПОТВОРЕНИХ КОДОВИХ СЛІВ**Вступ**

Задача про відновлення невідомого двійкового лінійного блокового коду за набором його спотворених кодових слів привертає увагу, принаймні, останні 20 років, що пов'язано як з практичними потребами в ефективних методах вивідування конфіденційної інформації, так і з задачами криптоаналізу деяких симетричних криптосистем (див. публікації [1 – 10] та наведені у них посилання).

Майже усі відомі методи відновлення лінійних блокових кодів запропоновані для випадку двійкових кодів і базуються на такому спостереженні. Розглянемо $m \times n$ -матрицю Y , яка складається з випадкових слів лінійного (n, k) -коду C , спотворених у двійковому симетричному каналі зв'язку з імовірністю помилки $p \in (0, 1/2)$, а також довільний двійковий вектор x довжини n та ваги W . Тоді середня вага випадкового вектора Yx^T дорівнює $m/2 \cdot (1 - (1 - 2p)^W)$ або $m/2$ в залежності від того, чи належить вектор x коду C^\perp , дуальному до C , чи ні. Таким чином, для відновлення коду C^\perp (а, отже, і коду C) достатньо знайти $n - k$ лінійно незалежних векторів x , для яких слова вигляду Yx^T , що належать коду, породженому стовпцями матриці Y , мають достатньо малу вагу. Для пошуку слів малої ваги у зазначеному коді застосовуються відомі швидкі алгоритми [11 – 13] (відзначимо роботу [7], де уніфіковано та оптимізовано раніше відомі методи відновлення двійкових лінійних блокових кодів шляхом пошуку слів малої ваги у (неспотворених) лінійних блокових кодах).

Аналіз публікацій [1 – 8] показує, що для оцінювання трудомісткості деяких відомих алгоритмів (зокрема, [5, 7]) потрібно мати певну додаткову інформацію про шуканий код (наприклад, знати частину вагового спектру дуального коду C^\perp), що не завжди можливо на практиці. Крім того, обґрунтування оцінок трудомісткості деяких алгоритмів, які застосовуються для пошуку слів малої ваги у двійкових кодах [11, 12], базується на евристичних припущеннях, тому для підтвердження цих оцінок потрібні обчислювальні експерименти. Окрім того, складність зазначених алгоритмів швидко зростає з ростом довжини n двійкового коду, що відновлюється (принаймні, як поліном від n , степінь якого залежить лінійно від W), що робить їх малопрактичними вже при $n \geq 2000$ та помірних значеннях W . Нарешті, кореляційні атаки на певні симетричні кодові шифросистеми [9, 10] приводять до задачі відновлення лінійних блокових кодів над довільними скінченними полями чи навіть скінченними абелевими групами.

Мета цієї статті – запропонувати метод відновлення лінійних блокових кодів над довільним скінченним полем, який відрізняється за сутністю від відомих [1 – 8] і полягає у відновленні шуканого коду шляхом розв'язання задачі LPN. Остання добре відома в теорії обчислювальних алгоритмів та криптоаналізі. Вона рівносильна задачі декодування випадкового лінійного блокового коду, а на її складності базується стійкість багатьох сучасних постквантових криптосистем (див., наприклад, [14 – 17]).

На відміну від [1 – 8], де з певною достовірністю відновлюються випадкові слова коду C^\perp , запропонований метод полягає у відновленні канонічної твірної матриці коду C , яка визначається за кодом однозначно. При цьому відновлення цієї матриці здійснюється шляхом розв'язання (не більше ніж) $n - 1$ систем лінійних рівнянь зі спотвореними правими частинами від k (або меншої кількості) невідомих кожна.

Показано, що запропонований метод надає можливість застосовувати для відновлення лінійних блокових кодів більш широкий клас алгоритмів в порівнянні з раніше відомими, зокрема, алгоритми типу ВКВ [18, 19], а також алгоритми, викладені в [20 – 22]. При цьому, на відміну від раніше відомих, складність запропонованого методу залежить лінійно від довжини n шуканого коду, проте зростає з ростом його вимірності k відповідно до того, який алгоритм розв'язання задачі LPN застосовується.

Означення основних понять та допоміжні твердження

Позначимо F скінченне поле з q елементів, $F_{m,n}$ – множину $m \times n$ -матриць над цим полем, $w(x) = |\{i \in \overline{1, n} : x_i \neq 0\}|$ – вагу вектора $x = (x_1, \dots, x_n) \in F^n$.

Для будь-якого $\varepsilon \in (0, 1)$ наведемо ε -нерівномірний розподіл ймовірностей на полі F , який визначається за правилом

$$p(0) = q^{-1}(1 + (q-1)\varepsilon), \quad p(a) = q^{-1}(1 - \varepsilon), \quad a \in F \setminus \{0\}. \quad (1)$$

Надалі закон розподілу (1) позначатимемо символом $U(\varepsilon)$.

Безпосередньо з наведеного означення та формули повної ймовірності випливає такий результат.

Лема 1 [10]. Нехай ξ та η є незалежними випадковими величинами на полі F , що мають ε_1 -нерівномірний та ε_2 -нерівномірний розподіли ймовірностей відповідно. Тоді для будь-якого $c \in F \setminus \{0\}$ випадкова величина $c\xi$ має ε_1 -нерівномірний, а випадкова величина $\xi + \eta$ має $\varepsilon_1\varepsilon_2$ -нерівномірний розподіл ймовірностей на полі F .

Задача LPN з параметрами (m, n, q, ε) відома у двох варіантах [14 – 17]. Перший з них називається задачею розпізнавання та полягає в наступному.

Спостерігається послідовність незалежних випадкових векторів

$$(A_1, b_1), \dots, (A_m, b_m), \quad (2)$$

де A_1, \dots, A_m – випадкові рівноймовірні вектори довжини n над полем F , а b_1, \dots, b_m або є випадковими рівноймовірними елементами цього поля, що не залежать від A_1, \dots, A_m (гіпотеза H_0), або розподілені за законом

$$b_i = A_i x + \xi_i, \quad i \in \overline{1, m}, \quad (3)$$

де $x = (x_1, \dots, x_n) \in F^n$ – невідомий вектор, ξ_1, \dots, ξ_m є незалежними випадковими величинами, розподіленими за законом $U(\varepsilon)$ (гіпотеза H_1). Треба побудувати критерій для перевірки зазначених гіпотез.

Другий варіант задачі LPN полягає у розв'язанні системи рівнянь зі спотвореними правими частинами (3), яка формується зазначеним вище чином. По суті ця задача еквівалентна декодуванню випадкового $(n, k)_q$ -коду (тобто коду довжини n та вимірності k над полем з q елементів) у q -му симетричному каналі зв'язку. При $q=2$ вона зводиться до класичної задачі LPN, на якій базується стійкість багатьох постквантових криптосистем [15 – 17].

Зрозуміло, що вміння розв'язувати задачу LPN у другому варіанті її постановки надає можливість розв'язувати її розпізнавальну версію практично з такими ж трудомісткістю та достовірністю. Має місце також обернене твердження, доведення якого майже дослівно повторює доведення леми 4.2 в [23].

Лема 2. Нехай існує алгоритм A , який розрізняє зазначені вище гіпотези H_0 , H_1 з максимальною ймовірністю помилки $\max\{\mathbf{P}(H_0 | H_1), \mathbf{P}(H_1 | H_0)\} \leq \delta$, виконуючи T операцій.

Тоді існує алгоритм, який розв'язує систему рівнянь (3) з імовірністю помилки не вище ніж $qn\delta$ за $O(qn(T+m))$ операцій.

Формальна постановка задачі та основні результати

Нехай C – невідомий лінійний $(n, k)_q$ -код з твірною матрицею G . Спостерігається послідовність випадкових векторів

$$Y^{(i)} = U^{(i)}G + \eta^{(i)}, \quad i \in \overline{1, m}, \quad (4)$$

де $U^{(1)}, \dots, U^{(m)}, \eta^{(1)}, \dots, \eta^{(m)}$ є незалежними в сукупності випадковими векторами, розподіленими за законами

$$\mathbf{P}(U^{(i)} = a) = q^{-k}, \quad a \in F^k, \quad \mathbf{P}(\eta^{(i)} = x) = (q^{-1}(1-\varepsilon))^{wt(x)}(q^{-1}(1+(q-1)\varepsilon))^{n-wt(x)}, \quad x \in F^n.$$

Треба відновити код C за випадковою послідовністю (4).

Для викладення запропонованого методу розв'язання цієї задачі введемо додаткові позначення.

Для будь-якої множини $I \subseteq \overline{1, n}$ та довільної матриці M , стовпці якої занумеровані числами від 1 до n , позначимо M_I підматрицю матриці M , що складається з її стовпців з номерами із множини I . Якщо $I = \{i\}$ є одноелементною множиною, то замість $M_{(i)}$ використовуватимемо позначення M_i для i -го стовпця матриці M ; i -й рядок матриці M позначатимемо символом $M^{(i)}$.

За означенням матриця $G \in F_{k \times n}$ рангу k називається *спеціальною ступеневою*, якщо вона має вигляд

$$G = \begin{pmatrix} \mathbf{0} \dots \mathbf{0} & \mathbf{1} * \dots * \mathbf{0} * \dots * \mathbf{0} * \dots * \\ \mathbf{0} \dots \mathbf{0} & \mathbf{0} \mathbf{0} \dots \mathbf{0} & \mathbf{1} * \dots * \mathbf{0} * \dots * \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \mathbf{0} \dots \mathbf{0} & \mathbf{0} \mathbf{0} \dots \mathbf{0} & \mathbf{0} \mathbf{0} \dots \mathbf{0} & \mathbf{1} * \dots * \end{pmatrix}, \quad (5)$$

де $*$ позначає довільний елемент поля F , $1 \leq i_1 < \dots < i_k \leq n$. З відомих теорем лінійної алгебри (див., наприклад, [24, розд. VII]) випливає, що кожен код C має єдину твірну матрицю, яка є спеціальною ступеневою і називається *канонічною твірною матрицею* коду C .

Зафіксуємо множину $I \subseteq \overline{1, n}$ потужності $l \in \overline{1, k}$ та елемент $j \in \overline{1, n}$ такі, що $\text{rank}(G_I) = l$, $j \notin I$, і розглянемо матрицю A , яка складається з рядків $A^{(i)} = U^{(i)}G_I + (\eta^{(i)})_I$, $i \in \overline{1, m}$, а також вектор-стовпець b з координатами $b_i = U^{(i)}G_j + (\eta^{(i)})_j$, $i \in \overline{1, m}$.

Лема 3. Мають місце такі твердження:

- 1) рядки $A^{(1)}, \dots, A^{(m)}$ є незалежними випадковими рівномірними двійковими векторами довжини l ;
- 2) якщо вектор G_j лінійно не залежить від стовпців матриці G_I , то b є випадковим рівномірним вектором, що не залежить від матриці A ;
- 3) якщо вектор G_j є лінійною комбінацією стовпців матриці G_I : $G_j = G_I x$, де $x \in F^l$, то x є розв'язком задачі LPN $Az = b = Ax + \xi$, де координати ξ_1, \dots, ξ_m випадкового вектора ξ мають вигляд $\xi_i = (\eta^{(i)})_j - (\eta^{(i)})_I x$, $i \in \overline{1, m}$, та розподілені за законом $U(\varepsilon^{wt(x)+1})$.

Доведення. Справедливість твердження 1) випливає безпосередньо з наведених означень, а твердження 2) є наслідком твердження 1), оскільки лінійна незалежність вектора G_j від стовпців матриці G_I рівносильна умові $\text{rank}(G_{I \cup \{j\}}) = l$.

Для доведення твердження 3) помітимо, що на підставі наведених вище означень

$$b_i - A^{(i)}x = U^{(i)}G_j + (\eta^{(i)})_j - (U^{(i)}G_I + (\eta^{(i)})_I)x =$$

$$= U^{(i)}(G_j - G_l x) + (\eta^{(i)})_j - (\eta^{(i)})_l x = \xi_i, \quad i \in \overline{1, m}.$$

При цьому вектор ξ не залежить від (випадкової рівномірної) матриці A , а його координати розподілені за законом $U(\varepsilon^{wt(x)+1})$ на підставі леми 1.

Отримана лема складає основу наступного методу відновлення канонічної твірної матриці G коду C за випадковою послідовністю (4).

Не обмежуючи загальності, припустимо, що кожен стовпець матриці G має вагу від 1 до w , де $w \in \overline{1, k}$. Якщо східці цієї матриці починаються у стовпцях з номерами $1 \leq i_1 < \dots < i_k \leq n$ (див. формулу (5)), то $i_1 = 1$ і для кожного $l \in \overline{1, k}$ стовпець з номером i_l матриці G не залежить лінійно від її попередніх стовпців, а стовпці цієї матриці з номерами $i \in \{i_l + 1, \dots, i_{l+1} - 1\}$ є лінійними комбінаціями її стовпців з номерами i_1, \dots, i_l (тут і далі вважаємо, що $i_{k+1} = n + 1$).

Алгоритм відновлення матриці G (рис. 1) використовує, як допоміжний, довільний фіксований алгоритм \mathbf{A} розв'язання задачі LPN. Останній отримує на вхід впорядкований набір (A, b, θ, δ) , де A – випадкова рівномірна $m \times l$ -матриця над полем F , b – вектор вигляду $b = Ax + \zeta$, де $x \in F^l$, $\zeta = (\zeta_1, \dots, \zeta_m)$ – випадковий вектор з незалежними координатами, розподіленими за законом $U(\theta)$, $\theta, \delta \in (0, 1)$. При цьому вважається, що існує функція $N_A = N_A(l, \theta, \delta)$ така, що за умови $m \geq N_A(l, \theta, \delta)$ виконується нерівність $\mathbf{P}(\mathbf{A}(A, b, \theta, \delta) \neq x) \leq \delta$, тобто ймовірність помилки алгоритму \mathbf{A} (відносно сумісного розподілу матриці A та вектора ζ) не перевищує δ , якщо число рівнянь у системі зі спотвореними правими частинами $Ax + \zeta = b$ є не менше ніж $N_A(l, \theta, \delta)$. Трудомісткість алгоритму \mathbf{A} визначається як його часова складність у найгіршому випадку та позначається $T_A(l, \theta, \delta)$.

Зафіксуємо число $m_1 \in \overline{1, m}$ та позначимо Y' і Y'' підматриці, які містяться відповідно в перших m_1 та останніх $m_2 = m - m_1$ рядках матриці Y . Алгоритм на рис. 1 складається з $n - 1$ кроків і починає роботу зі стовпця $G_1 = (1, 0, \dots, 0)^T$ довжини k та множини $I = \{i_1 = 1\}$.

Вхідні дані:

– $m \times n$ -матриця $Y = \begin{pmatrix} Y' \\ Y'' \end{pmatrix}$, що складається з рядків (4).

– алгоритм \mathbf{A} розв'язання задачі LPN;

– числа $m_1 \in \overline{1, m}$, $w \in \overline{1, k}$, $\varepsilon, \delta \in (0, 1)$;

1. Покласти $G_1 = (1, 0, \dots, 0)^T$, $I = \{1\}$, $j = 2$.

2. Поки $j \leq n$:

2.1. Покласти

$$A' = Y'_I, \quad b' = Y'_j, \quad l = |I|, \quad l_* = \min\{l, w\}, \quad p_{l_*} = q^{-1}(q-1)(1 - \varepsilon^{l_*+1}).$$

2.2. Обчислити $x = \mathbf{A}(A', b', \varepsilon^{l_*+1}, \delta/2n)$.

2.3. Покласти $m_2 = m - m_1$, $\Delta = m_2 \left(\frac{q^{-1}(q-1) + p_{l_*}}{2} \right)$, $A'' = Y''_I$, $b'' = Y''_j$.

2.4. Якщо $wt(b'' - A''x) \leq \Delta$, покласти $G_j = (x, \underbrace{0, \dots, 0}_{k-1})^T$, $j = j + 1$;

інакше покласти $G_j = (0, \dots, \underbrace{1}_{l+1}, \dots, 0)^T$, $I = I \cup \{j\}$, $j = j + 1$.

Результат: матриця (G_1, \dots, G_n) .

Рис. 1. Алгоритм відновлення канонічної твірної матриці лінійного блокового коду за набором спотворених кодових слів

Нехай на $(j-1)$ -му кроці алгоритму, $j \in \overline{2, n}$, вже побудовані стовпці G_1, \dots, G_{j-1} матриці G та множина $I = \{i_1, \dots, i_l\}$, яка складається з номерів, у яких починаються східці матриці (G_1, \dots, G_{j-1}) , $1 \leq l \leq k$, $i_l < j \leq i_{l+1}$. Тоді на j -му кроці алгоритму здійснюється перевірка, чи є стовпець G_j лінійною комбінацією стовпців G_{i_1}, \dots, G_{i_l} , та знаходження такої лінійної комбінації у випадку позитивного результату перевірки.

Перевірка базується на лемі 3 та полягає в застосуванні алгоритму \mathbf{A} до матриці A' і вектора b' , які визначаються на кроці 2.1 (рис. 1). Алгоритм \mathbf{A} повертає певний вектор $x \in F^l$, який розглядається як кандидат на розв'язок системи лінійних рівнянь зі спотвореними правими частинами $A'z = b'$. Далі підраховується вага вектора $b'' - A''x$, яка порівнюється з порогом Δ . Якщо $wt(b'' - A''x) \leq \Delta$, то вектор G_j визначається за формулою: $G_j = (x, \underbrace{0, \dots, 0}_{k-l})^T$ (при цьому множина I не змінюється). Якщо ж $wt(b'' - A''x) > \Delta$, то G_j визначається як двійковий стовпець довжини k , усі координати якого, за виключенням $(l+1)$ -ї, дорівнюють нулю; при цьому множина I приймає нове значення $I = I \cup \{j\}$.

Алгоритм завершує роботу на кроці $j = n$.

Наступне твердження встановлює умови, за яких алгоритм на рис. 1 знаходить шукану матрицю G із заданою ймовірністю помилки, а також надає оцінку трудомісткості цього алгоритму.

Твердження 1. Припустимо, що $T_{\mathbf{A}}(l, \theta, \delta)$ та $N_{\mathbf{A}}(l, \theta, \delta)$ є неспадними функціями кожного з параметрів l, θ при фіксованих значеннях решти. Тоді за умови

$$m_1 \geq N_{\mathbf{A}}(k, \varepsilon^{w+1}, \delta/2n), \quad m_2 \geq 2 \left(\frac{q^{-1}(q-1)\varepsilon^{w+1}}{2} \right)^{-2} \ln(2n\delta^{-1}) \quad (6)$$

ймовірність помилки алгоритму на рис. 1 не перевищує δ . При цьому його трудомісткість становить $O(nT_{\mathbf{A}}(k, \varepsilon^{w+1}, \delta/2n) + m_2n)$ операцій.

Доведення. Позначимо π_j ймовірність події, яка полягає в тому, що стовпці G_1, \dots, G_{j-1} матриці G відновлено правильно, а стовпець G_j – ні, $j \in \overline{2, n}$. Тоді ймовірність помилки алгоритму дорівнює $\pi_2 + \dots + \pi_n$.

Для оцінювання ймовірності π_j позначимо $I = \{i_1, \dots, i_l\}$ множину номерів стовпців, у яких починаються східці матриці (G_1, \dots, G_{j-1}) , та розглянемо два можливих випадки: $i_l < j < i_{l+1}$ та $j = i_{l+1}$.

У першому випадку ймовірність помилкового відновлення стовпця G_j не перевищує суми ймовірностей двох подій:

$$\Omega_1 = \{x \neq \mathbf{A}(A', b', \varepsilon^{l_*+1}, \delta/2n)\},$$

$$\Omega_2 = \{x = \mathbf{A}(A', b', \varepsilon^{l_*+1}, \delta/2n)\} \cap \{wt(b'' - A''x) > \Delta\}.$$

На підставі монотонності функції $N_{\mathbf{A}}$ та першої нерівності (6) маємо $m_1 \geq N_{\mathbf{A}}(k, \varepsilon^{w+1}, \delta/2n) \geq N_{\mathbf{A}}(l, \varepsilon^{l_*+1}, \delta/2n)$. Отже, за означенням функції $N_{\mathbf{A}}$ ймовірність події Ω_1 не перевищує $\delta/2n$. Далі, якщо відбулася подія Ω_2 , то на підставі леми 3

$wt(b'' - A''x) = \sum_{i=1}^{m_2} \xi_i$, де ξ_1, \dots, ξ_{m_2} є незалежними випадковими величинами, розподіленими за законом $\mathbf{P}(\xi_i = 1) = 1 - \mathbf{P}(\xi_i = 0) = q^{-1}(q-1)(1 - \varepsilon^{l_*+1})$, $i \in \overline{1, m_2}$. Звідси, використовуючи умову $l_* \leq w$, нерівність Гефдінга [25] та другу нерівність (6), отримаємо, що ймовірність події Ω_2 не перевищує

$$\begin{aligned} \mathbf{P}(wt(b'' - A''x) > \Delta) &= \mathbf{P}\left(\sum_{i=1}^{m_2} \xi_i > m_2 \left(\frac{q^{-1}(q-1) + p_{l^*}}{2}\right)\right) \leq \exp\left\{-2m_2 \left(\frac{q^{-1}(q-1)\varepsilon^{l^*+1}}{2}\right)^2\right\} \leq \\ &\leq \exp\left\{-2m_2 \left(\frac{q^{-1}(q-1)\varepsilon^{w+1}}{2}\right)^2\right\} \leq \delta/2n. \end{aligned}$$

Таким чином, у першому випадку ($i_l < j < i_{l+1}$) ймовірність π_j не перевищує $\mathbf{P}(\Omega_1) + \mathbf{P}(\Omega_2) \leq \delta/n$. Аналогічно доводиться, що у другому випадку ($j = i_{l+1}$) ймовірність π_j не перевищує $\delta/2n$. Отже, $\pi_j \leq \delta/n$ для кожного $j \in \overline{2, n}$ і ймовірність помилки алгоритму є $\pi_2 + \dots + \pi_n \leq \delta$.

Нарешті, трудомісткість j -го кроку дорівнює

$$O(T_A(l, \varepsilon^{l^*}, \delta/2n) + m_2) = O(T_A(k, \varepsilon^{w+1}, \delta/2n) + m_2)$$

операцій, $j \in \overline{2, n}$, а, отже, трудомісткість алгоритму в цілому становить $O(nT_A(k, \varepsilon^{w+1}, \delta/2n) + nm_2)$. Твердження доведено.

Зауважимо, що при практичному застосуванні алгоритму на рис. 1 слушно використовувати різні алгоритми розв'язання систем лінійних рівнянь зі спотвореними правими частинами на кроці 2.2 в залежності від кількості невідомих у системах. Так, для помірних значень l (наприклад, $l \leq 20$) можна використовувати метод максимуму правдоподібності із застосуванням швидкого перетворення Фур'є [17]. Для більших значень l краще застосовувати алгоритми типу ВКВ [18, 19] або (при $q=2$, якщо кількість спотворених кодових слів є обмеженою) – алгоритми, викладені в [20, 21]. На останніх кроках (починаючи з $j = i_k + 1$) можна прискорити роботу алгоритму на рис. 1, розв'язуючи одночасно декілька систем лінійних рівнянь зі спотвореними правими частинами та однаковою матрицею коефіцієнтів, як це робиться в [26] при відновленні систематичних лінійних блокових кодів. При цьому стовпці G_{i_k+1}, \dots, G_n шуканої матриці G співпадають з розв'язками відповідних систем рівнянь, а кроки 2.3, 2.4 (рис. 1) виконувати не треба.

Зауважимо також, що у випадку, коли відома нижня межа d' дуальної відстані коду C , виконання алгоритму на рис. 1 можна почати безпосередньо з кроку $j = d'$, визначаючи G_j як двійковий стовпець довжини k , усі координати якого, за виключенням j -ї, дорівнюють нулю, $j \in \overline{1, d' - 1}$.

На завершення розглянемо модифікацію наведеного алгоритму (рис. 2), яка використовує в ролі A довільний алгоритм розв'язання розрізнявальної версії задачі LPN.

Позначимо $N_A = N_A(n, \varepsilon, \delta)$ нижню межу числа m векторів у послідовності (2), для якого алгоритм A розв'язує розрізнявальну версію задачі LPN з параметрами (m, n, q, ε) з максимальною ймовірністю помилки не вище ніж δ . Символом $T_A = T_A(n, \varepsilon, \delta)$ позначимо трудомісткість алгоритму A .

Твердження 2. Припустимо, що N_A і T_A є неспадними функціями кожного з трьох аргументів при фіксованих значеннях решти. Тоді за умови $m \geq N_A(k, \varepsilon^{w+1}, \delta/qn^2)$ ймовірність помилки алгоритму на рис. 2 не перевищує δ . При цьому його трудомісткість становить $O(qn^2(T_A(k, \varepsilon^{w+1}, \delta/2n) + m))$ операцій.

Доведення. Позначимо π_j ймовірність того, що стовпці G_1, \dots, G_{j-1} матриці G відновлено правильно, а стовпець G_j – ні, $j \in \overline{2, n}$. Для оцінювання ймовірності π_j позначимо $I = \{i_1, \dots, i_l\}$ множину номерів стовпців, у яких починаються східці матриці (G_1, \dots, G_{j-1}) , та розглянемо два можливих випадки: $j = i_{l+1}$ та $i_l < j < i_{l+1}$.

Вхідні дані:

- $m \times n$ -матриця Y , що складається з рядків (4).
- алгоритм A розв'язання розрізняювальної версії задачі LPN;
- числа $w \in \overline{1, k}$, $\varepsilon, \delta \in (0, 1)$;

1. Покласти $G_1 = (1, 0, \dots, 0)^T$, $I = \{1\}$, $j = 2$.

2. Поки $j \leq n$:

Покласти

$$A = Y_I, b = Y_j, l = |I|, l_* = \min\{l, w\}, p_{l_*} = q^{-1}(q-1)(1-\varepsilon^{l_*+1})$$

та застосувати алгоритм A до вхідних даних $A, b, \varepsilon^{l_*+1}, \delta/2n$.

Якщо A повертає висновок про справжність гіпотези H_0 , покласти

$$G_j = (0, \dots, \underset{l+1}{1}, \dots, 0)^T, I = I \cup \{j\}, j = j+1.$$

Інакше відновити розв'язок x системи лінійних рівнянь зі спотвореними правими частинами $Az = b$ шляхом застосування алгоритму A до вхідних даних

$$A, b, \varepsilon^{l_*+1}, \delta/2qn^2 \text{ (див. лему 2) та покласти } G_j = (x, \underbrace{0, \dots, 0}_{k-1})^T, j = j+1.$$

Результат: матриця (G_1, \dots, G_n) .

Рис. 2. Модифікований алгоритм відновлення канонічної твірної матриці лінійного блокового коду за набором спотворених кодових слів

В першому випадку помилкове завершення алгоритму на рис. 2 є виключно наслідком помилки алгоритму A при його застосуванні до вхідних даних $A, b, \varepsilon^{l_*+1}, \delta/2n$ на кроці 2 і, оскільки $m \geq N_A(k, \varepsilon^{w+1}, \delta/2qn^2) \geq N_A(l, \varepsilon^{l_*+1}, \delta/2n)$, то на підставі означення функції N_A маємо $\pi_j \leq \delta/2n$. В другому випадку π_j не перевищує суму ймовірностей двох подій, перша з яких полягає у помилковому завершенні алгоритму A при його застосуванні до вхідних даних $A, b, \varepsilon^{l_*+1}, \delta/2n$, а друга – у помилковому завершенні цього алгоритму при його застосуванні до вхідних даних $A, b, \varepsilon^{l_*+1}, \delta/2qn^2$ (як зазначено у формулюванні леми 2) за умови заперечення першої події. Отже, згідно з лемою 2, $\pi_j \leq \delta/2n + (qn)(\delta/2qn^2) = \delta/n$.

Таким чином, $\pi_j \leq \delta/n$ для кожного $j \in \overline{2, n}$ і ймовірність помилки алгоритму є $\pi_2 + \dots + \pi_n \leq \delta$.

Нарешті, оцінка трудомісткості алгоритму на рис. 2 впливає безпосередньо з його опису та леми 2. Твердження доведено.

Висновки

Отримані результати показують, що відновлення $(n, k)_q$ -коду C за набором його слів, спотворених у q -му симетричному каналі з ймовірністю помилки $q^{-1}(1-\varepsilon)$, є не складніше ніж розв'язання n систем лінійних рівнянь від k невідомих з правими частинами, спотвореними з імовірністю $q^{-1}(1-\varepsilon^{w+1})$, де w – максимальна вага стовпців канонічної твірної матриці коду C . Це надає можливість застосовувати для відновлення лінійних блокових кодів більш широкий клас алгоритмів в порівнянні з раніше відомими. При цьому, на відміну від раніше відомих методів [1 – 8], складність запропонованого методу залежить лінійно від довжини шуканого коду (проте зростає з ростом його вимірності відповідно до того, який алгоритм розв'язання задачі LPN застосовується).

Запропонований метод показує, що основним параметром, від якого залежить складність відновлення лінійного блокового коду, є його вимірність (а не довжина), що, в принципі, надає можливість помітно пришвидшити відомі алгоритми відновлення двійкових лінійних блокових кодів за наборами спотворених кодових слів.

Список літератури:

1. Valembois A. Detection and recognition of a binary linear code // *Discrete applied mathematics*. 2001. Vol. 111, No. 1–2. P. 199–218. DOI: [https://doi.org/10.1016/s0166-218x\(00\)00353-x](https://doi.org/10.1016/s0166-218x(00)00353-x).
2. Cluzeau M. Block code reconstruction using iterative decoding techniques // *IEEE Conference ISIT'06*. 2006. P. 2269–2273. DOI: <https://doi.org/10.1109/isit.2006.261971>.
3. Barbier J., Sicot G., Houcke S. Algebraic approach of the reconstruction of linear and convolutional error correcting codes // *World Academy of Science, Engineering and Technology*. 2006. Vol. 16. P. 66–71.
4. Sicot G., Houcke S. Blind detection of interleaver parameters // *Signal Process*. 2009. Vol. 89 (4). P. 450–462.
5. Cluzeau M., Finiasz M. Recovering a code's length and synchronization from a noisy intercepted bitstream // *IEEE Conference ISIT'09*. 2009. P. 2737–2731. DOI: <https://doi.org/10.1109/isit.2009.5205843>.
6. Karimian Y., Ziapuor S., Attari M.A. Parity-check matrix recognition from noisy codewords // *ArXiv: 1205.4641v1 [cs.IT]*. 2012. 22 p.
7. Carrier K., Tillich J.-P. Identifying an unknown code by partial Gaussian elimination // *Designs, Codes and Cryptography*. 2018. Vol. 87, No. 2–3. P. 685–713. DOI: <https://doi.org/10.1007/s10623-018-00593-7>.
8. Fast Blind Recovery of Linear Block Codes over Noisy Channels / P. Wang et al. // *2023 IEEE International Symposium on Information Theory (ISIT), Taipei, Taiwan, 25–30 June 2023*. 2023. DOI: <https://doi.org/10.1109/isit54713.2023.10206775>.
9. Олексійчук А.М., Шевчук О. С. Оцінка ефективності атак на основі підібраних відкритих текстів на криптосистему Рао-Нама над скінченною абелевою групою // *Радіотехніка*. 2021. Т. 1, № 205. С. 22–31. DOI: <https://doi.org/10.30837/rt.2021.2.205.02>.
10. Шевчук О. С. Рандомізована симетрична криптосистема Мак-Еліса на основі узагальнених кодів Ріда-Соломона // *Радіотехніка*. 2020. Т. 1, № 200. С. 25–36. DOI: <https://doi.org/10.30837/rt.2020.1.200.03>.
11. Canteaut A., Chabaud F. A new algorithm for finding minimum-weight words in a linear code: application to McEliece's cryptosystem and to narrow-sense BCH codes of length 511 // *IEEE Transactions on Information Theory*. 1998. Vol. 44, No.1. P. 367–378. DOI: <https://doi.org/10.1109/18.651067>.
12. Chose P., Joux A., Mitton M. Fast Correlation Attacks: An Algorithmic Point of View // *Advances in Cryptology – EUROCRYPT 2002*. Berlin, Heidelberg, 2002. P. 209–221. DOI: https://doi.org/10.1007/3-540-46035-7_14.
13. Dubiner M. Bucketing Coding and Information Theory for the Statistical High-Dimensional Nearest-Neighbor Problem // *IEEE Transactions on Information Theory*. 2010. Vol. 56, No. 8. P. 4166–4179. DOI: <https://doi.org/10.1109/tit.2010.2050814>.
14. Cryptographic Primitives Based on Hard Learning Problems / A. Blum et al. // *Advances in Cryptology – CRYPTO'93*. Berlin, Heidelberg, 1994. P. 278–291. DOI: https://doi.org/10.1007/3-540-48329-2_24.
15. Pietrzak K. Cryptography from Learning Parity with Noise // *SOFSEM 2012: Theory and Practice of Computer Science*. Berlin, Heidelberg, 2012. P. 99–114. DOI: https://doi.org/10.1007/978-3-642-27660-6_9.
16. Bogos S. LPN in cryptography: an algorithmic study. PhD thesis. Ecole Polytechnique Federale de Lausanne. 2017. p.177. URL: https://infoscience.epfl.ch/record/228977/files/EPFL_TH7800.pdf.
17. Ігнатенко С. М. Методи розв'язання задачі LPN над скінченними кільцями для оцінювання стійкості симетричних постквантових шифросистем : дис. ... канд. техн. наук : 05.13.21. Харків, 2021. 179 с. DOI: <http://dspace.univer.kharkov.ua/handle/123456789/16047>.
18. Blum A., Kalai A., Wasserman H. Noise-tolerant learning, the parity problem, and the statistical query model // *Journal of the ACM*. 2003. Vol. 50, No. 4. P. 506–519. DOI: <https://doi.org/10.1145/792538.792543>.
19. Bogos S., Tramer S., Vaudenay S. On solving LPN using BKW and variants. Implementation and analysis // *Cryptology ePrint Archive, Report 2015/049*. URL: <http://eprint.iacr.org/2015/049>.
20. Алексейчук А.Н., Грязнухин А.Ю. Быстрый алгоритм восстановления истинного решения фиксированного веса системы линейных булевых уравнений с искаженной правой частью // *Прикладная дискретная математика*. 2013. Т. 20. С. 59–70.
21. Grigorescu E., Reyzin L., Vempala S. On Noise-Tolerant Learning of Sparse Parities and Related Problems // *Lecture Notes in Computer Science*. Berlin, Heidelberg, 2011. P. 413–424. DOI: https://doi.org/10.1007/978-3-642-24412-4_32.

22.Zhang B., Xu C., Meier W. Fast Correlation Attacks over Extension Fields, Large-Unit Linear Approximation and Cryptanalysis of SNOW 2.0 // Lecture Notes in Computer Science. Berlin, Heidelberg, 2015. P. 643–662. DOI: https://doi.org/10.1007/978-3-662-47989-6_31.

23.Regev O. On lattices, learning with errors, random linear codes, and cryptography // Journal of the ACM. 2009. Vol. 56, No. 6. P. 1–40. DOI: <https://doi.org/10.1145/1568318.1568324>.

24.Глухов М.М., Елизаров В.П, Нечаев А.А. Алгебра : учебник в 2-х т., Т. 1. Москва : Гелиос АРВ, 2003. 336 с.

25.Hoeffding W. Probability Inequalities for Sums of Bounded Random Variables // Journal of the American Statistical Association. 1963. Vol. 58, No. 301. P. 13–30. DOI: <https://doi.org/10.1080/01621459.1963.10500830>.

26.Алексейчук А.Н., Грязнухин А.Ю. Метод восстановления систематических линейных кодов по наборам искаженных кодовых слов // Прикладная дискретная математика. 2013. Т. 12, № 2. С. 313–318.

Надійшла до редколегії 11.10.2023

Відомості про авторів:

Олексійчук Антон Миколайович – д-р техн. наук, доц., Інститут спеціального зв'язку та захисту інформації Національного технічного університету України “Київський політехнічний інститут імені Ігоря Сікорського”, професор спеціальної кафедри № 1; Україна; e-mail: alex-dtn@ukr.net

Шевчук Ольга Сергіївна – викладач спеціальної кафедри № 5; Інститут спеціального зв'язку та захисту інформації Національного технічного університету України “Київський політехнічний інститут імені Ігоря Сікорського”, Україна; e-mail: olia13511@gmail.com

І.Д. ГОРБЕНКО, д-р техн. наук, Є.Ю. КАПТБОЛ

АНАЛІЗ ТА ПОРІВНЯННЯ БЕЗПЕКИ ЕЛЕКТРОННИХ ПІДПИСІВ, ЩО ГРУНТУЮТЬСЯ НА НОВИХ КВАНТОВОСТІЙКИХ ПРОБЛЕМАХ

Вступ

В результаті проведення трьох раундів NIST PQC було обрано для стандартизації чотири кандидати (механізм інкапсуляції ключа CRYSTALS-Kyber та електронні підписи (ЕП) CRYSTALS-Dilithium, Falcon та SPHINCS+) та визначено кандидатів для проведення четвертого раунду (механізми інкапсуляції ключів BIKE, Classic McEliece, HQC та SIKE (котрий розробники визнали ненадійним)) [1, 2].

Через специфіку обраних алгоритмів NIST потребував додаткових кандидатів з числа ЕП загального призначення, котрі не були б засновані на використанні решіток. Через це було розпочато процес стандартизації додаткових ЕП для квантовостійкої криптографії. Серед поданих на розгляд до першого раунду цього процесу стандартизації можна виділити наступні види підписів [3, 4]: підписи, засновані на кодах; підписи на лізогеніях; мультिवаріативні підписи; симетричні підписи; MPC-in-the-head та підписи, визначені NIST як "інші".

Метою роботи є аналіз та порівняння кандидатів на квантовостійкий ЕП, що ґрунтуються на нових та перспективних квантовостійких проблемах, стійких до класичних та квантових атак та атак бічними каналами.

Основна частина

Конкурс NIST PQC було спрямовано на обрання постквантових кандидатів криптопримітивів для стандартизації. З часом, під час розгляду та відкритого коментування проєктів стандартів криптографічною спільнотою було прийнято замінити термін «постквантовий» на більш точний «квантовостійкий» [5]. Саме тому в цій роботі буде використовуватись саме термін «квантовостійкий».

В межах роботи розглядаються кандидати на квантовостійкий ЕП, що були представлені на процес стандартизації додаткових ЕП від NIST.

Особливий інтерес для порівняння представляють підписи, котрі не були віднесені до жодної з груп та були об'єднані під назвою "інші підписи". Серед них наявні наступні варіанти ЕП [3]: ALTEQ, eMLE-Sig 2.0, KAZ-SIGN, Xifrat1-Sign.I, Preon.

В даній роботі розглянуто лише схеми ЕП ALTEQ, eMLE-Sig 2.0, KAZ-SIGN, Xifrat1-Sign.I.

Розглянемо схему ЕП ALTEQ.

Схема ЕП ALTEQ ґрунтується на складності проблеми рівності альтернованих трилінійних форм (ATFE), яка використовує групову дію загальної лінійної групи над скінченним полем.

Загальна структура ALTEQ полягає в наступному.

Спочатку за прикладом Голдеріх – Мікалі – Вігдерсон (GMW) розроблено протокол з нульовим розголошенням, що опирається на складність ATFE. Далі застосовується перетворення Фіат – Шаміра (FS) для усунення взаємодії від протоколу нульового розголошення, що приводить до схеми ЕП.

Протокол складається з двох частин [6]. Спочатку йде застосування протоколу GMW до рівності альтернованих трилінійних форм для отримання протоколу ідентифікації (або Сігма протоколу). Далі йде застосування перетворення Фіат – Шаміра до протоколу ідентифікації.

Базова структура GMW-FS. GMW-FS приймає групову дію і надає схему ЕП.

Групова дія, що лежить в основі ATFE [6]. Нехай G – скінченна група, S – скінченна множина, а $\alpha: G \times S \rightarrow S$ – груповая дія. Припускається, що елементи цих груп та множини

ефективно представлені в алгоритмах, α може бути ефективно обчислено та елементи з G та S можуть бути ефективно відібрано випадковим чином.

Схема ALTEQ отримується шляхом інстанціювання групової дії $\alpha : G \times S \rightarrow S$ наступним чином.

Параметри для групової дії ATFE.

1. n : розмірність векторного простору.

2. q : порядок кінечного поля.

Визначення групової дії ATFE.

1. Група $G \in \text{GL}(n, q)$, загальна лінійна група над скінченним полем порядку q .

2. Набір S є набором альтернуючих трилінійних форм $\text{ATF}(n, q) := \{ \phi : \mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^n \rightarrow \mathbb{F}_q \}$,

де ϕ є трилінійним (лінійним в кожному аргументі)

та альтернуючим (ϕ прирівнюється до 0 коли два аргументи ідентичні).

3. Дія α визначається наступним чином. Для $A \in \text{GL}(n, q)$ та $\phi \in \text{ATF}(n, q)$,

$\phi \circ A$ становить альтернуючу трилінійну форму

визначену $(\phi \circ A)(u, v, w) = \phi(A^t(u), A^t(v), A^t(w))$.

Нотація. Для $n \in \mathbb{N}^c$, $[n] := \{1, 2, \dots, n\}$. Нотація \leftarrow_R позначає рівномірну випадкову вибірку; наприклад $g \leftarrow_R G$ позначає, що g є рівномірною випадковою виборкою з G .

Параметри для базової структури GMW-FS.

1. $C = 2^c$: Число наборів елементів в якості відкритого ключа та число груп елементів в якості секретного ключа.

2. r : Число раундів схеми.

Генерація ключів.

1. $s_1 \leftarrow_R S$.

2. $g_1 := Id$, елемент ідентичності в групі G .

3. $g_2, \dots, g_C \leftarrow_R G$

4. Для $i = 2, \dots, C$, $s_i := \alpha(g_i, s_1)$.

5. Відкритий ключ $(s_1, \dots, s_C) \in S^C$.

6. Секретний ключ $(g_1, \dots, g_C) \in G^C$.

Алгоритм генерації ключів ЕП ALTEQ [7] наведено на рис. 1.

Input: The variable number $n \in \mathbb{N}$, a prime power q , the alternating trilinear form number $C + 1$.

Output: Public key: $C + 1$ alternating trilinear forms $\phi_i \in \text{ATF}(n, q)$ such that $\phi_i \cong \phi_j$ for any $i, j \in \{0, \dots, C\}$.

Private key: C matrices A_0, \dots, A_{C-1} , such that $\phi_i \circ A_i = \phi_C$.

1 Randomly sample an alternating trilinear form $\phi_C : \mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^n \rightarrow \mathbb{F}_q$.

2 Randomly sample C invertible matrices, $A_0, \dots, A_{C-1} \in \text{GL}(n, q)$.

3 For every $i \in \{0, \dots, C - 1\}$, $\phi_i \leftarrow \phi_C \circ A_i$.

4 For every $i \in \{0, \dots, C - 1\}$, $A_i \leftarrow A_i^{-1}$.

5 **return** Public key: $\phi_0, \phi_1, \phi_2, \dots, \phi_C$. Private Key: A_0, \dots, A_{C-1} .

Рис. 1. Алгоритм генерації ключів ЕП ALTEQ

Підпис. Нехай M – підписуване повідомлення. Нехай $H : \{0,1\}^* \rightarrow \{0,1\}^l$ – геш-функція, де $l = r \cdot c$.

1. Для $i \in [r]$, $h_i \leftarrow_R G$. Нехай $t_i := \alpha(h_i, s_i)$.

2. Нехай $L := H(M | t_1 | \dots | t_r) \in \{0, 1\}^l$.

L розділяється на r c -бітних рядків, наприклад $L = b_1 | \dots | b_r$, де $b_i \in \{0, 1\}^c$.

3. Для $i \in [r]$, нехай $f_i := h_i \cdot g_{b_i}^{-1}$.

4. Підпис $(b_1, \dots, b_r, f_1, \dots, f_r)$.

Варто зауважити, що $\alpha(f_i s_{b_i}) = \alpha(h_i \cdot g_{b_i}^{-1}, s_{b_i}) = \alpha(h_i, \alpha(g_{b_i}^{-1}, s_{b_i})) = \alpha(h_i, s_i) = t_i$.

Алгоритм генерації підпису ЕП ALTEQ [7] наведено на рис. 2.

Input: The public key $\phi_0, \dots, \phi_C \in \text{ATF}(n, q)$. The private key $A_0, \dots, A_{C-1} \in \text{GL}(n, q)$. $r, C, \lambda \in \mathbb{N}$.
Let $A_C = I$, the identity matrix. The message M . A hash function $H : \{0, 1\}^* \rightarrow \{0, 1\}^{2\lambda}$. An expander $\text{Expand} : \{0, 1\}^{2\lambda} \rightarrow \{a_i\}_{i \in \{0, \dots, r-1\}}$, where $a_i \in \{0, \dots, C\}$.

Output: The signature S on M .

```
1 for  $i \in \{0, \dots, r-1\}$  do
2   | Randomly sample  $B_i \in \text{GL}(n, q)$ .
3   |  $\psi_i \leftarrow \phi_C \circ B_i$ .
4 end
5 Compute  $\text{cha} = H(M | \psi_0 | \dots | \psi_{r-1}) \in \{0, 1\}^{2\lambda}$ .
6  $(b_0, \dots, b_{r-1}) \leftarrow \text{Expand}(\text{cha})$ 
7 for  $i \in \{0, \dots, r-1\}$  do
8   |  $D_i \leftarrow A_{b_i} B_i$ ; // Note that  $\phi_{b_i} \circ D_i = \psi_i$ .
9 end
10 return  $S = (\text{cha}, D_0, \dots, D_{r-1})$ .
```

Рис. 2. Алгоритм генерації підпису ЕП ALTEQ

Перевірка. Перевірювач отримує повідомлення M та підпис $(b_1, \dots, b_r, f_1, \dots, f_r)$.

1. Для $i \in [r]$, нехай $t'_i := \alpha(f_i, s_{b_i})$.

2. Нехай $L' := H(M | t'_1 | \dots | t'_r)$.

3. Прийняти якщо L' ідентично $L = b_1 | \dots | b_r$. В іншому випадку відхилити.

Алгоритм перевірки підпису ЕП ALTEQ [7] наведено на рис. 3.

Input: The public key $\phi_0, \dots, \phi_C \in \text{ATF}(n, q)$. The signature $S = (\text{cha}, D_0, \dots, D_{r-1})$, $b_i \in \{0, \dots, C\}$, $D_i \in \text{GL}(n, q)$. The message M . A hash function $H : \{0, 1\}^* \rightarrow \{0, 1\}^{2\lambda}$. An expander $\text{Expand} : \{0, 1\}^{2\lambda} \rightarrow \{a_i\}_{i \in \{0, \dots, r-1\}}$, where $a_i \in \{0, \dots, C\}$.

Output: “Yes” if S is a valid signature for M . “No” otherwise.

```
1 for  $i \in \{0, \dots, r-1\}$  do
2   | Compute  $\psi'_i = \phi_{b_i} \circ D_i$ .
3 end
4 Compute  $\text{cha}' = H(M | \psi'_0 | \dots | \psi'_{r-1}) \in \{0, 1\}^{2\lambda}$ .
5  $(b'_0, \dots, b'_{r-1}) \leftarrow \text{Expand}(\text{cha}')$ 
6 if for every  $i \in \{0, \dots, r-1\}$ ,  $b_i = b'_i$  then
7   | return Yes
8 else
9   | return No
```

Рис. 3. Алгоритм перевірки підпису ЕП ALTEQ

Реалізація схеми ALTEQ включає декілька заходів для підвищення продуктивності системи.

У схемі впроваджено незбалансовані виклики. В протоколі ідентифікації GMW кількість викликів встановлюється на певне значення, так що відповідь складає випадкову матрицю,

що розгортається з короткого seed, котрий призначений для передачі (таким чином досягається скорочення підпису). З іншого боку, впровадження такого seed призводить до збільшення кількості раундів, а отже і збільшення часу підпису та перевірки.

Заявлено два варіанти підпису: Balanced з малим відкритим ключем та звичайним підписом та ShortSig з коротким підписом (розмір відкритого ключа значно більший).

Запропоновано набори параметрів для категорій безпеки NIST I та III, а також виділено орієнтовний набір параметрів для категорії безпеки NIST V. Загальносистемні параметри для схеми наведено в табл. 1 [6].

Таблиця 1

Загальносистемні параметри для схеми ЕП ALTEQ (біт)

Категорія безпеки NIST	Режим	Параметри (n, q, r, K, C)	Секретний ключ	Відкритий ключ	Підпис
I	Збалансований	$(13, 2^{32} - 5, 84, 22, 7)$	128	64192	127168
	Короткий підпис	$(13, 2^{32} - 5, 16, 14, 458)$	128	4191744	76224
III	Збалансований	$(20, 2^{32} - 5, 201, 28, 7)$	192	255552	392000
	Короткий підпис	$(20, 2^{32} - 5, 39, 20, 229)$	192	8354112	260032
V	Збалансований	$(25, 2^{32} - 5, 119, 48, 8)$	256	589056	978688
	Короткий підпис	$(25, 2^{32} - 5, 67, 25, 227)$	256	16707456	511264

В ході першого раунду конкурсу зі стандартизації додаткових схем ЕП було виявлено недоліки в схемі підпису ALTEQ, що призвело до розробки нової версії у відповідь на критику та наведені вектори та приклади атак.

Маркку – Джухані О. Саарінен [8] було наведено приклад атаки на підробку підпису, що базується на зниженні складності підробки за умови, що частини підпису "seed_i" та "D_i" встановлено нулями, притому, що підпис складається з трьох частин cha, seed_i, D_i. Сама атака складається із знаходження відповідного результуючого значення функції expandChallenge() в зменшеному просторі.

В результаті розробниками було додано перевірку зворотності матриць в процесі перевірки підпису та покращено швидкодію на ~2x для процедури перевірки для збалансованого варіанту та ~4x для варіанту з коротким підписом, що в поєднанні з незначним прискоренням процедури підпису та процедури генерації ключів в частини наборів параметрів не призвело до загального зниження швидкодії через додавання перевірки зворотності матриць.

Далі розглянемо **eMLE-Sig 2.0**.

eMLE-Sig 2.0 є схемою ЕП, що ґрунтується на новій, оптимізованій для практичного застосування версії проблеми eMLE (англ. Embedded Multilayer Equations) та базується на алгебраїчних решітках. Заявлено покращення безпеки та ефективності нової eMLE у порівнянні зі звичайною. Особливу увагу автори звернули на атаку редуції решіток, запропоновану Пенні Лоренц, яку було застосовано до попередньої версії схеми eMLE.

Сутність проблеми eMLE полягає в наступному [9]: Нехай d позначає кількість шарів в eMLE, а p – перелік з d цілих чисел, що виступають в якості модулів для кожного шару. Таким чином, для нижнього шару модулем виступає $p[0]$, для верхнього $p[d-1]$. Всі числа в p – взаємно прості, а $p[i] < p[j]$ для $0 \leq i < j < d$. Нехай n – ціле число, що визначає вимірність векторів.

Приклад нового запропонованого eMLE з трьома шарами (тобто $d = 3$), де відкритими є лише $h \in \mathbb{Z}_{p[2]}^n$ та $g_l \in \mathbb{Z}_{p[l]}^n (l \in \{0, 1, 2\})$

$$h = g_2 \otimes x + h_1 \bmod p[2]$$

$$h_1 = (g_1 \otimes x + h_0 \bmod p[1]) + k_1 * p[1]$$

$$h_0 = (g_0 \otimes x \bmod p[0]) + k_0 * p[0]$$

Тут оператор \otimes позначає результат згортки двох векторів.

Нотація [9, 10]:

- n : вимірність за замовчуванням для всіх векторів;
- d : кількість шарів в eMLE (в поданні на конкурс зафіксовано як 3);
- p : перелік з d цілих взаємно простих чисел, з $p[l]$ в якості модуля для шару l при $0 \leq l \leq d-1$;
- G : перелік з d векторів, з $G[l]$ використовується для побудування значення шару l ;
- x_max : ціле число, що вказує на максимальні абсолютні значення елементів секретного вектору x ;
- c_max : ціле число, що обмежує елементи у змагальному векторі, що використовується у підписанні та верифікації алгоритмів;
- vc : перелік, що складається з чотирьох цілих чисел, що використовується для перевірки розмірів значень при перевірці підпису;
- H : геш-функція, нахшталт SHA3-256.

Алгоритм генерації ключів ЕП eMLE-Sig 2.0 [10] наведено на рис. 4.

```

input :  $n, d, x\_max, c\_max, p, G$ 
output:  $x_1, x_2, F_1, F_2, h_1, h_2, pkh$ 

1 while true do
2    $x_1 \leftarrow [-x\_max, x\_max]^n$ 
3    $x_2 \leftarrow [-x\_max, x\_max]^n$ 
4    $sumX = \sum_{i=0}^{n-1} (x_1[i] + x_2[i])$ 
5   if  $|sumX| < \frac{n}{2}$  then
6     | break
7   end
8 end
9 while true do
10   $h_1, F_1, sumR_1 = eMLE(n, d, c\_max, p, G, x_1, G[1], 0)$ 
11   $h_2, F_2, sumR_2 = eMLE(n, d, c\_max, p, G, x_2, G[1], 0)$ 
12  if  $|sumR_1 + sumR_2| < n * n$  then
13    | break
14  end
15 end
16  $pkh = \mathcal{H}(h_1, h_2)$ 
17 return  $x_1, x_2, F_1, F_2, h_1, h_2, pkh$ 

```

Рис. 4. Алгоритм генерації ключів ЕП eMLE-Sig 2.0

Алгоритм генерації підпису ЕП eMLE-Sig 2.0 [10] наведено на рис. 5.

```

input :  $n, d, x\_max, c\_max, p, G, vc, x_1, x_2, F_1, F_2, pkh, m, mlen$ 
output:  $u, s$ 

1 Let  $sumXn$  be the sum of negative integers in  $x_1$  and  $x_2$ 
2 Let  $sumXp$  be the sum of positive integers in  $x_1$  and  $x_2$ 
3  $c'_1, c'_2 = \text{hashVec}(n, c\_max, m, mlen, \text{null}, pkh)$ 
4 while true do
5   if  $sumXp > |sumXn|$  then
6      $y\_min \leftarrow \left[ \left\lfloor \frac{|sumXn| * c\_max}{10} \right\rfloor, \left\lfloor \frac{|sumXn| * c\_max}{8} \right\rfloor \right]$ 
7      $y\_gap \leftarrow \left[ \left\lfloor \frac{sumXp * c\_max}{7} \right\rfloor, \left\lfloor \frac{sumXp * c\_max}{5} \right\rfloor \right]$ 
8   else
9      $y\_min \leftarrow \left[ \left\lfloor \frac{|sumXn| * c\_max}{7} \right\rfloor, \left\lfloor \frac{|sumXn| * c\_max}{5} \right\rfloor \right]$ 
10     $y\_gap \leftarrow \left[ \left\lfloor \frac{sumXp * c\_max}{10} \right\rfloor, \left\lfloor \frac{sumXp * c\_max}{8} \right\rfloor \right]$ 
11  end
12   $y \leftarrow [y\_min, \left\lfloor \frac{n * x\_max * c\_max}{2} \right\rfloor - y\_gap]^n$ 
13   $u, F, \_ = \text{eMLE}(n, d, c\_max, p, G, y, c'_1 + c'_2, 1)$ 
14   $c_1, c_2 = \text{hashVec}(n, c\_max, m, mlen, u, pkh)$ 
15   $s = x_1 \otimes c_1 + x_2 \otimes c_2 + y$ 
16   $v = \text{check}(n, d, x\_max, c\_max, p, G, vc, F_1, F_2, F, s, c_1, c_2, c'_1 + c'_2)$ 
17  if  $v = \text{true}$  then
18    break
19  end
20 end
21 return  $s, u$ 

```

Рис. 5. Алгоритм генерації підпису ЕП eMLE-Sig 2.0

Алгоритм перевірки підпису ЕП eMLE-Sig 2.0 [10] наведено на рис. 6.

```

input :  $n, d, x\_max, c\_max, p, G, vc, h_1, h_2, s, u, m, mlen$ 
output: true or false

1  $pkh = \mathcal{H}(h_1, h_2)$ 
2  $c'_1, c'_2 = \text{hashVec}(n, c\_max, m, mlen, \text{null}, pkh)$ 
3  $c_1, c_2 = \text{hashVec}(n, c\_max, m, mlen, u, pkh)$ 
4  $v = \text{checkS}(n, d, x\_max, c\_max, vc, s)$ 
5  $t = h_1 \otimes c_1 + h_2 \otimes c_2 + u \text{ mod } p[d - 1]$ 
6 for  $l = d - 1$  to 0 do
7   if  $l = 0$  then
8      $g = G[1] \otimes (c_1 + c_2) \text{ mod } p[0]$ 
9      $k = \frac{t - (G[0] \otimes (s + g + c'_1 + c'_2) \text{ mod } p[0])}{p[0]}$ 
10     $a = \left\lfloor \frac{\sum_{i=0}^{n-1} k[i]}{n} \right\rfloor$ 
11     $k = k - \mathbf{1} * a$ 
12     $v = v \text{ and } (\sum_{i=0}^{n-1} (k[i] * k[i]) \geq vc[2]) \text{ and } (\sum_{i=0}^{n-1} (k[i] * k[i]) \leq vc[3])$ 
13     $t = t - G[l] \otimes (s + g + c'_1 + c'_2) \text{ mod } p[l]$ 
14  else
15     $t = t - G[l] \otimes s \text{ mod } p[l]$ 
16  end
17 end
18  $v = v \text{ and } (t = 0)$ 
19 return  $v$ 

```

Рис. 6. Алгоритм перевірки підпису ЕП eMLE-Sig 2.0

Авторами заявлено, що ця версія eMLE у порівнянні зі старою версією має підвищені безпеку та ефективність за рахунок таких факторів [9]:

- рандомізація внутрішніх шарів h_1 та h_0 за рахунок рандомізованих шумів k_1 та k_0 . За рахунок використання в них більших рандомізованих цілих чисел очікуваний вектор рішень збільшується у просторі розв'язку;
- використання згортки векторів в кожному шарі дозволяє збільшити розмірність векторів (збільшити n) без збільшення розмірів підпису;
- секретний вектор x може бути зконфігурований таким чином, щоб в ньому були менші значення для зменшення розмірів підпису та підвищення стійкості.

Запропоновано набори загальносистемних параметрів для відповідних категорій безпеки NIST наведені в табл. 2 [10].

Таблиця 2

Загальносистемні параметри для схеми ЕП eMLE-Sig 2.0 (біт)

Категорія безпеки NIST	n	d	x_{max}/c_{max}	vc	p	G	Секретний ключ	Відкритий ключ	Підпис
I	64	3	4	vc64	[5,557, 67108864]	GG64	6400	3328	2240
III	96	3	4	vc96	[5,823, 268435456]	GG96	9600	5376	3648
V	128	3	4	vc128	[5,1097, 1073741824]	GG128	12800	7680	5120

В ході першого раунду конкурсу зі стандартизації додаткових схем ЕП було виявлено недоліки в схемі підпису eMLE-Sig 2.0, що призвело до доробки схеми підпису у відповідь на критику та наведені вектори та приклади атак. Незважаючи на це, було наведено приклади успішних атак на актуальну версію підпису та визнано схему недостатньо захищеною від витіку секретного ключа в підписах. Тібоучі запропонував атаку на основі цього, а Лоренц реалізував програмне забезпечення для здійснення атаки [11].

Розглянемо ЕП **KAZ-SIGN**.

Kriptografi Atasi Zarah Digital Signature (KAZ-SIGN) ґрунтується на математичній проблемі 2-DLP (з англ. – проблема дискретного логарифму другого порядку), яка ще потребує більш детального криптоаналізу для визначення потенційної стійкості як до класичного, так і квантового криптоаналізу [12, 13]. Ідея полягає в складності відтворення DLP (проблеми дискретного логарифму) з відомого параметру для отримання секретного параметру. KAZ-SIGN спрямований на отримання квантової стійкості з короткими ключами та підписами та високою швидкістю виконання за умови використання простої математики для отримання потенційного кандидата для легкого переходу сучасного програмного та апаратного забезпечення.

Сутність проблеми 2-DLP можна пояснити наступним чином [12]: нехай N – складене число, g – випадкове просте число з \mathbb{Z}_N порядку G_g , де $G_g \approx N^\delta$ щонайбільше для $\delta \in (0,1)$ та $\delta \rightarrow 0$. Потрібно обрати випадкове просте число $Q \in \mathbb{Z}_{\phi(N)}$ порядку G_Q , де $G_Q \approx \phi(N)^\varepsilon$ для $\varepsilon \rightarrow 1$. Тобто, обрати Q великого порядку з $\mathbb{Z}_{\phi(N)}$. Таке Q має власний натуральний порядок із $\mathbb{Z}_{\phi(G_g)}$. Цей порядок буде позначено як G_{Qg} . Відношення може бути відображено як $Q^{G_{Qg}} \equiv 1 \pmod{G_g}$ та $\phi(N) \equiv 0 \pmod{G_g}$.

Після цього обирається випадкове ціле число $x \in \mathbb{Z}_{\phi(G_g)}$, де $x \approx \phi(G_g)$. З рівняння

$$g^{Q^x \pmod{\phi(N)}} \equiv A \pmod{N} \quad (1)$$

проблему дискретного логарифму (DLP) вирішено за поліноміальний час на класичному комп'ютері та отримано значення X при відсутності еквівалентності $Q^x \equiv X \pmod{\phi(N)}$ та при виконанні $g^X \equiv A \pmod{N}$.

2-DLP полягає в тому, що при заданих значеннях (A, g, N, Q) потрібно визначити $x \in \phi(G_g)$ при $x \approx \phi(G_g)$ такому, що виконується (1).

Алгоритм генерації ключів ЕП KAZ-SIGN [13] наведено на рис. 7.

Input: System parameters $(g, n, n_{\phi(G_g)}, N, \phi(N), \phi(\phi(N)), R, G_g)$

Output: Public verification key, V , and private signing key, α

- 1: Choose random $\alpha \in (2^{n_{\phi(G_g)}-2}, 2^{n_{\phi(G_g)}-1})$.
 - 2: Compute verification key, $V \equiv g^{R\alpha \pmod{\phi(N)}} \pmod{N}$.
 - 3: Compute the discrete logarithm $v = \text{DLog}_g(V \pmod{N})$.
 - 4: Compute $z_1 = v - R\alpha \pmod{\phi(N)}$.
 - 5: **if** $z_1 \equiv 0 \pmod{\phi(N)}$ **then**
 - 6: repeat steps 1 till 4.
 - 7: **else** continue step 9
 - 8: **end if**
 - 9: Compute the discrete logarithm $z_2 = \text{DLog}_R(v \pmod{\phi(N)})$.
 - 10: **if** z_2 has a solution **then**
 - 11: repeat steps 1 till 9.
 - 12: **else** continue step 14
 - 13: **end if**
 - 14: Output public verification key V and private signing key α .
-

Рис. 7. Алгоритм генерації ключів ЕП KAZ-SIGN

Алгоритм генерації підпису ЕП KAZ-SIGN [13] наведено на рис. 8.

Input: System parameters $(g, n, n_{\phi(G_g)}, N, \phi(N), \phi(\phi(N)), R, G_g)$, private signing key, α , and message to be signed, $m \in \mathbb{Z}_N$

Output: Signatures, (S_1, S_2) , salt, σ .

- 1: Generate a random salt, $\sigma \in \{0, 1\}^{32}$ corresponding to message, m .
- 2: Compute the hash value of the message, $h = H(m \parallel \sigma)$.
- 3: Choose random ephemeral prime $r \in (2^{n_{\phi(G_g)}-2}, 2^{n_{\phi(G_g)}-1})$.
- 4: Compute $S_0 \equiv g^{Rr} \pmod{\phi(N)}$ (mod N).
- 5: Compute the discrete logarithm $S_1 = \text{DLog}_g(S_0 \pmod{N})$.
- 6: Compute $z_3 = S_1 - Rr \equiv 0 \pmod{\phi(N)}$.
- 7: **if** $z_3 = S_1 - Rr \equiv 0 \pmod{\phi(N)}$ **then**
- 8: Repeat steps 3 till 6.
- 9: **else** Continue step 11
- 10: **end if**
- 11: Compute the discrete logarithm $z_4 = \text{DLog}_R(S_1 \pmod{\phi(N)})$.
- 12: **if** z_4 has a solution **then**
- 13: Repeat steps 3 till 11.
- 14: **else** Continue step 16
- 15: **end if**
- 16: Compute $S_2 \equiv (\alpha + h)r^{-1} \pmod{\phi(\phi(N))}$.
- 17: Compute the discrete logarithm $v = \text{DLog}_g(V \pmod{N})$.
- 18: Compute the discrete logarithm $S_{2f} = \text{DLog}_{S_1}(vR^h \pmod{\phi(N)})$.
- 19: **if** $S_2 \equiv S_{2f} \pmod{\phi(\phi(N))}$ **then**
- 20: Repeat steps 3 till 18
- 21: **else** Continue step 23.
- 22: **end if**
- 23: Compute $\alpha_F = \text{DLog}_R(v \pmod{G_g})$.
- 24: Compute $W_0 \equiv (\alpha_F + h)S_2^{-1} \pmod{\phi(\phi(N))}$.
- 25: **if** W_0 does not exist **then**
- 26: Repeat steps 1 till 24.
- 27: **else** Continue 29.
- 28: **end if**
- 29: Compute $w_1 \equiv g^{S_1} \pmod{N}$.
- 30: Compute $w_2 \equiv g^{R^{W_0}} \pmod{\phi(N)}$ (mod N).
- 31: **if** $w_1 = w_2$ **then**
- 32: Repeat steps 1 till 30.
- 33: **else** Continue 35.
- 34: **end if**
- 35: Output signature (S_1, S_2) , salt, σ and destroy r .

Рис. 8. Алгоритм генерації підпису ЕП KAZ-SIGN

Кроки 17, 18, 19 та 20 процедури підписання утворюють процедуру виявлення підробки ЕП KAZ-SIGN type-1.

Кроки 23, 24, 25, 26, 27, 28, 29, 30, 31 та 32 становлять процедуру виявлення придатності параметрів KAZ-SIGN.

Алгоритм перевірки підпису ЕП KAZ-SIGN [13] наведено на рис. 9.

Input: System parameters $(g, n, n_{\phi(G_g)}, N, \phi(N), \phi(\phi(N)), R, G_g)$, public verification key, V , message, m , signatures, (S_1, S_2) and salt corresponding to M , σ .

Output: Accept or reject

- 1: Compute the hash value of the message and its corresponding salt, σ to be verified, $h = H(m || \sigma)$.
- 2: Compute the discrete logarithm $v = \text{DLog}_g(V \pmod{N})$.
- 3: Compute the discrete logarithm $S_{2f} = \text{DLog}_{S_1}(vR^h \pmod{\phi(N)})$.
- 4: **if** $S_2 \equiv S_{2f} \pmod{\phi(\phi(N))}$ **then**
- 5: reject signature \perp
- 6: **else** continue step 9
- 7: **end if**
- 8: Compute $\alpha_F = \text{DLog}_R(v \pmod{G_g})$.
- 9: Compute $W_0 \equiv (\alpha_F + h)S_2^{-1} \pmod{\phi(\phi(N))}$.
- 10: Compute $w_1 \equiv g^{S_1} \pmod{N}$.
- 11: Compute $w_2 \equiv g^{R^{W_0} \pmod{\phi(N)}} \pmod{N}$.
- 12: **if** $w_1 = w_2$ **then**
- 13: reject signature \perp
- 14: **else** continue step 16
- 15: **end if**
- 16: Compute $y_1 \equiv g^{S_1^{S_2} \pmod{\phi(N)}} \pmod{N}$.
- 17: Compute $y_2 \equiv v^{R^h \pmod{\phi(N)}} \pmod{N}$.
- 18: **if** $y_1 = y_2$ **then**
- 19: accept signature
- 20: **else** reject signature \perp
- 21: **end if**

Рис. 9. Алгоритм перевірки підпису ЕП KAZ-SIGN

Кроки 2, 3, 4 та 5 в процедурі перевірки утворюють процедуру виявлення підробки ЕП KAZ-SIGN type-1.

Кроки 8, 9, 10, 11, 12 та 13 утворюють процедуру виявлення підробки ЕП KAZ-SIGN type-2.

Складність вирішення 2-DLP може бути описана наступним чином [13].

Нехай $n_{\phi(G_g)} = \ell(\phi(G_g))$. Складність отримання x становить $O\left(2^{n_{\phi(G_g)}}\right)$. За умови застосування алгоритму Гровера на квантовому комп'ютері, складність отримання x становить $O\left(2^{\frac{n_{\phi(G_g)}}{2}}\right)$. Іншими словами, так як $\phi(G_g) \approx G_g \approx N^\delta$, складність отримання x становить $O(N^\delta)$. За умови застосування алгоритму Гровера на квантовому комп'ютері, складність отримання x становить $O\left(N^{\frac{\delta}{2}}\right)$.

Запропоновані авторами набори загальносистемних параметрів для відповідних категорій безпеки NIST [12] наведено в табл. 3.

Загальносистемні параметри для схеми ЕП KAZ-SIGN (біт)

Категорія безпеки NIST	Число простих множників в P, j	Рівень безпеки, k	Довжина параметра N	Розмір ключа, (V, N)	Розмір підпису (S_1, S_2)	Розмір ключа ЕК
I	68	128	458	916	590	256
III	100	192	738	1476	930	384
V	125	256	970	1940	1220	521

В ході першого раунду конкурсу зі стандартизації додаткових схем ЕП було виявлено недоліки в схемі підпису KAZ-SIGN, що призвело до розробки чотирьох оновлень схеми підпису у відповідь на критику та наведені вектори та приклади атак (зокрема Бернштейном [14]). Незважаючи на це, було наведено приклади успішних атак з підпису на актуальну версію підпису. Атака створює підпис для будь-якого бажаного повідомлення з будь-яким відкритим ключем і перевіряє, чи підпис проходить перевірку за допомогою еталонної реалізації. Стверджується, що атака працює для всіх 100 КАТ у каталогах kaz1509, kaz2321 і kaz3241.

Xifrat1-Sign.I є схемою ЕП, що входить до сімейства крипто алгоритмів, що ґрунтуються на використанні випадково згенерованих абелевих квазігруп з 16 елементів та передбачає створення трьох шарів абелевих квазігруп зі зростаючим розміром. В рамках Xifrat1-Sign.I передбачається використання геш-функції з безпекою 256 біт та виводом 768 біт, дві половини якого оброблюються Dup-функцією.

Також автори заявляють про подвоєння безпеки проти атак "грубої сили" проти Dup-функції з 192 біт до 384 біт.

Авторами Xifrat1-Sign.I передбачається лише категорія безпеки NIST III [15].

У схемі підпису використовується геш-функція, створена на основі XOF SHAKE-256. Її початкові вихідні дані у розмірі 768 біт інтерпретуються як 12 64-бітних не підписаних цілих чисел малого порядку. Ця геш-функція позначається як $Hx_{768}(m)$.

Алгоритм генерації ключів ЕП Xifrat1-Sign.I [16] зводиться до наступного:

1. Рівномірно випадково згенерувати 3 криптограми: c , k та q .
2. Обчислити $p_1 = D(c, k)$, $p_2 = D(k, q)$,
3. Повернути відкритий ключ $pk = (c, p_1, p_2)$ та секретний ключ $sk = (c, k, q)$.

Алгоритм генерації підпису ЕП Xifrat1-Sign.I [16] зводиться до наступного:

1. Вхідні дані: m – повідомлення
2. Обчислити $h = Hx_{768}(m)$,
3. Обчислити $s = D(h, q)$,
4. Повернути s .

Алгоритм перевірки підпису ЕП Xifrat1-Sign.I [16] зводиться до наступного:

1. Вхідні дані: m – повідомлення, S – підпис
2. Обчислити $h = Hx_{768}(m)$,
3. Обчислити $t_1 = D(p_1, s)$,
4. Обчислити $t_2 = D(D(c, h), p_2)$,
5. Якщо $t_1 = t_2$ повернути [VALID]; у іншому випадку повернути [INVALID].

Доказом коректності схеми полягає в наступному:

$$t_1 = D(p_1, s) = D(D(c, k), D(h, q))$$

$$t_2 = D(D(c, h), p_2) = D(D(c, h), D(k, q))$$

За обмеженою комутативністю $t_1 = t_2$.

Запропоновані набори загальносистемних параметрів для категорії безпеки NIST III [15] наведено в табл. 3.

Таблиця 4
Загальносистемні параметри для схеми ЕП Xifrat1-Sign.I (біт)

Параметри	Особистий ключ	Відкритий ключ	Підпис
Xifrat1-Sign.I	3840	2304	768
Варіант з обмеженою безпекою	2560	1536	512

В ході першого раунду конкурсу зі стандартизації додаткових схем ЕП було виявлено недоліки в схемі підпису Xifrat1-Sign.I. Пенні Лоренц в офіційних коментарях [17] наведено приклад атаки, що розраховує секретний ключ з відкритого. Заявлено, що виконання атаки займає 4 хвилини на комп'ютері з 24 ядрами. Атака заснована на тому, що множення квазігруп $x * y$ переписується як $C + Ax + By$, де $+$ позначає абелеву групу, а A та B є комутативними автоморфізмами. У зв'язку з тим, що всі використані функції змішування є афінно-лінійними картами щодо $+$, система, що пов'язує секретний та відкритий ключі, є лінійною і може бути зведена до лінійної алгебри. Через це використана група є ізоморфною до \mathbb{F}_2^4 , що полегшує реалізацію атаки, котра також є актуальною і для загального випадку.

На жаль, жодного рішення для цієї атаки з боку розробників не було надано.

Порівняння підписів за параметрами.

Порівняння підписів можливе за певними параметрами або критеріями. В даному випадку будемо використовувати деякі із безумовних критеріїв.

До безумовних критеріїв [18] відносяться ті критерії, виконання яких для криптопримітиву є обов'язковим, тобто безумовним. Для асиметричних криптоперетворень типу АСШ, ППК та ЕП цілком можна вибрати однакову систему безумовних критеріїв.

До переліку безумовних критеріїв можна віднести наступні:

- 1) $I_{ст.}$ – рівень криптографічної стійкості з використанням безумовних критеріїв;
- 2) $I_{в.к.}$ – можливі довжини відкритого ключа;
- 3) $I_{о.к.}$ – можливі довжини особистого (секретного) ключа;
- 4) $I_{рез.}$ – довжина результату криптоперетворення (збитковість);
- 5) $T_{пр.}$ – складність (швидкість) прямого криптоперетворення;
- 6) $T_{зв.}$ – складність (швидкість) зворотного криптоперетворення;
- 7) $T_{ген.зп.}$ – складність (швидкість) генерування загальних параметрів для відповідного режиму роботи криптоперетворення (у залежності від довжин загальних параметрів та ключів);
- 8) $T_{ген.кл.}$ – складність (швидкість) генерування ключа (ключової пари) у залежності від режиму роботи тощо.

Із наведеного переліку в контексті даної статті будемо розглядати наступні безумовні критерії:

- можливі довжини відкритого ключа;
- можливі довжини особистого (секретного) ключа;
- довжина результату криптоперетворення (збитковість);

Порівняння цих параметрів для наведених схем ЕП наведено у табл. 5 та на рис. 10.

Розміри підпису та ключів (біт)

Параметри	ALTEQ (збалансований)			eMLE-Sig 2.0			KAZ-SIGN			Xifrat1-Sign.1
	I	III	V	I	III	V	I	III	V	III
Особистий ключ	128	192	256	6400	9600	12800	256	384	521	3840
Відкритий ключ	64192	255552	589056	3328	5376	7680	916	1476	1940	2304
Підпис	127168	392000	978688	2240	3648	5120	590	930	1220	768

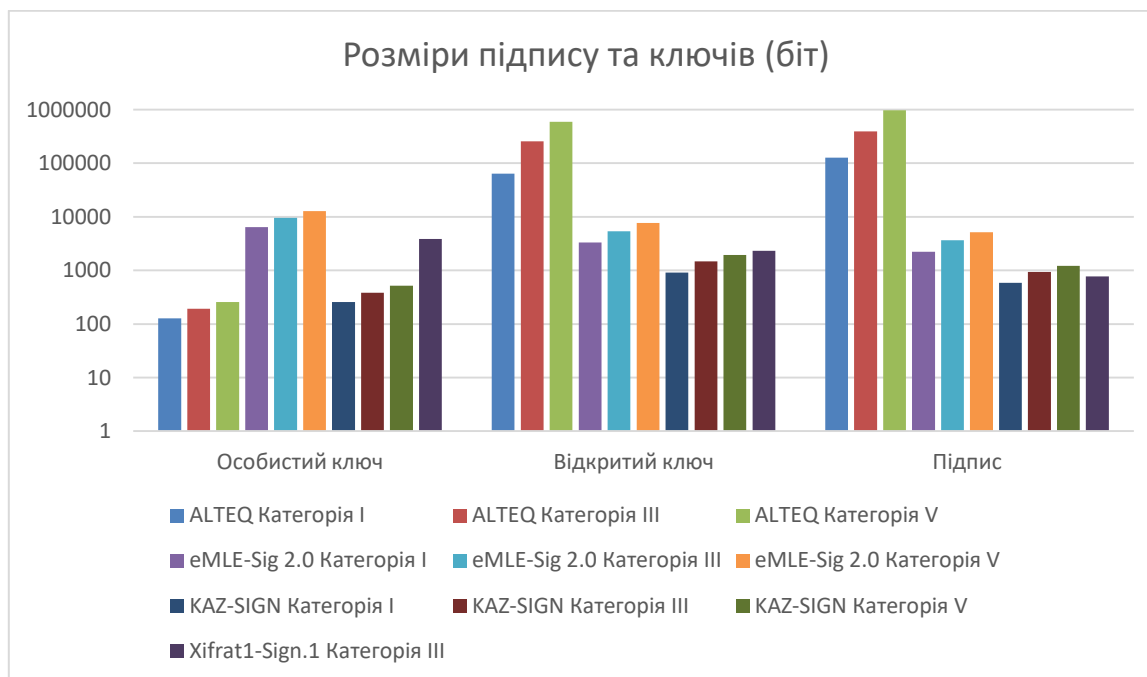


Рис. 10. Розміри підпису та ключів наведених алгоритмів ЕП

З табл. 5 та рис. 10 видно, на що робився більший наголос при розробці схем ЕП. Так, наприклад, ALTEQ явно зосереджено на зведенні до мінімуму розміру особистого ключа, хоча це і призвело до неймовірного збільшення розмірів відкритого ключа та підпису. eMLE-Sig 2.0 та Xifrat1-Sign.1 зводять до мінімуму розмір підпису. KAZ-SIGN має розміри особистого ключа, близькі до розмірів особистого ключа ALTEQ, але розміри відкритого ключа та підпису найменші з усіх порівнюваних.

Таким чином, можна побачити, що наведені схеми можуть використовуватись в різних ситуаціях. Так, наприклад, якщо дуже важливий розмір особистого ключа, але взагалі не важливі розміри відкритого ключа та підпису – цілком доцільним є використання ALTEQ. Якщо, навпаки, неважливий розмір особистого ключа, але важливі інші параметри – краще обрати іншу схему. Якщо дуже важливо звести всі розміри до мінімуму – кращим з наведених варіантів буде KAZ-SIGN.

Важливо зазначити, що таке порівняння за частиною критеріїв не є повним та не враховує затрат швидкодії та захищеність схем ЕП від конкретних атак.

Якщо розширити фокус, то можна побачити, що до кожної з наведених схем підпису було знайдено вектори атак. Додатково вартим уваги є те, що атаки бічними каналами на схеми підпису зазвичай обходять увагою, а навіть якщо на них звертають увагу, то здебільшого в контексті того, що схема підпису або цілком від них незахищена, або захищена тільки від окремих векторів атак бічними каналами, в той час як захищеність від решти навіть не розглядалась.

Висновки

Розглянуто схеми ЕП, що є кандидатами на застосування та стандартизацію в рамках процесу стандартизації додаткових ЕП для квантовостійкої криптографії від NIST. Було розглянуто основні ідеї та проблеми, що використовуються в наведених схемах ЕП для отримання квантової стійкості. Також було проведено порівняння загальносистемних параметрів для різних категорій безпеки NIST.

Так, було виявлено, що не всі кандидати орієнтовані на задоволення всіх категорій безпеки NIST. А саме ЕП Xifrat1-Sign.1 передбачено лише категорію безпеки NIST III.

Також було виявлено зосередженість різних схем ЕП на зменшенні розміру різних параметрів, що призводить до переваг для різних застосувань цих схем. Таким чином, виконується одна із основних задач додаткового раунду відбору, а саме – урізноманітнення набору ЕП для стандартизації.

Окрім підписів, що можуть бути віднесені до категорій: підписи засновані на кодах; підписи на лізогеніях; мультिवаріативні підписи; симетричні підписи; MPC-in-the-head; кандидати, що визначені NIST як "інші" представляють можливі підходи до квантовостійкої стійкості за рахунок використання нових, покращених та перспективних підходів та надають набори параметрів, що задовольняють вимоги NIST за різними категоріями безпеки NIST за умови використання криптографічно адекватних системних параметрів.

Список літератури:

1. Post-Quantum Cryptography PQC. Selected Algorithms 2022 : web-site. URL: <https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022>
2. Post-Quantum Cryptography PQC. Round 4 Submissions. URL: <https://csrc.nist.gov/Projects/post-quantum-cryptography/round-4-submissions>
3. Post-Quantum Cryptography: Digital Signature Schemes. Round 1 Additional Signatures. URL: <https://csrc.nist.gov/projects/pqc-dig-sig/round-1-additional-signatures>
4. Call for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process. URL: <https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/call-for-proposals-dig-sig-sept-2022.pdf>
5. Public Comments on draft FIPS 203. Comment period: August 24, 2023 – November 22, 2023. URL: <https://csrc.nist.gov/files/pubs/fips/203/ipd/docs/fips-203-initial-public-comments-2023.pdf>
6. The ALTEQ Signature Scheme: Algorithm Specifications and Supporting Documentation. ALTEQ Specification Document. URL: <https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/ALTEQ-Spec-web.pdf>
7. Gang Tang, Dung Hoang Duong, Antoine Joux, Thomas Plantard, Youming Qiao, and Willy Susilo. Practical post-quantum signature schemes from isomorphism problems of trilinear forms. In Orr Dunkelman and Stefan Dziembowski, editors, Advances in Cryptology – EUROCRYPT 2022 – 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part III, volume 13277 of Lecture Notes in Computer Science, pages 582–612. Springer, 2022.
8. Official Comments (Round 1 Additional Signatures) – ALTEQ. URL: <https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/official-comments/ALTEQ-round1-dig-sig-official-comment.pdf>
9. eMLE-Sig 2.0: A Signature Scheme based on Embedded Multilayer Equations with Heavy Layer Randomization. eMLE-Sig 2.0 Specification Document. URL: <https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/eMLE-spec-web.pdf>
10. Liu D. Embedded multilayer equations: a new hard problem for constructing post-quantum signatures smaller than RSA (without hardness assumption). IACR Cryptol. ePrint Arch. (2021). URL: <https://eprint.iacr.org/2021/1338>
11. Official Comments (Round 1 Additional Signatures) – eMLE-Sig 2.0. URL: <https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/official-comments/emle-sig2.0-round1-dig-sig-official-comment.pdf>
12. Kriptografi Atasi Zarah Digital Signature (KAZ-SIGN) Algorithm Specifications and Supporting Documentation. KAZ-SIGN Specification Document. URL: <https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/kaz-sign-spec-web.pdf>
13. KAZ-SIGN PQC Digital Signature Scheme. KAZ-SIGN NIST submissions official site. URL: <https://www.antrapol.com/KAZ-SIGN>
14. Official Comments (Round 1 Additional Signatures) – KAZ-SIGN. URL: <https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/official-comments/KAZ-SIGN-round1-dig-sig-official-comment.pdf>

15. NIST Submission: Xifrat1-Sign.I DSS. Xifrat1-Sign.I DSS Specification Document.
URL: <https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/xifrat1-sign-i-spec.pdf>
16. Jianfang "Danny" Niu. Resurrecting Xifrat – Compact Cryptosystems 2ndAttempt.
URL: <https://ia.cr/2022/429>
17. Official Comments (Round 1 Additional Signatures) – Xifrat1-Sign.I.
URL: <https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/official-comments/Xifrat1-Sign-I-round1-dig-sig-official-comment.pdf>
18. Горбенко Ю. І. Науково-методичні основи аналізу, оцінки та результати порівняння існуючих та перспективних (постквантових) асиметричних криптографічних примітивів електронного підпису, протоколів асиметричного шифрування та протоколів інкапсуляції ключів / Ю. І. Горбенко, М. В. Єсіна, В. А. Пономар, І. Д. Горбенко, Є. Ю. Каптьол // Радіотехніка. 2023. Вип. 212. С. 42–65. Режим доступу: http://nbuv.gov.ua/UJRN/rvmnts_2023_212_7.

Надійшла до редколегії 15.11.2023

Відомості про авторів:

Горбенко Іван Дмитрович – д-р техн. наук, проф., Харківський національний університет ім. В.Н. Каразіна, проф. кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, АТ «Інститут Інформаційних Технологій», головний конструктор, Україна; e-mail: gorbenkoi@iit.kharkov.ua; ORCID: <https://orcid.org/0000-0003-4616-3449>

Каптьол Євгеній Юрійович – Харківський національний університет ім. В.Н. Каразіна, аспірант кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, АТ «Інститут Інформаційних Технологій», аналітик із систем захисту інформації, Україна; e-mail: kaptevg@gmail.com; ORCID: <https://orcid.org/0000-0001-8612-2196>

*Є.В. КОТУХ, канд. техн. наук, Г.З. ХАЛІМОВ, д-р техн. наук,
М.В. КОРОБЧИНСЬКИЙ, д-р техн. наук*

МЕТОД НАПРАВЛЕНОГО ШИФРУВАННЯ В КРИПТОСИСТЕМІ MST3 НА ОСНОВІ УЗАГАЛЬНЕНОЇ 2-ГРУПИ СУЗУКІ ТА ГОМОМОРФНОГО ШИФРУВАННЯ

Вступ

Останні розвідки в сфері квантових обчислень суттєво впливають на розробку безпечних криптосистем з відкритим ключем. Одним з основних напрямів у цій області є рішення задачі знаходження спряженого елемента в теорії некомутативних груп і розв'язання проблем введення в групах та напівгрупах.

Проблема складності слова, запропонована Вагнером і Маджаріком [1], була реалізована у декількох криптосистемах. Однією з найбільш вивчених є система, що базується на факторизації в кінцевих групах перестановок і відома як логарифмічна сигнатура [2 – 5].

Magliveras та співавтори [6] у 2008 р. провели всебічний аналіз криптосистеми MST3, визначивши обмеження для логарифмічного підпису і заявивши, що транзитивний логарифмічний підпис не підходить для MST3. У 2009 р. Lemrken та інші описали криптосистему з відкритим ключем MST3, засновану на логарифмічному підписі та 2-групі Сузукі [7]. Криптосистеми на неабелевих групах та їх властивості активно вивчались в [8, 9].

У 2010 р. Сваба та інші [10] проаналізували всі відомі атаки на криптографію MST і створили більш безпечну криптосистему eMST3, включивши секретне гомоморфне накриття. Т. ван Трунг у 2018 р. [11] запропонував загальний метод побудови сильних аперіодичних логарифмічних сигнатур для абелевих p -груп, що є важливим внеском у розвиток і практичне застосування криптосистем MST.

Криптоаналіз схем шифрування на основі проблеми слова з використанням логарифмічних підписів відкрив подальші можливості для вдосконалення [12 – 16]. Як приклад, для криптосистем MST було виявлено їх вразливість до атак на основі виділеного тексту. Це пов'язано з конструктивною особливістю відомих реалізацій MST, яка полягає у наявності відомих текстів і, відповідно, можливості криптоаналізу.

У відповідь на ці виклики було запропоновано безпечну схему шифрування на основі загальної 2-групи Сузукі, яка включає гомоморфне шифрування. Гомоморфне шифрування дозволяє виконувати певні обчислення над зашифрованими даними без необхідності їх розшифровувати, тим самим забезпечуючи додатковий рівень безпеки. Впровадження такої технології у криптосистему MST може значно підвищити її стійкість до різноманітних атак, зокрема атак з виділеним текстом.

Розробка криптосистем MST на основі багатопараметричних некомутативних груп, як зазначено в [17 – 28], відкриває нові можливості для оптимізації параметрів і підвищення секретності криптосистем. Ці системи дозволяють більш гнучко управляти параметрами, необхідними для забезпечення безпеки, що підвищує ефективність і надійність. Узагальнені 2-групи Сузукі, які є багатоваріантними і мають високий груповий порядок порівняно з іншими багатоваріантними групами, є особливо перспективними в цьому контексті. Однак перша реалізація криптосистеми на основі узагальненої 2-групи Suzuki не забезпечувала захист від атак методом грубого перебору з послідовним відновленням ключа. Значний науковий та практичний інтерес має розробка саме підходу на узагальнених Сузукі 2-групах та вдосконалення її криптографічних властивостей.

Узагальнені Сузукі 2-групи

Узагальнення 2-груп Сузукі визначено над скінченним полем F_q , $q = 2^n$, $n > 0$ для натурального числа l та $a_1, a_2, \dots, a_l \in F$ для деякого автоморфізму θ як F [10]:

$$A_l(n, \theta) = \{S(a_1, a_2, \dots, a_l) \mid a_i \in F_q\}$$

Кожен елемент $A_l(n, \theta)$ можна виразити однозначно, і з цього випливає, що $|A_l(n, \theta)| = 2^{nl}$ і $A_l(n, \theta)$ визначають групу порядку 2^{nl} . Якщо $l = 2$, ця група ізоморфна 2-групі Сузукі $A(n, \theta)$.

Групова операція визначається як продукт:

$$S(a_1, a_2, \dots, a_l)S(b_1, b_2, \dots, b_l) = S(a_1 + b_1, a_2 + (a_1\theta)b_1 + b_2, a_3 + (a_2\theta)b_1 + (a_1\theta^2)b_2 + b_3, \dots, a_l + (a_{l-1}\theta)b_1 + \dots + (a_1\theta^{l-1})b_{l-1} + b_l).$$

з елементом тотожності $S(0, 0, \dots, 0)$.

Обернений елемент визначається як

$$S(a_1, a_2, a_3, \dots, a_l)^{-1} = S(a_1, a_2 + a_1\theta a_1, a_3 + a_2\theta a_1 + a_1\theta^2(a_2 + a_1\theta a_1), \dots, a_l + a_{l-1}\theta a_1 + \dots).$$

Група є неабелевою і має нетривіальний центр

$$Z(G) = \{S(0, 0, \dots, c) \mid c \in F_q\}.$$

Припустимо, що θ – це автоморфізм $F, \theta: x \rightarrow x^2$ Фробеніуса. Для фіксованого кінцевого поля $A_l(n, \theta)$ порядок групи більший, ніж у класичній Сузукі 2-групі.

У новій реалізації криптосистеми ми змінили алгоритм шифрування та пропонуємо використовувати гомоморфне шифрування для випадкових накриттів. У цьому випадку складність атаки відновлення ключа буде визначатися шляхом вичерпного пошуку по всій групі.

Метод, що пропонується

Наша пропозиція полягає у створенні логарифмічної сигнатури для всієї узагальненої 2-групи Сузукі та гомоморфного шифрування випадкових накриттів у логарифмічній сигнатурі.

Давайте розглянемо основні етапи шифрування – генерація ключів, шифрування та дешифрування. Для початку етапу генерації ключів фіксуємо велику групу $A_l(n, \theta) = \{S(a_1, a_2, \dots, a_l) \mid a_i \in F_q\}$, $q = 2^n$.

Побудуємо ручні логарифмічні підписи $\beta_k = [B_{1(k)}, \dots, B_{s(k)}] = (b_{ij})_k = S(0, \dots, 0, b_{ij(k)}, 0, \dots, 0)$ типу

$$(r_{1(k)}, \dots, r_{s(k)}), \quad i = \overline{0, s(k)}, \quad j = \overline{1, r_{i(k)}}, \quad b_{ij(k)} \in F_q, \quad k = \overline{1, l}.$$

Встановимо випадкову обкладинку:

$$\alpha_k = [A_{1(k)}, \dots, A_{s(k)}] = (a_{ij})_k = S(a_{ij(k)}^{(1)}, a_{ij(k)}^{(2)}, \dots, a_{ij(k)}^{(l)})$$

того самого типу β_k , де $a_{ij} \in A_l(n, \theta)$, $a_{ij}^{(v)} \in F_q \setminus \{0\}$, $i = \overline{1, s}$, $j = \overline{1, r_{i(k)}}$, $k = \overline{1, l}$.

Виберимо випадкові обкладинки:

$$w_{(k)} = [W_{1(k)}, \dots, W_{s(k)}] = (w_{ij})_{(k)} = S(w_{ij(k)}^{(1)}, w_{ij(k)}^{(2)}, \dots, w_{ij(k)}^{(l)})$$

тих самих типів β_k , де $w_{ij} \in A_l(n, \theta)$, $w_{ij} \in F_q \setminus \{0\}$, $i = \overline{0, s(k)}$, $j = \overline{1, r_{i(k)}}$, $k = \overline{1, l}$.

Згенеруємо випадкові $t_{0(k)}, \dots, t_{s(k)} \in A_l(n, \theta) \setminus Z$, $t_{i(k)} = S(t_{i1(k)}, \dots, t_{i l(k)})$, $t_{ij(k)} \in F^\times$, $i = \overline{0, s(k)}$, $k = \overline{1, l}$.

Виберимо

$$\tau_{0(k)}, \dots, \tau_{s(k)} \in A_l(n, \theta) \setminus Z, \quad \tau_{i(k)} = S(\tau_{i1(k)}, \dots, \tau_{i l(k)}), \quad \tau_{ij(k)} \in F^\times, \quad i = \overline{0, s(k)}, \quad k = \overline{1, l}.$$

Візьмемо $t_{s(k-1)} = t_{0(k)}$, $\tau_{s(k-1)} = \tau_{0(k)}$, $k = \overline{1, l}$.

Визначимо додаткову групову операцію:

$$S(a_1, a_2, \dots, a_l) \circ^{(k)} S(b_1, b_2, \dots, b_l) =$$

$$S(a_1 + b_1, a_2 + b_2, \dots, a_k + b_k, a_{k+1} + a_k^2 b_1 + \dots + a_1^{2^k} b_k + b_{k+1}, \dots, a_l + a_{l-1}^2 b_1 + \dots + a_1^{2^{l-1}} b_{l-1} + b_l).$$

Зворотним елементом $S^{-(k)}$ для групової операції $\circ^{(k)}$ є

$$S^{-(k)}(a_1, a_2, \dots, a_l) = S(a_1, a_2, \dots, a_k, \alpha_{k+1}, \dots, \alpha_l)$$

де

$$\begin{aligned}\alpha_{k+1} &= a_{k+1} + a_k^2 a_1 + \dots + a_2^{2^{k-1}} a_{k-1} + a_1^{2^k} a_k, \\ \alpha_{k+2} &= a_{k+2} + a_{k+1}^2 a_1 + \dots + a_3^{2^{k-1}} a_{k-1} + a_2^{2^k} a_k + a_1^{2^{k+1}} \alpha_{k+1}, \\ &\dots \\ \alpha_l &= a_l + a_{l-1}^2 a_1 + \dots + a_{l-k}^{2^k} a_k + a_{l-k-1}^{2^{k+1}} \alpha_{k+1} + \dots + a_l^{2^{l-1}} \alpha_{l-1}\end{aligned}$$

Застосування додаткової групової операції $\circ^{(k)}$ призводить до гомоморфного представлення елементів групи $S(a_1, a_2, \dots, a_l) \rightarrow S(a_1, a_2, \dots, a_k, \alpha_{k+1}, \dots, \alpha_l) = S^{(k)}$.

Застосуємо обернене гомоморфне перетворення для обернених і прямих елементів S_1^{-k} групи $S_2^{(k)}$ для обчислення в групі з лівим оберненим елементом S_1^{-n} : $S_3 = S_1^{-k} \circ S_2^{(k)}$; для S_1^{-k} маємо:

$$S^{-(k)\circ} = S^\circ(a_1, a_2, \dots, a_k, \alpha_{k+1}, \dots, \alpha_l) = S(\alpha_1, \dots, \alpha_k, \alpha_{k+1}, \dots, \alpha_l),$$

де $\alpha_1 = a_1, \alpha_2 = a_2 + a_1^2 a_1, \dots, \alpha_k = a_k + a_{k-1}^2 a_1 + \dots, a_l^{2^{k-1}} a_{k-1}$ і $S_2^{(k)}$ відповідно до $S_3 = S_1^{-k} \circ S_2^{(k)}$; отримуємо

$$\begin{aligned}S^{(k)\circ} &= S^\circ(b_1, b_2, \dots, b_k, \beta_{k+1}, \dots, \beta_l) = S(\beta_1, \dots, \beta_k, \beta_{k+1}, \dots, \beta_l) \\ \beta_1 &= b_1, \beta_2 = b_2 + a_1^2 (b_1 + a_1), \dots \\ \beta_k &= b_k + a_{k-1}^2 (b_1 + a_1) + \dots, a_l^{2^{k-1}} (b_{k-1} + a_{k-1}).\end{aligned}$$

Гомоморфні перетворення для $S^{-(k)\circ}, S^{(k)\circ}$ необхідні для того, щоб не порушувати групову операцію при обчисленні елементів групи $A_l(n, \theta)$.

Нехай $f(e)$ – гомоморфне криптографічне перетворення відносно додавання $f(a+b) = f(a) + f(b)$ і $e, a, b \in F_q$ – відповідне обернене перетворення $\hat{f}(e) = e$. Обчислюємо накриття логарифмічних сигнатур:

$$h_{(k)} = [h_{1(k)}, \dots, h_{s(k)}] = t_{(i-1)(k)}^{-k} \circ^{(k)} (w_{ij}^{(k)}) \circ^{(k)} (b_{ij}^{(k)}) \circ^{(k)} t_{i(k)}$$

та накриття гомоморфного криптографічного перетворення:

$$g_{(k)} = [g_{1(k)}, \dots, g_{s(k)}] = \tau_{(i-1)(k)}^{-k} \circ^{(k)} f(w_{ij}^{(k)}) \circ^{(k)} \tau_{i(k)},$$

де

$$f(w_{(k)}) = f(w_{ij}^{(k)}) = S(f(w_{ij(k_1)}), f(w_{ij(k_2)}), \dots, f(w_{ij(k_l)})), \quad i = \overline{1, s(k)}, \quad j = \overline{1, r_{(k)}}, \quad k = \overline{1, l}.$$

Вихідним відкритим ключем є (a_k, h_k, g_k) , а закритим ключем $[f, \beta_{(k)}, (t_{0(k)}, \dots, t_{s(k)}), (\tau_{0(k)}, \dots, \tau_{s(k)})]$, $k = \overline{1, l}$ відповідно.

На етапі шифрування виконуємо наступне. Нехай повідомлення буде $x = S(x_1, \dots, x_l)$ і відкритим ключем (a_k, h_k, g_k) , $k = \overline{1, l}$ відповідно. Вибираємо випадковий $R = (R_1, \dots, R_l)$, $R_j, \dots, R_l \in \square_{|F_q|}$.

Обчисліть зашифрований текст y_1, y_2, y_3 як

$$\begin{aligned}y_1 &= \alpha(R) \cdot x = \alpha_1(R_1) \cdot \alpha_2(R_2) \cdots \alpha_l(R_l) \cdot x \\ &= S\left(\sum_{k=1}^l \sum_{i=1, j=R_i(k)}^{s(k)} a_{ij(k)}^{(1)} + x_1, \sum_{k=1}^l \sum_{i=1, j=R_i(k)}^{s(k)} a_{ij(k)}^{(2)} + x_2 + *, \dots, \sum_{k=1}^l \sum_{i=1, j=R_i(k)}^{s(k)} a_{ij(k)}^{(l)} + x_l + *, \right), \\ y_2 &= h(R) = h_1(R_1) \circ^{(1)} (h_2(R_2) \circ^{(2)} \cdots (h_{l-1}(R_{l-1}) \circ^{(l-2)} (h_{l-1}(R_{l-1}) \circ^{(l-1)} h_l(R_l)))) \\ &= S\left(\sum_{k=1}^l \sum_{i=1, j=R_i(k)}^{s(k)} w_{ij(k)}^{(1)} + \sum_{i=1, j=R_i(1)}^{s(1)} \beta_{ij(1)}, \sum_{k=1}^l \sum_{i=1, j=R_i(k)}^{s(k)} w_{ij(k)}^{(2)} + \right. \\ &\quad \left. \sum_{i=1, j=R_i(2)}^{s(2)} \beta_{ij(2)} + *, \dots, \sum_{k=1}^l \sum_{i=1, j=R_i(k)}^{s(k)} w_{ij(k)}^{(l)} + \sum_{i=1, j=R_i(l)}^{s(l)} \beta_{ij(l)} + * \right)\end{aligned}$$

Тут (*) компоненти визначаються перехресними обчисленнями в груповій операції добутку $t_{0(k)}, \dots, t_{s(k)}$ та добутку $w_{(k)}(R_k) + \beta_{(k)}(R_k)$:

$$y_3 = g(R) = g_1(R_1) \circ^{(1)} (g_2(R_2) \circ^{(2)} \dots (g_{l-1}(R_{l-1}) \circ^{(l-2)} (g_{l-1}(R_{l-1}) \circ^{(l-1)} g_l(R_l))) =$$

$$S \left(\sum_{k=1}^l \sum_{i=1, j=R_{i(k)}}^{s(k)} f(w_{ij}^{(1)}) + \sum_{k=1}^l \sum_{i=1, j=R_{i(k)}}^{s(k)} f(w_{ij}^{(2)}) + *, \dots, \right.$$

$$\left. \sum_{k=1}^l \sum_{i=1, j=R_{i(k)}}^{s(k)} f(w_{ij}^{(l)}) + * \right)$$

Тут (*) компоненти визначаються перехресними обчисленнями в груповій операції добутку $\tau_{0(k)}, \dots, \tau_{s(k)}$ та добутку $f(w_{(k)}(R_k))$.

Вихід : зашифрований текст (y_1, y_2, y_3) повідомлення x .

Для дешифрування візьмемо зашифрований текст (y_1, y_2, y_3) і особистий ключ $[f, \beta_{(k)}, t_{i(k)}, \tau_{i(k)}]$, $i = \overline{0, s(k)}$, $k = \overline{1, l}$.

Щоб розшифрувати повідомлення x , потрібно відновити випадкові числа $R = (R_1, R_2, \dots, R_l)$.

Обчислимо

$$D^{(1)}(R) = D^{(1)}(R_1, R_2, \dots, R_l) = t_{0(1)} \circ^{(1)} y_2 \circ^{(1)} t_{s(1)}^{-1} = S \left(\sum_{i=1, j=R_{i(1)}}^{s(1)} w_{ij}^{(1)} + \beta_1(R_1), *, \dots, * \right),$$

$$G^{(1)}(R) = G^{(1)}(R_1, R_2, \dots, R_l) = \tau_{0(1)} \circ^{(1)} y_3 \circ^{(1)} \tau_{s(1)}^{-1} = S \left(\sum_{i=1, j=R_{i(1)}}^{s(1)} f(w_{ij}^{(1)}), *, \dots, * \right),$$

$$D^{(1)}(R)' = D^{(1)}(R) \circ^{(1)} \hat{f}(G^{(1)}(R))^{-1} = S \left(\sum_{i=1, j=R_{i(1)}}^{s(1)} \beta_{ij(1)}, *, * \right)$$

Відновлюємо R_1 з $\beta_{(1)}(R_1) = \sum_{i=1, j=R_{i(1)}}^{s(1)} \beta_{ij(1)}$, використовуючи $\beta_{(1)}(R_1)^{-1}$, оскільки β_1 є простим.

Для подальшого розрахунку необхідно видалити компонент $h_1(R_1)$ від y_2 і $g_1(R_1)$ від y_3 .

Обчислимо

$$y_2^{(1)} = h_1(R_1)^{-1} \circ y_2, \quad y_3^{(1)} = g_1(R_1)^{-1} \circ y_3, \quad D(R)^{(2)} = t_{0(2)} \circ^{(2)} y_2^{(1)} \circ^{(2)} t_{s(2)}^{-1},$$

$$G(R)^{(2)} = \tau_{0(2)} \circ^{(2)} y_3^{(1)} \circ^{(2)} \tau_{s(2)}^{-1},$$

$$D^{(2)}(R)' = D^{(2)}(R) \circ^{(2)} \hat{f}(G^{(2)}(R))^{-1} = S(0, \sum_{i=1, j=R_{i(2)}}^{s(2)} \beta_{ij(2)}, *)$$

і відновлюємо R_2 з $\beta_{(2)}(R_2) = \sum_{i=1, j=R_{i(2)}}^{s(2)} \beta_{ij(2)}$, використовуючи $\beta_{(2)}(R_2)^{-1}$, оскільки β_2 є простим.

Продовжуємо обчислення ітераційно до останнього значення R_l . Маємо такі рекурентні співвідношення для $n = \overline{1, l-1}$:

$$y_2^{(n)} = h_n(R_n)^{-1} \circ y_2^{(n-1)}, \quad y_3^{(n)} = g_n(R_n)^{-1} \circ y_3^{(n-1)},$$

$$D^{(n+1)}(R) = t_{0(n+1)} \circ^{(n+1)} y_2^{(n)} \circ^{(n+1)} t_{s(n+1)}^{-1}, \quad G^{(n+1)}(R) = \tau_{0(n+1)} \circ^{(n+1)} y_3^{(n)} \circ^{(n+1)} \tau_{s(n+1)}^{-1},$$

$$D^{(n+1)}(R)' = D^{(n+1)}(R) \circ^{(n+1)} \hat{f}(G^{(n+1)}(R))^{-1} = S(0, 0, \dots, 0, \sum_{i=1, j=R_{i(n+1)}}^{s(n+1)} \beta_{ij(n+1)}, *)$$

Відновлюємо R_{n+1} з $\beta_{(n+1)}(R_{n+1}) = \sum_{i=1, j=R_{i(n+1)}}^{s(n+1)} \beta_{ij(n+1)}$, використовуючи $\beta_{(n+1)}(R_{n+1})^{-1}$.

Відновлюємо повідомлення $x = a(R_1, R_2, \dots, R_l)^{-1} \cdot y_1$.

Практичні обчислення

Правильність отриманих виразів покажемо на простому прикладі.

Зафіксуємо чотирипараметричну узагальнену групу Сузукі $G = A_4(n, \theta)$ над скінченним полем F_q , $q = 2^5$, $g(x) = x^5 + x^3 + 1$. Припустимо, що θ – це автоморфізм $F_q, \theta: \alpha \rightarrow \alpha^2$ Фробеніуса. Групова операція визначається як

$$S(a_1, a_2, a_3, a_4)S(b_1, b_2, b_3, b_4) = S(a_1 + b_1, a_2 + a_1^2 b_1 + b_2, a_3 + a_2^2 b_1 + a_1^4 b_2 + b_3, a_4 + a_3^2 b_1 + a_2^4 b_2 + a_1^8 b_3 + b_4).$$

Обернений елемент визначається як

$$S(a_1, a_2, a_3, a_4)^{-1} = S(a_1, a_2 + a_1^3, a_3 + a_2^2 a_1 + a_1^4 a_2', a_4 + a_3^2 a_1 + a_2^4 a_2' + a_1^8 a_3'),$$

де $a_2' = a_2 + a_1^3$, $a_3' = a_3 + a_2^2 a_1 + a_1^4 a_2'$.

Розглянемо основні етапи розрахунків. Перший етап – це генерація ключів.

Перший етап полягає в генерації ручної логарифмічної сигнатури з розмірністю відповідного вибраного типу $(r_{1(k)}, \dots, r_{s(k)})$ та кінцевим полем F_q . Побудова масивів логарифмічних сигнатур представлена в [11]. Для нашого прикладу використовуємо побудову простих логарифмічних підписів, не аналізуючи деталі їх секретності. Для $\beta_{(k)}$ матимемо $k = \overline{1,3}$ типи $(2^2, 2^3)$, $(2, 2^2, 2^2)$, $(2^2, 2, 2^2)$, $(2^2, 2^2, 2)$. Вони представлені у вигляді рядків і елементів групи над полем F_q у табл. 1

Таблиця 1

Генерація логарифмічного підпису

$\beta_k = [B_{1(k)}, B_{2(k)}, B_{3(k)}, B_{4(k)}] = (b_{ij})_{(k)}, (b_{ij})_{(k)} \in A_{t=4}(n, \theta)$							
B₁₍₁₎		B₁₍₂₎		B₁₍₃₎		B₁₍₄₎	
00000	0,0,0,0	00000	0,0,0,0	00000	0,0,0,0	00000	0,0,0,0
10000	$\alpha^0, 0, 0, 0$	10000	$0, \alpha^0, 0, 0$	10000	$0, 0, \alpha^0, 0$	10000	$0, 0, 0, \alpha^0$
01000	$\alpha^1, 0, 0, 0$	01000	$0, \alpha^1, 0, 0$	B₂₍₃₎		01000	$0, 0, 0, \alpha^1$
11000	$\alpha^{14}, 0, 0, 0$	11000	$0, \alpha^{14}, 0, 0$	00000	$0, 0, 0, 0$	11000	$0, 0, 0, \alpha^{14}$
B₂₍₁₎		B₂₍₂₎		11000	$0, 0, \alpha^{14}, 0$	B₂₍₄₎	
01000	$\alpha^1, 0, 0, 0$	11000	$0, \alpha^{14}, 0, 0$	10100	$0, 0, \alpha^{28}, 0$	00000	$0, 0, 0, 0$
10100	$\alpha^{28}, 0, 0, 0$	11100	$0, \alpha^{22}, 0, 0$	01100	$0, 0, \alpha^{15}, 0$	00100	$0, 0, 0, \alpha^2$
11010	$\alpha^{26}, 0, 0, 0$	10010	$0, \alpha^5, 0, 0$	B₃₍₃₎		B₃₍₄₎	
00110	$\alpha^{16}, 0, 0, 0$	00110	$0, \alpha^{16}, 0, 0$	01000	$0, 0, \alpha^1, 0$	01000	$0, 0, 0, \alpha^1$
10001	$\alpha^{25}, 0, 0, 0$	B₃₍₂₎		10010	$0, 0, \alpha^5, 0$	00110	$0, 0, 0, \alpha^{16}$
11101	$\alpha^{21}, 0, 0, 0$	10000	$0, \alpha^0, 0, 0$	01101	$0, 0, \alpha^{27}, 0$	00001	$0, 0, 0, \alpha^4$
10011	$\alpha^{18}, 0, 0, 0$	10011	$0, \alpha^{18}, 0, 0$	10111	$0, 0, \alpha^9, 0$	11011	$0, 0, 0, \alpha^{19}$
11111	$\alpha^{20}, 0, 0, 0$						

Побудуємо випадкові накриття α_k для того самого типу, що й $\beta_{(k)}$:

$$\alpha_k = [A_{1(k)}, \dots, A_{s(k)}] = (a_{ij})_k = S(a_{ij(k)}^{(1)}, a_{ij(k)}^{(2)}, a_{ij(k)}^{(3)}, a_{ij(k)}^{(4)}),$$

де $a_{ij} \in A_{t=4}(n, \theta)$, $a_{ij(k)}^{(v)} \in F_q \setminus \{0\}$, $i = \overline{1, s}$, $j = \overline{1, r_{i(k)}}$, $k = \overline{1, 4}$.

У полі подання α_k має наступний вигляд (табл. 2).

Таблиця 2

Побудова випадкового накриття

$\alpha_k = [A_{1(k)}, \dots, A_{s(k)}] = (a_{ij})_k = S(a_{ij(k)}^{(1)}, a_{ij(k)}^{(2)}, a_{ij(k)}^{(3)}, a_{ij(k)}^{(4)})$			
$k = 1$	$k = 2$	$k = 3$	$k = 4$
A₁₍₁₎	A₁₍₂₎	A₁₍₃₎	A₁₍₄₎
$\alpha^6, \alpha^{11}, \alpha^{17}, \alpha^{27}$	$\alpha^{17}, \alpha^5, \alpha^{26}, \alpha^{28}$	$\alpha^0, \alpha^2, \alpha^{14}, \alpha^{20}$	$\alpha^{20}, \alpha^{14}, \alpha^{30}, \alpha^{13}$
$\alpha^{11}, \alpha^5, \alpha^7, \alpha^5$	$\alpha^{20}, \alpha^{14}, \alpha^{19}, \alpha^{24}$	$\alpha^{17}, \alpha^{27}, \alpha^{16}, \alpha^{10}$	$\alpha^4, \alpha^2, \alpha^{13}, \alpha^{17}$
$\alpha^{21}, \alpha^{18}, 0, \alpha^{16}$	$\alpha^{30}, \alpha^{21}, \alpha^6, \alpha^3$	A₂₍₃₎	$\alpha^{19}, \alpha^{13}, \alpha^{26}, \alpha^{22}$
$\alpha^5, \alpha^{29}, \alpha^{12}, \alpha^{16}$	$\alpha^6, \alpha^9, \alpha^{13}, \alpha^{22}$	$\alpha^{28}, \alpha^{29}, 0, \alpha^{25}$	$\alpha^6, \alpha^{28}, \alpha^{12}, \alpha^4$
A₂₍₁₎	A₂₍₂₎	$\alpha^{10}, \alpha^{12}, \alpha^{22}, \alpha^{30}$	A₂₍₄₎

$\alpha^4, \alpha^7, \alpha^4, \alpha^2$	$\alpha^{30}, \alpha^{14}, \alpha^{27}, \alpha^{30}$	$\alpha^{13}, \alpha^{23}, \alpha^{19}, \alpha^{19}$	$\alpha^{18}, \alpha^1, \alpha^1, \alpha^{24}$
$\alpha^{12}, \alpha^{11}, \alpha^3, \alpha^1$	$\alpha^1, \alpha^{18}, 0, \alpha^{13}$	$\alpha^0, \alpha^{10}, \alpha^1, \alpha^{20}$	$\alpha^{26}, \alpha^{28}, \alpha^{15}, \alpha^0$
$\alpha^{18}, \alpha^{15}, \alpha^{14}, \alpha^{30}$	$\alpha^1, \alpha^{18}, \alpha^{28}, \alpha^{30}$	$A_{3(3)}$	$A_{3(4)}$
$\alpha^3, \alpha^{19}, \alpha^{26}, \alpha^2$	$\alpha^{25}, \alpha^5, \alpha^0, \alpha^{13}$	$\alpha^{11}, \alpha^{27}, \alpha^{29}, \alpha^{18}$	$\alpha^{16}, \alpha^{17}, \alpha^{29}, \alpha^{17}$
$\alpha^{11}, \alpha^{18}, \alpha^{21}, \alpha^{28}$	$A_{3(2)}$	$\alpha^5, \alpha^1, \alpha^{12}, \alpha^{22}$	$\alpha^{18}, \alpha^0, \alpha^1, \alpha^{15}$
$\alpha^{16}, \alpha^{18}, \alpha^{10}, \alpha^{24}$	$\alpha^3, \alpha^{29}, \alpha^{25}, 0$	$\alpha^{30}, \alpha^{18}, \alpha^6, \alpha^{11}$	$\alpha^4, \alpha^9, \alpha^{23}, \alpha^{19}$
$\alpha^{17}, \alpha^{16}, 0, \alpha^{27}$	$\alpha^{25}, \alpha^{19}, \alpha^{23}, \alpha^2$	$0, 0, \alpha^{17}, \alpha^{23}$	$\alpha^{19}, \alpha^{20}, \alpha^{30}, \alpha^{10}$
$\alpha^{25}, \alpha^{17}, \alpha^8, \alpha^{12}$			

Вибираємо випадково $A_l(n, \theta) \quad t_{0(k)}, t_{1(k)}, \dots, t_{s(k)} \in A_l(n, \theta), \quad s_{(k)}, \quad k = \overline{1, 4} \quad t_{2(1)} = t_{0(2)}, \quad t_{3(2)} = t_{0(3)},$
 $t_{3(3)} = t_{0(4)}$ (табл. 3).

Таблиця 3

Випадкові t вектори

$t_{0(k)}, t_{1(k)}, \dots, t_{s(k)} \in A_{l=4}(n, \theta), \quad s_{(k)}, \quad k = \overline{1, 4}$			
$k = 1$	$k = 2$	$k = 3$	$k = 4$
$\alpha^1, \alpha^5, \alpha^{17}, \alpha^{16}$ $\alpha^{25}, \alpha^{17}, \alpha^{23}, \alpha^{27}$ $\alpha^{13}, \alpha^0, \alpha^{28}, \alpha^{10}$	$\alpha^{13}, \alpha^0, \alpha^{28}, \alpha^{10}$ $\alpha^{30}, \alpha^2, \alpha^{17}, \alpha^2$ $\alpha^6, \alpha^7, \alpha^{30}, \alpha^{18}$ $\alpha^9, \alpha^4, \alpha^9, \alpha^{20}$	$\alpha^9, \alpha^4, \alpha^9, \alpha^{20}$ $\alpha^{14}, \alpha^{28}, \alpha^{17}, \alpha^{22}$ $\alpha^{26}, \alpha^5, \alpha^{16}, \alpha^{30}$ $\alpha^{12}, \alpha^{15}, \alpha^{17}, \alpha^6$	$\alpha^{12}, \alpha^{15}, \alpha^{17}, \alpha^6$ $\alpha^{22}, \alpha^{30}, \alpha^{22}, \alpha^{16}$ $\alpha^{24}, \alpha^{29}, \alpha^{15}, \alpha^{30}$ $\alpha^3, 0, \alpha^{14}, \alpha^9$

Зворотні елементи $t_{0(k)}^{-(k)}, t_{1(k)}^{-(k)}, \dots, t_{s(k)}^{-(k)}$ групи $A_4(n, \theta)$ обчислені, як показано в табл. 4.

Таблиця 4

Обчислення обернених елементів $t_{0(k)}^{-(k)}, t_{1(k)}^{-(k)}, \dots, t_{s(k)}^{-(k)}$

$t_{0(k)}^{-(k)}, t_{1(k)}^{-(k)}, \dots, t_{s(k)}^{-(k)}$			
$k = 1$	$k = 2$	$k = 3$	$k = 4$
$\alpha^1, \alpha^0, \alpha^{22}, \alpha^{21}$ $\alpha^{25}, \alpha^7, \alpha^3, \alpha^{15}$ $\alpha^{13}, \alpha^{19}, \alpha^7, \alpha^{24}$	$\alpha^{13}, \alpha^0, \alpha^7, \alpha^{24}$ $\alpha^{30}, \alpha^2, \alpha^{15}, \alpha^{21}$ $\alpha^6, \alpha^7, \alpha^{28}, \alpha^{24}$ $\alpha^9, \alpha^4, \alpha^8, \alpha^{25}$	$\alpha^9, \alpha^4, \alpha^9, \alpha^{25}$ $\alpha^{14}, \alpha^{28}, \alpha^{17}, \alpha^{21}$ $\alpha^{26}, \alpha^5, \alpha^{16}, \alpha^{13}$ $\alpha^{12}, \alpha^{15}, \alpha^{17}, \alpha^{30}$	$\alpha^{12}, \alpha^{15}, \alpha^{17}, \alpha^6$ $\alpha^{22}, \alpha^{30}, \alpha^{22}, \alpha^{16}$ $\alpha^{24}, \alpha^{29}, \alpha^{15}, \alpha^{30}$ $\alpha^3, 0, \alpha^{14}, \alpha^9$

Аналогічно вибираємо випадкові $\tau_{0(k)}, \tau_{1(k)}, \dots, \tau_{s(k)} \in A_l(n, \theta), \quad s_{(k)}, \quad k = \overline{1, 4} \quad t_{2(1)} = t_{0(2)}, \quad t_{3(2)} = t_{0(3)},$
 $t_{3(3)} = t_{0(4)}$ (табл. 5):

Таблиця 5

Обчислення випадкових τ векторів $\tau_{0(k)}, \tau_{1(k)}, \dots, \tau_{s(k)} \in A(P_\infty) \setminus Z$

$\tau_{0(k)}, \tau_{1(k)}, \dots, \tau_{s(k)} \in A(P_\infty) \setminus Z, \quad s_{(k)}, \quad k = \overline{1, 4}$			
$k = 1$	$k = 2$	$k = 3$	$k = 4$
$\alpha^4, \alpha^{22}, \alpha^7, \alpha^{12}$ $\alpha^8, 0, \alpha^{13}, \alpha^{16}$ $\alpha^{29}, \alpha^{21}, \alpha^{30}, \alpha^{13}$	$\alpha^{29}, \alpha^{21}, \alpha^{30}, \alpha^{13}$ $\alpha^{24}, \alpha^{20}, \alpha^{17}, \alpha^{25}$ $\alpha^4, \alpha^7, \alpha^{16}, \alpha^{30}$ $\alpha^2, \alpha^{17}, \alpha^{22}, \alpha^2$	$\alpha^2, \alpha^{17}, \alpha^{22}, \alpha^2$ $0, \alpha^{22}, \alpha^{16}, \alpha^{24}$ $\alpha^6, \alpha^{21}, \alpha^{25}, \alpha^{18}$ $\alpha^{20}, 0, \alpha^3, \alpha^0$	$\alpha^{20}, 0, \alpha^3, \alpha^0$ $\alpha^{21}, \alpha^{16}, \alpha^{12}, \alpha^{16}$ $\alpha^{16}, \alpha^{28}, \alpha^{19}, \alpha^{16}$ $\alpha^{28}, \alpha^{17}, \alpha^{26}, \alpha^4$

і обернені елементи $\tau_{0(k)}^{-(k)}, \tau_{1(k)}^{-(k)}, \dots, \tau_{s(k)}^{-(k)}$ (табл. 6):

Таблиця 6

Обчислення обернених елементів $\tau_{0(k)}^{-(k)}, \tau_{1(k)}^{-(k)}, \dots, \tau_{s(k)}^{-(k)}$

$\tau_{0(k)}^{-(k)}, \tau_{1(k)}^{-(k)}, \dots, \tau_{s(k)}^{-(k)}$			
$k = 1$	$k = 2$	$k = 3$	$k = 4$
$\alpha^4, \alpha^{18}, \alpha^9, \alpha^0$ $\alpha^8, \alpha^{24}, \alpha^2, \alpha^{30}$ $\alpha^{29}, \alpha^{15}, \alpha^2, \alpha^5$	$\alpha^{29}, \alpha^{21}, \alpha^2, \alpha^5$ $\alpha^{24}, \alpha^{20}, \alpha^{22}, \alpha^{29}$ $\alpha^4, \alpha^7, \alpha^{12}, \alpha^{28}$ $\alpha^2, \alpha^{17}, \alpha^{24}, \alpha^{11}$	$\alpha^2, \alpha^{17}, \alpha^{22}, \alpha^{11}$ $0, \alpha^{22}, \alpha^{16}, \alpha^2$ $\alpha^6, \alpha^{21}, \alpha^{25}, \alpha^3$ $\alpha^{20}, 0, \alpha^3, \alpha^{22}$	$\alpha^{20}, 0, \alpha^3, \alpha^0$ $\alpha^{21}, \alpha^{16}, \alpha^{12}, \alpha^{16}$ $\alpha^{16}, \alpha^{28}, \alpha^{19}, \alpha^{16}$ $\alpha^{28}, \alpha^{17}, \alpha^{26}, \alpha^4$

Побудуємо випадкові накриття w_k для того самого типу, що й $\beta_{(k)}$:

$w_{(k)} = [W_{1(k)}, \dots, W_{s(k)}] = (w_{ij}^{(k)}) = S(w_{ij(k)}^{(1)}, w_{ij(k)}^{(2)}, \dots, w_{ij(k)}^{(l)})$, де $w_{ij} \in A_{i=4}(n, \theta)$, $w_{ij(k)}^{(v)} \in F_q$, $i = \overline{0, s(k)}$, $j = \overline{1, r_{i(k)}}$, $k = \overline{1, 4}$ (табл. 7).

Таблиця 7

Випадкові накриття w_k

$w_{(k)} = [W_{1(k)}, \dots, W_{s(k)}] = (w_{ij}^{(k)}) = S(w_{ij(k)}^{(1)}, \dots, w_{ij(k)}^{(4)})$			
$k = 1$	$k = 2$	$k = 3$	$k = 4$
$W_{1(1)}$	$W_{1(2)}$	$W_{1(3)}$	$W_{1(4)}$
$\alpha^{20}, \alpha^{20}, \alpha^{12}, \alpha^4$	$\alpha^9, \alpha^{28}, \alpha^{27}, \alpha^2$	$\alpha^3, \alpha^2, \alpha^{10}, 0$	$\alpha^{30}, \alpha^{14}, \alpha^1, \alpha^{28}$
$\alpha^7, \alpha^9, \alpha^{17}, \alpha^{20}$	$\alpha^{16}, \alpha^{13}, \alpha^6, \alpha^{21}$	$\alpha^5, \alpha^{10}, \alpha^{19}, \alpha^{16}$	$\alpha^6, \alpha^{28}, \alpha^{30}, \alpha^{20}$
$\alpha^{25}, \alpha^6, \alpha^{23}, \alpha^{27}$	$\alpha^{25}, 0, \alpha^4, \alpha^{27}$	$W_{2(3)}$	$\alpha^{13}, \alpha^{19}, \alpha^{26}, \alpha^{11}$
$\alpha^3, \alpha^0, \alpha^{23}, \alpha^{29}$	$\alpha^1, \alpha^0, \alpha^{17}, \alpha^{17}$	$\alpha^{12}, \alpha^{20}, \alpha^{14}, \alpha^3$	$\alpha^{16}, \alpha^{27}, \alpha^9, \alpha^{21}$
$W_{2(1)}$	$W_{2(2)}$	$\alpha^{23}, \alpha^{12}, \alpha^5, \alpha^{27}$	$W_{2(4)}$
$\alpha^7, \alpha^{21}, \alpha^6, \alpha^{21}$	$\alpha^{21}, \alpha^{14}, \alpha^{14}, \alpha^0$	$\alpha^2, \alpha^3, \alpha^{24}, \alpha^{16}$	$\alpha^2, \alpha^{21}, \alpha^8, \alpha^{29}$
$\alpha^{18}, \alpha^{21}, \alpha^{22}, \alpha^6$	$\alpha^{19}, \alpha^{29}, \alpha^{19}, \alpha^{13}$	$\alpha^{12}, \alpha^5, \alpha^{21}, \alpha^{14}$	$\alpha^4, \alpha^2, \alpha^1, \alpha^{23}$
$\alpha^{18}, \alpha^{19}, \alpha^{12}, \alpha^{15}$	$\alpha^{25}, \alpha^{26}, \alpha^{12}, \alpha^{17}$	$W_{3(3)}$	$W_{3(4)}$
$\alpha^{16}, \alpha^{12}, \alpha^{14}, \alpha^6$	$\alpha^{10}, \alpha^{19}, \alpha^{23}, \alpha^4$	$\alpha^{14}, \alpha^6, \alpha^0, \alpha^{17}$	$0, \alpha^0, \alpha^{25}, \alpha^3$
$\alpha^{23}, \alpha^4, \alpha^1, \alpha^{30}$	$W_{3(2)}$	$\alpha^{17}, \alpha^{13}, \alpha^7, \alpha^4$	$\alpha^3, \alpha^{19}, \alpha^{17}, \alpha^{24}$
$\alpha^5, \alpha^{26}, \alpha^6, \alpha^{19}$	$\alpha^{28}, \alpha^0, \alpha^{13}, \alpha^{17}$	$\alpha^{25}, \alpha^{24}, \alpha^{27}, \alpha^8$	$\alpha^{28}, \alpha^{28}, \alpha^{14}, \alpha^{26}$
$\alpha^{22}, \alpha^{17}, \alpha^{13}, \alpha^{21}$	$\alpha^{14}, \alpha^0, \alpha^3, \alpha^3$	$\alpha^{13}, 0, \alpha^{21}, \alpha^7$	$\alpha^{24}, \alpha^{18}, \alpha^{27}, \alpha^{13}$
$\alpha^{28}, \alpha^{27}, \alpha^9, \alpha^{24}$			

Наступним кроком є обчислення масивів h_k (табл. 8). В рамках умови прикладу отримуємо: $h_{(k)} = [h_{1(k)}, \dots, h_{s(k)}] = t_{(i-1)(k)}^{-1} \circ^{(k)} (w_{ij}^{(k)}) \circ^{(k)} (b_{ij}^{(k)}) \circ^{(k)} t_{i(k)}$; $i = \overline{1, s(k)}$, $j = \overline{1, r_{i(k)}}$, $k = \overline{1, 4}$.

Виконаємо гомоморфне криптографічне перетворення для елемента поля $e \Rightarrow \rho_i e$, де ρ_i є секретним параметром. Перетворення вибрано найпростіше. Також можна використовувати більш складні гомоморфні перетворення щодо операції додавання. Визначимо гомоморфне криптографічне перетворення для елемента групи S як

$$f(S(e_1, e_2, e_3, e_4)) = S(\rho_1 e_1, \rho_2 e_2, \rho_3 e_3, \rho_4 e_4) \text{ і } \rho = (\rho_1, \rho_2, \rho_3, \rho_4) = (\alpha^4, \alpha^5, \alpha^6, \alpha^7).$$

Таблиця 8

Масиви h_k

$h_k = S(h_{ij(k)}^{(1)}, h_{ij(k)}^{(2)}, h_{ij(k)}^{(3)}, h_{ij(k)}^{(4)})$			
$k = 1$	$k = 2$	$k = 3$	$k = 4$
$h_{1(1)}$	$h_{1(2)}$	$h_{1(3)}$	$h_{1(4)}$
$\alpha^{16}, \alpha^{20}, \alpha^{22}, \alpha^{30}$	$\alpha^{24}, 0, \alpha^{16}, 0$	$\alpha^{27}, \alpha^{25}, \alpha^{27}, \alpha^{30}$	$\alpha^7, \alpha^{25}, \alpha^9, \alpha^{19}$
$\alpha^{20}, \alpha^7, \alpha^{21}, \alpha^{15}$	$\alpha^7, \alpha^{25}, \alpha^{21}, \alpha^3$	$\alpha^{21}, \alpha^{15}, \alpha^{20}, \alpha^{14}$	$\alpha^{26}, \alpha^{21}, \alpha^{26}, 0$
$0, \alpha^{27}, \alpha^{26}, \alpha^{13}$	$\alpha^4, \alpha^{22}, 0, \alpha^{21}$	$h_{2(3)}$	$\alpha^{16}, \alpha^5, \alpha^{30}, \alpha^{10}$
$\alpha^{17}, \alpha^{16}, \alpha^{28}, \alpha^{26}$	$\alpha^{14}, \alpha^{22}, \alpha^3, \alpha^5$	$\alpha^{27}, \alpha^{10}, \alpha^{21}, \alpha^{23}$	$\alpha^{13}, \alpha^2, \alpha^1, \alpha^{29}$
$h_{2(1)}$	$h_{2(2)}$	$\alpha^{15}, \alpha^6, \alpha^{12}, \alpha^9$	$h_{2(4)}$
$\alpha^{26}, 0, \alpha^{29}, \alpha^{11}$	$\alpha^{25}, \alpha^5, \alpha^3, \alpha^{26}$	$\alpha^{16}, \alpha^2, \alpha^7, \alpha^{17}$	$\alpha^{20}, \alpha^5, \alpha^{19}, \alpha^6$
$\alpha^{17}, \alpha^7, \alpha^{26}, \alpha^{29}$	$\alpha^9, \alpha^2, \alpha^{12}, \alpha^{14}$	$\alpha^{27}, \alpha^{28}, \alpha^{28}, \alpha^{11}$	$\alpha^{26}, \alpha^8, \alpha^{14}, \alpha^6$
$\alpha^{27}, \alpha^{11}, \alpha^{28}, \alpha^{16}$	$\alpha^{21}, \alpha^{26}, \alpha^{25}, \alpha^{21}$	$h_{3(3)}$	$h_{3(4)}$
$\alpha^2, \alpha^3, \alpha^{11}, \alpha^4$	$\alpha^{13}, \alpha^{12}, \alpha^{22}, \alpha^7$	$\alpha^{27}, \alpha^9, \alpha^{21}, \alpha^{15}$	$\alpha^{30}, \alpha^{26}, \alpha^{30}, \alpha^{14}$
$\alpha^{19}, \alpha^{16}, \alpha^{25}, \alpha^5$	$h_{3(2)}$	$\alpha^7, \alpha^8, \alpha^4, \alpha^4$	$\alpha^{24}, \alpha^{25}, \alpha^9, \alpha^{18}$
$\alpha^8, \alpha^8, \alpha^{19}, \alpha^{19}$	$\alpha^{29}, \alpha^9, \alpha^1, \alpha^{12}$	$\alpha^2, \alpha^{10}, \alpha^{30}, \alpha^{24}$	$\alpha^{25}, \alpha^{11}, \alpha^{15}, \alpha^6$
$\alpha^8, \alpha^{10}, \alpha^1, \alpha^{30}$	$\alpha^{16}, \alpha^{28}, \alpha^1, \alpha^3$	$0, \alpha^{11}, \alpha^{12}, \alpha^{21}$	$\alpha^3, \alpha^{10}, \alpha^{10}, \alpha^{22}$
$\alpha^{12}, \alpha^{27}, 0, \alpha^{21}$			

Далі обчислюємо масиви g_k за допомогою гомоморфного перетворення

$$g_{(k)} = [g_{1(k)}, \dots, g_{s(k)}] = \tau_{(i-1)(k)}^{-1} \circ^{(k)} f(w_{ij}) \circ^{(k)} \tau_{i(k)}$$

$i = \overline{1, s(k)}$, $j = \overline{1, r_{i(k)}}$, $k = \overline{1, 4}$. Результати надано в табл. 9.

Таблиця 9

Масиви g_k

$g_k = S(g_{ij(k)}^{(1)}, g_{ij(k)}^{(2)}, g_{ij(k)}^{(3)}, g_{ij(k)}^{(4)})$			
$k = 1$	$k = 2$	$k = 3$	$k = 4$
$g_{1(1)}$	$g_{1(2)}$	$g_{1(3)}$	$g_{1(4)}$
$\alpha^{27}, \alpha^{21}, \alpha^{17}, \alpha^{13}$	$\alpha^{14}, \alpha^{16}, \alpha^7, \alpha^{18}$	$\alpha^5, \alpha^6, \alpha^{22}, \alpha^{30}$	$0, \alpha^{21}, \alpha^{19}, \alpha^9$
$\alpha^{28}, \alpha^{18}, \alpha^2, \alpha^1$	$\alpha^5, \alpha^{25}, \alpha^{18}, 0$	$\alpha^{18}, \alpha^{18}, \alpha^8, \alpha^7$	$\alpha^{19}, \alpha^3, \alpha^{20}, \alpha^{19}$
$0, \alpha^{17}, \alpha^1, \alpha^{13}$	$\alpha^{24}, \alpha^3, \alpha^1, \alpha^{13}$	$g_{2(3)}$	$\alpha^4, \alpha^4, \alpha^{30}, \alpha^{30}$
$\alpha^{22}, \alpha^9, \alpha^{29}, \alpha^{26}$	$\alpha^{20}, \alpha^0, 0, \alpha^{23}$	$\alpha^{12}, \alpha^0, \alpha^1, \alpha^0$	$\alpha^{21}, \alpha^{23}, \alpha^4, \alpha^3$
$g_{2(1)}$	$g_{2(2)}$	$\alpha^2, \alpha^3, \alpha^6, 0$	$g_{2(4)}$
$\alpha^{20}, \alpha^{29}, \alpha^{17}, \alpha^{13}$	$\alpha^9, \alpha^5, \alpha^{25}, \alpha^{30}$	$0, \alpha^{29}, \alpha^5, \alpha^{11}$	$\alpha^5, \alpha^1, \alpha^{15}, \alpha^5$
$\alpha^{21}, \alpha^0, \alpha^{25}, \alpha^{28}$	$\alpha^1, \alpha^8, \alpha^7, \alpha^{17}$	$\alpha^{12}, \alpha^{14}, \alpha^{26}, \alpha^{23}$	$\alpha^0, \alpha^2, \alpha^3, \alpha^{30}$
$\alpha^{21}, \alpha^{27}, \alpha^{21}, \alpha^{21}$	$\alpha^{15}, \alpha^{10}, \alpha^{13}, \alpha^9$	$g_{3(3)}$	$g_{3(4)}$
$\alpha^{11}, \alpha^{30}, \alpha^{22}, \alpha^5$	$\alpha^{11}, \alpha^{23}, \alpha^{29}, \alpha^{18}$	$\alpha^{30}, \alpha^{17}, \alpha^{26}, \alpha^2$	$\alpha^5, \alpha^{30}, \alpha^{25}, \alpha^{11}$
$\alpha^{15}, \alpha^{24}, \alpha^{17}, \alpha^{24}$	$g_{3(2)}$	$\alpha^8, \alpha^{23}, \alpha^{16}, \alpha^9$	$\alpha^2, \alpha^0, \alpha^{12}, \alpha^9$
$\alpha^7, \alpha^{30}, \alpha^{20}, \alpha^{24}$	$\alpha^{27}, \alpha^{24}, \alpha^6, \alpha^9$	$\alpha^{22}, \alpha^9, \alpha^9, \alpha^{10}$	$\alpha^{26}, \alpha^{18}, \alpha^{11}, \alpha^{17}$
$\alpha^{19}, \alpha^{19}, \alpha^3, \alpha^2$	$\alpha^7, \alpha^{24}, \alpha^{25}, \alpha^{26}$	$\alpha^{13}, \alpha^{21}, \alpha^{11}, \alpha^{26}$	$\alpha^{16}, \alpha^{10}, \alpha^{30}, \alpha^{14}$
$\alpha^6, \alpha^{10}, \alpha^{17}, \alpha^{17}$			

Вихідний відкритий ключ (a_k, h_k, g_k) і закритий ключ $[f, \beta_{(k)}, (t_{0(k)}, \dots, t_{s(k)}), (\tau_{0(k)}, \dots, \tau_{s(k)})]$, $k = \overline{1, 4}$.

На етапі шифрування маємо повідомлення $m \in A_i(n, \theta)$, $m = S(m_1, m_2, m_3, m_4)$ та $m_i \in F_q$ відкритий ключ $[f_k, (a_k, h_k, g_k)]$, $k = \overline{1, 4}$

$$\text{Дозволяємо } m = (\alpha^1, \alpha^2, \alpha^3, \alpha^4) = S(\alpha^1, \alpha^2, \alpha^3, \alpha^4).$$

Вибираємо випадковий $R = (R_1, R_2, R_3, R_4) = (10, 20, 30, 14)$.

Отримуємо наступні R_i розкладання для заданих типів $(r_{1(k)}, \dots, r_{s(k)})$, $k = \overline{1, 4}$:

$$R_1 = (R_{1(1)}, R_{2(1)}) = (2, 2) = 10,$$

$$R_2 = (R_{1(2)}, R_{2(2)}, R_{3(2)}) = (0, 1, 1) = 20,$$

$$R_3 = (R_{1(3)}, R_{2(3)}, R_{3(3)}) = (0, 3, 3) = 30.$$

$$R_4 = (R_{1(4)}, R_{2(4)}, R_{3(4)}) = (2, 1, 1) = 14$$

Обчислюємо зашифрований текст:

$$y_1 = a'(R) \cdot m = a_1'(R_1) \cdot a_2'(R_2) \cdot a_3'(R_3) \cdot a_4'(R_4) \cdot m = S(\alpha^7, \alpha^6, \alpha^{22}, \alpha^{11})$$

де

$$\begin{aligned} a_1'(R_1) &= a_1(10) = a_{1(1)}(2) a_{2(1)}(2) = S(\alpha^{23}, \alpha^{13}, \alpha^{20}, \alpha^{20}), \\ a_2'(R_2) &= a_2(20) = a_{1(2)}(0) a_{2(2)}(1) a_{3(2)}(1) = S(\alpha^{26}, \alpha^3, \alpha^5, \alpha^{29}), \\ a_3'(R_3) &= a_3(30) = a_{1(3)}(0) a_{2(3)}(3) a_{3(3)}(3) = S(0, \alpha^{27}, \alpha^8, \alpha^4), \\ a_4'(R_4) &= a_4(14) = a_{1(4)}(2) a_{2(4)}(1) a_{3(4)}(1) = S(\alpha^5, \alpha^{12}, \alpha^{21}, \alpha^{16}). \end{aligned}$$

Обчислюємо

$$y_2 = h_1(R_1) \circ^{(1)} (h_2(R_2) \circ^{(2)} (h_3(R_3) \circ^{(3)} h_4(R_4))) = S(0, \alpha^8, \alpha^{16}, \alpha^{17}).$$

Компоненти $h_k'(R_k)$ обчислюються аналогічно $a_k'(R_k)$ компонентам, але з використанням відповідної операції множення. Обчислимо компонент y_3 :

$$y_3 = g_1(R_1) \circ^{(1)} (g_2(R_2) \circ^{(2)} (g_3(R_3) \circ^{(3)} g_4(R_4))) = S(\alpha^{16}, \alpha^{14}, \alpha^1, \alpha^4).$$

Отримаємо вихід $y_1 = (\alpha^7, \alpha^6, \alpha^{22}, \alpha^{11})$, $y_2 = (0, \alpha^8, \alpha^{16}, \alpha^{17})$, $y_3 = (\alpha^{16}, \alpha^{14}, \alpha^1, \alpha^4)$.

На етапі дешифрування маємо зашифрований текст (y_1, y_2, y_3) і особистий ключ $[f, \beta_{(k)}, t_{i(k)}, \tau_{i(k)}]$, $i = \overline{0, s(k)}$, $k = \overline{1, 4}$.

На виході очікуємо отримати повідомлення $m \in A(P_\infty)$, що відповідає зашифрованому тексту (y_1, y_2, y_3) .

Щоб розшифрувати повідомлення m , потрібно відновити випадкові числа $R = (R_1, R_2, R_3)$.

Обчислюємо

$$D^{(1)}(R) = t_{0(1)} \circ^{(1)} y_2 \circ^{(4)} t_{s(4)}^{-4} = S(\alpha^{29}, \alpha^8, \alpha^{24}, \alpha^{28}),$$

$$G^{(1)}(R) = \tau_{0(1)} \circ^{(1)} y_3 \circ^{(4)} \tau_{s(4)}^{-4} = S(\alpha^{18}, \alpha^5, \alpha^7, \alpha^{30}),$$

$$D^{(1)}(R)' = D^{(1)}(R) \circ^{(1)} \hat{f}(G^{(1)}(R))^{-1} = S(\alpha^5, \alpha^{22}, \alpha^{21}, \alpha^0).$$

Відновлюємо R_1 з $\beta_{(1)}(R_1) = \sum_{i=1, j=R_1(i)}^{s(1)} \beta_{ij(i)}$, використовуючи $\beta_{(1)}(R_1)^{-1}$, оскільки β_1 є простим.

Отримуємо $\beta_1(R_1) = \alpha^5 = (10010)$. Виконаємо обернені обчислення $\beta_{(1)}(R_1)^{-1}$.

$$\begin{array}{ll} 10|010 & R_1 = (*, 2) \\ 11|010 & \text{ряд 1 з } B_{4(1)} \\ 10|010 - 11|010 = 01|000 & R_1 = (2, 2) \end{array}$$

Отримуємо $\beta_1(R_1)^{-1} = (2, 2) = 10$

Для подальшого розрахунку необхідно видалити компонент $h_1'(R_1)$ від y_2 і $g_1'(R_1)$ від y_3 .

Обчислюємо:

$$y_2^{(1)} = h_1(R_1)^{-1} \circ y_2 = S(\alpha^{26}, \alpha^{16}, \alpha^{17}, \alpha^{19}),$$

$$y_3^{(1)} = g_1(R_1)^{-1} \circ y_3 = S(\alpha^{19}, \alpha^{18}, \alpha^{12}, \alpha^{19}),$$

$$D^{(2)}(R) = t_{0(2)} \circ^{(2)} y_2^{(1)} \circ^{(4)} t_{s(4)}^{-4} = S(\alpha^{26}, \alpha^{18}, \alpha^{16}, \alpha^2),$$

$$G^{(2)}(R) = \tau_{0(2)} \circ^{(2)} y_3^{(1)} \circ^{(4)} \tau_{s(4)}^{-4} = S(\alpha^{30}, \alpha^{27}, \alpha^0, \alpha^{11}),$$

$$D^{(2)}(R)' = D^{(2)}(R) \circ^{(2)} \hat{f}(G^{(2)}(R))^{-2} = S(0, \alpha^{12}, \alpha^4, \alpha^{30}).$$

Відновлюємо R_2 з $\beta_{(2)}(R_2) = \sum_{i=1, j=R_2(i)}^{s(2)} \beta_{ij(i)}$, використовуючи $\beta_{(2)}(R_2)^{-1}$, оскільки β_2 є простим. Ми

отримуємо $\beta_2(R_2) = \alpha^{12} = (01111)$. Відновити R_2 за допомогою $\beta_2(R_2)$. Використовуємо ті самі обчислення, що й у прикладі для $\beta_2(R_2)^{-1}$, і отримуємо:

$$\begin{array}{ll} 01|11|1 & R_2 = (*, *, 1) \\ 10|01|1 & \text{ряд 1 з } B_{3(2)} \\ 01|11|1 - 10|01|1 = 11|10|0 & R_2 = (*, 1, 1) \\ 11|10|0 & \text{ряд 0 з } B_{3(2)} \\ 11|10|0 - 11|10|0 = 00|00|0 & R_2 = (0, 1, 1) \end{array}$$

Отримуємо $\beta_2(R_2)^{-1} = (0, 1, 1) = 20$.

Видаляємо компонент $h_2'(R_2)$ від $y_2^{(1)}$ і $g_2'(R_2)$ від $y_3^{(1)}$, отримуємо

$$y_2^{(2)} = h_2(R_2)^{-2} \circ y_2^{(1)} = S(\alpha^{19}, \alpha^{18}, \alpha^{22}, \alpha^{15}),$$

$$y_3^{(2)} = g_2(R_2)^{-2} \circ y_3^{(1)} = S(\alpha^{21}, \alpha^{10}, \alpha^0, \alpha^{19}),$$

$$D^{(3)}(R) = t_{0(3)} \circ^{(3)} y_2^{(2)} \circ^{(4)} t_{s(4)}^{-4} = S(\alpha^{23}, \alpha^5, \alpha^{18}, \alpha^{21}),$$

$$G^{(3)}(R) = \tau_{0(3)} \circ^{(3)} y_3^{(2)} \circ^{(4)} \tau_{s(4)}^{-4} = S(\alpha^{21}, \alpha^{10}, \alpha^7, \alpha^{13}),$$

$$D^{(3)}(R)' = D^{(3)}(R) \circ^{(3)} \hat{f}(G^{(3)}(R))^{-3} = S(0, 0, \alpha^{19}, \alpha^6)$$

Отримуємо $\beta_3(R_3) = \alpha^{19} = (11011)$.

Виконуємо обернені обчислення $\beta_3(R_3)^{-1}$.

1|10| 11 $R_3 = (*, *, 3)$
 1|01|11 ряд 3 з $B_{3(3)}$
 1|10| 11 -1|01|11=0| 11 |00 $R_3 = *, 3, 3)$
 0|11|00 ряд 3 з $B_{2(3)}$
 0| 11 |00-0|11|00= 0 |00|00 $R_3 = (0, 3, 3)$

Отримуємо $\beta_3(R_3)^{-1} = (0, 3, 3) = 30$.

Видаляємо компонент $h_3'(R_3)$ від $y_2^{(2)}$ і $g_3'(R_3)$ від $y_3^{(2)}$, в результаті отримуємо:

$$y_2^{(3)} = h_3(R_3)^{-3} \circ y_2^{(2)} = S(\alpha^{19}, \alpha^1, \alpha^{29}, \alpha^{17}),$$

$$y_3^{(3)} = g_3(R_3)^{-3} \circ y_3^{(2)} = S(\alpha^{13}, \alpha^{13}, \alpha^0, \alpha^{16}),$$

$$D^{(4)}(R) = t_{0(4)} \circ^{(4)} y_2^{(3)} \circ^{(4)} t_{s(4)}^{-4} = S(\alpha^7, \alpha^2, \alpha^{25}, \alpha^{21}),$$

$$G^{(4)}(R) = \tau_{0(4)} \circ^{(3)} y_3^{(3)} \circ^{(4)} \tau_{s(4)}^{-4} = S(\alpha^{11}, \alpha^7, \alpha^0, \alpha^{16}),$$

$$D^{(3)}(R)' = D^{(4)}(R) \circ^{(4)} \hat{f}(G^{(4)}(R))^{-4} = S(0, 0, 0, \alpha^{29})$$

01010

Отримуємо $\beta_4(R_4) = \alpha^{29} = (01010)$. Виконуємо обернені обчислення $\beta_4(R_4)^{-1}$.

01|0| 10 $R_3 = (*, *, 1)$
 00|1|10 ряд 1 з $B_{3(4)}$
 01|0| 10 -00|1|10=01| 1 |00 $R_3 = (*, 1, 1)$
 00|1|00 ряд 1 з $B_{2(4)}$
 01| 1 |00-00|1|00= 01 |0|00 $R_3 = (2, 1, 1)$

Отримуємо $\beta_4(R_4)^{-1} = (2, 1, 1) = 14$.

Далі отримуємо повідомлення $m = a'(R)^{-1} y_1 = S(\alpha^1, \alpha^2, \alpha^3, \alpha^4)$.

Аналіз параметрів безпеки та оцінка вартості

Розглянемо атаку грубої сили для відновлення ключа. Можливі три схеми такої атаки.

Атака грубою силою на зашифрований текст. Вибравши $R = (R_1, R_2, \dots, R_l)$, спробуємо розшифрувати текст $y_1' = \alpha'(R') \cdot m = \alpha_1'(R_1') \cdot \alpha_2'(R_2') \cdot \dots \cdot \alpha_l'(R_l') \cdot m$. Обкладинки $\alpha_k = (a_{ij})_k = S(a_{ij(k)}^{(1)}, a_{ij(k)}^{(2)}, \dots, a_{ij(k)}^{(l)})$ вибираються випадковим чином, а значення визначається множенням у групі без координатних обмежень. Результуючий вектор $\alpha'(R')$ залежить від усіх компонентів $\alpha_i'(R_i')$. Перелік ключових значень $R = (R_1, R_2, \dots, R_l)$ має оцінку складності. Для практичної атаки повідомлення m також невідоме та має невизначеність на вибір q^l . Це робить атаку грубою силою на ключ неможливою. Якщо взяти модель атаки з відомим текстом, то складність атаки залишається незмінною і дорівнює q^l .

Атака грубою силою на зашифрований текст y_2 . Виберіть $R = (R_1, R_2, \dots, R_l)$ відповідність y_2 . Вектор y_2 має таке визначення над компонентами $\alpha_i'(R_i)$:

$$y_2 = S \left(\sum_{k=1}^l \sum_{i=1, j=R_i(k)}^{s(k)} w_{ij(k)}^{(1)} + \sum_{i=1, j=R_i(1)}^{s(1)} \beta_{ij(1)} + \sum_{k=1}^l \sum_{i=1, j=R_i(k)}^{s(k)} w_{ij(k)}^{(2)} + \sum_{i=1, j=R_i(2)}^{s(2)} \beta_{ij(2)} + * , \dots, \sum_{k=1}^l \sum_{i=1, j=R_i(k)}^{s(k)} w_{ij(k)}^{(l)} + \sum_{i=1, j=R_i(1)}^{s(1)} \beta_{ij(1)} + * \right)$$

Значення координат y_2 визначаються розрахунками над векторами $w_1'(R_1), w_2'(R_2), \dots, w_l'(R_l)$. Ключі $R = (R_1, R_2, \dots, R_l)$ пов'язані, і зміни будь-якого з них призводять до змін y_2 . Атака грубою силою на ключ R має складність q^l .

Атака грубою силою на зашифрований текст y_3 . Виберіть $R = (R_1, R_2, \dots, R_l)$ відповідність y_3 . Вектор y_3 має таке визначення над компонентами $\rho_i w_i'(R_i)$:

$$y_3 = S \left(\sum_{k=1}^l \sum_{i=1, j=R_i(k)}^{s(k)} f(w_{ij(k)}^{(1)}) + \sum_{k=1}^l \sum_{i=1, j=R_i(k)}^{s(k)} f(w_{ij(k)}^{(2)}) + * \dots + \sum_{k=1}^l \sum_{i=1, j=R_i(k)}^{s(k)} f(w_{ij(k)}^{(l)}) + * \right).$$

Значення координат y_3 визначаються розрахунками над векторами $w_1'(R_1), w_2'(R_2), \dots, w_l'(R_l)$. Ключі R_1, R_2, \dots, R_l пов'язані, і зміни будь-якого з них призводять до змін y_3 . Атака грубою силою на ключ R має складність q^l .

Атака грубою силою на вектори $(t_{0(k)}, \dots, t_{s(k)})$ і $(\tau_{0(k)}, \tau_{1(k)}, \dots, \tau_{s(k)})$. Атака грубою силою $(t_{0(k)}, \dots, t_{s(k)})$ є загальною для криптосистем MST і для розрахунку в полі F_q над центром групи $Z(G)$ має оптимістичну оцінку складності, що дорівнює q . Для запропонованого алгоритму всі обчислення виконуються на всій групі $|A_l(n, \theta)| = q^l$, і складність атаки грубою силою на $(t_{0(k)}, \dots, t_{s(k)})$ і $(\tau_{0(k)}, \tau_{1(k)}, \dots, \tau_{s(k)})$ дорівнюватиме q^l .

Атака на алгоритм. Атака на алгоритм реалізації криптосистеми MST на основі узагальненої 2-групи Сузукі є багатогранною. Практичні атаки розглядають особливості логарифмічних підписів і випадкових накриттів, відомих криптоаналітику. Одним із рішень є використання аперіодичних логарифмічних підписів. У новій криптосистемі з гомоморфним шифруванням випадкові накриття є секретом для криптоаналітика. У цьому випадку відомі атаки на основі слабкості логарифмічних сигнатур неможливі.

Оцінимо параметри безпеки та ключів узагальненої групової криптосистеми Suzuki-2. Зафіксуємо узагальнену 2-групу Сузукі $A_l(n, \theta) = \{S(a_1, a_2, \dots, a_l) \mid a_i \in F_q\}$, яка визначена над полем F_q , $q = 2^n$. Тоді для l -параметричної групи досягаємо $K = nl$ бітової криптографії. Логарифмічний масив підписів і випадкові накриття є відомими параметрами, які використовуються в шифруванні таким чином:

$$\alpha_k = [A_{1(k)}, \dots, A_{s(k)}] = (a_{ij})_k = S(a_{ij(k)}^{(1)}, a_{ij(k)}^{(2)}, \dots, a_{ij(k)}^{(l)}),$$

$$h_{(k)} = [h_{1(k)}, \dots, h_{s(k)}] = S(h_{ij(k)}^{(1)}, h_{ij(k)}^{(2)}, \dots, h_{ij(k)}^{(l)}).$$

Крім того, ми знаємо випадкове накриття з гомоморфним шифруванням

$$g_{(k)} = [g_{1(k)}, \dots, g_{s(k)}] = S(g_{ij(k)}^{(1)}, g_{ij(k)}^{(2)}, \dots, g_{ij(k)}^{(l)})$$

для $k = \overline{1, l}$.

Кількість векторів у масивах α_k , $h_{(k)}$, $g_{(k)}$ визначається типом логарифмічної сигнатури $(r_{1(k)}, \dots, r_{s(k)})$ і дорівнює $N = \sum_{k=1}^l (r_{1(k)} + r_{2(k)} + \dots + r_{s(k)})$.

Оскільки масиви α_k є випадковими і можуть бути побудовані за допомогою детермінованого генератора випадкових бітів з деякого початкового вектора V , $g_{(k)}$, то можемо визначити α_k над $g_{(k)}$ вектором V . Зафіксуємо довжину вектора V рівною nl бітам.

Розмір масиву $g_{(k)}$ дорівнює: $N_g = l \sum_{k=1}^l (r_{1(k)} + r_{2(k)} + \dots + r_{s(k)}) n$ -бітовим словам.

До секретних параметрів криптосистеми відносяться вектори t , τ , ρ :

$$t_{0(k)}, \dots, t_{s(k)} \in A_l(n, \theta) \setminus Z, \quad t_{i(k)} = S(t_{i1(k)}, \dots, t_{il(k)}),$$

$$\tau_{0(k)}, \dots, \tau_{s(k)} \in A_l(n, \theta) \setminus Z, \quad \tau_{i(k)} = S(\tau_{i1(k)}, \dots, \tau_{il(k)}), \quad \rho = (\rho_1, \rho_2, \dots, \rho_l), \quad k = \overline{1, l}.$$

Кількість векторів $t_{i(k)}$ дорівнює $\tau_{i(k)}$: $N_t = N_\tau = l \sum_{k=1}^l s(k) n$ -бітовим словам.

Довжина вектора ρ дорівнює nl бітам.

Очевидно, що N_g , N_t , N_τ залежать від типу $(r_{1(k)}, \dots, r_{s(k)})$.

Нехай секретність криптографічних перетворень визначається K бітами.

Визначимо тип $(r_{1(k)}, \dots, r_{s(k)}) = (2, \dots, 2)$, потім $s(k) = n$ над полем $F(2^n)$. Отримуємо наступні значення:

$$N_g = nl \sum_{k=1}^l (r_{1(k)} + r_{2(k)} + \dots + r_{s(k)}) = 2n^2 l^2 = 2K^2 \text{ біт},$$

$$N_i = N_r = nl \sum_{k=1}^l s(k) = n^2 l^2 = K^2 \text{ біт}.$$

Довжина векторів V , ρ дорівнює $N_V = N_\rho = nl = K$ бітам. Визначимо тип $(r_{1(k)}, \dots, r_{s(k)}) = (2^8, \dots, 2^8)$, $s(k) = n/8$ над полем $F(2^n)$. Досягаємо

$$N_g = nl \sum_{k=1}^l (r_{1(k)} + r_{2(k)} + \dots + r_{s(k)}) = 2^5 n^2 l^2 = 2^5 K^2 \text{ біт},$$

$$N_i = N_r = nl \sum_{k=1}^l s(k) = n^2 l^2 / 8 = 2^{-3} K^2 \text{ біт}.$$

Приблизні витрати на впровадження представлені в табл. 10.

Витрати пам'яті для масивів спільних і секретних параметрів не залежать від поля $F(2^n)$ і кількості параметрів узагальненої групи Сузукі. Вибір поля F_q та параметрів групи Suzuki визначатиме швидкість обчислень по групі та залежить від програмної реалізації.

Таблиця 10

Орієнтовні витрати на впровадження

$K = 256, (r_{1(k)}, \dots, r_{s(k)}) = (2, \dots, 2)$			
$F(2^n)$	N_g Кбайт	$N_i (N_r)$, Кбайт	$N_V (N_\rho)$, біт
$F(2^8), \dots, F(2^{256})$	4	2	256
$K = 256, (r_{1(k)}, \dots, r_{s(k)}) = (2^8, \dots, 2^8)$			
$F(2^8), \dots, F(2^{256})$	64	0,25	256
$K = 512, (r_{1(k)}, \dots, r_{s(k)}) = (2, \dots, 2)$			
$F(2^8), \dots, F(2^{512})$	64	32	512
$K = 512, (r_{1(k)}, \dots, r_{s(k)}) = (2^8, \dots, 2^8)$			
$F(2^8), \dots, F(2^{512})$	1024	8	512

Висновки

Узагальнені 2-групи Сузукі є багатопараметричними групами і можуть мати як завгодно великий порядок. Криптосистеми MST на основі узагальненої групи Сузукі 2 мають перевагу над іншими реалізаціями схем у секретності та реалізації. Можемо побудувати високозахищену криптосистему з груповими обчисленнями в невеликому кінцевому полі. Застосування гомоморфного шифрування до випадкових накриттів у логарифмічному підписі забезпечує захист від відомих атак на реалізації логарифмічного підпису. Для побудови криптосистеми можна використовувати захищені логарифмічні підписи простої конструкції, що призводить до низьких витрат на загальні параметри криптосистеми. Запропонована криптосистема з гомоморфним шифруванням є хорошим кандидатом для постквантової криптографії.

Список літератури:

1. K.H. Ko, S.J. Lee, J.H. Cheon, J.W. Han, J. Kang, and C. Park. New public-key cryptosystem using braid groups // Advances in cryptology—CRYPTO 2000, vol.1880of Lecture Notes in Computer Science, pp. 166–183, Springer, Berlin, Germany, 2000.
2. B. Eick and D. Kahrobaei. Polycyclic groups: a new platform for cryptology // <http://arxiv.org/abs/math/0411077>.

3. V. Shpilrain and A. Ushakov. Thompsons group and public key cryptography // Applied Cryptography and Network Security, vol. 3531 of Lecture Notes in Computer Science, pp. 151–164, 2005.
4. D. Kahrobaei, C. Koupparis, and V. Shpilrain. Public key exchange using matrices over group rings // Groups, Complexity, and Cryptology ,vol.5,no.1, pp.97–115, 2013.
5. N.R. Wagner and M.R. Magyarik. A public-key cryptosystem based on the word problem // Proc. Advances in Cryptology–CRYPTO 1984, LNCS 196, Springer-Verlag (1985), pp. 19–36.
6. S.S. Magliveras. A cryptosystem from logarithmic signatures of finite groups // Proceedings of the 29th Midwest Symposium on Circuits and Systems , pp. 972–975, Elsevier Publishing, Amsterdam, The Netherlands, 1986.
7. W. Lempken, S.S. Magliveras, Tran van Trung and W. Wei. A public key cryptosystem based on non-abelian finite groups // Journal of Cryptology, 22 (2009), 62–74.
8. H.Hong, J.Li, L.Wang, Y. Yang, X.Niu. A Digital Signature Scheme Based on MST3 Cryptosystems // Hindawi Publishing Corporation, Mathematical Problems in Engineering, vol 2014, 11 p., <http://dx.doi.org/10.1155/2014/630421>
9. Y. Cong, H. Hong, J. Shao, S. Han, J. Lin and S. Zhao. A New Secure Encryption Scheme Based on Group Factorization Problem // IEEEExplore, November 20, 2019 Digital Object Identifier 10.1109/ACCESS.2019.2954672 <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8907845>
10. P. Svaba and T. van Trung. Public key cryptosystem MST3 cryptanalysis and realization // Journal of Mathematical Cryptology,vol.4,no.3,pp.271–315,2010
11. T. van Trung. Construction of strongly aperiodic logarithmic signatures // Journal Math. Cryptol., vol. 12, no. 1, pp. 23–35, 2018.
12. Kotukh Y., Severinov E., Vlasov O., Tenytska A., Zarudna E. Some results of development of cryptographic transformations schemes using non-abelian groups // Радіотехніка. 2021. Вип. 204. С. 66–72.
13. Котух Є., Северінов О., Власов А. та ін. Методи побудови та властивості логарифмічних підписів // Радіотехніка. 2021. Вип. 205. С. 94–99. <https://doi.org/10.30837/rt.2021.2.205.09>
14. Kotukh Y., Khalimov G. Hard Problems for Non-abelian Group Cryptography, 2021 // Fifth International Scientific and Technical Conference "Computer and Information systems and technologies". <https://doi.org/10.30837/csitic52021232176>
15. Халімов Г., Котух Є., Сергійчук Ю., Марухненко О. Аналіз складності реалізацій криптосистеми на групі Сузукі // Радіотехніка. 2018. Вип. 193. С. 75–81.
16. Котух Є., Охріменко Т., Дяченко О., Ротаньова Н., Козіна Л., Зеленський Д. Криптоаналіз систем на основі проблеми слова з використанням логарифмічних підписів // Радіотехніка. 2021. Вип. 206. С. 106–114. <https://doi.org/10.30837/rt.2021.3.206.09>
17. Kotukh Y., Khalimov G. Towards practical cryptoanalysis of systems based on word problems and logarithmic signatures // Proceedings of II International Conference Information security: problems and prospects, 25 Nov 2022, Baku, Azerbaijan, pp. 55–58.
18. Khalimov G., Kotukh Y. et al. Towards advance encryption based on a Generalized Suzuki 2-groups // 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME). Mauritius, 2021, pp. 1–6. doi: 10.1109/ICECCME52200.2021.9590932.
19. Khalimov G., Kotukh Y., Khalimova S. MST₃ Cryptosystem Based on a Generalized Suzuki 2-Groups [Electronic resource]. Access mode : <http://ceur-ws.org/Vol-2711/paper1.pdf>
20. Khalimov G., Kotukh Y., Didmanidze I., Sievierinov O., Khalimova S. and Vlasov A. Towards three-parameter group encryption scheme for MST3 cryptosystem improvement // 2021 Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4), London, United Kingdom, 2021, pp. 204–211. doi: 10.1109/WorldS451998.2021.9514009.
21. Khalimov G., Kotukh Y., Didmanidze I., Khalimova S. 2021. Encryption scheme based on small Ree groups // Proceedings of the 2021 7th International Conference on Computer Technology Applications (ICCTA '21). ACM, New York, NY, USA, 33–37. <https://doi.org/10.1145/3477911.3477917>
22. Khalimov G., Kotukh Y., Shonia O., Didmanidze I., Sievierinov O., Khalimova S. Encryption Scheme Based on the Automorphism Group of the Suzuki Function Field // 2020 IEEE PIC S&T, Kharkiv, Ukraine, 2020, pp. 383–387. doi: 10.1109/PICST51311.2020.9468089.
23. Khalimov G., Kotukh Y., Khalimova S. Encryption scheme based on the extension of automorphism group of the Hermitian function field // Book of Abstract 20th Central European Conference on Cryptology. 2020. P. 30 – 32.
24. Khalimov G., Kotukh Y. et al. (2022). Encryption Scheme Based on the Generalized Suzuki 2-groups and Homomorphic Encryption // Chang SY., Bathen L., Di Troia F., Austin T.H., Nelson A.J. (eds). Silicon Valley Cybersecurity Conference. SVCC 2021. Communications in Computer and Information Science, vol 1536. Springer, Cham. https://doi.org/10.1007/978-3-030-96057-5_5
25. Khalimov G., Sievierinov O., Khalimova S., Kotukh Y., Chang S.-Y. and Balytskyi Y. Encryption Based on the Group of the Hermitian Function Field and Homomorphic Encryption // 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T). Kharkiv, Ukraine, 2021, pp. 465–469. doi: 10.1109/PICST54195.2021.9772219.
26. Kotukh Y., Khalimov G., Korobchinsky M. Construction of a three-parameter encryption scheme on Hermitian groups in the MST3 cryptosystem // Radiotekhnika. 2023. 213. P. 49–55. <https://doi.org/10.30837/rt.2023.2.213.05>

27. Kotukh Y., Khalimov G., Korobcninskiy M. Method of Security Improvement for MST2 Cryptosystem Based on Automorphism Group of Ree Function Field // 2023 Theoretical and applied cybersecurity, vol.5, no. 2, pp. 31–39. <https://doi.org/10.20535/tacs.2664-29132023.2.290414>

28. Khalimov G., Kotukh Y., Khalimova S. Improved encryption scheme based on the automorphism group of the Ree function field // 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), IEEE Xplore. 2021.

Надійшла до редколегії 12.10.2023

Відомості про авторів:

Котух Євген Володимирович – канд. техн. наук, доцент, професор кафедри кібербезпеки; Національний технічний університет «Дніпровська політехніка»; Дніпро, Україна; e-mail: yevgenkotukh@gmail.com; ORCID: <https://orcid.org/0000-0003-4997-620X>

Халімов Геннадій Зайдулович – д-р техн. наук, професор, завідувач кафедри безпеки інформаційних технологій; Харківський національний університет радіоелектроніки; Харків, Україна; e-mail: hennadii.khalimov@nure.ua; ORCID: <https://orcid.org/0000-0002-2054-9186>

Коробчинський Максим Володимирович, д-р техн. наук, професор, начальник 2-ї кафедри технічних видів розвідки та інформаційних технологій 2-го навчального інституту Военної академії імені Євгенія Березняка Міністерства оборони України, м. Київ, Україна; mars_kor@ukr.net; ORCID: <https://orcid.org/0000-0001-8049-4730>,

PHYSICS OF DEVICES, ELEMENTS AND SYSTEMS ФІЗИКА ПРИЛАДІВ, ЕЛЕМЕНТІВ І СИСТЕМ

УДК 621.357

DOI:10.30837/rt.2023.4.215.06

*В.М. БОРЩОВ, д-р техн. наук, О.М. ЛІСТРАТЕНКО, канд. техн. наук,
М.І. СЛІПЧЕНКО, д-р фіз.-мат. наук, М.А. ПРОЦЕНКО, канд. техн. наук,
І.Т. ТИМЧУК, канд. техн. наук, О.В. КРАВЧЕНКО, І.В. БОРЩОВ*

НОВІ ПІДХОДИ ДЛЯ СТВОРЕННЯ ЕФЕКТИВНИХ КОМБІНОВАНИХ ДРУКОВАНИХ ПЛАТ НА ТЕПЛОПРОВІДНИХ ОСНОВАХ З ДІЕЛЕКТРИКАМИ З ПОЛІМІДУ

Вступ

Різноманітність виконання сучасних напівпровідникових пристроїв, їх застосування для широкого спектру завдань, необхідність відведення великої кількості тепла, робота в жорстких умовах експлуатації – все це зумовлює пошук нових конструкторських та технологічних рішень при виготовленні електронних модулів та друкованих вузлів підвищеної потужності. Для їх реалізації необхідні спеціальні матеріали, що мають високу технологічність та виправдану собівартість для забезпечення необхідних експлуатаційних характеристик виробів, які використовують напівпровідникові чіпи з типовими максимальними робочими температурами від +85 до +150°C. Навіть за +125...+150°C висока температура може стати однією з основних причин зниження терміну експлуатації та відмов напівпровідникових приладів та інтегральних схем [1].

У зв'язку з цим дослідниками постійно проводяться роботи з вибору та використання, а також розробки нових матеріалів з покращеними теплопровідними властивостями, та оптимізації конструкції і технології складання електронних пристроїв. При цьому застосування нових матеріалів з покращеними теплопровідними властивостями часто залишається єдиним прийнятним способом ефективного відведення тепла від напівпровідникових чіпів.

Застосування в теплопровідних платах у якості діелектриків поліімідних (ПІ) плівок дає змогу виділити такі плати за конструкцією в особливий ряд, оскільки в них використовують ПІ плівки порівняно малої товщини, близько 0,02 – 0,025 мм проти 0,1 мм у існуючих стандартних промислових платах на металевих основах [2]. Хоча поліімідні плівки мають низькі значення теплопровідності близько 0,12 – 0,14 Вт/(м·К), проте їхня мала товщина в платах забезпечує доволі малий тепловий опір тепловідної системи загалом. При цьому ПІ плівки, не дивлячись на малу товщину, мають високу електричну міцність (до 160 кВ/мм та більше) порівняно з іншими типами плат на алюмінієвих основах. А використання композитних, зокрема теплопровідних ПІ плівок з підвищеною теплопровідністю, дає змогу ще більше зменшити сумарний тепловий опір друкованих плат на металевих основах з тонкими ПІ діелектриками [3 – 5].

Поліімідні широко застосовуються у спеціальній техніці завдяки поєднанню високих фізико-механічних показників, термостійкості, термостабільності, вогнестійкості, хімічної стійкості та здатності протистояти радіації та УФ-випромінюванню. Повністю ароматичні ПІ плівки успішно використовуються в промисловості вже понад півстоліття завдяки своїм чудовим комплексним властивостям як у звичайних, так і в екстремальних умовах.

Термозварювальні поліімід-фторопластові плівки (ПМФ) також можуть бути успішно застосовані для створення комбінованих плат на теплопровідних жорстких основах, що вимагають покращених фізико-механічних властивостей матеріалів, стійкості до впливу температури та високої надійності за збереженням вже досягнутих для поліімідів інших функціональних властивостей високого рівня. Такий підхід дозволяє суттєво розширити інноваційні можливості нових електронних модулів і друкованих вузлів, що розробляються,

практично для всіх областей спеціального приладобудування, у тому числі із застосуванням Chip-on-board (COB) і Chip-on-flex (COF) технологій складання. Таким чином, метою цієї роботи було:

- розробка конструктивно-технологічних рішень (КТР) та способів виготовлення комбінованих друкованих плат на теплопровідних алюмінієвих основах з промисловими тонкими теплопровідними поліімідними діелектриками з теплопровідністю від 0,12 до 0,46 Вт/(м·К) із термозварювальними фторполімерними покриттями;

- розробка конструктивно-технологічних рішень та способів виготовлення комбінованих друкованих плат на теплопровідних алюмінієвих основах із застосуванням удосконалених безадгезивних мідь-поліімідних та алюміній-поліімідних лакофольгових діелектриків з теплопровідністю композитних лакових поліімідних шарів від 0,36 до 1,0 Вт/(м·К) та більше [6];

- виготовлення експериментальних зразків та дослідження основних хімічних, механічних, електричних та теплових властивостей різних типів комбінованих друкованих плат на алюмінієвих основах з тонкими теплопровідними поліімідними діелектриками.

1. Предмет та методи дослідження

1.1. Конструктивно-технологічні рішення комбінованих друкованих плат на теплопровідних основах з тонкими поліімідними діелектриками

На рис. 1 представлено структурні схеми комбінованих друкованих плат на теплопровідних алюмінієвих основах. У тому числі плата, до складу якої входить тонкий діелектрик з ПІ плівки-основи з термозварюваними термопластичними покриттями з двох сторін (рис.1, *а*), та плата, до складу якої входить тонкий діелектрик з ПІ шару з одностороннім адгезивним покриттям (рис. 1, *б*). До складу плат (рис. 1, *а*, *б*) входять також верхні шари, що комунують, і які являють собою алюмінієву або мідну фольгу.

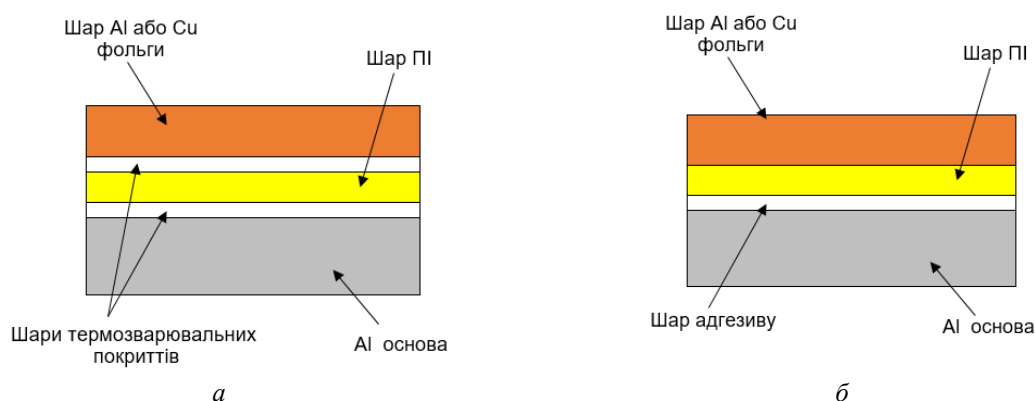


Рис. 1. Структурні схеми комбінованих плат з ПІ діелектриками: *а* – плата, до складу якої входить тонкий діелектрик з ПІ плівки-основи з термозварюваними термопластичними покриттями з двох сторін; *б* – плата, до складу якої входить тонкий діелектрик із ПІ шару з одностороннім адгезивним покриттям

Найпростішим типом комбінованих друкованих плат на теплопровідній металевій основі і, отже, найбільш економічно ефективним для поверхневого монтажу є комбіновані друковані плати з алюмінієвою основою. Така конструкція плати є одношаровою друкованою платою, яка наклеєна на алюмінієву підкладку. Тепло, що генерується, легко проходить через діелектрик, а потім швидко розсіюється через плоский алюмінієвий радіатор. Хоча мідь має кращі теплопровідні властивості, алюміній є найбільш застосовуваним матеріалом для плат з металевією основою, тому що він є значно дешевшим і, при цьому, досить легким і міцним матеріалом. Так, наприклад, для плат із металевими основами широко використовуються наступні теплопровідні алюмінієві сплави: алюміній 1100 (аналог АТ) – 222 Вт/(м·К); алюміній 5052 (аналог АМг2,5) – 138 Вт/(м·К); алюміній 6061 (аналог АД33) – 167 В/(м·К). Друковані плати на алюмінієвих основах в основному застосовуються в електронних виробках

з малими габаритними розмірами, що не потребують примусового охолодження. Такий підхід суттєво спрощує проектування електронних пристроїв, особливо з підвищеною потужністю, оскільки відведення тепла перестає суттєво залежати від взаємного розташування елементів на платі, оскільки основне тепло розсіюється через підкладку такої плати. Відпадає необхідність у застосуванні в конструкції плати додаткового відведення тепла іншими способами. В підсумку збільшується рівень інтеграції компонентів на платі і, навіть, знижуються її габаритні розміри. При ідентичності таких показників плат, як площа, товщина фольги для міжелементних з'єднань, товщина клейового або паяного з'єднання між напівпровідниковим чіпом та контактною площиною на фользі, товщина багатошарового діелектрика та теплопровідність його шарів будуть визначальними для загального теплового опору друкованих плат.

Нові підходи при розробці КТР комбінованих друкованих плат на алюмінієвих основах з ПІ діелектриками, у тому числі теплопровідними, засновані в першу чергу на застосуванні в їх конструкції різних типів тонких ПІ діелектриків, які забезпечують доволі малий загальний тепловий опір тепловідної системи плат (від $\sim 0,23$ до $\sim 0,06$ C/Вт) [1]. У тому числі термозварюваних ПМФ плівок, що промислово випускаються:

- багатошарова термозварювана ПМФ плівка Kapton®120FN 616 зі стандартною ПІ плівкою-основою DuPont™ Kapton® HN товщиною 25 мкм з мінімальною теплопровідністю 0,12 Вт/(м·К) та з фторполімерними двосторонніми покриттями Teflon® FEP товщиною 2,5 мкм кожне. Об'ємний опір $>10^{17}$ Ом·см при 25°C, електрична міцність до 4,2 кВ/мил (~ 168 кВ/мм) [3, 7];

- багатошарова термозварювальна ПМФ плівка Kapton®120FMT616 з теплопровідною ПІ плівкою-основою Kapton® MT товщиною 25 мкм з теплопровідністю 0,46 Вт/(м·К) та фторполімерними двосторонніми покриттями Teflon® FEP товщиною 2,5 мкм кожне. Об'ємний опір $>10^{17}$ Ом·см при 25°C, електрична міцність до 5,2 кВ/мил (~ 208 кВ/мм) [4, 8];

- багатошарова термозварювана ПМФ плівка KYMIDE KYPIFMT 616 компанії Suzhou Kyung Industrial Materials Co.Ltd (Китай) з теплопровідною ПІ плівкою-основою KYPI-MT товщиною 25 мкм з теплопровідністю 0,36 Вт/(м·К) та фторполімерними двосторонніми покриттями Teflon® FEP товщиною 3,0 мкм кожне. Об'ємний опір $>10^{16}$ Ом·см при 25°C, електрична міцність до 4,1 кВ/мил (~ 160 кВ/мм) [5, 9].

У свою чергу, при розробці нових підходів для створення комбінованих друкованих плат авторами також були застосовані нові теплопровідні безадгезивні лакофольгові ПІ діелектрики власного виробництва, які виготовлені на мідній або алюмінієвій фользі товщиною від 30 до 100 мкм. Розрахункова ефективна теплопровідність удосконалених композиційних ПІ шарів товщиною 25–30 мкм у лакофольгових ПІ діелектриках у різному виконанні становить від 0,38 до 1,4 Вт/(м·К) при об'ємній концентрації наповнювачів (високодисперсних AlN частинок) у ПІ матриці від 40 до 70 об. % [6].

Запропоновані технічні рішення дозволяють виготовити комбіновані друковані плати шляхом приклеювання безадгезивних мідь-поліімідних або алюміній-поліімідних лакофольгових діелектриків до алюмінієвої основи плати товщиною 1 мм. Приклеювання здійснюється за допомогою однокомпонентного вологозатверджувального полідиметилсилоксанового адгезиву SE 4485 компанії Dow Corning Corporation з теплопровідністю $\sim 2,8$ Вт/(м·К), що має хорошу адгезію до 2 МПа при зсуві внахлест до більшості матеріалів без використання праймерів. У тому числі до металів, кераміки, скла та більшості пластиків. До переваг кремній-органічних адгезивів необхідно віднести їхню високу термостійкість і вологостійкість, а також електричну міцність до 24 кВ/мм [10].

1.2. Вибір способів виготовлення комбінованих друкованих плат на алюмінієвих основах з тонкими ПІ діелектриками

При виборі способів виготовлення комбінованих плат на алюмінієвих теплопровідних підставах застосовані нові технічні рішення з використанням різних типів тонких ПІ діелектриків. За допомогою програмного комплексу COMSOL MULTIPHYSICS проведено моделю-

вання залежності максимальних очікуваних робочих температур на платах електронних модулів від розмірів плат та розроблено теплові моделі досліджуваних електронних модулів. В тому числі модель 1 електронного модуля на комбінованій платі з удосконаленим теплопровідним композиційним безадгезивним лакофольговим мідь-поліімідним діелектриком з теплопровідністю композиційного III шару до 1,0 Вт/(м·К). Модель 2 електронного модуля на комбінованій платі з багатошаровою теплопровідною термозварюваною ПМФ плівкою Kapton®120FMT616 з теплопровідністю 0,46 Вт/(м·К) та модель 3 електронного модуля на комбінованій платі з багатошаровою ПМФ плівкою DuPont™ Kapton® 120FN 616 з теплопровідністю 0,12 Вт/(м·К). У моделях електронних модулів досліджувалися теплові властивості плат на алюмінієвих основах товщиною 1 мм з розмірами від 30 × 30 мм до 50 × 50 мм, на яких методом паяння розміщувалися джерела тепла потужністю ~ 2 Вт з розмірами 3 × 3 мм. При цьому в моделях досліджувалися теплові властивості плат для відносно сприятливих умов експлуатації модулів при температурі навколишнього середовища $T_a = 25\text{ }^\circ\text{C}$ з конвекційним коефіцієнтом теплопередачі від плоского алюмінієвого тепловідводу $h = \sim 22\text{ Вт/м}^2\text{ К}$ та для відносно несприятливих умов експлуатації при $T_a = 45\text{ }^\circ\text{C}$ з конвекційним коефіцієнтом теплопередачі від плоского алюмінієвого тепловідводу $h = \sim 15\text{ Вт/м}^2\text{ К}$.

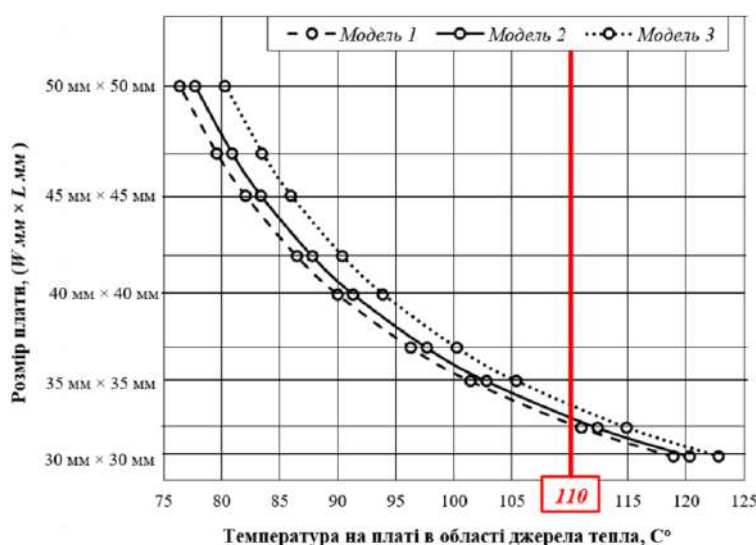


Рис. 2. Залежність максимальних робочих температур плат в області джерел тепла від розмірів плат для відносно несприятливих умов експлуатації

З графіків (рис. 2) слідує, що теплопровідні Al основи з товщиною 1 мм у плат з розмірами від 35 × 35 мм і більше забезпечують усереднені значення максимальних температур плат в області джерел тепла потужністю до 2 Вт близько 105 – 110 °С для всіх досліджених моделей електронних модулів з можливістю зменшення температури до ~ 75 – 80 °С зі збільшенням розмірів алюмінієвих основ плат до 50 × 50 мм навіть за несприятливих умов експлуатації електронних модулів.

Таким чином, для виготовлення зразків плат із тонкими III діелектриками і тестових структур якості (ТСЯ) плат та ТСЯ електронних модулів для експериментальних досліджень хімічних, механічних, електричних та теплових властивостей, а також оцінки технологічних процесів виготовлення плат було відібрано конструктивно-технологічні рішення експериментальних комбінованих плат на основі наступних типів діелектричних III шарів, а саме:

- комбінована плата на основі промислової стандартної багатошарової термозварюваної ПМФ плівки DuPont™ Kapton® 120FN 616 з теплопровідністю 0,12 Вт/(м·К);
- комбінована плата на основі промислової теплопровідної багатошарової термозварюваної ПМФ плівки Kapton®120FMT616 з теплопровідністю 0,46 Вт/(м·К);
- комбінована плата з удосконаленим теплопровідним композиційним безадгезивним лакофольговим мідь-поліімідним діелектриком з теплопровідністю композиційного III шару до 1,0 Вт/(м·К).

2. Виготовлення комбінованих друкованих плат

2.1. Спосіб виготовлення комбінованих друкованих плат на алюмінієвих основах з промисловими тонкими поліїмід-фторопластовими термозварюваними плівками

При виготовленні експериментальних зразків комбінованих плат на основі тонких поліїмід-фторопластових термозварюваних плівок збираються пакети з листа алюмінієвого сплаву 1100 (основи плати) товщиною 1000 мкм з розмірами 35 × 35 мм та листа мідної або алюмінієвої фольги товщиною 100 мкм з розмірами 35 × 35 мм, а також листа багатошарової поліїмідної плівки DuPont™ Kapton®120FMT616 або багатошарової поліїмідної плівки DuPont™ Kapton®120FN 616 з двостороннім термопластичним термозварюваним фторполімерним покриттям із загальною товщиною 30 мкм, які розташовуються між алюмінієвою основою та листом із фольги. Приклеювання до багатошарової ПМФ плівки з двох сторін фольги зверху та алюмінієвої основи плати знизу здійснюється за допомогою термообробки під тиском.

Зібраний пакет поміщають у спеціальне технологічне оснащення (приспособлення з рухомою опорою) за допомогою еластичних прокладок з фторопластової плівки, розташованих зверху та знизу пакета. Об'єм приспособлення з рухомою опорою доводять до об'єму пакета, приспособлення затягують гвинтом, щоб забезпечити тиск 50–100 кгс/см² (5 – 10 МПа) або більше і поміщають в лабораторну електропечі типу СНОл-6.6.6/350 ГЦ-00.04, яку попередньо нагрівають до 120 °С. Температуру електропечі піднімають від 120 до 270–280 °С (до температури плавлення фторполімерних покриттів Teflon® FEP) і витримують при цій температурі протягом 10 хвилин.

Після закінчення зазначеного часу електропечі відключають і пристрій охолоджують разом з електропечістю до кімнатної температури. Відпресована комбінована плата на алюмінієвій основі виймається з технологічного оснащення.

2.2. Спосіб виготовлення комбінованих друкованих плат на алюмінієвих основах з безадгезивними мідь-поліїмідними або алюміній-поліїмідними лакофольговими теплопровідними III діелектриками

При виготовленні експериментальних зразків комбінованих плат з тонкими лакофольговими теплопровідними III діелектриками на першому етапі здійснюється виготовлення безадгезивних лакофольгових III діелектриків на основі розроблених авторами експериментальних композиційних теплопровідних III шарів товщиною 25–30 мкм з теплопровідністю до 1,0 Вт/(м·К), які фольговані міддю або алюмінієм завтовшки 100 мкм. Потім виготовляються експериментальні зразки комбінованих плат. Для цього на листи з алюмінієвого сплаву 1100 (основи плати) товщиною 1000 мкм з розмірами 35 × 35 мм наносяться шари однокомпонентного вологезатверджувального полідиметилсилоксанового адгезиву SE 4485 товщиною до 30 мкм з теплопровідністю ~ 2,8 Вт/(м·К). Адгезивні шари витримуються на повітрі при кімнатній температурі і вологості 55–65 % протягом 10 хвилин. Потім на алюмінієві основи з нанесеними адгезивними шарами укладаються мідь-поліїмідні або алюміній-поліїмідні теплопровідні лакофольгові діелектрики. Приклеювання мідь-поліїмідного або алюміній-поліїмідного лакофольгового діелектрика зверху на алюмінієву основу плати здійснюється в технологічному оснащенні з притисканням до повного затвердіння протягом 24 годин.

3. Результати та їх обговорення

На рис. 3 представлені експериментальні комбіновані друковані плати на алюмінієвих основах з тонкими III діелектриками, які вкриті мідною або алюмінієвою фольгою. На рис. 4 представлено ТСЯ плат для перевірки основних хімічних, механічних та електричних властивостей розроблених комбінованих друкованих плат та ТСЯ електронного модуля для дослідження теплових властивостей плат.

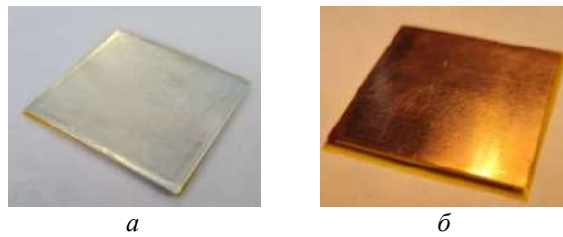


Рис. 3. Експериментальні комбіновані друковані плати на алюмінієвих основах з ПІ діелектриками, які вкриті мідною (а) або алюмінієвою фольгою (б)

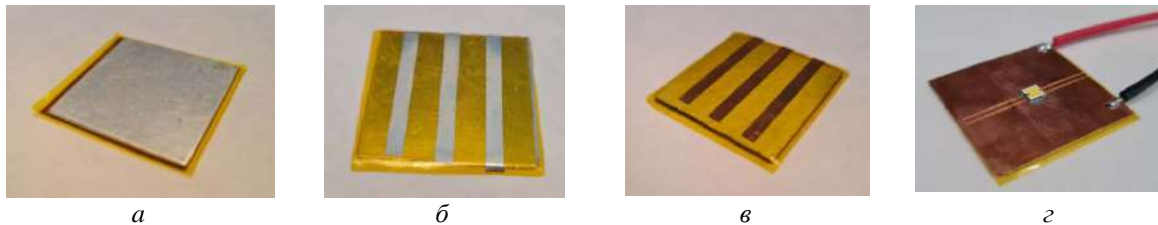


Рис. 4. Тестові структури якості для перевірки основних властивостей розроблених комбінованих друкованих плат: а – для перевірки електричної міцності; б – для перевірки міцності на відшаровування алюмінієвої фольги; в – для перевірки міцності на відшаровування мідної фольги; г – для перевірки теплових властивостей

Дослідження основних хімічних, механічних, електричних та теплових властивостей виготовлених експериментальних зразків комбінованих друкованих плат на алюмінієвих основах з тонкими ПІ діелектриками проводились у нормальних кліматичних умовах. Перевірка зовнішнього вигляду плат проводилася візуальним оглядом із застосуванням, за необхідності, оптичних приладів (лупа, мікроскоп), кратність збільшення яких не менше чотирьох.

Експериментальні комбіновані плати та тестові структури якості плат проходили перевірку на сумісність їх процесів виготовлення із основними технологічними процесами, які прийняті у виробництві друкованих плат. У тому числі на сумісність з процесами нанесення фоторезисту на алюмінієву та мідну фольгу та на композиційні теплопровідні ПІ шари в платах. Проводилася також перевірка на сумісність із процесами формування фоторезистивних масок, рідинного травлення алюмінієвої та мідної фольги та композиційних ПІ шарів, а також видалення фоторезистивних масок та фінішного очищення плат.

Перевірка механічних та електричних властивостей розроблених комбінованих плат і ТСЯ плат проводилася відповідно до стандарту IPC-TM-650 Test Methods Manual (Посібник з методів випробувань, США), який є найбільш всебічним довідником і який широко використовується за методами випробувань фольгованих діелектриків і за допомогою яких перевіряються їх основні властивості [11].

Перевірка міцності на відшаровування мідної або алюмінієвої фольги проводилася відповідно до гармонізованого стандарту IPC-TM-650, метод тестування 2.4.9. Міцність на відшаровування мідної або алюмінієвої фольги перевірялася на трьох зразках шириною 3 мм та довжиною 35 мм, підготовлених за допомогою фотолітографії, методом відшаровування під кутом 180°. Перед випробуванням один кінець кожної смужки мідної або алюмінієвої фольги відокремлювали вручну від лакового ПІ шару і закріплювали його в затиску вимірювального пристрою. На кожній смужці визначали мінімальне стійке значення навантаження, що викликає відрив смужки фольги на довжину щонайменше 20 мм. Міцність зчеплення фольги визначалася як середнє арифметичне значення величини навантаження при мініальному та максимальному відшаровуванні смужок. За позитивний результат приймалося середнє арифметичне значення навантажень трьох паралельних вимірювань фольги.

Перевірка електричної міцності ПІ діелектриків комбінованих плат на теплопровідній алюмінієвій основі проводилася відповідно до гармонізованого стандарту IPC-TM-650, метод тестування 2.5.6.3 «Напруга пробєю діелектрика та діелектрична міцність» за допомогою вимірювача напруги пробєю АІМ-90.

При проведенні випробувань зразків комбінованих плат на основі промислових стандартних багат шарових термозварюваних ПМФ плівок DuPont™ Kapton® 120FN 616, в яких застосовано плівку-основу Kapton® HN товщиною 25 мкм з теплопровідністю 0,12 Вт/(м·К), були отримані наступні результати:

- усереднені значення міцності на відшарування мідної або алюмінієвої фольги у зразків, що випробовуються, від ПІ діелектрика склали не менше 0,25 кгс/см (250 г/см або 2,5 Н/см);

- усереднені значення напруги пробою діелектричної теплопровідної ПІ плівки Kapton® 120FN 616 склали від 4,0 кВ/мил (160 В/мкм) до 5,0 кВ/мил (200 В/мкм).

При проведенні випробувань зразків комбінованих плат на основі промислових теплопровідних термозварюваних ПМФ плівок Kapton®120FMT616, в яких застосовано плівку-основу Kapton®120FMT616 товщиною 25 мкм з теплопровідністю 0,46 Вт/(м·К), було отримано наступні результати:

- усереднені значення міцності на відшарування мідної або алюмінієвої фольги від ПІ діелектрика у зразків, що випробовуються, склали не менше 0,25 кгс/см (250 г/см або 2,5 Н/см);

- усереднені значення напруги пробою діелектричної ПІ плівки Kapton® 120FN 616 становили понад 4,0 кВ/мил (160 В/мкм).

При проведенні випробувань зразків комбінованих плат на основі безадгезивних мідь-поліімідних або алюміній-поліімідних лакофольгових діелектриків з ПІ шаром товщиною 25–30 мкм з теплопровідністю до 1,0 Вт/(м·К), були отримані наступні результати:

- усереднені значення міцності на відшарування безадгезивного лакофольгового теплопровідного ПІ діелектрика фольгованого міддю або алюмінієм від силіконового адгезиву SE 4485 у зразків, що випробовуються, склали не менше 0,2 кгс/см (200 г/см або 2,0 Н/см);

- усереднені значення напруги пробою експериментального високотеплопровідного композиційного ПІ шару товщиною 25–30 мкм з теплопровідністю 1,0 Вт/(м·К) становили понад 3,0 кВ/мил (120 В/мкм).

Експериментальні дослідження теплових властивостей плат проводилися в термошафі за допомогою ТСЯ електронного модулю з комбінованою платою на алюмінієвій основі з промисловою стандартною багат шаровою термозварюваною ПМФ плівкою DuPont™ Kapton® 120FN 616 зі стандартною теплопровідністю $\sim 0,12$ Вт/(м·К) при задовільних та погіршених умовах експлуатації.

На рис. 5 представлено графіки залежності температур нагріву плати ТСЯ електронного модулю з розміром плати 35×35 мм в області паяння джерела тепла потужністю до 2 Вт, та температур зворотної сторони алюмінієвої основи плати товщиною 1 мм від часу до переходу у стійкий температурний стан.

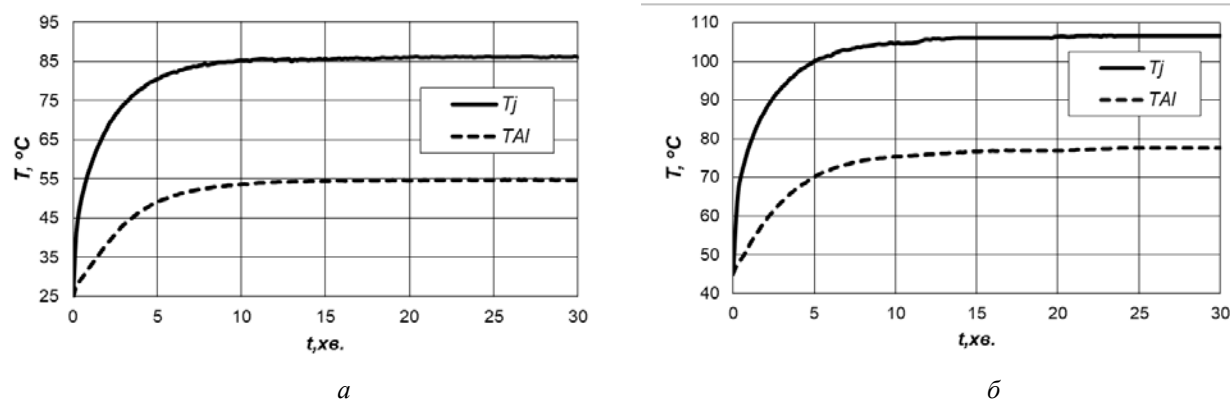


Рис. 5. Залежність зміни температури нагріву на платі електронного модулю з розміром 35×35 мм в області паяння джерела тепла T_j та температури зворотної сторони алюмінієвої основи плати T_{Al} від часу при переході у стабільний температурний стан: *a* – температура довкілля $T_a = 25^\circ\text{C}$; *б* – температура довкілля, $T_a = 45^\circ\text{C}$

З графіка на рис. 5, *a* видно, що при використанні джерела тепла площею $4,55 \text{ мм}^2$ з потужністю 2 Вт при температурі навколишнього середовища $T_a = 25^\circ\text{C}$ температура в області паяння на платі досягає $86,1^\circ\text{C}$ за 20 хвилин, переходячи у стійкий стан. Температура зворотної сторони алюмінієвої основи плати за цей проміжок часу переходить у стійкий стан при $54,8^\circ\text{C}$.

З графіка на рис. 5, *б* слідує, що за температури навколишнього середовища $T_a = 45^\circ\text{C}$ температура в області пайки на платі досягає $106,6^\circ\text{C}$ за 20 хвилин, переходячи у стійкий стан. Температура зворотної сторони алюмінієвої основи плати переходить у стійкий стан при $77,5^\circ\text{C}$.

Результати експериментальних досліджень температур на платі ТСЯ електронного модуля з комбінованою платою на основі промислової стандартної багат шарової термозварювальної ПМФ плівки DuPont™ Kapton® 120FN 616 зі стандартною теплопровідністю $\sim 0,12 \text{ Вт}/(\text{м}\cdot\text{К})$ практично збігаються з результатами моделювання теплових властивостей плати з розміром $35 \times 35 \text{ мм}$ моделі 3 електронного модуля на основі комбінованої плати з багат шаровою ПМФ плівкою DuPont™ Kapton® 120FN 616, які були проведені за допомогою програмного комплексу COMSOL MULTIPHYSICS при погіршених умовах експлуатації (рис. 2).

Таким чином, результати проведених досліджень експериментальних зразків комбінованих друкованих плат на алюмінієвих основах з тонкими ПІ діелектриками підтвердили правильність обраних конструктивно-технологічних рішень, способів виготовлення плат та застосованих у них матеріалів. Експериментальні комбіновані плати пройшли успішну перевірку на сумісність їх технологічних процесів виготовлення з основними технологічними процесами, які прийняті у виробництві друкованих плат.

Нові підходи при розробці комбінованих друкованих плат на алюмінієвих основах з ПІ діелектриками, у тому числі теплопровідними, забезпечують значно менший загальний тепловий опір розробленої тепловідвідної системи плат (від $\sim 0,23$ до $\sim 0,06^\circ\text{C}/\text{Вт}$) [1], що мають кращі показники в порівнянні з середніми значеннями ($\sim 0,43^\circ\text{C}/\text{Вт}$) повних теплових опорів діелектричних шарів на основі сучасних стандартних теплопровідних адгезивів із полімерів із добавками дрібнодисперсних порошків теплопровідних керамік і які не поступаються за тепловою ефективністю промисловим платам MC PCB таких визнаних світових виробників плат як Ruikai, Totking, (Китай) і Bergquist (США) [12].

Висновки

Авторами запропоновано нові підходи для виготовлення комбінованих плат на алюмінієвих основах з різними типами тонких ПІ діелектриків, у тому числі теплопровідних, які вкриті мідною або алюмінієвою фольгою.

Розроблено конструктивно-технологічні рішення, способи виготовлення та виготовлено експериментальні зразки комбінованих друкованих плат на алюмінієвих основах із застосуванням як діелектриків промислових тонких поліімідних плівок з теплопровідністю від $0,12$ до $0,46 \text{ Вт}/(\text{м}\cdot\text{К})$ з термозварюваними двосторонніми фторполімерними покриттями Teflon® FEP. Розроблено конструктивно-технологічні рішення, способи виготовлення і виготовлено експериментальні зразки комбінованих друкованих плат на алюмінієвих основах із застосуванням розроблених безадгезивних мідь-поліімідних та алюміній-поліімідних лакофольгових діелектриків з теплопровідністю лакових поліімідних шарів від $0,12 \text{ Вт}/(\text{м}\cdot\text{К})$ до $1,0 \text{ Вт}/(\text{м}\cdot\text{К})$ та більше.

Досліджено основні хімічні, механічні, електричні та теплові властивості різних типів експериментальних комбінованих друкованих плат на алюмінієвих основах з тонкими поліімідними діелектриками для застосування в електронних модулях та друкованих вузлах для світлодіодних джерел світла, приймачів концентрованого сонячного випромінювання, мікроелектронних сенсорних модулів електромагнітних випромінювань, детекторів елементарних частинок та інших електронних виробів. У тому числі із застосуванням COB та COF технологій збирання різноманітних модулів з безкорпусними напівпровідниковими чіпами з підвищеною потужністю.

Список літератури:

1. Боднар Д. Металеві та композитні теплопровідні матеріали для потужних напівпровідникових корпусів // Компоненти та технології. 2014. № 12. С. 155–160.
2. Комбіновані теплопровідні плати з діелектриками з полііміду / В.М. Борщов, О.М. Лістратенко, М.А. Проценко, І.Т. Тимчук, О.В. Кравченко, О.В. Суддя, І.В. Борщов, М.І., Сліпченко // Радіотехніка. 2023. Вип. 212. С. 115–126.
3. Поліімідна плівка DuPont™ Kapton® HN, <https://www.dupont.com/products/kapton-hn.html> // офіційний сайт (дата звернення 05.12.2023).
4. Теплопровідна поліімідна плівка DuPont Kapton MT, <https://www.dupont.com/products/kapton-mt.html> // офіційний сайт (дата звернення 05.12.2023).
5. Теплопровідна електроізолююча поліімідна плівка типу KYPI-MT (Китай), <https://www.kying.com> // офіційний сайт (дата звернення 05.12.2023).
6. Structural modeling and calculation of thermal conductivity of polyimide composite materials / V.M. Borshchov, O.M. Listratenko, M.A. Protsenko, I.T. Tymchuk, O.V. Kravchenko, O.V. Syddia, I.V. Borshchov, M.I. Slipchenko // Radiotekhnika. 2022. №211. P. 133–142.
7. Поліімідно-фторопластова плівка DuPont™Kapton® 120FN616, <https://www.dupont.com/products/kapton-fmt.html> // офіційний сайт (дата звернення 05.12.2023).
8. Теплопровідна поліімідно-фторопластова плівка DuPont™ Kapton® 120FMT616, <https://www.dupont.com/products/kapton-fmt.html> // офіційний сайт (дата звернення 05.12.2023).
9. Теплопровідна поліімідно-фторопластова плівка, що термозварюється KYMIDE KYPIFMT 616 (Китай), <https://www.kying.com> // офіційний сайт (дата звернення 05.12.2023).
10. Dow Corning SE 4485 thermally conductive silicone adhesive, <https://www.dowcorning.com> // офіційний сайт (дата звернення 05.12.2023).
11. Стандарт IPC-TM-650:2002. Test Methods Manual : посібник із вибору методів контролю друкованих плат.
12. Максимов А. Порівняльне дослідження теплопровідних властивостей матеріалів // Напівпровідникова світлотехніка. 2013. №4. С. 3–15.

Надійшла до редколегії 15.12.2023

Відомості про авторів:

Борщов Вячеслав Миколайович – д-р техн. наук, професор, ТОВ «Науково-виробниче підприємство «ЛТУ», перший заступник директора – головний конструктор; Україна; e-mail: viatcheslav.borshchov@cern.ch; ORCID: <https://orcid.org/0000-0002-5579-8932>

Лістратенко Олександр Михайлович – канд. техн. наук, ТОВ «Науково-виробниче підприємство «ЛТУ», провідний науковий співробітник; Україна; e-mail: sasha.listratenko.12@gmail.com; ORCID: <https://orcid.org/0000-0001-7643-5295>

Сліпченко Микола Іванович – д-р фіз.-мат. наук, професор, Інститут скінтіляційних матеріалів НАНУ, провідний науковий співробітник; Україна; e-mail: naukovets.big@gmail.com; ORCID: <https://orcid.org/0000-0002-4242-4800>

Проценко Максим Анатолійович – канд. техн. наук, ТОВ «Науково-виробниче підприємство «ЛТУ», начальник відділення – заступник головного конструктора; Україна; e-mail: max.protsenko.1978@gmail.com; ORCID: <https://orcid.org/0000-0001-9313-1701>

Тимчук Ігор Трохимович – канд. техн. наук, ТОВ «Науково-виробниче підприємство «ЛТУ», головний технолог; Україна; e-mail: ihortymchuk78@gmail.com; ORCID: <https://orcid.org/0000-0002-6436-7253>

Кравченко Олександр Вікторович – заступник начальника відділу; ТОВ «Науково-виробниче підприємство «ЛТУ», Україна; e-mail: kravcenkoaleksandr671@gmail.com; ORCID: <https://orcid.org/0000-0002-7145-4304>

Борщов Ілля Вячеславович – інженер; ТОВ «Науково-виробниче підприємство «ЛТУ», Україна, e-mail: illia.borshchov1@nure.ua; ORCID: <https://orcid.org/0000-0002-6598-6988>

*М.С. АЛФЬОРОВ, М.В. ВОЛОВЕНКО, І.О. МОЩЕНКО, канд. техн. наук,
О.М. НІКІТЕНКО, канд. техн. наук*

ПОРІВНЯННЯ ВИХІДНОГО СПЕКТРУ ДЛЯ ЧОТИРЬОХ МОДЕЛЕЙ ПРИЛАДІВ ЗІ СХРЕЩЕНИМИ ПОЛЯМИ

Вступ

У попередніх роботах [1 – 3] розглянуто дві моделі приладів зі схрещеними полями: магнетрона та магнетронного діода.

Прилади зі схрещеними полями є генераторами НВЧ сигналів великої потужності. Ці прилади асоціюються з високою ефективністю, малою вагою, достатньою пропускнуою здатністю та хорошою продуктивністю щодо різних параметрів [4].

Прилади зі схрещеними полями, такі як магнетронний діод, магнетрон, магнетронний підсилювач тощо, використовують у промисловості, науці, медицині, побуті [3, 5].

Магнетрон є одним з найдавніших та таких, що широко розповсюджені, мікрохвильових генераторів. У цих приладах електрони рухаються у схрещених статичних електричному та магнітному полях та взаємодіють з високочастотними електромагнітними полями.

Конструктивно сучасний магнетрон містить три частини:

- катодний вузол;
- анод з об'ємними резонаторами;
- вузлом виводу високочастотної енергії [1].

Рух електронів у таких приладах, як магнетрони, відбувається під дією схрещених статичних електричних і магнітних полів з взаємодією з радіочастотними електромагнітними полями [1].

Вважається, що домінуючим типом взаємодії в таких пристроях є взаємодія заряджених частинок (електронів) з високочастотними електромагнітними полями (діокотронний ефект). Така взаємодія призводить до нелінійної нестійкості класичного бріллуенівського потоку, що має місце у присутності високочастотних хвиль, які розповсюджуються в уповільнювальних системах, що містять такі прилади [6].

Роботи таких приладів аналізують за допомогою РС (частинка в комірці) кодів та теорії ведучих центрів [6], хоча останню майже не застосовують.

Після набуття робочого профілю щільності високочастотна хвиля зростає до досягнення насичення. Основна високочастотна хвиля буде конкуруватиме з будь-якими іншими високочастотними хвилями (шумом) у приладі і потім генеруватимуть усі можливі гармоніки та биття хвиль [6].

Тут розглянемо такі енергетичні показники, як індукований струм і його спектри, й порівняємо ці спектри для гладкого анода (магнетронний діод) і анода з резонаторами з порожниною (магнетрон).

Мета роботи – показати різницю між вихідними спектрами приладів з гладким анодом (магнетронний діод) і приладів з анодом, що містить порожнинні резонатори (магнетрон) та порівняти спектральні складові з основною частотою реального приладу.

Теоретичні засади

Розглянемо дві форми циліндричних систем зі схрещеними полями: найпростішу форму – магнетронний діод та магнетрон і дві форми площинних систем зі схрещеними полями такі ж самі як і циліндричні. Схематичне зображення циліндричних конструкцій наведено на рис. 1. Циліндричний магнетронний діод (рис. 1, *а*) складається з двох коаксіальних циліндрів. Внутрішній циліндр є катодом з відносним радіусом, який дорівнює 1. Зовнішній циліндр є анодом з відносним радіусом, який дорівнює s_a . Циліндричний магнетрон (рис. 1, *б*)

містить внутрішній циліндр, що є катодом з відносним радіусом, який дорівнює 1, та зовнішній електрод з порожнистими резонаторами.

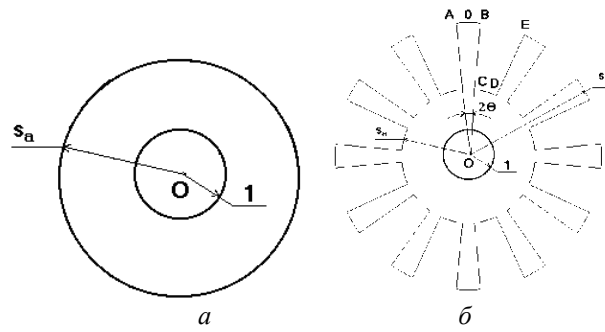


Рис. 1. Простір взаємодії: *a* – циліндричний магнетронний діод; *б* – циліндричний магнетрон

Площинні конструкції наведено на рис. 2. Площинний діод (рис. 2, *a*) складається з двох паралельних площин, відстань між якими дорівнює *d*. Магнетрон (рис. 2, *б*) містить одну площину, яка є катодом. На відстані *d* від неї розташований анод, який містить ламелі.

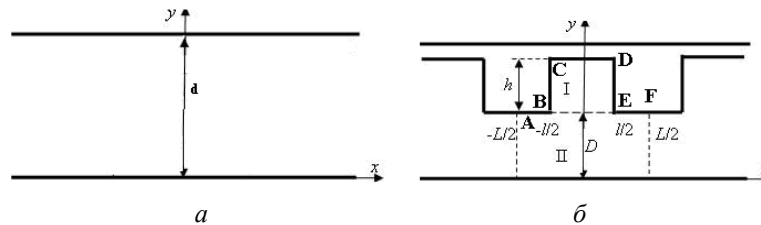


Рис. 2. Простір взаємодії: *a* – площинний магнетронний діод; *б* – площинний магнетрон

Індукований струм є струмом, наводиться на аноді хвилею просторового заряду і передає енергію від хвилі до аноду і визначається як $i = q\vec{v}\vec{E}$, де q – заряд частинки; \vec{v} – швидкість, з якою рухається ця частинка; \vec{E} – напруженість електричного поля.

Напруженість електричного поля визначають як градієнт розподілу електростатичного потенціалу, який у свою чергу є розв'язком рівняння Лапласа $\Delta U = 0$.

Швидкість зарядженої частинки визначають з розв'язків рівнянь руху.

У загальному випадку рівняння руху у полярних координатах (s, φ) є задачею Коші та описують такими рівняннями:

$$\begin{aligned} \frac{d^2s}{dt^2} &= -s \left(\frac{d\varphi}{dt} \right)^2 = \eta \left(E_s + Bs \frac{d\varphi}{dt} \right) \\ s \frac{d^2\varphi}{dt^2} + 2 \frac{ds}{dt} \frac{d\varphi}{dt} &= \eta \left(E_\varphi - B \frac{ds}{dt} \right), \end{aligned} \quad (1)$$

де s – безрозмірний радіус r/r_c ; $\eta = 1,76 \cdot 10^{11}$ Кл/кг – відносний заряд електрона; B – напруженість аксіального магнітного поля; E_s – напруженість електростатичного поля по радіальній координаті; E_φ – напруженість електростатичного поля по азимутальній координаті з початковими умовами

$$\begin{aligned} s(0) &= 1; \quad \left. \frac{ds}{dt} \right|_{t=0} = 0; \\ \varphi(0) &= 0; \quad \left. \frac{d\varphi}{dt} \right|_{t=0} = 0. \end{aligned} \quad (2)$$

Напруженість електростатичного поля у циліндричному магнетронному діоді визначають як

$$E_s = \frac{\eta}{r_k^2 \omega_H^2} \frac{U_a}{s \ln s_a}, E_\varphi = 0.$$

Вищезгадана система (1) для циліндричного магнетронного діода перетворюється у

$$\begin{aligned} \frac{d^2 s}{dt^2} &= -\frac{s}{4} + \frac{b}{s} + \frac{1}{4s^3}; \\ \frac{d\varphi}{dt} &= \frac{1}{2} \left(1 - \frac{1}{s^2} \right). \end{aligned} \quad (3)$$

Тут $b = \frac{\eta U_a}{r_c^2 \omega_H^2} \ln s_a$.

Для циліндричного магнетрона напруженість електростатичного поля з [7, 8] визначаємо як

$$\begin{aligned} E_s &= \frac{a_0 z}{s} \left(1 - 2N \ln \frac{s_v}{s_a} \sum_{n=1}^{\infty} a_n \operatorname{cor} s^{Nn} \cos Nn\varphi \right); \\ E_\varphi &= 2a_0 z N \ln \frac{s_v}{s_a} \sum_{n=1}^{\infty} a_n \operatorname{sir} s^{Nn} \sin Nn\varphi \end{aligned}$$

де N – кількість резонаторів; $a_0 = \frac{U_a}{\ln s_a + \frac{N\theta}{\pi} \ln \frac{s_v}{s_a}}$,

$$a_n = \frac{\sin Nn\theta}{(Nn\theta + \sin 2Nn\theta) (\operatorname{sir} s_v^{Nn} - \operatorname{sir} s_a^{Nn}) + \pi \operatorname{sir} s_a^{Nn}},$$

$$z = \frac{U_a}{\omega_H^2 r_k^2}; \operatorname{sir} x = \frac{x - x^{-1}}{2}; \operatorname{cor} x = \frac{x + x^{-1}}{2}.$$

Система (1) для циліндричного магнетрона перетворюється у

$$\begin{aligned} \frac{d^2 s}{dt^2} + \left(1 - \frac{d\varphi}{dt} \right) \frac{d\varphi}{dt} s &= \eta E_s; \\ \frac{d^2 \varphi}{dt^2} + \frac{1}{s} \frac{ds}{dt} \left(2 \frac{d\varphi}{dt} - 1 \right) &= \eta E_\varphi. \end{aligned} \quad (4)$$

У загальному випадку рівняння руху у декартових координатах (x, y) є задачею Коші та описують рівняннями

$$\begin{aligned} \frac{d^2 x}{dt^2} &= \eta \left(E_x + B \frac{dy}{dt} \right) \\ \frac{d^2 y}{dt^2} &= \eta \left(E_y - B \frac{dx}{dt} \right) \end{aligned}, \quad (5)$$

де E_s – напруженість електростатичного поля вздовж осі абсцис, E_φ – напруженість електростатичного поля вздовж осі ординат з початковими умовами

$$x(0) = 0; \left. \frac{dx}{dt} \right|_{t=0} = 0; y(0) = 0; \left. \frac{dy}{dt} \right|_{t=0} = 0. \quad (6)$$

Напруженість електростатичного поля у площинному магнетронному діоді визначають як

$$E_x = 0, E_y = \eta \frac{U_a}{D}.$$

Система (5) для площинного магнетронного діоду перетворюється у

$$\begin{aligned} \frac{d^2 x}{dt^2} &= \omega_H \frac{dy}{dt} \\ \frac{d^2 y}{dt^2} &= \frac{\eta U_a}{d} - B \frac{dx}{dy} \end{aligned} \quad (7)$$

Ця система рівнянь має аналітичний розв'язок для початкових умов (6):

$$\begin{aligned} x &= \frac{\eta U_a}{\omega_H^2} (\omega_H t - \sin \omega_H t) \\ y &= \frac{\eta U_a}{\omega_H^2} (1 - \cos \omega_H t) \end{aligned}$$

Для площинного магнетрону напруженість електростатичного поля визначають з [7, 11] як

$$\begin{aligned} E_x &= \frac{4\pi h}{L} A_0 \sum_{n=1}^{\infty} n A_n \sin \frac{2\pi n x}{L} \operatorname{sh} \frac{ny}{D} \\ E_y &= A_0 \left(1 - \frac{4\pi h}{D} \sum_{n=1}^{\infty} n A_n \cos \frac{2\pi n x}{L} \operatorname{ch} \frac{ny}{D} \right) \end{aligned}$$

де

$$\begin{aligned} A_0 &= \frac{U_a}{D + \frac{lh}{L}} \\ A_n &= \frac{\sin \frac{\pi n l}{L}}{\left(\frac{\pi n l}{L} + \sin \frac{2\pi n l}{L} \right) \left(\operatorname{sh} \frac{n(h+D)}{D} - \operatorname{sh} n \right) + \pi \operatorname{sh} n} \end{aligned}$$

Тут використовують систему рівнянь (5) без будь-яких перетворень.

Результати

Рівняння руху (3) з початковими умовами (2) не мають аналітичного розв'язку, тому, використовуючи чисельне розв'язування методом Рунге – Кутти, отримуємо траєкторії руху електронів у циліндричному магнетронному діоді. Вигляд цих траєкторій наведено на рис. 3.

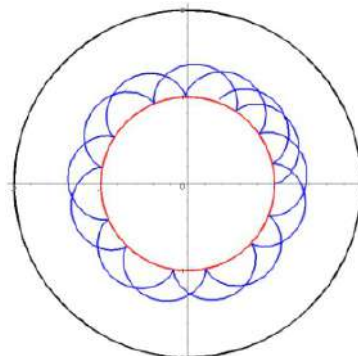


Рис. 3. Траєкторії руху електронів у циліндричному магнетронному діоді

Рівняння руху (4) з початковими умовами (2) не мають аналітичного розв'язку, тому, використовуючи чисельне розв'язування методом Рунге – Кутти, отримуємо траєкторії руху електронів в магнетроні. Вигляд цих траєкторій наведено на рис. 4.

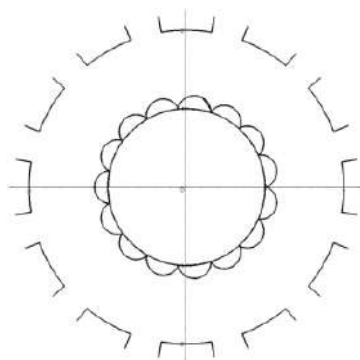


Рис. 4. Траєкторії руху електронів у циліндричному магнетроні

Такий вигляд траєкторій (рис. 3 та 4) не суперечить загальноприйнятим уявленням про траєкторії заряджених частинок у схрещених електричному та магнітному полях. Ці траєкторії схожі на циклоїди, але не є епіциклоїдами.

Як відомо і базуючись на розв'язку системи рівнянь (7), у площинному магнетронному діоді траєкторії електронів є циклоїдами.

Рівняння руху (5) з початковими умовами (6) не мають аналітичного розв'язку, тому, використовуючи чисельне розв'язування методом Рунге – Кутти, отримуємо траєкторії руху електронів у площинному магнетроні. Вигляд цих траєкторій наведено на рис. 5.

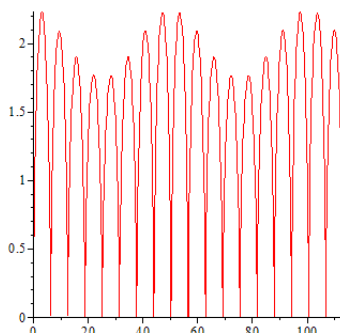


Рис. 5. Траєкторії руху електронів у площинному магнетроні

Така поведінка траєкторії визначається модуляцією електронного потоку просторово-періодичним розподілом електростатичного поля у площинному магнетроні.

Обговорення

За траєкторіями руху заряджених частинок практично неможливо визначити частоти коливальних процесів, що мають місце в системах зі схрещеними електричним і магнітним полями.

Для їх визначення доцільно використовувати якусь енергетичну характеристику, наприклад індукований струм.

Через те, що цей струм отримуємо чисельними методами, то для визначення спектральних характеристик індукційного струму доцільно скористатися методом швидкого перетворення Фур'є.

Застосовуючи метод швидкого перетворення Фур'є до індукованого струму в магнетронному діоді, ми отримали спектр, який наведено на рис. 6.

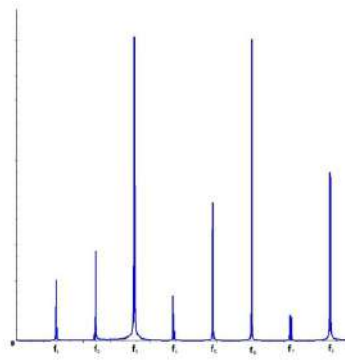


Рис. 6. Спектр індукованого струму у циліндричному магнетронному діоді

Застосовуючи метод швидкого перетворення Фур'є до індукованого струму у циліндричному магнетронному діоді, ми отримали спектр, який наведено на рис. 7.

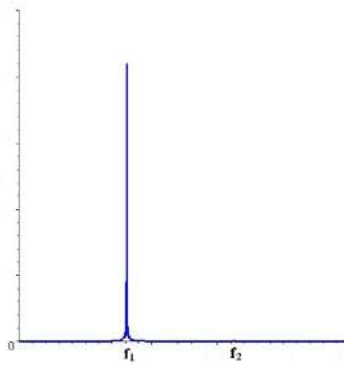


Рис. 7. Спектр індукованого струму у циліндричному магнетроні

Спектр, що наведено на рис. 6, має вісім компонентів. Третя гармоніка у цьому спектрі знаходиться поблизу основної частоти магнетрона для мікрохвильової пічки М-105, який є базою для проведення досліджень. У цьому випадку різниця між обчисленою частотою та реальною становить близько 10%.

Спектр, що наведено на рис. 7, містить дві компоненти. Перша гармоніка цього спектру розташована поблизу основної частоти магнетрона для мікрохвильової пічки. У цьому випадку різниця між обчисленою частотою та реальною не перевищує 3%. Таку маленьку розбіжність між обчисленою та реальною частотами можна пояснити наявністю просторово-періодичного розподілу електростатичного поля [9, 10].

Рух електронів у приладах зі схрещеного поля вздовж електродів призводить до виникнення індукційного струму, який визначають як $i = q\vec{v}\vec{E}$.

Проаналізувавши розбіжність електричного поля у площинному магнетронному діоді, ми отримали такий результат для індукованого струму

$$i = e \left(v_x 0 + v_y \frac{U_a}{d} \right) = e v_y \frac{U_a}{d}.$$

Тоді з рівнянь руху добудемо

$$v_y = \frac{\eta U_a}{d \omega_H} \sin \omega_H t.$$

Таким чином, індукований струм у площинному магнетронному діоді можна описати виразом

$$i = e \frac{\eta U_a^2}{d^2 \omega_H} \sin \omega_H t .$$

Отже, індукований струм у площинному магнетронному діоді має лише одну складову з частотою, яка дорівнює циклотронній. Ця частота майже вдвічі перевищує частоту генерації магнетрона для мікрохвильової пічки.

Спектр індукованого струму у площинному магнетроні має три компоненти: центральна з циклотронною частотою та дві бічні компоненти з частотою модулювання. Ці частоти мають велику різницю з частотою генерації магнетрона для мікрохвильової пічки.

Висновки

Описано чотири моделі приладів зі схрещеним полями, які найчастіше використовують у теоретичних дослідженнях таких приладів: циліндричний магнетрон, циліндричний магнетронний діод, площинний магнетронний діод і площинний магнетрон. Як базовий прилад для дослідження вибрано магнетрон, який використовують у мікрохвильовій пічці (М-105).

В результаті досліджень спектру індукованого струму у циліндричному магнетронному діоді виявлено, що він містить вісім компонент. Найближчою до основної частоти магнетрона для мікрохвильової пічки є третя гармоніка. У цьому випадку розбіжність між частотами, які порівнюють, становить близько 10 %. Отже, модель циліндричного магнетронного діода не дуже добре підходить для моделювання роботи приладів зі схрещеними полями.

Під час моделювання у циліндричному магнетроні виявлено дві складові у спектрі індукованого струму. Найближчою до основної частоти магнетрона для мікрохвильової пічки є перша гармоніка. У цьому випадку розбіжність між частотами, які порівнюють, не перевищує 3 %. Таку невелику розбіжність між обчисленою та реальною частотами можна пояснити наявністю просторово-періодичного розподілу електростатичного поля [9, 10]. Таким чином, модель циліндричного магнетрона добре підходить для моделювання роботи приладів зі схрещеними полями.

В площинному магнетронному діоді в спектрі індукованого струму виявлено лише одну компоненту, частота якою збігається з циклотронною частотою. Розбіжність між реальною частотою та частотою, що отримана в результаті моделювання, є надто великою. Таким чином, модель площинного магнетронного діода не дуже добре підходить для моделювання роботи приладів зі схрещеними полями.

Спектр індукованого струму у площинному магнетроні має три компоненти: центральна з циклотронною частотою та дві бічні компоненти з частотою модулювання. Ці частоти мають велику різницю з частотою генерації магнетрона для мікрохвильової пічки. Отже, модель площинного магнетронного діода не дуже добре підходить для моделювання роботи приладів зі схрещеними полями.

Список літератури:

1. Nikitenko O. Has a magnetron abnormal current // The Fourth International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo'2019) Odesa. doi: 10.1109/UkrMiCo47782.2019.9165516.
2. I. Tahir, A. C. Dexter, R. G. Carter Frequency and phase modulation performance of an injection-locked CW magnetron // [IEEE Transactions on Electron Devices](#) 53(7), 2006, 1721 – 1729
3. The shearing modes approach to the theory of the diocotron instability of the cylindrical electron layer / V.V. Mykhaylenko, Hae June Lee, V.S. Mykhaylenko, N.A. Azarenkov // Питання атомної науки і техніки. — 2013. — № 4. — С. 25-29.
4. Wadhwa R.D. Crossed-field microwave devices // IETE Journal of Research. 1978. Vol 24, issue 10-11. P. 418-437.
5. Nikitenko O., Volovenko V. Changed particles motion in crossed-field system under dissipation // International Conference Modern Problems of radio Engineering, Telecommunications and Computer Science. Proceeding of the International Conference TCSET 2002. Lviv Polytechnic National University. February 18–23, 2002. Lviv-Slavske, Ukraine, 2002. P. 59–60.

6. Kaup D.J., El-Reedy J.O., Thomas G.E. Parametric interactions inside a magnetron // Journal Plasma Physics. 2000. Vol. 64, part 4. P. 489–506.
7. Nikitenko O.M. Distribution of electrostatic potential in crossedfield system with complex electrodes' configuration // Journal of Microwaves and Optoelectronics. 2000. Vol. 2, No. 2. P. 1–9.
8. P A Tsygankov, E A Orozco, V D Dugar-Zhabon, J E L´opez, and P A C´ardenas Simulation of the electron dynamics in a magnetron sputtering device with equipotential and non-equipotential cathode // Journal of Physics: Conference Series 1386 (2019) 012127 IOP Publishing doi:10.1088/1742-6596/1386/1/012127.
9. Kim J.I., Won J.H., Park G.S., Ha H.J., Shon J.C. Reduction of Noise in Strapped Magnetron by Electric Priming Using Anode Shape Modification // 2006 IEEE International Vacuum Electronic Conference April 25 – 27, 2006, Monterey, USA. P. 355–356.
10. Kim J.I., Won J.H., Park G.S., Ha H.J., Shon J.C. Reduction of Noise in Strapped Magnetron by Electric Priming Using Anode Shape Modification // Applied Physics Letters 88. 2006. P. 221501-1–221501-3.
11. Крохмаль Т. М., О.М. Нікітенко Особливості траєкторій руху заряджених частинок у схрещених електричному та магнітному полях // Зб. наук. пр. фіз.-мат. ф-ту ДДПУ. Слов'янськ : ДДПУ, 2021. № 11, С. 59–72. <https://doi.org/10.31865/2413-26672415-3079112021234838>

Надійшла до редколегії 17.10.2023

Відомості про авторів:

Алфьоров Микола Євгенович – Харківський національний університет радіоелектроніки, старший викладач кафедри радіотехнологій інформаційно-комунікаційних систем; Україна; e-mail: mykola.alforov@nure.ua; ORCID: <https://orcid.org/0000-0002-1590-3902>

Воловенко Микола Володимирович – Національний Науковий Центр «Харківський фізико-технічний інститут», молодший науковий співробітник; Україна; e-mail: mykolauz@gmail.com; ORCID: <https://orcid.org/0000-0001-7216-2058>

Мощенко Інна Олексіївна – Харківський національний університет радіоелектроніки, старший викладач кафедри інформаційно-вимірювальних технологій; Україна; e-mail: inna.moshchenko@nure.ua; ORCID: <https://orcid.org/0000-0002-2738-0037>

Нікітенко Олександр Миколайович – канд. техн. наук, Харківський національний університет радіоелектроніки, адміністратор баз даних наукової бібліотеки; Україна; e-mail: nikonxipe@gmail.com; ORCID: <https://orcid.org/0000-0002-1082-5247>

MICROWAVE ANTENNAS AND DEVICES АНТЕНИ І ПРИСТРОЇ МІКРОХВИЛЬОВОЇ ТЕХНІКИ

УДК 621.396; 004.8

DOI:10.30837/rt.2023.4.215.08

M.V. ROZHNOVSKYI, PhD, I.Yu. ROZHNOVSKA, PhD

APPLICATION OF ARTIFICIAL INTELLIGENCE METHOD IN ADAPTIVE ANTENNA SYSTEM

Introduction

The rapid development of modern telecommunications is leading to the evolution of communication technology generations from 5G [1] to 6G [2 – 4]. One of the main components of 5G and 6G telecommunication networks are radio networks [1 – 4], and obviously the quality of their functioning directly depends on the antenna technologies and antenna systems used. When designing antenna systems for 5G and 6G networks, the main issue is the full implementation of so-called "smart antennas" [5, 6] that can meet the requirements of modern radio networks. The physical implementation of a smart antenna is based on modern interpretations of phased antenna arrays [5, 6], e.g. UM-MIMO antennas are expected to be used in 6G radio networks [7, 8]. The analysis of papers [1 – 8] allows to determine the main requirements for antenna systems in the scope of application of 6G networks, namely, antennas should provide, first, maximum energy efficiency and broadband [5, 6], second, the ability to form a multi-beam radiation pattern [5, 6, 8], then, the possibility of controlling individual beams of the radiation pattern in real time [1, 5, 6, 9], and the possibility of selecting a separate beam of the radiation pattern a specific mobile user equipment (UE) (UE group) [1, 6, 8, 9].

Thus, according to the above mentioned study of modern antenna systems, one of the important challenges is the analysis of the possibility of real-time control (with minimal time delays) of a separate beam of the radiation pattern for a specific mobile UE (UE group).

Methods of controlling the radiation pattern of an antenna array by changing the amplitude-phase characteristics at the feed points of the antenna array elements are well described in the literature [5, 6, 9, 10]. However, it is not described how the antenna adaptive processor [6, 10] that controls the antenna system should understand and learn, taking into account the UE movement patterns within the cell, and predict the direction of the specific UE movement to ensure proper radiation pattern control.

Therefore, the purpose of this paper is to propose a method that provides the antenna system with an understanding and prediction of the UE movement patterns within the cell and, based on the received knowledge, potentially allows the antenna radiation pattern to be controlled in real time (with minimal time delays).

Integration of an artificial intelligence unit into the block diagram of an adaptive antenna system

To achieve the goal described in this article, it is necessary to solve the problem of training the antenna system (array) to understand and predict the direction of movement of a given subscriber within the cell, i.e. to make the array truly "smart". This task can be achieved by integrating artificial intelligence algorithms and systems into the process of controlling the antenna array pattern.

Analyzing the literature [5, 6, 10, 11] allows us to draw the following block diagram of a modern adaptive antenna system. The block diagram shown in Fig. 1 consists of an antenna array containing four antenna elements, each antenna element is connected to a phase shifter that provides a change in the phase characteristics of the signal emitted by a particular antenna element of the array.

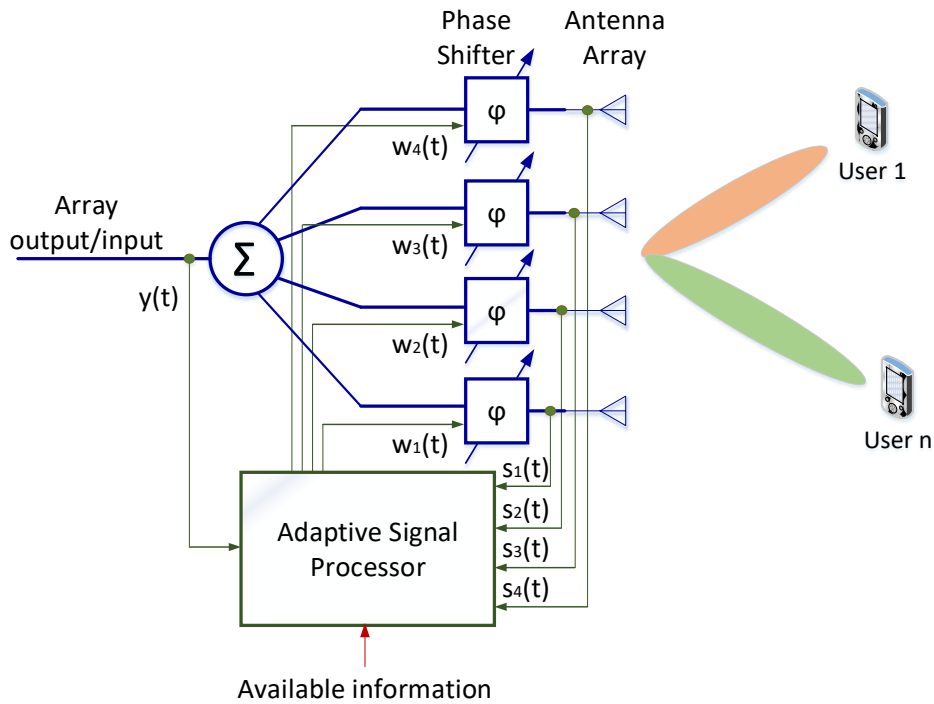


Fig. 1. Block diagram of an adaptive antenna system [5, 6, 10, 11]

The change in phase characteristics occurs in accordance with the adjustable complex weights formed by the adaptive signal processor – a vector of complex weights [10]

$$w(t) = [w_1(t), w_2(t), w_3(t), w_4(t)]^T \quad (1)$$

where T means transpose [10]. The adaptive signal processor is a structural unit that controls the antenna array pattern by means of control signals (1) that it generates on the basis of some collected information, namely

- the complex signal vector (voltage matrix) formed on the antenna elements of the antenna array [10]

$$s(t) = [s_1(t), s_2(t), s_3(t), s_4(t)]^T ; \quad (2)$$

- the feedback signal [10]

$$y(t) = s^T(t)w(t) ; \quad (3)$$

- “available information” [11] – other information that is necessary for the formation of the signal (1), for example, in mobile communication systems, this may be information about the coordinates of subscriber terminals in the operator's network, etc.

At the next stage, we integrate the artificial intelligence unit (AIU) [12] into the structure shown in Fig. 1.

In Fig. 2, the AIU is added to the block diagram of the adaptive antenna system [5, 6, 10, 11], which interacts with the communication system core through an interface and receives available information, and also has interfaces through which it interacts with the adaptive signal processor.

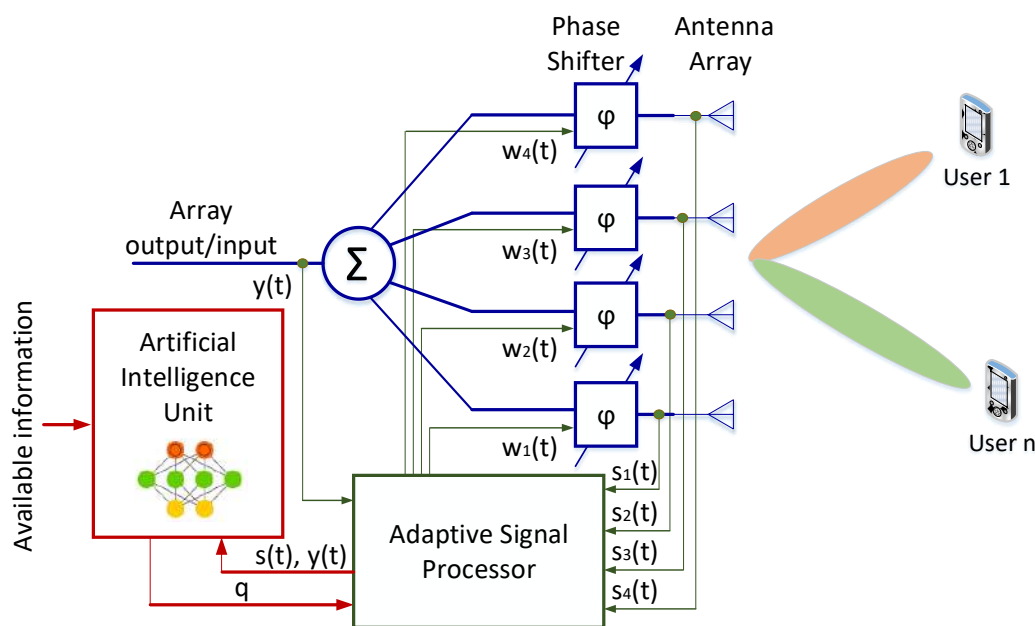


Fig. 2. Block diagram of an adaptive antenna system with AIU

The AIU receives data from the communication system core and data from the Adaptive Signal Processor, for example, (2) and (3), and processes them using one of the machine learning algorithms. As a result of the machine learning algorithm, the AIU forms a certain knowledge system about the environment in which the antenna array operates. The adaptive signal processor, in turn, uses the knowledge system formed in the AIU (receives the coefficients q) to more accurately control the antenna array pattern. In this case, we can write expression (1) in the following form

$$w(t)' = q[w_1(t), w_2(t), w_3(t), w_4(t)]^T. \quad (4)$$

In expression (4) $w(t)'$ denotes the vector of complex weights (control signal for the adaptive antenna array) that takes into account the coefficient q generated by the AIU based on the machine learning algorithm.

It should be noted that the value q can be represented in different forms, depending on the knowledge system (data structure) formed by the AIU, q can express some coefficients, or it can be represented by some signal constructions, etc.

At the next stage of this paper, we will consider one of the artificial intelligence methods that can be applied in AIU.

Artificial intelligence method for adaptive antenna system

To form a knowledge system for an adaptive antenna system that can understand, learn, and also predict the UE movement patterns within the cell is proposed to use one of the methods of artificial intelligence, an intelligent agent [13 – 18].

In AI, an intelligent agent is an entity that observes and acts on an environment [13, 17]. When machine learning algorithms are applied to intelligent agents, their behavior becomes rational and their actions are always aimed at achieving a goal. In this context, intelligent agents act with the rudiments of thinking like human thinking or intellectually developed beings [13 – 18]. As a result of learning, intelligent agents can generate an answer when there is no ready solution, perform a cognitive selection of objective conditions essential for action, perform a generalized, indirect reflection of reality, search for and discover significantly new things, identify and achieve intermediate goals [13 – 15].

The machine learning process can be implemented using the reinforcement learning of intelligent agents [13 – 18]. Consider the process of reinforcement learning based on Q-learning tech-

nique. In this technique, an intelligent agent must learn the environment in which it acts and find the best possible actions to reach the end point from the initial one. After reaching the goal, the agent receives a certain reward in the form of accumulated points [13 – 18]. The final goal of the agent is to receive maximum rewards and learn optimal policy for the given Markov decision process, which means to develop a behavioral model of optimal action in the specified environment. The basis of Q-learning is the so-called quality function (Q-function), which can be defined using [14 – 18]

$$Q(s, a) = (1 - \alpha)Q(s, a) + \alpha \left[R(s, a) + \lambda \max_{a' \in A} Q(s', a') \right]. \quad (5)$$

In equation (1),

s is the current state of an agent from a set of states $S(s_1, s_2, \dots, s_n)$,

a is the current action of an agent in state s from a set of actions $A(a_1, a_2, \dots, a_n)$,

α is a learning rate that can be set between 0 and 1,

s' is a next state from a set of states $S(s_1, s_2, \dots, s_n)$,

a' is a possible action of an agent from $A(a_1, a_2, \dots, a_n)$ in the state s' ,

λ is a discount factor that can also be set between 0 and 1 (recommended 0,8 [14, 18]),

$R(s, a)$ is reward for transition between states,

$\max_{a' \in A} Q(s', a')$ is a next action with maximum reward.

If $\alpha=1$ [14, 18], equation (1) can be rewritten as

$$Q(s, a) = R(s, a) + \lambda \max_{a' \in A} Q(s', a'). \quad (6)$$

The process of learning an intelligent agent operating in an environment that is a mobile communication cell can be illustrated by the diagram in Fig. 3 [16].

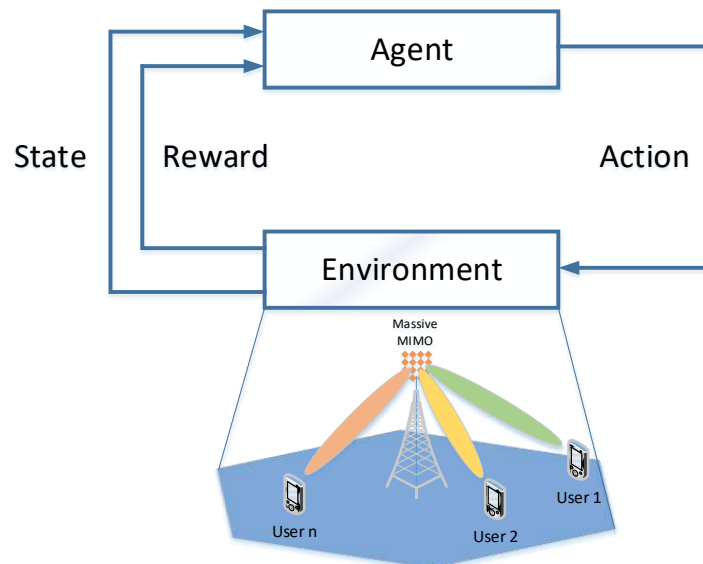


Fig. 3. Diagram of Q-learning

At the next stage of this paper, we will consider in detail an environment that is a cell of a mobile communication system in which an intelligent agent operates.

Mobile communication cell as intelligent agent application environment

Consider a cell of the mobile communication system operating in the conditions of urban development as an application environment of the intelligent agent. In the center of the cell, the access point/base transceiver station (BTS) equipment is located with the adaptive antenna system, which forms a multibeam radiation pattern capable of changing the radiation direction angle of a single beam of the radiation pattern in the horizontal and vertical planes. Thus, the intelligent agent will operate in a non-homogeneous, limited circular BTS coverage area, an urban development environment with a fixed grid of streets and placement of buildings. Within the BTS coverage area, subscribers (UEs) move continuously along the street grid. The challenge for an intelligent agent is to learn the movement patterns of subscribers on the street grid and perform Q-learning to develop a behavioral model that allows the adaptive antenna system to optimally control the directional radiation characteristics of each beam of the radiation pattern. The final model of the agent's behavior as a result of Q-learning will enable the antenna system to control the radiation pattern in real time, resulting in the optimal distribution of the BTS energy resource to the subscribers within the coverage area.

There are several patterns of movement of subscribers that can be identified during a certain time interval, for example, a day, in any cell of a cellular network. Such patterns depend on the social nature of life in the area where the cell is implemented. In this paper we consider one of the possible patterns, namely the movement of students (potential subscribers of a cellular network) between a university and a student campus.

Fig. 4 shows a cell of a mobile communication system as a geometry of a specific environment.

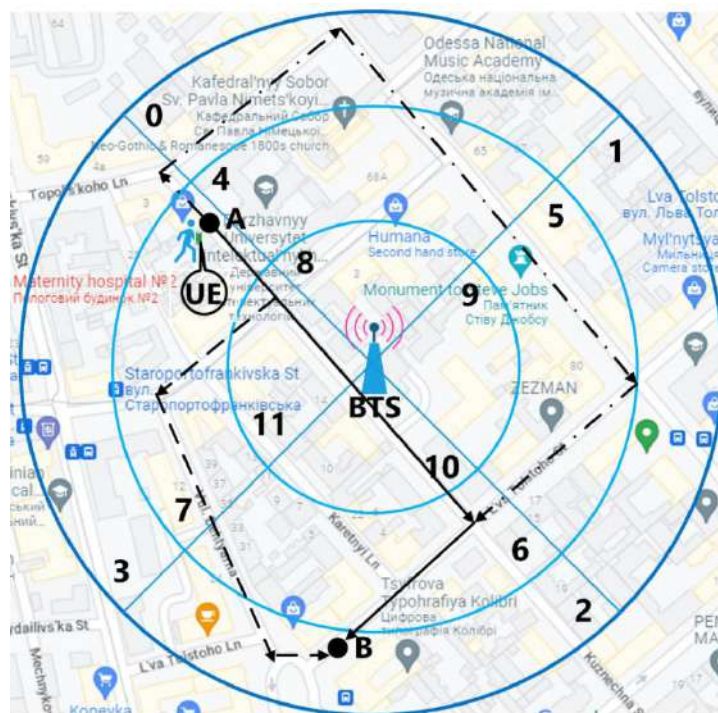


Fig. 4. Cell of a mobile communication system

Fig. 4 shows the map of the urban area where the BTS equipment is located. The coverage area of the specified access point is bounded by the circle with the largest radius of 0,22 km. Within the specified circle, the coverage area is divided into 12 conventional sectors numbered from 0 to 11. Sector 7 at point A shows a subscriber with UE. There is also a university near point A where many students (potential subscribers) study. Point B is on a student campus. The subscriber aims to move along the grid of city streets from point A (sector 7) to point B (sector 2).

Thus, within the considered cell, we can postulate the subscriber movement pattern between the university and the student campus at a certain time of day. It is this pattern that the intelligent agent must understand, learn and develop a behavioral model that allows the adaptive antenna system to operate optimally in this environment.

So, Figure 4 shows three possible routes of the subscriber's movement. The first route is marked with a solid line and runs from sector 7 through sectors 11, 10, and 6 to sector 2. The second route is marked with a dashed line, and it passes through sectors 7, 11, 7, 6, 2, and the third route is marked with a dash-dotted line - sectors 7, 3, 0, 4, 5, 6, 2.

Q-learning of intelligent agent

Now, we formally demonstrate the application of Q-learning of an intelligent agent during the movement of a subscriber from point A to point B in Fig. 1 (in our case, the subscriber is an intelligent agent).

Numbered sectors and a grid of streets connecting them make it possible to describe the states in which the agent (subscriber) can be located, for example, state 0 – stay in sector 0, state 1 – stay in sector 1, and so on. The movement of the agent (subscriber) during the transition from one state to another (from one sector to another along the corresponding streets) is shown in the form of a graph in Fig. 5. The structure of the graph reflects the grid of streets (Fig. 4) and determines the possibility of the agent moving from one sector to another.

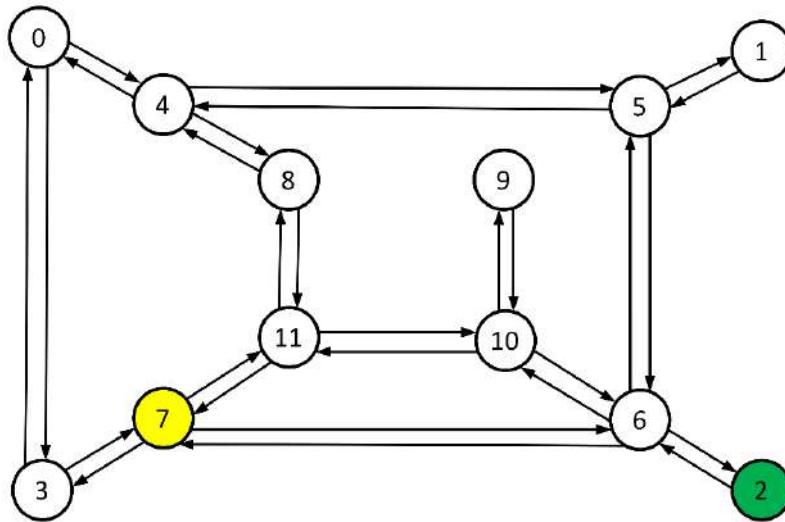


Fig. 5. Graph of possible agent states and actions

According to the graph in Fig. 5 we create a table of rewards – matrix R [13, 14, 18]. In this matrix, according to the Q-learning algorithm [13, 14, 18] the value -1 means the absence of a connection between the vertices of the graph and, accordingly, the impossibility of a direct transition of the agent (subscriber) between these vertices (sectors in Fig. 4), the value 0 means the ability of the agent to move directly between the vertices of the graph (there is the street connecting two sectors, Fig. 4), and the value 100 means an instant reward for the transition of the agent to the target vertex of the graph (subscriber has reached the target point B in sector 2, Fig.4).

Table 1

-	Action												
	-	0	1	2	3	4	5	6	7	8	9	10	11
State	0	-1	-1	-1	0	0	-1	-1	-1	-1	-1	-1	-1
	1	-1	-1	-1	-1	-1	0	-1	-1	-1	-1	-1	-1
	2	-1	-1	100	-1	-1	-1	0	-1	-1	-1	-1	-1
	3	0	-1	-1	-1	-1	-1	-1	0	-1	-1	-1	-1
	4	0	-1	-1	-1	-1	0	-1	-1	0	-1	-1	-1
	5	-1	0	-1	-1	0	-1	0	-1	-1	-1	-1	-1
	6	-1	-1	100	-1	-1	0	-1	0	-1	-1	0	-1
	7	-1	-1	-1	0	-1	-1	0	-1	-1	-1	-1	0
	8	-1	-1	-1	-1	0	-1	-1	-1	-1	-1	-1	0
	9	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	0	-1
	10	-1	-1	-1	-1	-1	-1	-1	0	-1	-1	0	-1
	11	-1	-1	-1	-1	-1	-1	-1	-1	0	0	-1	0

In the next stage, according to the Q-learning algorithm [13, 14, 18], we create a matrix Q – the so-called "memory" matrix of an intelligent agent. At the initial stage, the matrix Q is initialized with zero that is the memory of the intelligent agent does not contain any information. Further, as a result of training the matrix Q is gradually filled out, thus forming certain knowledge of an intelligent agent [13, 14, 18].

Consider the first step of filling out the Q matrix using expression (2), as well as the initial data of Fig. 4, Fig. 5, and matrix R – calculate the element Q(6,2):

$$Q(6,2) = R(6,2) + 0,8 \max(Q(2,6)) = 100 + 0,8 \max(0) = 100.$$

As a result, the element Q(6,2) of the matrix Q gets the value 100. Now we can perform the second step – calculate the element Q(10,6):

$$Q(10,6) = R(10,6) + 0,8 \max(Q(6,2), Q(6,5), Q(6,7), Q(6,10)) = 0 + 0,8 \max(100, 0, 0, 0) = 80.$$

Based on the calculated elements Q(6,2) and Q(10,6), we perform the corresponding calculations of the remaining elements of matrix Q in the same way, and present the results in Table 2.

Table 2

-	Action												
	-	0	1	2	3	4	5	6	7	8	9	10	11
State	0	0	0	0	26	41	0	0	0	0	0	0	0
	1	0	0	0	0	0	64	0	0	0	0	0	0
	2	0	0	0	0	0	0	0	0	0	0	0	0
	3	33	0	0	0	0	0	0	64	0	0	0	0
	4	33	0	0	0	0	64	0	0	33	0	0	0
	5	0	41	0	0	41	0	80	0	0	0	0	0
	6	0	0	100	0	0	64	0	64	0	0	64	0
	7	0	0	0	26	0	0	80	0	0	0	0	41
	8	0	0	0	0	41	0	0	0	0	0	0	41
	9	0	0	0	0	0	0	0	0	0	0	64	0
	10	0	0	0	0	0	0	80	0	0	41	0	41
	11	0	0	0	0	0	0	0	0	33	0	64	0

The results of the calculations given in the matrix Q are displayed on the graph (Fig. 6) as weighting coefficients for the transitions between the vertices of the graph.

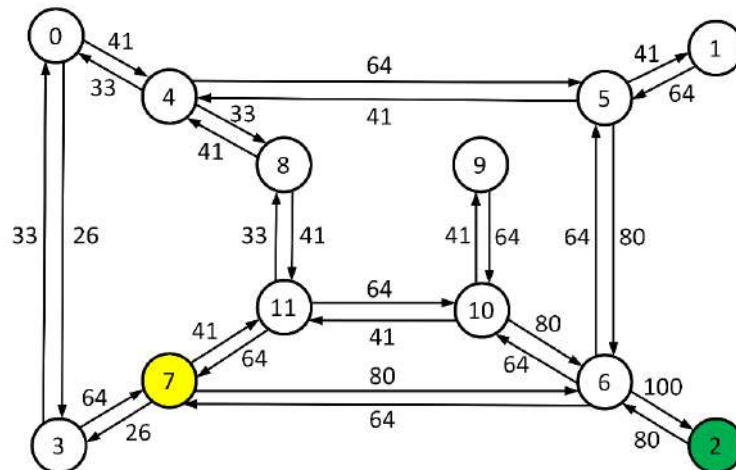


Fig. 6. Graph of possible states and actions of an agent when overcoming the path from vertex 7 to vertex 2

Weighting coefficients for transitions (Fig. 6) shows the probability of transition of an agent from one state to another, where the initial state of the agent is 7 and the target state is 2.

Thus, the results obtained in Table 2 and Figure 6 for an agent (subscriber of a cellular network) reflect the movement pattern of the subscriber within a cellular network between the university and the student campus. The obtained results can be used by the antenna controller for beam control of the adaptive antenna system radiation pattern assigned to a subscriber in real time or with minimum latency. Note that the obtained weighting coefficients are relevant both for a single subscriber and for each subscriber of the group on the considered routes, since each subscriber has an individual beam.

Accordingly, using the AI method, the intelligent agent telecommunication system can study the subscriber movement pattern within a cell and, based on the obtained pattern, forms a knowledge system as a Q -matrix. Then the antenna controller of an antenna system of a cell uses the received knowledge matrix Q to effectively control the beams of the radiation pattern, since matrix Q allows to predict the direction of the subscriber movement within the cell.

It should also be noted that in order to reduce the number of calculations when forming the Q -matrix, a relatively small number of sectors (states) in the cell is considered in order to demonstrate the possibility of using the Intelligence Agent method to form a knowledge system on the basis of which the antenna system radiation pattern can be controlled. Increasing the number of sectors in a cell leads to a more detailed analysis of the pattern of subscriber movement in the cell and, as a result, increases the accuracy of the antenna system pattern control. Improving the accuracy of antenna pattern management leads to improved energy efficiency. The idea is that the energy radiated by the antenna system is not arbitrarily distributed in space (and thus suffers additional space losses) within the base station service sector, but is focused in a certain narrow sector of space (a radiation pattern petal) for a particular subscriber [5, 6, 10, 11].

Conclusions

Therefore, in this paper the requirements for adaptive antenna systems in current and future fifth (5G) and sixth (6G) generation wireless networks were analyzed. The block diagram of a modern adaptive antenna system was considered, and in order to improve this block diagram the integration of an artificial intelligence unit into it was proposed. One example of the operation of an artificial intelligence unit as part of an adaptive antenna system was proposed using the intelligent agent method of artificial intelligence. It is shown that using the intelligent agent method it is possible to create a knowledge system capable of understanding and learning, taking into account the patterns

of movement of subscribers in the cell, and predicting the direction of movement of a particular user equipment (group of user equipment). The resulting knowledge system is formed in an artificial intelligence unit and can potentially be used by the adaptive signal processor to more accurately control the radiation pattern of the antenna system, which allows to realize the functions of a smart antenna and control the dedicated beam of the antenna system's radiation pattern in real time or with minimal time delay. Thus, the objective of this paper was achieved.

References:

1. Mamta A., Abhishek R., Navrati S. Next Generation 5G Wireless Networks: A Comprehensive Survey // IEEE Communications Surveys & Tutorials. 2016. Vol. 18, № 3. P. 1617–1655.
2. Dogra A., Rakesh K Jha, Jain S. A Survey on beyond 5G network with the advent of 6G: Architecture and Emerging Technologies // IEEE Access. 2020. Vol. 9. P. 67512–67547,
3. Abdel Hakeem S.A., Hussein H.H. and Kim H. Vision and research directions of 6G technologies and applications // Journal of King Saud University – Computer and Information Sciences. 2022. Vol. 34. P. 2419–2442.
4. Yang H., Alphones A., Xiong Z., Niyato D., Zhao J., Wu K. Artificial Intelligence-Enabled Intelligent 6G Networks // IEEE Network. 2020. Vol. 34, Issue 6. P. 272–280.
5. Constantine A. Balanis Modern antenna handbook. USA : Includes index. ISBN 978-0-470-03634-1 (cloth) 1. Antennas (Electronics) I. Title. TK7871.6.B354 2008. 1700 p.
6. Nathan Blaunstein, Christos G. Christodoulou. Radio propagation and adaptive antennas for wireless communication links. USA : Includes index. ISBN-13: 978-0-471-25121-7, ISBN-10: 0-471-25121-6, TK7871.67.A33.B55 2007. 614 p.
7. Jagadeesha R Bhat, Salman A. Al Qahtani. 6G Ecosystem: Current Status and Future Perspective // IEEE Access. 2021. Vol. 9. P. 43134–43167.
8. Robin Chataut, Robert Akl. Massive MIMO Systems for 5G and beyond Networks – Overview, Recent Trends, Challenges, and Future Research Direction // MDPI Sensors Academic Open Access Publishing. 2020. Vol. 20, Issue 10. P. 2753.
9. Qimei Cui, Yifei Yuan. Experimental investigation on a vertical sectorization system with active antenna // IEEE Communications Magazine. 2016. Vol. 54, no. 9. P. 89 – 97.
10. Alan J. Fenn. Adaptive Antennas and Phased Arrays for Radar and Communications. USA : Massachusetts Institute of Technology, Includes index. ISBN 13: 978-1-59693-273-9, 2008. 394 p.
11. Edvin J. Kitindi Capabilities of smart antenna in tracking the desired signal in wireless communication system through non-blind adaptive algorithms // International Journal of Advanced Research in Computer and Communication Engineering. 2015. Vol. 4, Issue 2. P. 5–9.
12. Meet the IBM Artificial Intelligence Unit. The access mode: <https://research.ibm.com/blog/ibm-artificial-intelligence-unit-aiu>
13. Gerhard Weiss. Multiagent Systems. A Modern Approach to Distributed Artificial Intelligence // The MIT Press.: Includes index. ISBN 9780262731317, 2000. 644 p.
14. Tanveer J., Haider A., Ali R., Kim A. Reinforcement Learning-Based Optimization for Drone Mobility in 5G and Beyond Ultra-Dense Networks // CMC Computers, Materials & Continua. 2021. Vol. 68, no. 3. P. 3807–3823.
15. Wen Tong, Peiyong Zhu. 6G: The Next Horizon: From Connected People and Things to Connected Intelligence. Cambridge University Press, Includes index. ISBN: 1108839320, 2021. 490 p.
16. Rozhnovskiy M.V., Rozhnovskaya I. Yu. Application of machine learning method in massive MIMO antenna technologies // Advanced Technology in Information and Communication Engineering : International Conference, July, 18, 2023 : proc. of conf. Odesa, Ukraine. P. 98–101.
17. Jawad Tanveer, Amir Haider, Rashid Ali, Ajung Kim. An Overview of Reinforcement Learning Algorithms for Handover Management in 5G Ultra-Dense Small Cell Networks // MDPI Applied Sciences. 2022. Vol. 12, Issue 1. P. 426.
18. Trotsko V.V. Methods of artificial intelligence: Educational and methodological manual (in ukr.). Kyiv : University of Economics and Law “KROC”, 2020. P. 86.

Received 27.11.2023

Information about the authors:

Mikhailo V. Rozhnovskiy – PhD, Assoc. Prof., State University of Intelligent Technologies and Telecommunications, Odesa; Ukraine; e-mail: mihail.exp@gmail.com; ORCID: <https://orcid.org/0009-0002-9219-123X>

Iryna Yu. Rozhnovska – PhD, Assoc. Prof., International Humanitarian University, Software engineer, Sigma Software Group, Odesa; Ukraine; e-mail: irina.rozhnovskay@gmail.com; ORCID: <https://orcid.org/0009-0007-2158-5721>

В.О. АЛЕКСЄЄВ, Д.В. ГРЕЦЬКИХ, *д-р техн. наук*, Д.С. ГАВВА, *канд. техн. наук*,
В.Г. ЛИХОГРАЙ, *канд. фіз.-мат. наук*, І.А. ХАНЬ

РЕКТЕНИ СИСТЕМ ЗБОРУ ЕЛЕКТРОМАГНІТНОЇ ЕНЕРГІЇ З НАВКОЛИШНЬОГО ПРОСТОРУ

Вступ

З 1960-х років ректени розглядали як кінцевий пристрій потужних систем безпроводної передачі енергії (БПЕ) сфокусованим мікрохвильовим променем: сонячних космічних електростанцій та енергосистем безпілотних літальних апаратів[1]. Комерційні системи БПЕ в основному обмежувалися безвипромінювальною передачею енергії в ближньому полі для безпроводної зарядки побутової електроніки або в радіочастотній ідентифікації ближньої дії. Досягнення у галузі мікроелектроніки дозволили зменшити енергоспоживання напівпровідникових радіоелектронних пристроїв. З початку 2000-х років виникла можливість розглядати питання живлення малопотужних пристроїв шляхом перетворення енергії навколишнього електромагнітного (ЕМ) випромінювання ректенами в постійний струм. Така навколишня енергія розглядається у світі як "безкоштовне" джерело живлення для малопотужних пристроїв, що робить цю технологію привабливою. У роботі [2] проведено аналіз існуючих технологій БПЕ. Зазначено, що одними з чинників, що визначають вибір тієї чи іншої технології БПЕ є відстань, на яку передається енергія та вид використовуваної ЕМ енергії. Наведено узагальнену структурну схему системи БПЕ. Розглянуто галузі застосування та тенденції подальшого розвитку технології передачі енергії на малі відстані за допомогою індукційного та резонансного методів, технології передачі енергії на великі відстані, технології збору ЕМ енергії з навколишнього простору та її перетворення у постійний струм для живлення малопотужних пристроїв. У статті розглядаються ректени для перетворення ЕМ енергії з навколишнього простору, що створюють радіоелектронні засоби (РЕЗ) різних класів та призначень (доступний рівень густини потоку потужності у навколишньому середовищі знаходиться в межах від 0.0017 до 0.8594 мкВт/см²) в енергію постійного струму. Ректени відносяться до класу антен з нелінійними елементами, і деякі типи таких антен вже розглядались у попередніх дослідженнях [3, 4].

Стаття складається з двох частин. У першій частині наведено параметри ректен. Друга частина присвячена огляду теорії та практики побудови ректен для систем збору ЕМ енергії.

1. Параметри ректен

У дальній зоні коефіцієнт корисної дії (ККД) ректени η_r визначається наступним чином:

$$\eta_r = P_0 / P_{\text{вх}}, \quad (1)$$

де $P_{\text{вх}} = e_a^2 / 8R_a(f_0)$ – максимальна потужність, яку може вилучити випромінювач ректени з поля падаючої ЕМ хвилі; e_a – амплітуда напруги холостого ходу, що наводиться падаючою хвилею на клеммах випромінювача; $R_a(f_0)$ – активна частина вхідного опору випромінювача на робочій частоті f_0 ; P_0 – потужність постійного струму у навантаженні ректени (під навантаженням будемо надалі розуміти різні компоненти системи збору ЕМ енергії, що потребують постійної напруги).

Коротко зупинимося на механізмах втрат потужності у ректенах (рис. 1). Потужність постійного струму P_0 в навантаженні ректени відрізняється від вхідної потужності $P_{\text{вх}}$ на величину потужності втрат, яка, в свою чергу, складається з потужності втрат у випромінювачі, потужності втрат в елементах кола узгодження (КУ) випромінювача та схеми випрям-

лення. Якщо схема випрямлення не узгоджена належним чином з випромінювачем, то частина падаючої потужності від випромінювача відбиватиметься назад в навколишнє середовище, що призведе до зменшення вхідної потужності на випрямлячі і, як наслідок, зменшення ККД ректени.

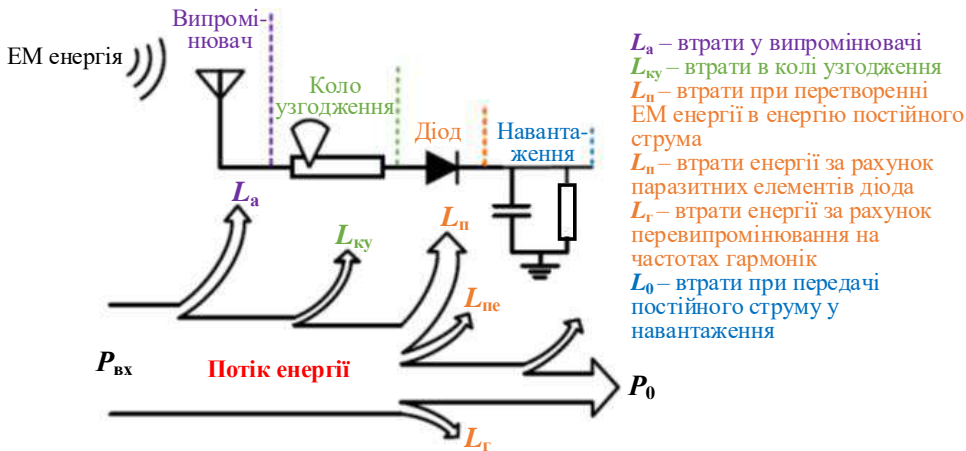


Рис.1. Механізми втрат потужності у ректені

при різних рівнях вхідної потужності. Тому дуже важливо, щоб КУ та випрямляч розроблялися разом, оскільки конструкція кожного з них значно впливає на їх ККД. Крім того, втрати в підкладці ректени та лініях передачі також можуть суттєво впливати на ККД. Потужність втрат у випрямному елементі обумовлена такими чинниками: втратами при перетворенні ЕМ енергії у постійний струм; паразитними елементами випрямних діодів (опір переходу, ємність переходу, паразитні ємності та індуктивності корпусу діода [1]); ємністю переходу та паразитними реактивними елементами корпусу діода, що обмежують максимальну частоту, при якій діод може працювати з прийнятним ККД; втратами потужності за рахунок випромінювання ректеною на частотах вищих гармонік і за рахунок проходження цих гармонік в навантаження.

Рівень побічного випромінювання ректен на частотах гармонік визначається наступним чином [1]:

$$\xi(nf_0) = P_{\Sigma}(nf_0) / P_{vx}, \quad n = 2, 3, \dots, \quad (2)$$

де $P_{\Sigma}(nf_0)$ – потужність, яку випромінює ректена на частоті n -ї гармоніки.

Втрати потужності мають місце й в елементах вихідного фільтра ректени.

Малопотужні ректени системи збору ЕМ енергії потрібно характеризувати таким параметром як чутливість. Чутливість визначається як мінімальна падаюча потужність, яка необхідна для запуску роботи системи збору енергії [2]. Чим вища чутливість системи збору енергії, тим краща ефективність перетворення потужності падаючого на ректену ЕМ випромінювання в постійний струм. Чутливість кількісно визначається таким виразом [2]:

$$S_{[дБм]} = 10 \lg(P_{\min} / 1 \text{ мВт}), \quad (3)$$

де P_{\min} – мінімальна потужність, яка необхідна ректені для перетворення ЕМ енергії в постійний струм для подальшої роботи навантаження.

Наприклад, для більшості конкуруючих RFID-схем дальнього поля чутливість у діапазоні від -25 до -10 дБм відповідає робочим рівням вхідної потужності від 3 до 100 нВт.

Результатом роботи системи збору ЕМ енергії є живлення кінцевих пристроїв постійним струмом. Тому вихідна потужність постійного струму P_0 ректени є ще одним показником оцінки ефективності роботи системи збору ЕМ енергії.

Під діаграмою спрямованості (ДС) ректени на основній частоті будемо розуміти залежність ККД ректени від кутових координат при незмінній густині потоку потужності падаючого поля та величини навантаження по постійному струму.

Вхідний опір схеми випрямлення змінюється в залежності від частоти і від вхідної потужності через нелінійність випрямних елементів. Внаслідок цього важко забезпечити ідеальне узгодження випромінювача зі схемою випрямлення у широкій смузі частот

Ефективність ректени для збору ЕМ енергії з навколишнього простору залежить від ефективності окремих її компонентів, тому одним із важливих завдань на шляху впровадження ректен для збору ЕМ енергій в різних сферах життєдіяльності є оптимізація її компонентів. Сучасний стан досліджень в цьому напрямку викладено в наступному розділі.

2. Ректени систем збору ЕМ енергії

2.1. Структурні схеми ректен для збору ЕМ енергії

На рис. 2 наведено типові варіанти схем побудови ректен [5]. Так, на рис. 2, а подано схеми однодіапазонних ректен, в яких вхідний опір випромінювача становить 50 Ом. На рис. 2, б, в, г показано багатодіапазонні та широкосмугові ректени, випромінювачі яких теж мають вхідний опір 50 Ом. У схемі на рис. 2, г може бути використане не широкосмугове КУ, а багатодіапазонне. Зазначимо, що терміни «багатодіапазонні» та «широкосмугові» ректени відрізняються неперервністю їх ширини робочої смуги частот за рівнем $S_{11} < -10$ дБ (на рис. 2 пунктирними лініями позначено площини, в яких необхідно забезпечити смугу пропускання за рівнем коефіцієнта відбиття $S_{11} < -10$ дБ). На рис. 2, д наведено схему побудови електрично малих ректен. На рис. 2, е, ж наведено схеми однодіапазонних та широкосмугових ректен, в яких випромінювачі мають комплексний вхідний опір, який комплексно спряжений з вхідним опором схеми випрямлення. В таких конструкціях ректен відпадає необхідність застосування КУ.

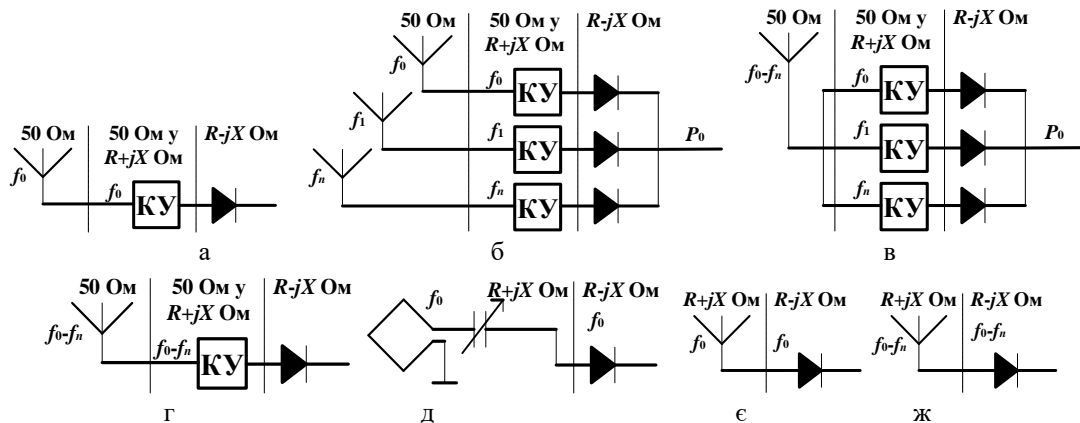


Рис. 2. Схеми побудови ректен

Розглянемо особливості технічної реалізації ректен, які побудовані за різними схемами, та визначимо існуючі проблеми й напрямки вдосконалення технічних характеристик ректен для збору енергії з навколишнього простору.

2.2. Однодіапазонні ректени

Радіочастотне з'єднання за допомогою бокового зв'язку між мікросмужковими лініями

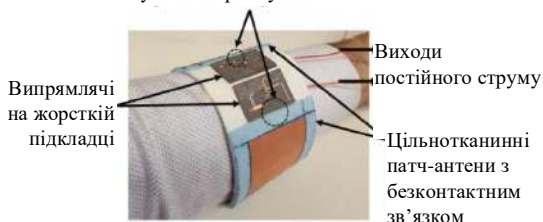


Рис. 3. Фото ректени

Однодіапазонні ректени різноманітних конструкцій були розроблені для збору ЕМ енергії для низьких частотних діапазонів: 2G/GSM-900/1800, 3G/UMTS, 4G/LTE, 5G (стільниковий зв'язок), Wi-Fi (абонентський радіодоступ), DTV (цифрове телебачення), FM та AM (радіомовлення). Наприклад, у роботі [6] запропоновано ректену для збору енергії на частоті 2,45 ГГц, яка побудована за схемою рис. 2, а. Ректена була розміщена на гнучкому браслеті (рис. 3) та складається з двох ректенних елементів, які можуть працювати незалежно, об'єднуватися по постійному струму послідовно або паралельно. Два прямокутних мікросмужкових випромінювача ректени реалізовано на багатошаровій підкладці з тканини, а схеми випрямлення розташовано на жорсткій підкладці. Зв'язок між випромінювачем та випрямлячем реалізовано за допомогою бокового зв'язку між мікросмужковими лініями (безконтактне електричне з'єднання).

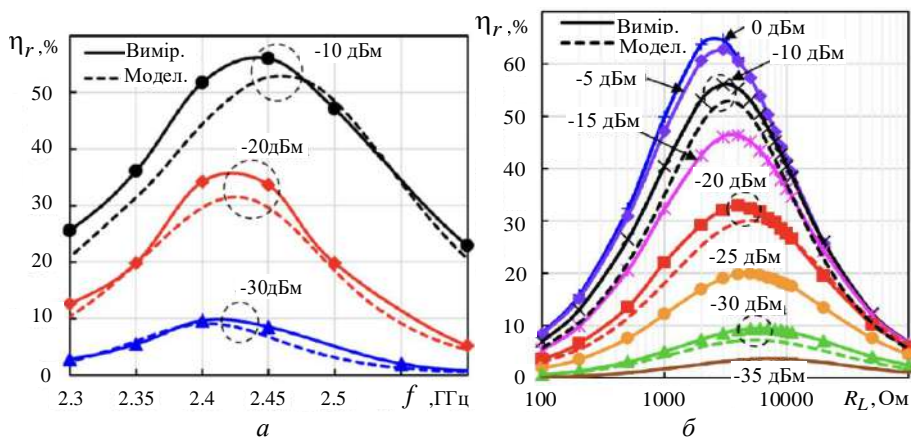


Рис. 4. Теоретичні та експериментальні залежності ККД випрямлення від частоти (а) та опору навантаження (б) при різних рівнях вхідної потужності

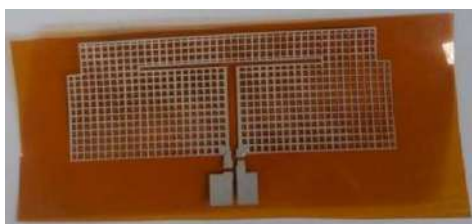


Рис. 5. Оптично прозора ректена

підкладці з втратами. Результати експериментальних досліджень показали, що така ректена може забезпечити в навантаженні потужність постійного струму 12,5 мкВт та напругу 500 мВ.

На сьогодні радіочастотна електроніка та антени в гнучкому виконанні розглядаються як технологія виготовлення пристроїв інтернету речей (IoT) та мереж датчиків на тілі людини без використання батарей живлення. Це призвело до великої кількості досліджень щодо використання носимих ректен, в яких використовуються як гнучкі та текстильні матеріали в якості підкладки, так і тверді підкладки нетекстильного типу [9 – 12].

Велика увага приділяється ректенам з диференціальним (симетричним) живленням. Диференціальний вхід у випрямлячі зазвичай призводить до підвищення ККД ректени в порівнянні з несиметричними випромінювачами та відповідає необхідності у додаткових балунах. У роботах [13 – 16] розроблено мікросмужкові ректени із диференційною схемою випрямлення. Типову схему побудови таких ректен наведено на рис. 6, а [13]. Для ректени, зображеної на рис. 6, б, максимальний ККД досягає 65,3 % при вхідній потужності 2,19 дБм на частоті 980 МГц.

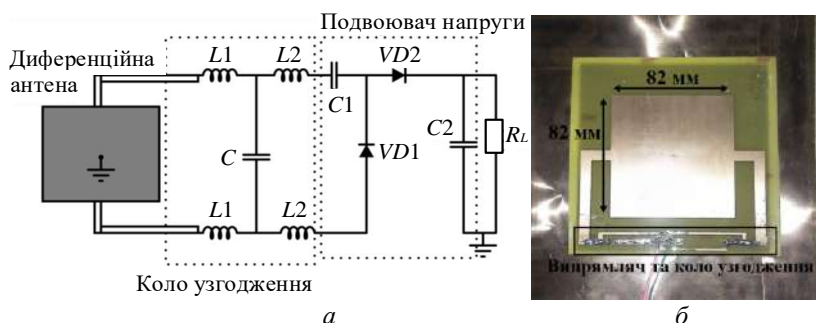


Рис. 6. Схема ректени з диференційною схемою випрямлення (а) та її фото зверху (б)

розроблено у [19]. При рівні вхідної потужності -20 дБм час зарядки двох суперконденсаторів ємністю 1F, з'єднаних паралельно, становить 6 годин для напруги в навантаженні 1 В. Діапазон FM є потенційним джерелом збору ЕМ енергії через його широку доступність, менші втрати на трасі поширення радіохвиль та більш прості конструктивні рішення ректен.

На рис. 4. наведено результати теоретичних та експериментальних досліджень характеристик ректени. З рис. 4,б видно, що ККД ректени нелінійно залежить від рівня вхідного впливу та опору навантаження. При деякому оптимальному опорі навантаження ККД досягає максимуму.

Останнім часом значний інтерес викликали оптично прозорі ректени. Наприклад, їх можна розміщувати на сонячних батареях [7], тим самим підвищуючи загальну ефективність енергосистеми. У [8] подана гнучка оптично прозора ректена (рис. 5) для збору енергії від базових станцій. Ректена побудована за схемою на рис. 2, є. Випромінювач ректени виготовлений на недорогому принтері з використанням срібного чорнила на

Для мініатюрних систем та пристроїв з безпроводним живленням, таких як медичні імпланти, пристрої IoT тощо, необхідні вбудовані компактні ректени, здатні ефективно захоплювати енергію ЕМ хвиль у заданому діапазоні частот та перетворювати її в постійний струм. Мініатюризація випромінювальних структур зазвичай виконується з використанням діелектриків чи магнітних матеріалів з високими відносними діелектричними та магнітними проникностями [20], зокрема метаматеріалів [21] або модифікації геометрії та конструкції випромінювача (навантаження провідних антен на реактивні елементи, застосуванням щілин та надрізів металізації, згинання та меандрування провідних елементів, фрактальні структури, тощо) [22 – 25]. На рис. 7 наведено приклади реалізації компактних ректен.

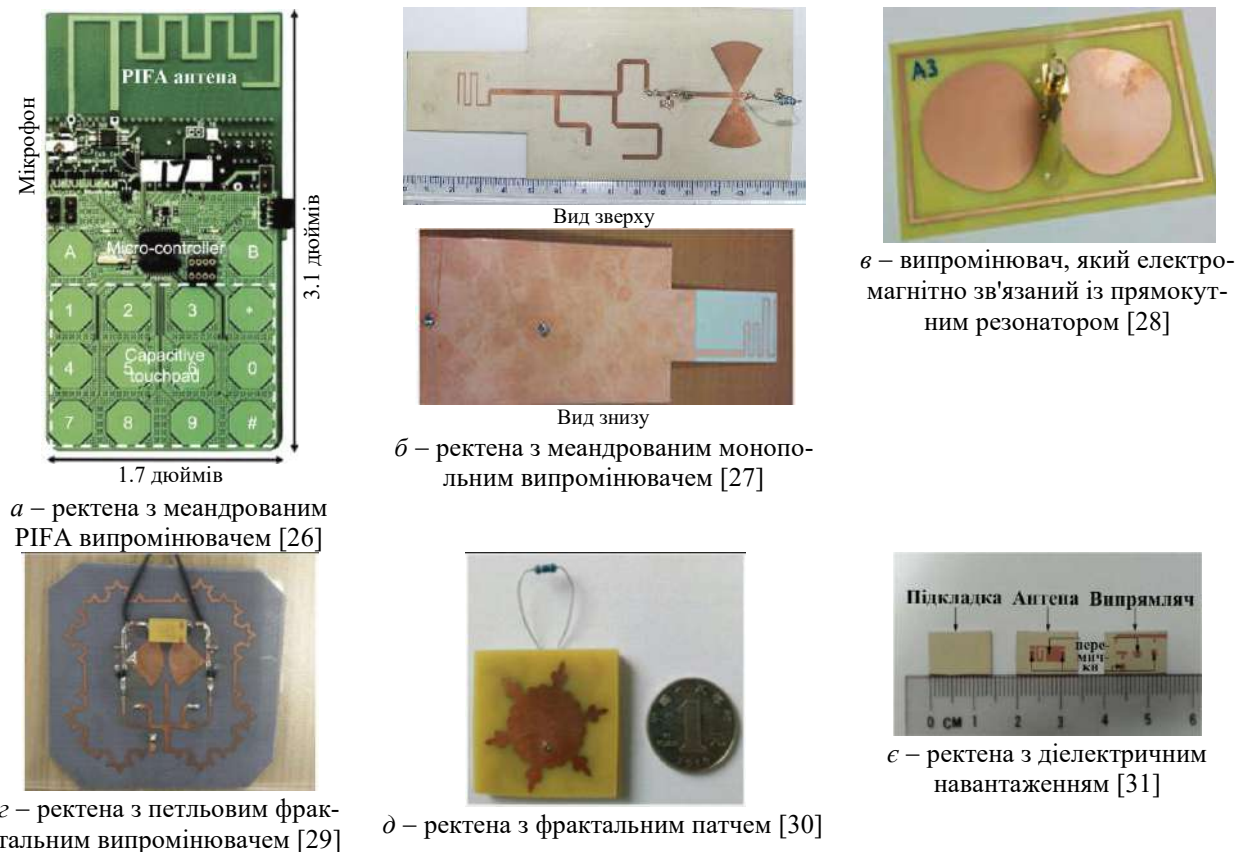


Рис. 7. Приклади реалізації компактних ректен

Ректени на основі меандрованої плоскої перевернутої F-антени (PIFA) є однією з найпопулярніших компактних конструкцій [26, 32 – 34]. Наприклад, ректена з меандрованим PIFA випромінювачем (рис. 7, а) була розроблена у [26] для створення мобільного телефону з безпроводним живленням. Інший метод мініатюризації включає проектування меандрованих монополярних або дипольних випромінюючих структур (рис. 7, б) ректен [27, 35]. Спосіб мініатюризації габаритних розмірів ректени за рахунок розміщення плоского дипольного випромінювача квазікруглої форми в прямокутному резонаторі (рис. 7, в), що дозволяє зменшити його розміри на 21,5 % без погіршення характеристик, запропоновано в роботі [28]. Авторами [29] розроблено компактну ректену за рахунок вбудови випрямляча всередину фрактальної рамкової випромінюючої структури (рис. 7, г). У роботах [30, 36, 37] були розроблені мініатюрні ректени на основі фрактальних патчів. Для подальшого зменшення розмірів ректен, які використовуються в медичних імплантах, в [31, 38, 39] були розроблені конструкції ректен з діелектричним навантаженням (рис. 7, е).

2.3. Електрично малі ректени

Використання електрично малих випромінювачів у ректенах має дві ключові переваги [40]: по-перше, немає необхідності включати додаткове КУ між випромінювачем та випрям-

лячем завдяки високому ємнісному/індуктивному вхідному опору самих випромінювачів, і, по-друге, ректени мають відносно невеликі розміри. Електрично малим випромінювачем вважається той, для якого виконується умова $ka \leq 1$ (де k – хвильове число у вільному просторі, a – радіус умовної сфери, що охоплює максимальний розмір випромінювача). Тобто, електрично малі випромінювачі мають розміри істотно менші за довжину хвилі, на якій вони працюють. Слід зазначити, що термін "малі" стосується електричних характеристик, а не габаритних розмірів. Електрично малі ректени викликають інтерес, коли ректену необхідно інтегрувати в малогабаритні пристрої або системи. Одним з інноваційних підходів у розробці електрично малих ректен є застосування метаматеріалів. Метаматеріали [41, 42] – це штучно створені композитні матеріали, які складаються з субхвильових металічних або діелектричних включень, що мають довільні розміри та форму. Штучна періодична структура модифікує діелектричну та магнітну проникності вихідного матеріалу, що дає можливість керувати законами дисперсії, заломленням та відбиттям ЕМ хвиль у метаматеріалі. Таким чином, метаматеріали є тривимірними структурами зі штучно створеними ЕМ властивостями, яких немає в природі. Метаповерхні є двовимірними еквівалентами метаматеріалів. Використання метаструктур дозволяє підвищити ККД перехоплення ЕМ енергії за рахунок узгодження поверхневого імпедансу з імпедансом вільного простору [43].

У роботах [44, 45] були створені електрично малі ректени шляхом об'єднання взаємно-ортогональних електричних та магнітних метаматеріальних резонаторів/диполів, що дозволило створити ДС ректени у формі кардіоїди (рис. 8), подібної ДС елемента Гюйгенса [46].

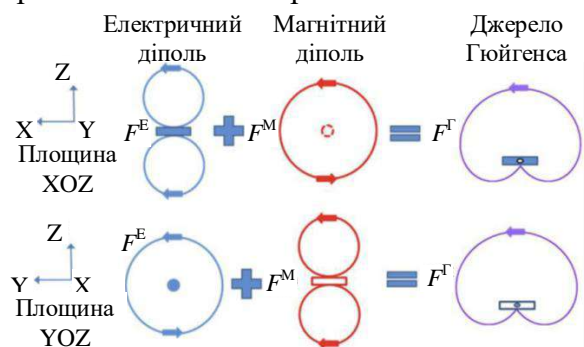


Рис. 8. Реалізація ректен Гюйгенса (F^E , F^H – нормовані діаграми спрямованості в Е та Н площинах)

У літературі такі ректени називають ректенами Гюйгенса [45]. Приклад випромінювача Гюйгенса з лінійною поляризацією та коаксіальним живленням наведений на рис. 9. Автори [47] у керуючий диполь (рис. 9, з) інтегрували схему випрямлення (рис. 10, а), яка реалізована на SMD компонентах Murata. Загальна довжина схеми випрямлення становила всього 7,3 мм ($0,02\lambda$).

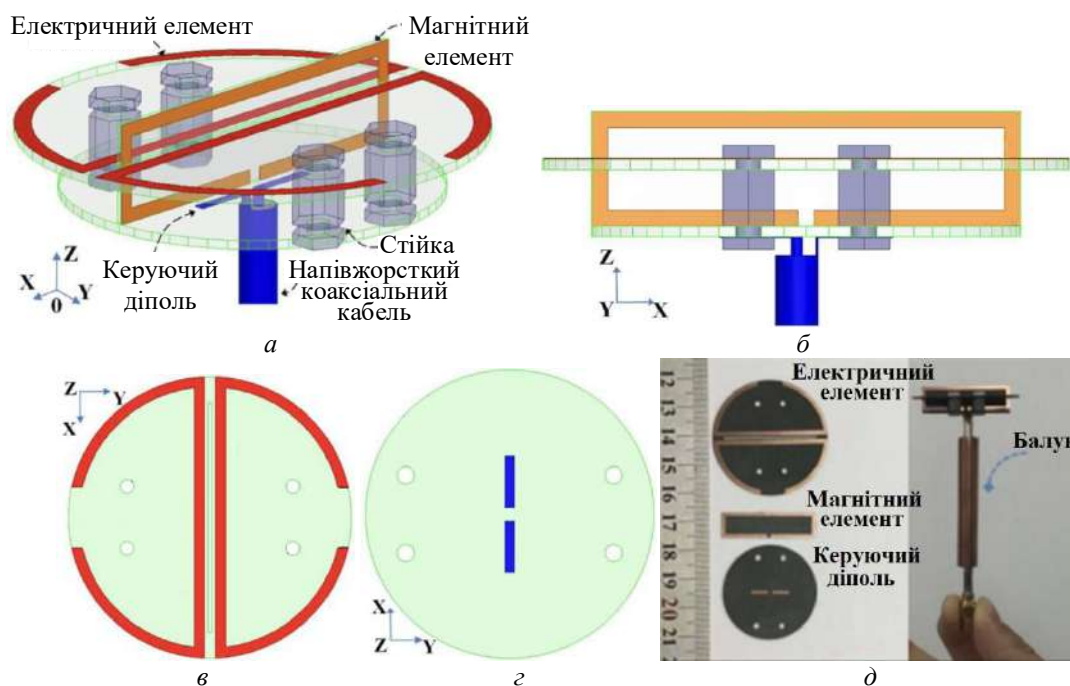


Рис. 9. Конструкція випромінювача Гюйгенса: а – тривимірне зображення, б – вид збоку на магнітний елемент, в – вид зверху на електричний елемент, г – вид знизу на керуючий диполь, д – фото випромінювача Гюйгенса

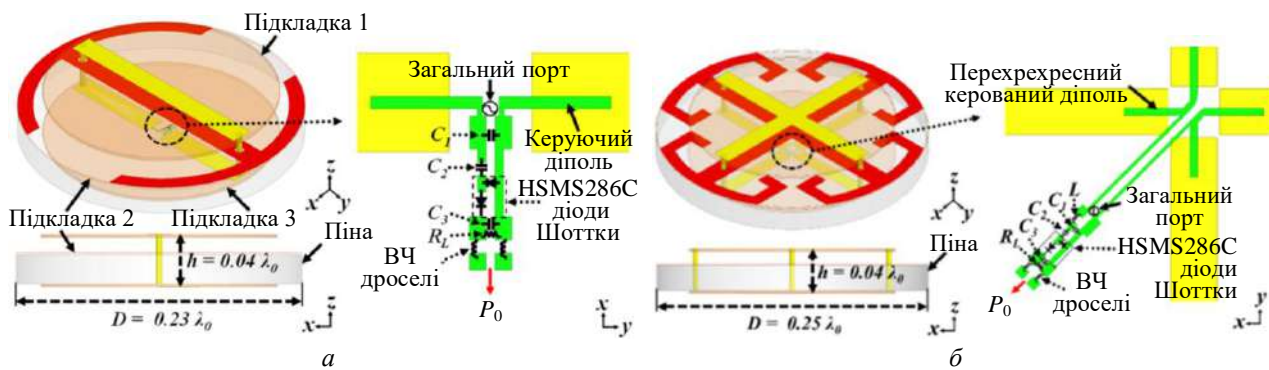


Рис. 10. Конфігурація електрично малих ректен Гюйгенса: *a* – з лінійною поляризацією, *б* – з круговою поляризацією

На відміну від дослідження [44], у [47] вхідний опір випромінювача був комплексним (замість звичайних 50 Ом), а саме комплексно спряженим з вхідним опором схеми випрямлення. Це дозволило уникнути використання КУ в конструкції ректени і, отже, знизити втрати при випрямленні приблизно на 6 %. Розроблена конструкція ректени компактна і електрично мала ($ka < 0.77$), здатна приймати ЕМ хвилі в широкому діапазоні кутів (ширина ДС $\pm 67^\circ$ на рівні -3 дБ) з високим ККД, який досягає 89 % на частоті 915 МГц.

Автори дослідження [44] стверджують, що ректени з круговою поляризацією мають значні переваги перед ректенами з лінійною поляризацією при певних сценаріях їх використання, особливо тоді, коли поляризація джерела випромінювання невідома. У роботі [45] була розроблена електрично мала ректена з круговою поляризацією (рис. 10, *б*), яка об'єднує дві ортогональні пари електричних і магнітних випромінювачів. Максимальний ККД цієї ректени склав 82,2 %, який виявився меншим, ніж у роботі [47] (88,9 %). Зниження ККД пояснюється наявністю КУ в конструкції ректени, зокрема індуктивності L (рис. 10, *б*), яка й зумовлює втрати. КУ було включено в структуру ректени тому, що не вдалося реалізувати опір випромінювача комплексно спряженим вхідному опору схеми випрямлення, як це було зроблено у [47].

Про успішне використання електрично малих ректен для забезпечення енергією датчиків температури та освітленості в музеї повідомляється в [48], а в [49] подана двофункціональна електрично мала ректена ($ka = 0,77$), яка може застосовуватися в системах одночасної безпроводної передачі інформації та енергії. Це особливо актуально в контексті створення сенсорних мереж з безпроводним живленням, де потрібно забезпечувати як передачу інформаційних сигналів, так і енергії між передавачем сенсорної мережі та її вузлами [50].

2.4. Ректенні решітки

Для деяких застосунків ректенний елемент в одній смузі частот не може забезпечити достатньої потужності постійного струму для живлення навантаження. Одним зі способів вирішення цієї проблеми є об'єднання ректенних елементів у решітки. При цьому важливо визначитися зі способом об'єднання ректенних елементів, особливо коли густина потоку потужності, що падає на ректену, є низькою. На основі аналізу численних теоретичних та експериментальних досліджень ректенних решіток [51 – 53] можна виділити три можливі варіанти їх побудови (рис. 11). Кожен із варіантів має як свої переваги, так і недоліки. У ректенних решітках, які реалізовані згідно зі схемою рис. 11, *а*, потужність складається на робочій частоті (когерентна схема) і потім спрямовується на загальну схему випрямлення. За рахунок спрямованих властивостей решітки (рис. 12, *а*), потужність, яка подається на схему випрямлення, збільшується, що в підсумку призводить до підвищення ККД ректени. Ректенні решітки, що побудовані за такою схемою, найбільше підходять для сценаріїв їх застосування, коли розташування джерела випромінювання фіксоване і відоме. У ректенних решітках, які побудовані за схемою рис. 11, *б*, потужність складається по постійному струму (некогерентна схема). Цей метод побудови ректенних решіток відрізняється простотою структури та

модульністю. Коефіцієнт підсилення, ширина ДС (рис. 12, б) та ККД аналогічні тим, що при-
таманні одиночному ректенному елементу решітки. Завдяки широкій ДС такі ректенні реші-
тки підходять для сценаріїв застосування, коли ЕМ хвилі надходять з різних довільних
напрямків, тобто коли положення джерела випромінювання невідоме. Вихідну потужність
постійного струму можна збільшити, додавши ректенні елементи.

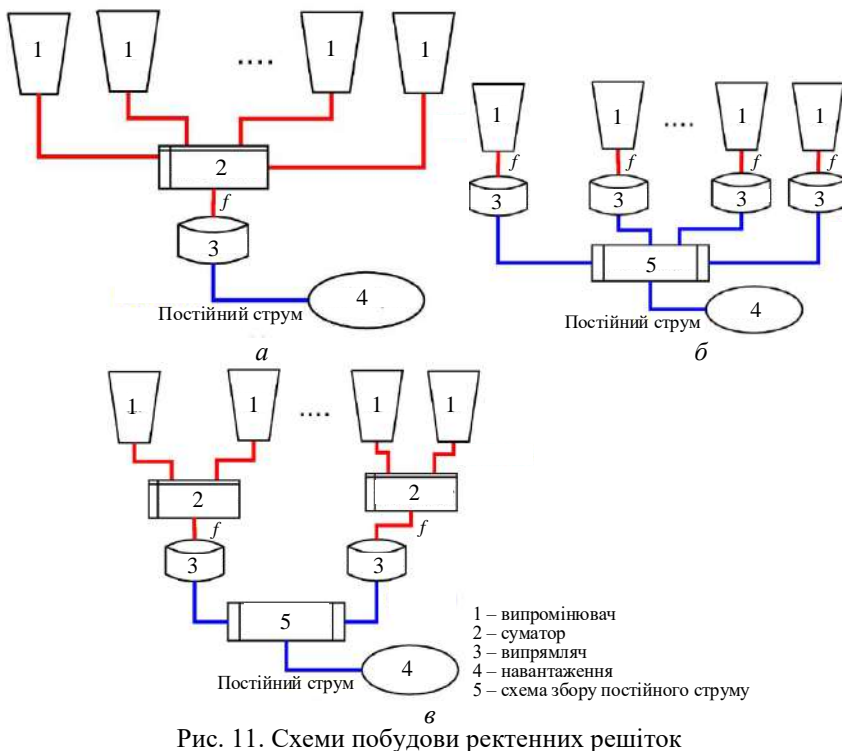


Рис. 11. Схеми побудови ректенних решіток

решіток є використання в них метаматеріалів. Такі ректенні решітки, які побудовані за
схемами на рис.11, а, б, досліджувалися в [45] (рис. 12).

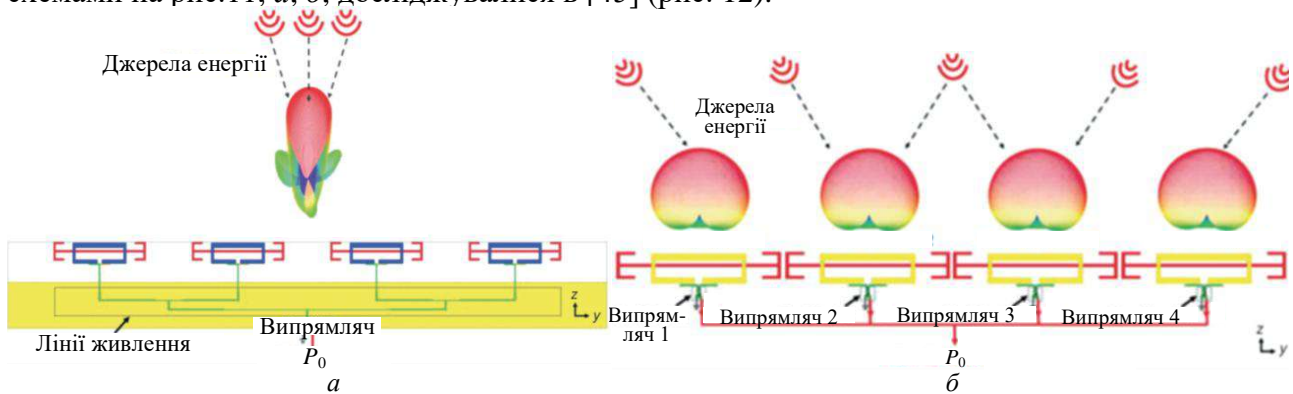


Рис. 12. Ректенні решітки та їх ДС: а – складання потужності на робочій частоті (рис. 11, а),
б – складання потужності по постійному струму (рис. 11, б)

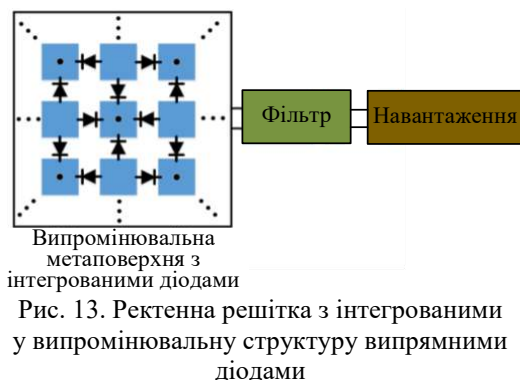


Рис. 13. Ректенна решітка з інтегрованими
у випромінювальну структуру випрямними
діодами

Компактні конструкції ширококутних та неза-
лежних від кута поляризації ректенних решіток
запропоновано в [43, 53]. Ректена складається з
періодичної решітки випромінювачів на основі
метаповерхонь з вбудованими в неї діодами
(рис. 13), фільтра нижніх частот і навантаження. КУ
між випромінювачами та випрямними діодами не
використовується, тому що в такій конструкції вда-
ється реалізувати опори випромінювачів комплекс-
но спряженими опорам випрямних діодів. На
рис. 14, 15 наведено приклади технічної реалізації

У роботі [52] запропо-
новано частково усунути
зазначені вище недоліки ре-
ктенних решіток, побудова-
них відповідно до схем на
рис. 11, а, б шляхом комбі-
нованого (на робочій частоті
і по постійному струму)
об'єднання ректенних еле-
ментів (рис. 11, в).

При збільшенні числа
ректенних елементів у ре-
шітці схема об'єднання по-
тужності стає складною, що
може призвести до значного
збільшення габаритних роз-
мірів решітки, втрат енергії,
підвищення вартості її
виготовлення. Одним зі
шляхів мінімізації габарит-
них розмірів ректенних

таких ректенних решіток і результати їх теоретичних та експериментальних досліджень. Автори [43] відзначають, що нелінійність діодів та виробничі помилки при їх виготовленні можуть викликати невеликий зсув частоти в експерименті, тобто призвести до інших результатів (рис. 14, в) на відміну від теоретичних досліджень.

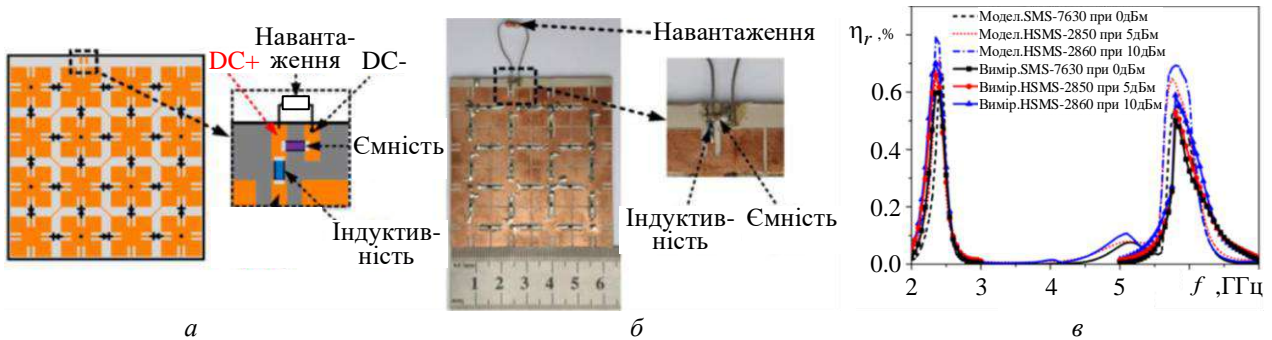


Рис. 14. 4×4 ректенна решітка [43]: а – топологія решітки, б – фото експериментального зразка, в – результати теоретичних та експериментальних досліджень ККД

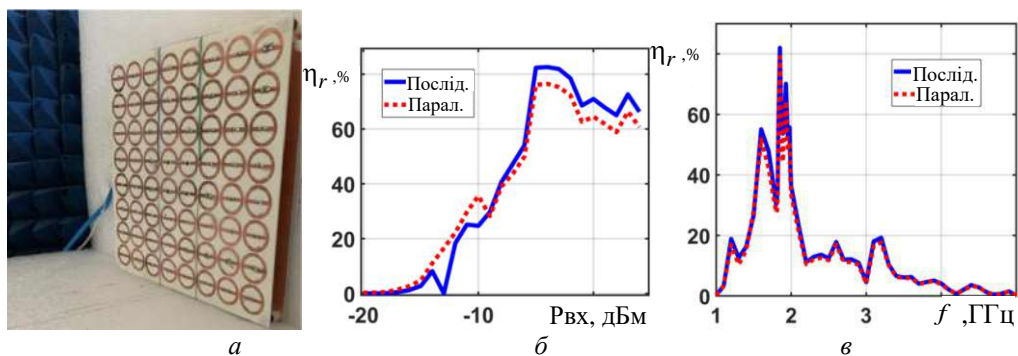


Рис. 15. Фото ректенної решітки 8×8 (а) [53], результати вимірювань ККД ректени при паралельному і послідовному з'єднанні ректенних елементів по постійному струму залежно від вхідної потужності (б) і частоти (в)

В [54] обґрунтовано ще один підхід конструктивної реалізації ректен для вирішення проблеми збільшення потужності постійного струму у навантаженні при низькій вхідній потужності. А саме, запропоновано конструкцію ректени на основі фокусувальної метаповерхні (рис. 16). Ректена розміщується у точці фокусування і перетворює концентрований ЕМ пучок в постійний струм.

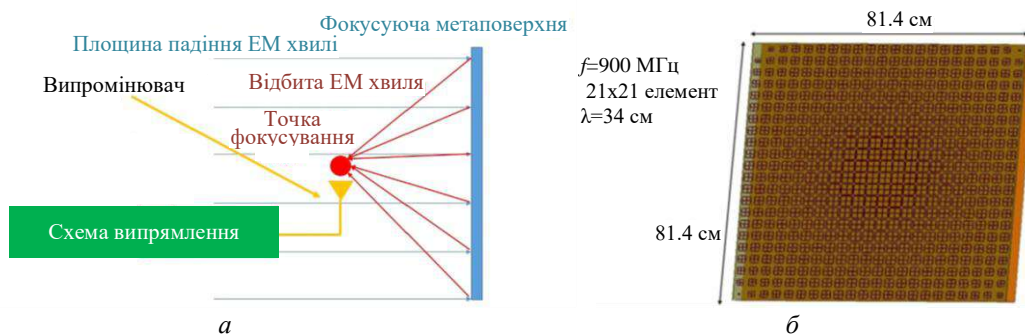


Рис. 16. Концепція побудови ректен на основі фокусувальної метаповерхні (а) та фото метаповерхні (б)

Перспективність застосування описаного підходу для збору ЕМ енергії з навколишнього простору підтверджується експериментальними даними. Показано, що виграш у прийнятій потужності стає більшим у вісім разів в порівнянні з ректеною без фокусувальної метаповерхні.

2.5. Багатодіапазонні та широкосмугові ректени

Конструкції однодіапазонних ректен сприяють досягненню високого рівня ККД перетворення ЕМ енергії в постійний струм, але кількість вихідної потужності постійного струму обмежена. Багатодіапазонні (багатосмугові) або широкосмугові ректени можуть накопичува-

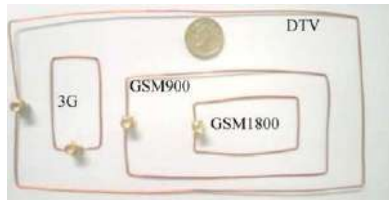


Рис. 17. Випромінювальна структура багатодіапазонної ректени

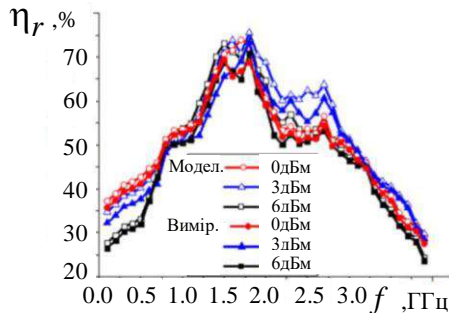
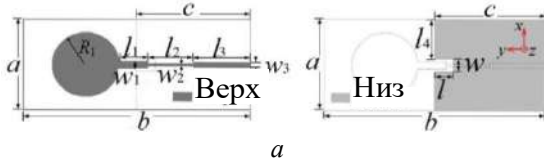


Рис. 18. НШС ректена

від заземленої копланарної лінії та широкосмуговим подвоювачем постійної напруги. Автори зазначають, що копланарні випромінювальні структури займають меншу площу, ніж аналогі в мікросмужковому виконанні, мають широкую смугу пропускання, а копланарні лінії передачі мають також низку переваг: простота інтеграції з активними та пасивними елементами ректени; висока щільність інтеграції схеми; мала дисперсія та відсутність перехідних отворів заземлення (спрощується проєктування схем випрямлення ректен).

Дослідженню широкосмугової ректени для збору ЕМ енергії у чотирьох частотних діапазонах: мереж стільникового зв'язку (GSM-900/1800, 3G/UMTS) та Wi-Fi присвячена робота [59]. Проведено порівняльний аналіз двох варіантів схем побудови ректен (рис. 2, в, г) з точки зору аналізу особливостей реалізації вхідних смугових фільтрів для узгодження опорів випромінювача та схеми випрямлення. Зазначено, що вхідний опір схеми випрямлення змінюється в залежності від частоти і рівня падаючої потужності. Опір випромінювача також залежить від частоти. Виходячи з цього, при узгодженні в кількох діапазонах (рис. 2, г) виникає два види втрат: втрати через неузгодженість опорів і втрати через складну конструкцію широкосмугового або багаточастотного фільтра (для ідеального узгодження на кількох частотах потрібні вхідні смугові фільтри високого порядку). Таким чином, щоб підвищити ККД перетворення ЕМ випромінювання в постійний струм, автори запропонували збирати енергію з кількох вузькосмугових радіочастотних діапазонів, а не з одного широкосмугового, використовуючи ректену, схема якої показана на рис. 2, в. У кожній смузі частот використовуються окремі смугові фільтри і схеми випрямлення, а виходи по постійному струму схем випрямлення підключаються до загального навантаження для складання зібраної потужності. В [59] також відзначено, що збір потужності у широкій смузі частот можна реалізувати кількома вузькосмуговими ректенами (рис. 2, б), проте такі конструкції не завжди підходять для компактних пристроїв через велику кількість використовуваних випромінювальних структур. Застосування широкосмугової випромінювальної структури (рис. 19, а) дозволяє створити більш компактну ректену.

У роботі [60] подано шестисмугову ректену для збору енергії ЕМ хвиль з довільною поляризацією. Ректена має широкую смугу пропускання від 550 МГц до 2,5 ГГц (охоплює шість

ти більше енергії від малопотужних навколишніх джерел і виробляти більшу вихідну потужність, ніж вузькосмугові [55]. Випромінювальна структура багатодіапазонної ректени, яка побудована за схемою на рис. 2, б, наведена на рис. 17 [56]. Петльові тонкопроводові однодіапазонні випромінювачі розміщені на підкладці з плексигласу. Збір ЕМ енергії в чотирьох частотних діапазонах дозволив при рівні вхідної потужності всього -29 дБм без будь-якого зовнішнього джерела живлення постійного струму запустити перетворювач напруги BQ25504 фірми Texas Instruments Incorporated.

Надширокосмугова (НШС) компактна ректена (рис. 18, а) з круглим мікросмужковим випромінювачем (розроблена за схемою рис. 2, г) запропонована у [57]. Результати моделювання та експериментальних досліджень у смузі частот від 0.9 до 3 ГГц (діапазони GSM, Wi-Fi та WLAN) наведені на рис. 18, б.

У [58] за схемою на рис. 2, г розроблено компактну широкосмугову ректену з щілинним випромінювачем (ширина ДС 60°), який живиться

діапазонів частот, включаючи частину діапазону цифрового телебачення та більшість діапазонів стільникового мобільного зв'язку та WLAN). Схему ректени наведено на рис. 20, а.

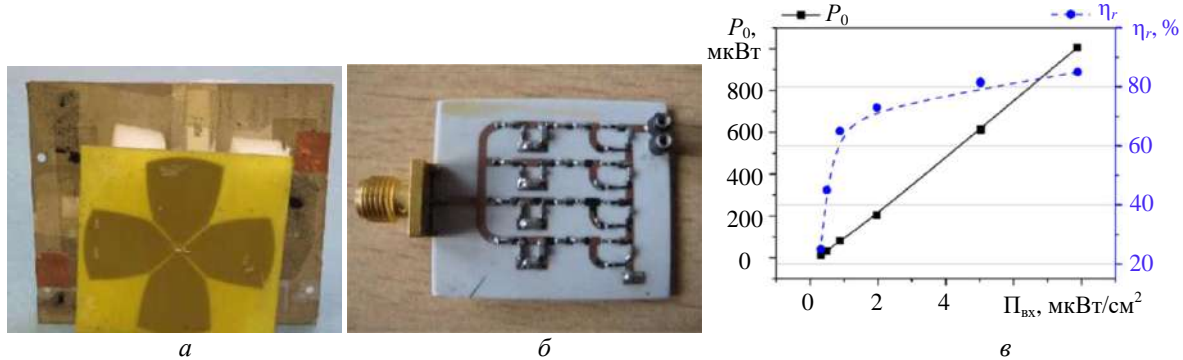


Рис. 19. Фото випромінювача (а) та схеми випрямляча ректени (б), результати вимірювання параметрів ректени на частотах 0,9; 1,8; 2,1; 2,4 ГГц (в) при навантаженні 11 кОм, що моделює типовий опір сучасних датчиків

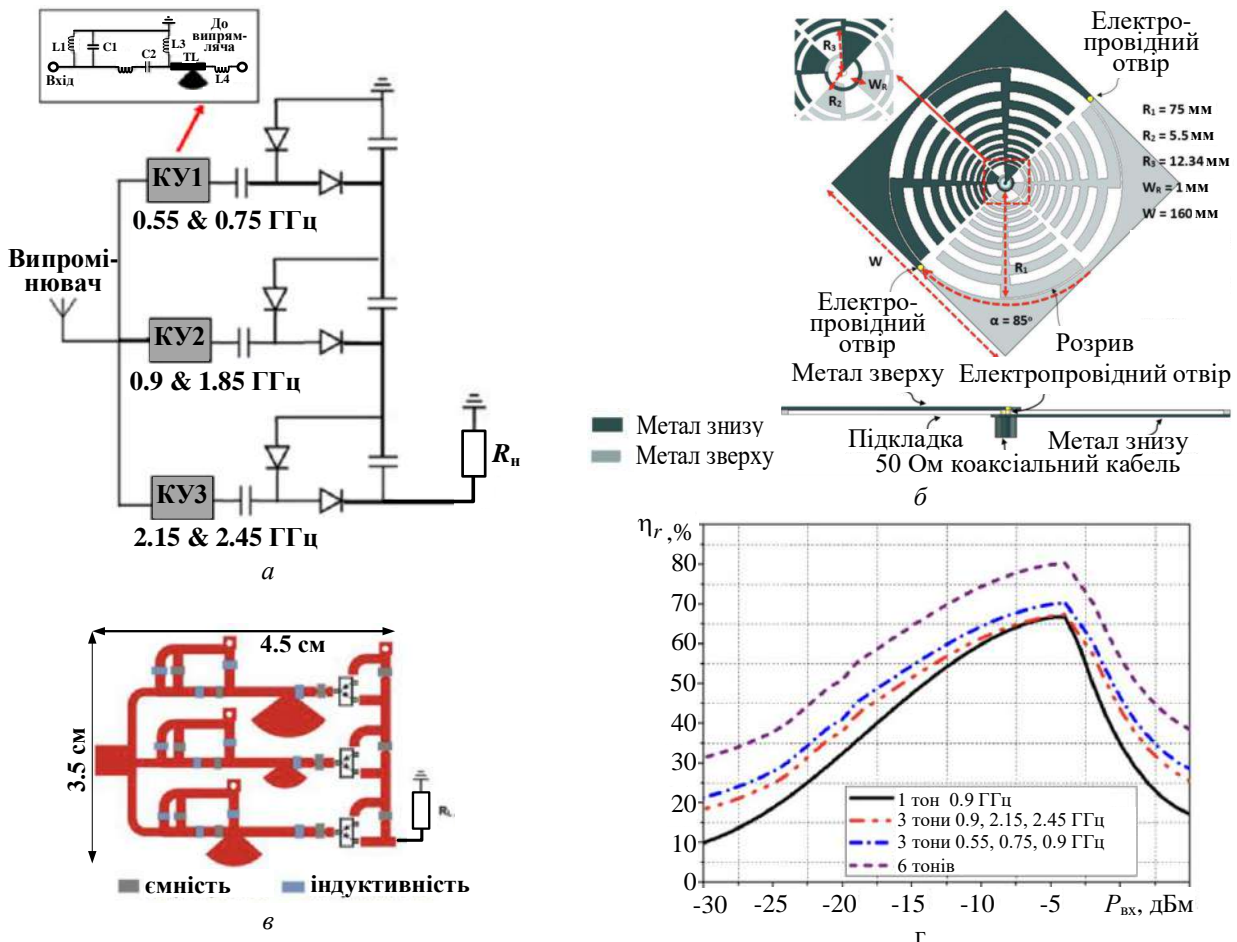


Рис. 20. Шестисмугова ректена: а – структурна схема; б – випромінювальна структура; в – топологія випрямної схеми; г – результати моделювання ККД

Ректена побудована як комбінація схем рис. 2, в, г. Для зменшення габаритних розмірів ректени було обрано кільцеву копланарну широкопasmову випромінювальну структуру (рис. 20, б). Покриття шести діапазонів частот було здійснено за допомогою трьох дводіапазонних кіл узгодження (КУ1, КУ2, КУ3), кожне з яких було підключено до однієї схеми випрямлення з подвоєнням напруги (рис. 20, а). Кола узгодження оптимізовані для рівнів вхідної потужності від -30 до -10 дБмВт і для опорів навантаження від 1 до 100 кОм. Три схеми випрямлення з'єднані послідовно, щоб отримати більш високу вихідну напругу. Топологія схеми випрямлення наведена на рис. 20, в, а результати моделювання ККД при опорі навантаження 25 кОм – на рис. 20, г.

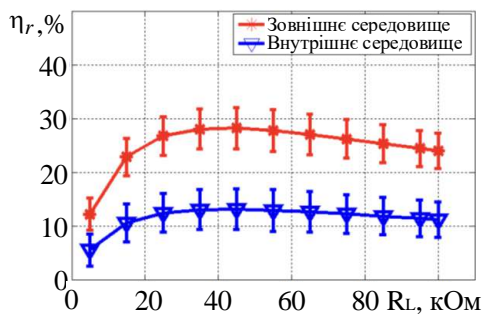


Рис. 21. Результати експериментальних досліджень ректени

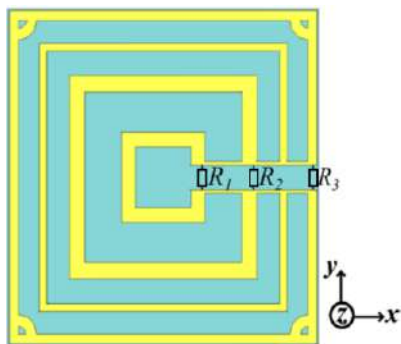
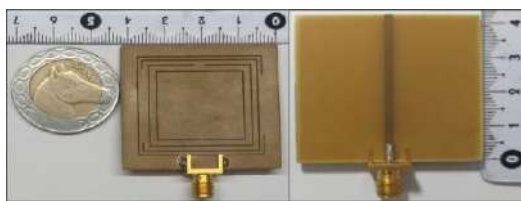


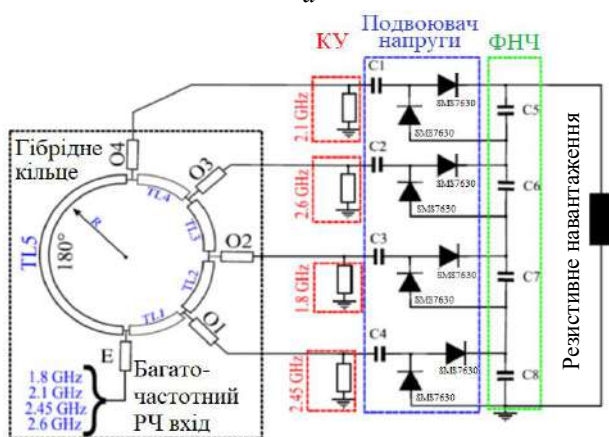
Рис. 22. Багато діапазонний випромінювач ректени

сті, відсутності взаємного зв'язку між їх елементами та багаточастотність.

В [62] подано чотиридіапазонну (GSM 1,8 ГГц, UMTS 2,1 ГГц, Wi-Fi 2,45 ГГц, 4G 2,6 ГГц) ректену на основі метаматеріалу з модифікованим гібридним кільцевим випрямлячем з чотирма гілками випрямлення.



а



б

Рис. 23. Випромінювач ректени (а) та її схема випрямлення (б)

На рис. 21 наведено результати експериментальних досліджень залежності ККД ректени від опорного навантаження в приміщенні та поза його межами. Показано, що ректена стабільно працює у широкому діапазоні навантажень від 10 до 75 кОм, що відповідає еквівалентному опорному навантаженню багатьох безпроводних датчиків та пристроїв. Максимальна потужність постійного струму ректени в типовому зовнішньому та внутрішньому середовищах відповідно становить 26 і 8 мкВт, тому ректену можна застосувати у низці безпроводних застосунків з низьким енергоспоживанням.

Автори [61] продемонстрували ректену на основі метаматеріалу для збору енергії в діапазонах частот GSM та Wi-Fi. Випромінювач складається з чотирьох вкладених резонаторів з роз'ємними кільцями, які з'єднані між собою на своїх роз'ємних частинах (рис. 22). ККД ректени становить 85,7 %, 82 %, 80,4 % і 69,8 % на частотах 0,90 ГГц, 1,80 ГГц, 2,6 ГГц та 5,8 ГГц відповідно, а середній ККД у чотирьох діапазонах становить 79,5 %. Показано, що при додаванні резонаторів у запропоновану структуру можна реалізувати збір енергії в п'яти- і шестичастотних смугах. Автори роботи наголошують, що випромінювальні структури на основі метаматеріалів мають низку переваг з точки зору компактності,

відсутності взаємного зв'язку між їх елементами та багаточастотність.

В [62] подано чотиридіапазонну (GSM 1,8 ГГц, UMTS 2,1 ГГц, Wi-Fi 2,45 ГГц, 4G 2,6 ГГц) ректену на основі метаматеріалу з модифікованим гібридним кільцевим випрямлячем з чотирма гілками випрямлення.

Габаритні розміри випромінювача (рис. 23, а) вдалося зменшити на 63,75 %, а схеми випрямлення (рис. 23, б) – на 23,62 % в порівнянні зі звичайними конструкціями. Гібридна кільцева сполука використовується для незалежного узгодження схем випрямлення в кожній смузі частот. Зі зміною електричної довжини і характеристичного опору кожної лінії передачі гібридного сполучного кільця був реалізований смуговий фільтр, який ділить вхідний багатотональний сигнал на однотональні, кожен з яких надходить на свій випрямляч (подвоювач напруги Віларда). Далі потужність складається по постійному струму. Ректена ефективно перетворює ЕМ енергію створювану базовою станцією в радіусі 50 м на корисну потужність постійного струму, що дозволило включити цифровий годинник без батареї.

Дводіапазонні ректени з фрактальними випромінювачами (рис. 24) досліджувалися у

[63, 64]. Наприклад, у роботі [63] подано компактну ректену (рис. 24, а), яка побудована за схемою рис. 2, в. Результати досліджень показали, що розроблена ректена демонструє відно-

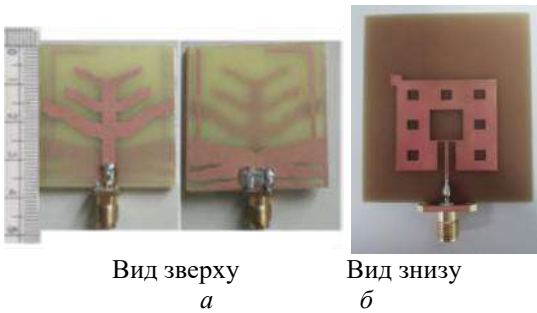


Рис. 24. Фрактальні випромінювачі ректен

сно стабільний ККД для значень навантаження в межах від 0,9 до 20 кОм при низькій вхідній потужності. Максимальний ККД становить 60 % на частоті 2,45 ГГц і 53 % на частоті 3,5 ГГц при вхідній потужності 0 дБм. У дослідженні [64] розроблено двочастотний (2,45 та 5,8 ГГц) випромінювач для ректени на основі фрактала Серпінського (рис. 24, б) зі зменшеним розміром (на 25,98 %) порівняно зі звичайним патч-випромінювачем. Додатково до мініатюризації

та дводіапазонного характеру розроблений випромінювач також усуває небажані гармоніки.

Очікуване масове розгортання ректен у застосунках IoT додає більш жорсткі обмеження щодо вартості та естетики [65]. Тому стають актуальними задачі, пов'язані з виготовленням ректен естетичного вигляду на підкладках із поширених конструктивних матеріалів (гіпс, дерево, оргскло тощо).

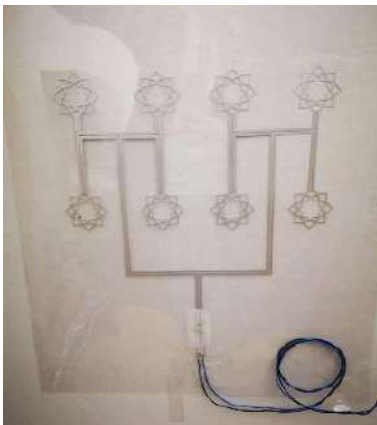


Рис. 25. Фото 8 елементної ректенної решітки

Наприклад, у [65] срібною фарбою на аркуші поліетилентерефталату надруковано випромінювальну структуру ректени, яка була розміщена на підкладці з гіпсокартону без поверхні заземлення для роботи в діапазоні 2,18 – 3,96 ГГц (рис. 25). Фрактальна решітка випромінювачів з восьми елементів забезпечує коефіцієнт підсилення 9,96 дБі на частоті 2,4 ГГц. Експериментальні результати показують, що ректенна решітка здатна забезпечити ККД більше 20 % при падаючій густині потоку потужності всього 0,028 мкВт/см², при цьому піковий ККД (61,3 %) забезпечується при падаючій густині потоку потужності 5,07 мкВт/см², що відповідає постійній напрузі 0,44 В у навантаженні 2,5 кОм. Отримані результати показують, що запропонована методологія виготовлення ректен може забезпечити масове

недороге розгортання у приміщенні мережі безпроводних датчиків для технології IoT. В майбутньому друкування випромінювальної структури можна реалізувати безпосередньо на гіпсокартоні.

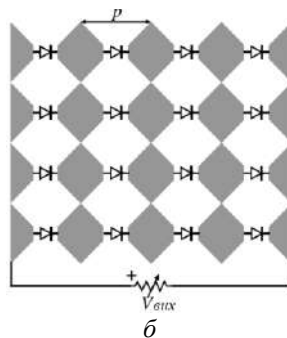
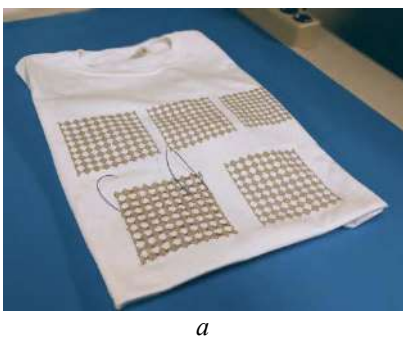


Рис. 26. Футболка з декількома ректенними решітками (а), та принципова схема підрешітки 4×4, яка показує з'єднання випрямних діодів з навантаженням (б)

У статті [66] подані 16- та 81- елементні широкосмугові ректенні решітки, які виготовлені методом трафаретного друку на бавовняній футболці (рис. 26), для збору ЕМ енергії з рівнями густини потоку потужності 4 – 130 мкВт/см² у діапазоні частот від 2 до 5 ГГц. Дослідження показали, що потужність постійного струму становить 32 мкВт у навантаженні 2 кОм при густині потоку падаючої потужності 4 мкВт/см².

Ще одним з підходів до збільшення потужності постійного струму у навантаженні є розробка тривимірних багатосмугових ректен [67, 68]. Чотиридіапазонна (FM-діапазон 98 МГц, GSM900, GSM1800, Wi-Fi 2,4 ГГц) тривимірна ректена для забезпечення живлення вузлів IoT була досліджена у [67]. Чотири ідентичні кросдипольні випромінювачі з подвійною поляризацією та асиметричними щілинами (рис. 27, а), що забезпечують приймання у трьох верхніх діапазонах частот, розташовані на тривимірній кубічній конструкції (10×10×10 см³). Усередині куба знаходиться суматор потужності та КУ. Несиметричний підвісний випромінювач з індуктивним наванта-

женням (рис. 27, б) використовується в нижньому діапазоні (98 МГц). Вихідна напруга у навантаженні ректени становить 2,38 В при вхідній потужності 10 дБм. ККД становить 70,28 %, 41,7 %, 33,37 % та 27,69 % на частотах 98 МГц, 0.9 ГГц, 1.8 ГГц та 2,4 ГГц, відповідно, при вхідній потужності 6 дБм.

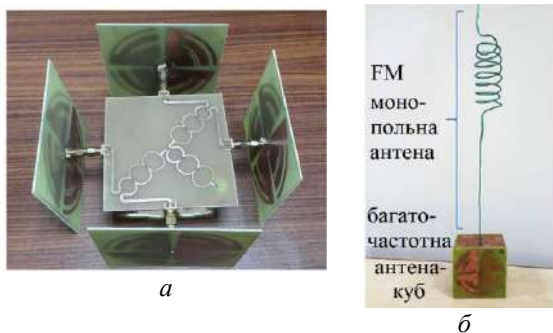


Рис. 27. Тривимірна ректена

У ректенах, які побудовані за схемами на рис. 2, а – г, кола узгодження та фільтрації вносять втрати (рис. 1), що призводить до зниження ККД й викликає труднощі при мініатюризації ректени [69, 70]. Усунути зазначені недоліки дозволяють ректени, які побудовані за схемами на рис. 2, е, ж. Смуговий фільтр можна інтегрувати у КУ [61] або у випромінювальну структуру [71 – 74] (випромінювач виконує функції фільтруючих та узгоджувальних кіл). Останній варіант кращий, тому що має низку переваг: невели-

кі габаритні розміри ректени; мінімальні втрати потужності, що дозволяє забезпечити на вході схеми випрямлення потужність приблизно рівну вхідній потужності; розширення робочої смуги ректени; придушення гармонік. Щоб забезпечити максимальну потужність у схемі випрямлення в робочій смузі частот повний вхідний опір випромінювача має бути комплексно спряженим з вхідним опором схеми випрямлення, тобто необхідно забезпечити слабку залежність модуля вхідного опору випромінювача від частоти. При безпосередньому з'єднанні випромінювача та схеми випрямлення головну роль у придушенні випромінювання на вищих гармоніках відіграє правильний вибір повного вхідного опору навантаження, функцію якого виконує вхідний опір випромінювача на частотах гармонік. Найкраща фільтрація гармонік досягається в тому випадку, коли на частотах гармонік активний опір випромінювача прагне до нуля. Отже, енергетичні параметри ректени значною мірою залежать від значення повного вхідного опору випромінювача. При розробці ректен за схемами рис. 2, е, ж необхідно одночасно вирішувати завдання проектування, моделювання та оптимізації випромінювача та кіл фільтрації. На рис. 28, 29 наведено приклади технічної реалізації широко-смугових ректен, які побудовані за схемою рис. 2, ж.

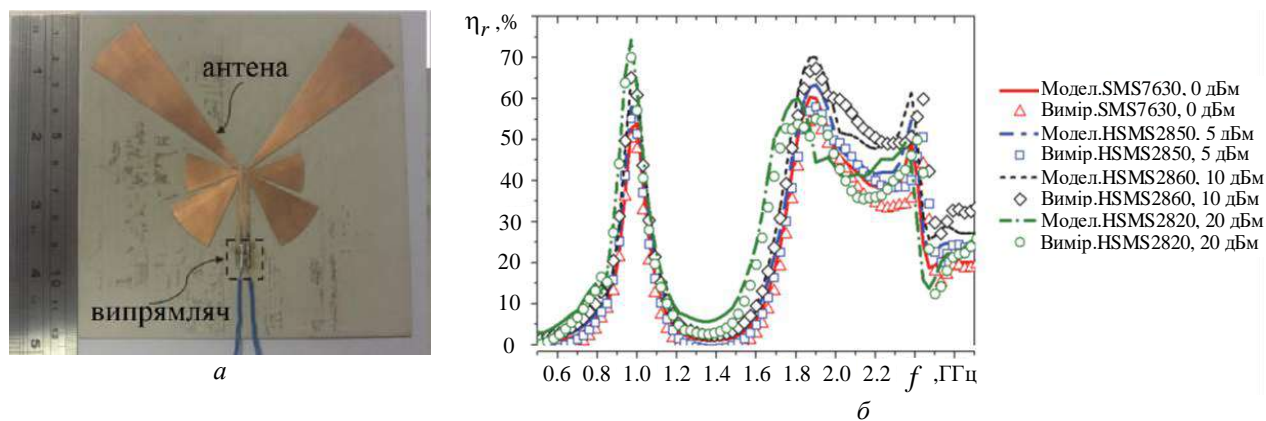


Рис. 28. Конструкція ректени (а) і результати теоретичних та експериментальних досліджень (б) [69]

Плечі диполя зі зміщенням від центру живленням мають форму типу краватка-метелик (рис. 28, а), що дозволяє розширити робочу смугу частот. Для забезпечення приймання ЕМ хвиль з довільною поляризацією диполі виконані однакового розміру та ортогональні один одному. Для управління імпедансом випромінювальної структури між двома диполями розміщено пару радіальних шлейфів. Дана конструкція ректени дозволяє зменшити вплив нелінійності випрямляча та забезпечити добре узгодження у широкому діапазоні значень імпедансу навантаження. Таким чином, ректена може ефективно працювати навіть при викорис-

танні різних типів діодів (рис. 28, б). Результати вимірювань показують, що ректена має високий ККД (більше 60 %) у двох широких діапазонах частот: 0,9 – 1,1 ГГц і 1,8 – 2,5 ГГц.

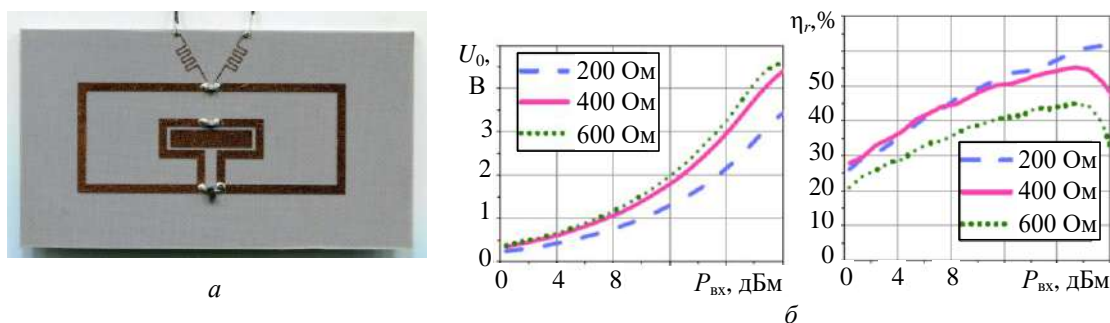


Рис. 29. Двосмугова ректена (а) та залежності постійної напруги U_0 та ККД від вхідної потужності на частоті 5,8 ГГц при різних опорах навантаження (б) [70]

На рис. 29, а дві меандровані лінії використовуються для виведення потужності постійного струму. Щоб уникнути взаємного зв'язку вони розташовані непаралельно одна одній.

2.6. Випрямні схеми ректен

Розглянемо деякі особливості проектування випрямлячів для ректен низької потужності. У загальному випадку вибір оптимальної конструкції випрямляча є нетривіальним завданням, оскільки він залежить від конкретної галузі застосування. Слід зазначити, що випрямляч, який ідеально підходить для одного сценарію застосування, може виявитися неефективним для іншого. За останні десятиліття було опубліковано багато досліджень на тему випрямних пристроїв для ректен систем збору ЕМ енергії. Рівень густини потоку потужності, що падає на ректену, зазвичай залишається невисоким. Це ускладнює розробку вискоелективних випрямлячів. Нелінійна поведінка випрямних елементів на високих частотах може викликати непередбачувані ємнісні та резистивні ефекти [1], змінюючи режим роботи кола узгодження та накопичувача енергії постійного струму. Тому важливе проведення оптимізації конструкції випрямляча, з урахуванням загальних рекомендацій щодо підвищення ККД, чутливості, зниження маси та габаритних розмірів, а також забезпечення надійної роботи. Ці аспекти слід адаптувати до конкретних вимог та умов експлуатації.

У ректенах для збирання та перетворення ЕМ енергії у постійний струм застосовуються напівпровідникові випрямні елементи. Діоди Шотткі широко використовуються через їхній низький поріг включення, меншу ємність переходу і стабільну роботу при різних температурах [75]. Низький поріг включення забезпечує ефективну роботу ректени при малих вхідних потужностях, а низька ємність переходу збільшує максимальну частоту, на якій ректена може працювати з заданими показниками якості. Дослідження [76] показують, що обернено-тунельні діоди можуть бути більш ефективними, ніж діоди Шотткі з точки зору ККД. Проте їхній високий імпеданс активної частини у діапазоні УВЧ ускладнює побудову КУ. Транзистори з діодним підключенням [77] мають напругу включення, близьку до порогової (менше 150 мВ), що дозволяє збирати енергію за дуже низької вхідної потужності. Транзистори з діодним підключенням дозволяють значно знизити площу випрямляча та зменшити вартість серійного виробництва ректен.

На рис. 30 подано кілька найбільш поширених схем випрямлячів. Для безпровідного енергопостачання малопотужних пристроїв серед різних схем випрямлячів ректен особливий інтерес становлять схеми, в яких за допомогою відповідного включення випрямних елементів і конденсаторів здійснюється не тільки випрямлення, але одночасно і множення випрямленої напруги (рис. 30, в – е) [78]. Робота помножувача напруги заснована на заряді та розряді конденсаторів через діоди. Схеми випрямлячів з множенням напруги дають можливість отримати на виході схеми напругу, помножену в кілька разів відносно вхідної. Коефіцієнт множення залежить від кількості ланок. Особливістю роботи випрямлячів з множенням напруги є використання властивостей конденсаторів накопичувати протягом деякого часу та

зберігати електричну енергію. Чим більша ємність конденсаторів, тим більше електричної енергії вони зберігають і тим вище при одному і тому ж навантаженні випрямлена напруга.

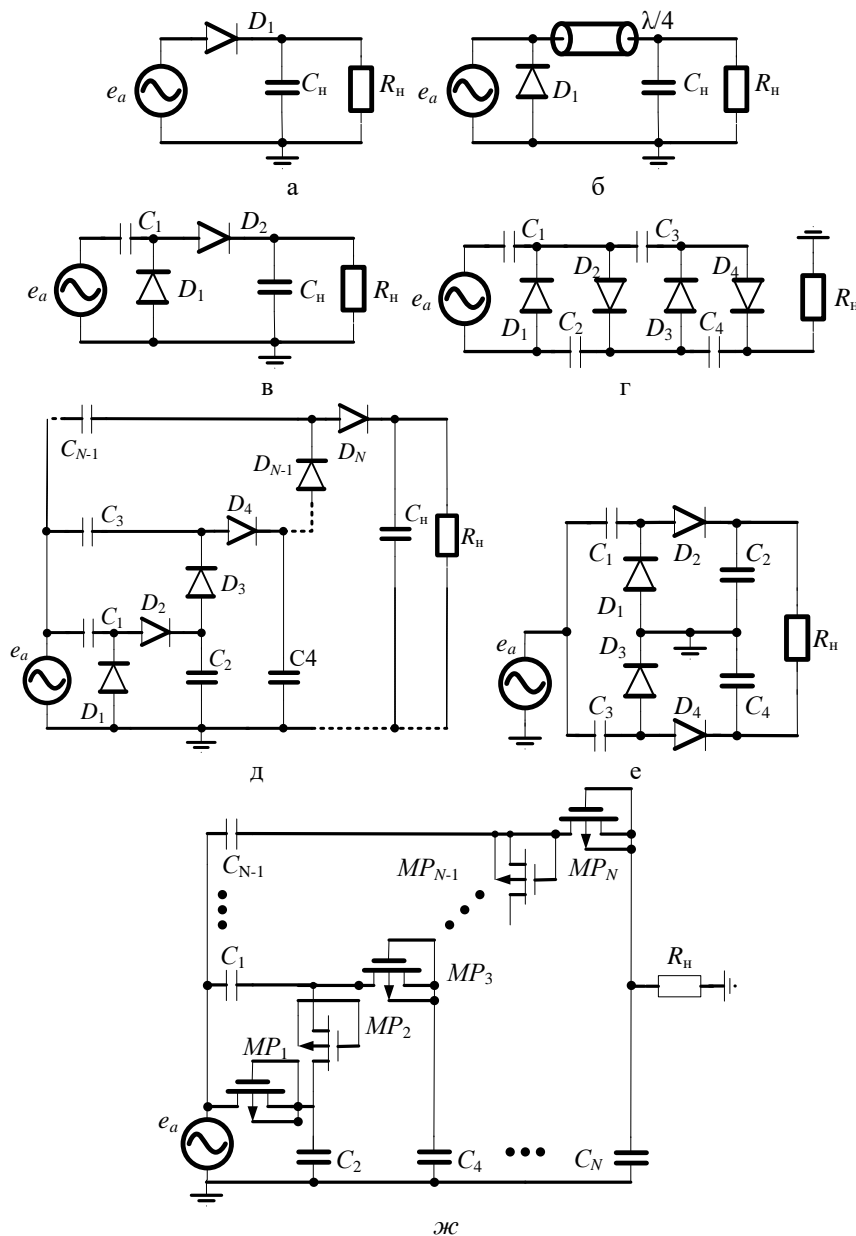


Рис. 30. а, б – однонапівперодні випрямлячі, в – однокаскадний помножувач напруги, г – помножувач Кокрофта–Уолтона–Грейнахера–Вілларда, д – помножувач Діксона, е – модифікований помножувач Кокрофта–Уолтона–Грейнахера, ж – транзисторний помножувач Діксона

При проектуванні помножувачів напруги необхідно підбирати оптимальну кількість ланок. Помножувачі з великою кількістю ланок забезпечують більший коефіцієнт множення напруги та знижують граничну напругу своєї першої ланки, що призводить до збільшення чутливості, проте при цьому зростають втрати потужності в елементах доданих ланок множення.

Помножувачі з меншою кількістю ланок мають менші втрати потужності, але при цьому мають вищий поріг включення при низькій вхідній потужності. Вибір оптимальної кількості ланок залежить від конкретних вимог застосунка.

В залежності від властивостей симетрії випрямлячі можна розділити на дві групи: з несиметричною топологією (наприклад, рис. 30, в) та симетричною (диференційною) топологією (рис. б).

Висновки

Розглянуто досягнення в галузі розробки ректен систем збору та перетворення енергії ЕМ полів,

що породжуються різними джерелами ЕМ енергії (РЕЗ різного класу та призначення), в енергію постійного струму. Ця технологія БПЕ [2] в даний час є однією з найбільш привабливих, враховуючи зростаючу щільність розташування РЕЗ різного призначення, особливо в мегаполісах. Лише у базі даних IEEE Xplore протягом останніх 17 років було виявлено понад 3800 публікацій за ключовими словами “RF Energy Harvesting”. Важливо відзначити, що ця стаття не претендує на вичерпний розгляд усіх аспектів технології збирання ЕМ енергії з довкілля. Цю роботу варто розглядати, перш за все, як визначення певної «відправної точки» для розробників при створенні ефективних ректен, які задовольняють сучасним вимогам практики. У статті наведено основні параметри ректен систем збору ЕМ енергії та типові

схеми їх побудови. Розглянуто різні варіанти конструктивної реалізації ректен та їх енергетичні характеристики.

Визначальними принципами при розробці ректен є досягнення високого ККД ректени, простоти конструкції, прийнятних масогабаритних показників, низької вартості, надійності і придатності для серійного виробництва. На енергетичні характеристики ректен впливає багато чинників, але є три взаємопов'язаних рівня вирішення проблеми створення якісних ректен. Перший рівень – поліпшення параметрів окремих випрямних елементів; другий рівень – оптимізація параметрів і характеристик окремих елементів ректени; третій рівень – оптимізація характеристик всієї ректени в цілому.

Загалом підхід до проектування високоефективних малопотужних ректен можна розділити на два основні аспекти.

Перший аспект полягає у розробці випромінювачів, які приймають енергію ЕМ хвиль з довільною поляризацією у широкій смузі частот або в кількох частотних діапазонах. Основні параметри випромінювачів, такі як форма ДС, коефіцієнт підсилення повинні забезпечувати необхідні характеристики ректени. У ректенах для збирання енергії зазвичай застосовують слабоспрямовані випромінювачі. Вони повинні мати високий ККД, високу механічну міцність, невеликі габаритні розміри і масу, також можливість функціонувати при коливаннях температури та атмосферного тиску. Крім зазначених загальних рекомендацій, вимоги до випромінювачів повинні враховувати специфіку їх роботи в ректені. Бажано, щоб у робочій смузі частот їх вхідний опір був близьким до величини оптимального навантаження випрямляча. У цьому випадку можливе підключення випромінювача до входу випрямляча або безпосередньо або із застосуванням простого КУ з невеликим числом елементів. Також, випромінювач і КУ повинні мати фільтруючі властивості для ослаблення рівня позасмугового випромінювання ректени.

Другий аспект полягає в розробці схем випрямлення з високим ККД перетворення енергії ЕМ полів у постійний струм і з високою чутливістю, а також оптимізації їх конструкції та топології, оптимального вибору механізмів випрямлення.

Проте з аналізу літературних джерел випливає, що в напрямку перетворення малопотужних ЕМ полів довільної структури все ж існує низка проблем. По-перше, є необхідність у розробці системного підходу, який дозволить розглядати систему збору електромагнітної енергії та перетворення її в корисну електричну енергію як єдину систему з врахуванням всіх нелінійних ефектів, що виникають у таких структурах. По-друге, ще недостатньо розвинені строгі теоретичні підходи до аналізу ректен, які збуджуються малопотужними нестационарними ЕМ полями довільної структури. Дослідження ректен при такому режимі збудження зараз проводяться при певних спрощеннях і припущеннях, які не дозволяють врахувати всю сукупність виникаючих в них нелінійних ефектів і приступити до серійного виробництва високоефективних ректен як енергосистем малопотужних пристроїв.

Список літератури

1. Шокало В.М., Лучанинов А.И., Рыбалко А.М., Грецких Д.В. Крупноапертурные антенны-выпрямители систем беспроводной передачи энергии микроволновым лучом. Харьков : Коллегиум, 2006. 308 с.
2. Алексеев В.О., Грецких Д.В., Гавва Д.С., Лихограй В.Г. Технологии беспроводной передачи энергии // Радиотехника. 2022. №211. С. 114–133.
3. Гавва Д.С., Грецких Д.В., Гомозов А.В., Пунин Д.В. Электродинамические устройства на основе радиоэлементов и материалов с нелинейными характеристиками // Технология приборостроения. 2018. № 2. С. 17–31.
4. Гавва Д.С., Грецких Д.В., Гомозов А.В., Преснякова А.Д. Электродинамические устройства с нелинейными характеристиками // Технология приборостроения. 2019. № 1. С. 20–35.
5. Wagih M., Weddell A.S., Beeby S. Rectennas for Radio-Frequency Energy Harvesting and Wireless Power Transfer: A Review of Antenna Design // IEEE Antennas and Propagation Magazine. 2020. Vol. 62, Is. 5. P. 95–107.
6. Adami S.-E., Proynov P., Geoffrey S. et al. A Flexible 2.45-GHz Power Harvesting Wristband With Net System Output From -24.3 dBm of RF Power // IEEE Transactions on Microwave Theory and Techniques. 2018. Vol. 66, No. 1.P. 380–395.
7. Zhang Y., Shen S., Chiu C.Y., Murch R. Hybrid RF-Solarenergy Harvesting Systems Utilizing Transparent Multiport Micromeshed Antennas // IEEE Transactions on Microwave Theory and Techniques. 2019. Vol. 67, No. 11.P. 4534–4546.

8. Wagih M., Weddell A.S., Beeby S. Meshed High-Impedance Matching Network-Free Rectenna Optimized for Additive Manufacturing // *IEEE Open Journal of Antennas and Propagation*. 2020. Vol. 1. P. 615–626.
9. Li X., Xiao H., Zhang H. et al. A High Gain Flexible Receiving Antenna for Microwave Wireless Power Transmission. *Authorea*. 2022. P. 1–3.
10. Eid A., Hester J., Costantine J. et al. A Compact Source-Load Agnostic Flexible Rectenna Topology for IoT Devices // *IEEE Transactions on Antennas and Propagation*. 2020. Vol. 68, Is. 4. P. 2621–2629.
11. Wagih M., Weddell A.S., Beeby S. Omnidirectional Dual-Polarized Low-Profile Textile Rectenna With Over 50% Efficiency for Sub- $\mu\text{W}/\text{cm}^2$ Wearable Power Harvesting // *IEEE Transactions on Antennas and Propagation*. 2021. Vol. 69, No. 5. P. 2522–2536.
12. Wagih M., Weddell A.S., Beeby S. High-Efficiency Sub-1 GHz Flexible Compact Rectenna Based on Parametric Antenna-Rectifier Co-Design // *Proceedings of 2020 IEEE/MTT-S International Microwave Symposium (IMS)*. 2020. P. 1–4.
13. Arrawatia M., Baghini M.S., Kumar G. Differential Microstrip Antenna for RF Energy Harvesting // *IEEE Transactions on Antennas and Propagation*. 2015. Vol. 63, Is. 4. P. 1581–1588.
14. Wei L.Q., Yin Z.X. Differential Rectifier Using Resistance Compression Network for Improving Efficiency Over Extended Input Power Range // *IEEE Transactions on Microwave Theory and Techniques*. 2016. Vol. 64, No. 9. P. 2943–2954.
15. Hucheng S. An Enhanced Rectenna Using Differentially-Fed Rectifier for Wireless Power Transmission // *IEEE Antennas and Wireless Propagation Letters*. 2015. Vol. 15. P. 32–35.
16. Zhang H., Zhong Z., Guo Y.-X., Wu W. Differentially-Fed Charge Pumping Rectifier Design with An Enhanced Efficiency for Ambient RF Energy Harvesting // *Proceedings of 2017 IEEE MTT-S International Microwave Symposium (IMS)*. 2017. P. 613–616.
17. Vyas R.J., Cook B.B., Kawahara Y., Tentzeris M.M. E-WEHP: A Batteryless Embedded Sensor-Platform Wirelessly Powered From Ambient Digital-TV Signals // *IEEE Transactions on Microwave Theory and Techniques*. 2013. Vol. 61, No. 6. P. 2491–2505.
18. Furuta T., Ito M., Nambo N. et al. The 500 MHz Band Low Power Rectenna for DTV in the Tokyo Area // *Proceedings of 2016 IEEE Wireless Power Transfer Conference (WPTC)*. 2012. P. 1–3.
19. Noguchi A., Arai H. Small Loop Rectenna for RF Energy Harvesting // *Proceedings of 2013 Asia-Pacific Microwave Conference Proceedings (APMC)*. 2013. P. 1–3.
20. John V., Chi-Chi C., Kyohei F. *Small Antennas: Miniaturization Techniques & Applications*. New York, NY, USA: McGraw-Hill, 2009.
21. Ouedraogo R.O., Rothwell E.J., Diaz A.R., Fuchi K., Temme A. Miniaturization of Patch Antennas Using a Metamaterial-Inspired Technique // *IEEE Transactions on Antennas and Propagation*. 2012. Vol. 60, No. 5. P. 2175–2182.
22. Ghosh B., Haque S.M., Mitra D. Miniaturization of Slot Antennas Using Slit and Strip Loading // *IEEE Transactions on Antennas and Propagation*. 2011. Vol. 59, No. 10. P. 3922–3927.
23. Takacs A., Fonseca N.J.G., Aubert H. Height Reduction of the Axial-Mode Open-Ended Quadrifilar Helical Antenna // *IEEE Antennas and Wireless Propagation Letters*. 2010. Vol. 9. P. 942–945.
24. Valteau J., Aubert H., Bellion A. et al. Resonant Metallic Rings With Irregular Contours for Spiral Antennas Miniaturization // *Proceedings of IEEE Conference Antenna Measurements & Applications (CAMA)*, Juan-les-Pins, France. 2014, P. 1–4.
25. Gaetano M. The Art of UHF RFID Antenna Design: Impedance-Matching and Size-Reduction Techniques // *IEEE Antennas and Propagation Magazine*. 2008. Vol. 50, Is. 1. P. 66–79.
26. Talla V., Kellogg B., Gollakota S., Smith J.R. Battery-Free Cellphone // *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2017. Vol. 1, Is. 2. P. 1–20.
27. Ho D.K., Ngo V.D., Kharrat I. et al. A Novel Dual-Band Rectenna for Ambient RF Energy Harvesting at GSM 900 MHz and 1800 MHz // *Advances in Science, Technology and Engineering Systems*. 2017. Vol. 2, Is. 3. P. 612–616.
28. Okba A., Takacs A., Aubert H. Compact Rectennas for Ultra-Low-Power Wireless Transmission Applications // *IEEE Trans. Microw. Theory Techn.* 2019. Vol. 67, No. 5. P. 1697–1707.
29. Zeng M., Andrenko A.S., Liu X. et al. A Compact Fractal Loop Rectenna for RF Energy Harvesting // *IEEE Antennas and Wireless Propagation Letters*. 2017. Vol. 16. P. 2424–2427.
30. Shi Y., Jing J., Fan Y., Yang L., Wang M. Design of a Novel Compact and Efficient Rectenna for WiFi Energy Harvesting // *Prog. Electromagn. Res.* 2018. Vol. 83. P. 57–70.
31. Liu C., Guo Y.X., Sun H., Xiao S. Design and Safety Considerations of an Implantable Rectenna for Far-Field Wireless Power Transfer // *IEEE Transactions on Antennas and Propagation*. 2014. Vol. 62, Is. 11. P. 5798–5806.
32. Gu X., Hemour S., Guo L., Wu K. Integrated Cooperative Ambient Power Harvester Collect in Ubiquitous Radio Frequency and Kinetic Energy // *IEEE Transactions on Microwave Theory and Techniques*. 2018. Vol. 66, Is. 9. P. 4178–4190.
33. Hosain M.K., Kouzani A.Z., Tye S.J. et al. Development of a Compact Rectenna for Wireless Powering of a Headmountable Deep Brain Stimulation Device // *IEEE Journal of Translational Engineering in Health and Medicine*. 2014. Vol. 2. P. 1–13.
34. Qudus A., Zahid S., Tahir F.A. et al. Dualband Compact Rectenna for UHF and ISM Wireless Power Transfer Systems // *IEEE Transactions on Antennas and Propagation*. 2021. Vol. 69, Is. 4. P. 2392–2397.

35. Eid A., Hester J.G.D, Costantine J. et al. A Compact Source-Load Agnostic Flexible Rectenna Topology for IoT Devices // *IEEE Transactions on Antennas and Propagation*. 2020. Vol. 68, Is. 4. P. 2621–2629.
36. Chuma E.L., Rodríguez L.D.L.T., Iano Y. et al. Compact Rectenna Based on a Fractal Geometry With a High Conversion Energy Efficiency Per Area // *IET Microwaves, Antennas & Propagation*. 2018. Vol. 12. Is. 2. P. 173–178.
37. Shrestha S., Lee S.R., Choi D.Y. A New Fractal-Based Miniaturized Dual Band Patch Antenna for RF Energy Harvesting // *International Journal of Antennas and Propagation*. 2014. Vol. 2014. P. 1–9.
38. Bakogianni S., Koulouridis S. A Dual-Band Implantable Rectenna For Wireless Data and Power Support at Sub-GHz Region // *IEEE Transactions on Antennas and Propagation*. 2019. Vol. 67. Is. 11. P. 6800–6810.
39. Cheng H.W., Yu T.C., Luo C.H. Direct Current Driving Impedance Matching Method for Rectenna Using Medical Implant Communication Service Band for Wireless Bcharging // *IET Microwaves, Antennas & Propagation*. 2013. Vol. 7, Is. 4. P. 277–282.
40. Assimonis S.D., Fusco V., Georgiadis A., Samaras T. Efficient and Sensitive Electrically Small Rectenna for Ultra-Low Power RF Energy Harvesting // *Scientific Reports*. 2018. Vol. 8, Is. 1. P. 1–12.
41. Amer A.A.G., Sapuan S.Z., Nasimuddin N. et al. A Comprehensive Review of Metasurface Structures Suitable for RF Energy Harvesting // *IEEE Access*. 2020. Vol. 8. P. 76433–76452.
42. Eteng A.A., Goh H.H., Alomainy S.-K.A.-R.A. A Review of Metasurfaces for Microwave Energy Transmission and Harvesting in Wireless Powered Networks // *IEEE Access*. 2021. Vol. 9. P. 27518–27539.
43. Aldhaebi M.A., Almoneef T.S. Highly Efficient Planar Metasurface Rectenna // *IEEE Access*. 2020. Vol. 8. P. 214019–214029.
44. Tang M.C., Wang H., Ziolkowski R.W. Design and Testing of Simple, Electrically Small, Low-Profile, Huygens Source Antennas With Broadside Radiation Performance // *IEEE Transactions on Antennas and Propagation*. 2016. Vol. 64, Is. 11. P. 4607–4617.
45. Lin W., Ziolkowski R.W. High Performance Electrically Small Huygens Rectennas Enable Wirelessly Powered Internet of Things Sensing Applications: A Review // *Engineering*. 2022. Vol. 11. P. 42–59.
46. Шокало В.М., Правда В.І., Усін В.А., Вунтесмері В.С., Грецьких Д.В. Електродинаміка та поширення радіохвиль. Ч.2. Випромінювання та поширення електромагнітних хвиль. Харків : Колегіум, 2010. 435 с.
47. Lin W., Ziolkowski R.W., Huang J. Electrically Small, Low Profile, Highly Efficient, Huygens Dipole Rectennas For Wirelessly Powering Internet-of-Things (IoT) Devices // *IEEE Transactions on Antennas and Propagation*. 2019. Vol. 67, Is. 6. P. 3670–3679.
48. Lin W., Ziolkowski R.W. Wirelessly Powered Light and Temperature Sensors Facilitated by Electrically Small Omnidirectional and Huygens Dipole Antennas // *Sensors*. 2019. Vol. 19, Is. 9.
49. Lin W., Ziolkowski R.W. Electrically Small Huygens Antenna-Based Fully Integrated Wireless Power Transfer and Communication System // *IEEE Access*. 2019. Vol. 7. P. 39762–39769.
50. Ponnimbaduge P.T.D., Jayakody D.N.K., Sharma S.K. et al. Simultaneous Wireless Information and Power Transfer (SWIPT): Recent Advance and Future Challenges // *IEEE Communications Surveys & Tutorials*. 2018. Vol. 20, Is. 1. P. 264–302.
51. Massa A., Oliveri G., Viani F., Rocca P. Array Designs for Long-Distance Wireless Power Transmission: State-of-the-Art and Innovative Solutions // *Proceedings of the IEEE*. 2013. Vol. 101, No 6. P. 1464–1481.
52. Shen S., Zhang Y., Chiu C.-Y., Murch R.A. Triple-Band High-Gain Multibeam Ambient RF Energy Harvesting System Utilizing Hybrid Combining // *IEEE Transactions on Industrial Electronics*. 2020. Vol. 67, Is. 11. P. 9215–9226.
53. Li L., Zhang X., Song C. et al. Compact Dual-Band, Wide-Angle, Polarization-Angle-Independent Rectifying Metasurface for Ambient Energy Harvesting and Wireless Power Transfer // *IEEE Transactions on Microwave Theory and Techniques*. 2021. Vol. 69, No. 3. P. 1518–1528.
54. Kalaagi M., Seetharamdoo D. Enhancing the Power Level Harvested by Rectenna Systems Based on Focusing Metasurfaces for Ambient Environments // *Journal of Applied Physics*. 2022. Vol. 132, Is. 22. P. 1–8.
55. Song C., Huang Y., Zhou J. et al. A High-Efficiency Broadband Rectenna for Ambient Wireless Energy Harvesting // *IEEE Transactions on Antennas and Propagation*. 2015. Vol. 63, No. 8. P. 3486–3495.
56. Pinuela M., Mitcheson P.D., Lucyszyn S. Ambient RF Energy Harvesting in Urban and Semiurban Environments // *IEEE Transactions on Microwave Theory and Techniques*. 2013. Vol. 61, No. 7. P. 2715–2726.
57. Lu P., Song C., Huang K.M. Ultra-Wideband Rectenna Using Complementary Resonant Structure for Microwave Power Transmission and Energy Harvesting // *IEEE Transactions on Microwave Theory and Techniques*. 2021. Vol. 69, No. 7. P. 3452–3462.
58. Nie M.-J., Yang X.-X., Tan G.-N., Han B. A Compact 2.45-GHz Broadband Rectenna Using Grounded Coplanar Waveguide // *IEEE Antennas and Wireless Propagation Letters*. 2015. Vol. 14. P. 986–989.
59. Kuhn V., Lahuec C., Seguin F., Person C. A Multi-Band Stacked RF Energy Harvester With RF-to-DC Efficiency Upto 84% // *IEEE Transactions on Microwave Theory and Techniques*. 2015. Vol. 63, Is. 5. P. 1768–1778.
60. Song C., Huang Y., Carter P. et al. A Novel Six-band Dual CP Rectenna Using Improved Impedance Matching Technique for Ambient RF Energy Harvesting // *IEEE Transactions on Antennas and Propagation*. 2016. Vol. 64, Is. 7. P. 3160–3171.
61. Karakaya E., Bagci F., Yilmaz A., Akaoglu B. Metamaterial-Based Four-Band Electromagnetic Energy Harvesting at Commonly Used GSM and Wi-Fi Frequencies // *Journal of Electronic Materials*. 2019. Vol. 48. P. 2307–2316.

62. Benayad A., Tellache M. A Compact Energy Harvesting Multiband Rectenna Based on Metamaterial Complementary Split Ring Resonator Antenna and Modified Hybrid Junction Ring Rectifier // International Journal of RF and Microwave Computer-Aided Engineering. 2019. Vol. 30, Is. 2. P. 1–11.
63. Wang M., Fan Y., Yang L. et al. Compact Dual-Band Rectenna for RF Energy Harvest Based on a Tree-Like Antenna // IET Microwaves, Antennas & Propag., 2019. Vol. 13, Is. 9. P. 1350–1357.
64. Shrestha S., Lee S.R., Choi D.-Y. A New Fractal-Based Miniaturized Dual Band Patch Antenna for Ration Energy Harvesting // International Journal of Antennas and Propagation. 2014. Vol. 8. P. 1–9.
65. Badamchi Z., Trinh N.D., Bois C., Djera T. Printed Fractal Folded Coplanar-Strips-Fed Array Rectenna for IoE Applications // Progress In Electromagnetics Research. 2022. Vol. 125. P. 161–177.
66. Estrada J.A., Kwiatkowski E., López-Yela A. et al. RF-Harvesting Tightly Coupled Rectenna Array Tee-Shirt With Greater Than Octave Bandwidth // IEEE Transactions on Microwave Theory and Techniques. 2020. Vol. 68, Is. 9. P. 3908–3919.
67. Khalid F., Saeed W., Shoaib N. et al. Quad-Band 3D Rectenna Array for Ambient RF Energy Harvesting // International Journal of Antennas and Propagation. 2020. Vol. 2020. P. 1–23.
68. Bui D.H.N., Vuong T.-P., Verdier J., Allard B., Benech P. Design and Measurement of 3D Flexible Antenna Diversity for Ambient RF Energy Scavenging in Indoor Scenarios // IEEE Access. 2019. Vol. 7. P. 17033–17044.
69. Song C., Huang Y., Zhou J. et al. Matching Network Elimination in Broadband Rectennas for High-Efficiency Wireless Power Transfer and Energy Harvesting // IEEE Transactions on Industrial Electronics. 2017. Vol. 64, Is. 5. P. 3950–3961.
70. He Z., Lin H., Liu C. Codesign of a Schottky Diode's and Loop Antenna's Impedances for Dual-Band Wireless Power Transmission // IEEE Antennas and Wireless Propagation Letters. 2020. Vol. 19, No. 10. P. 1813–1816.
71. Kuhn V., Lahuec C., Seguin F., Person C. A Multi-Band Stacked RF Energy Harvester With RF-to-DC Efficiency Upto 84 % // IEEE Transactions on Microwave Theory and Techniques. 2015. Vol. 63, Is. 5, P. 1768–1778.
72. Ma Z.K., Vandenbosch G.A.E. Wideband Harmonic Rejection Filter for Wireless Power Transfer // IEEE Transactions on Antennas Propagation. 2013. Vol. 62, No. 1. P. 371–377.
73. Chou J.-H., Lin D.-B., Weng K.-L., Li H.-J. All Polarization Receiving Rectenna With Harmonic Rejection Property for Wireless Power Transmission // IEEE Transactions on Antennas and Propagation. 2014. Vol. 62, No. 10. P. 5242–5249.
74. Dong Y., Gao S., Luo Q. et al. Broadband Circularly Polarized Filtering Antennas // IEEE Access. 2018. Vol. 6. P. 76302–76312.
75. Finkenzeller K. RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification. New York : Wiley, 2003.
76. Yao Y., Wu J., Shi Y., Dai F. A Fully Integrated 900-MHz Passive RFID Transponder Front End With Novel Zero-Threshold RF-DC Rectifier // IEEE Transaction on Industrial Electronics. 2009. Vol. 56, No. 7. P. 2317–2325.
77. Wang W., Wong H., Han Y. A High-Efficiency Full-Wave CMOS Rectifying Charge Pump for RF Energy Harvesting Applications // Microelectronics Journal. 2015. Vol. 46, Is. 12, Part B. P. 1447–1452.
78. Valenta C.R., Durgin G.D. Harvesting Wireless Power: Survey of Energy-Harvester Conversion Efficiency in Far-Field, Wireless Power Transfer Systems // IEEE Microwave Magazine. 2014. Vol. 15, Is. 4. P. 108–120.

Надійшла до редколегії 07.10.2023

Відомості про авторів:

Алексєєв Василь Олександрович – аспірант кафедри комп'ютерної радіоінженерії та систем технічного захисту інформації, Харківський національний університет радіоелектроніки, Україна, e-mail: vasyl.aliexsieiev@nure.ua, ORCID: <https://orcid.org/0000-0002-3282-5985>.

Грецьких Дмитро Вячеславович – д-р техн. наук, доцент, професор кафедри комп'ютерної радіоінженерії та систем технічного захисту інформації, Харківський національний університет радіоелектроніки, Україна, e-mail: dmytro.gretskih@nure.ua, ORCID: <https://orcid.org/0000-0002-2645-7872>.

Гавва Дмитро Сергійович – канд. техн. наук, доцент, доцент кафедри комп'ютерної радіоінженерії та систем технічного захисту інформації, Харківський національний університет радіоелектроніки, Україна, e-mail: dmytro.gavva@nure.ua, ORCID: <https://orcid.org/0000-0002-4033-7746>.

Лихограй Василь Григорович – канд. фіз.-мат. наук, доцент, доцент кафедри комп'ютерної радіоінженерії та систем технічного захисту інформації, Харківський національний університет радіоелектроніки, Україна, e-mail: vasyl.lykhograi@nure.ua, ORCID: <https://orcid.org/0000-0002-9226-1309>.

Хань Іван Анатолійович – студент кафедри комп'ютерної радіоінженерії та систем технічного захисту інформації, Харківський національний університет радіоелектроніки, Україна, e-mail: ivan.khan@nure.ua ORCID: <https://orcid.org/0009-0002-7866-8871>.

APPLICATION OF RADIO ENGINEERING METHODS ЗАСТОСУВАННЯ МЕТОДІВ РАДІОТЕХНІКИ

УДК 621.865.8 (045)

DOI:10.30837/rt.2023.4.215.10

О.Й. ДОВНАР, канд. техн. наук, В.І. ЧЕРКІС, О.М. ЗІНЧЕНКО, О.О. КАДАНЕР

ОДИН СПОСІБ ПІДВИЩЕННЯ ЯКОСТІ МЕДИЧНОГО МАНІПУЛЯТОРУ ДЛЯ СТЕРИЛЬНИХ БОКСІВ

Вступ

У 1985 р. була проведена операція 52-річному чоловіку, де пацієнт був зафіксований у комп'ютерному томографі. Складність операції була у незручності втручання та необхідності точного позиціонування голки, котру мали ввести у мозок. Маніпулятором виступила модель від General Motors – PUMA 200, операція завершилась успішно, хоча наведена модель не позиціонувала себе як медичне обладнання. Це було перше хірургічне втручання маніпулятора, і такий успіх відкривав нові можливості. Тому вже через рік був розроблений ROBODOC. Таким чином, з'явилися роботи-хірурги, а з ними – нові можливості і новий рівень операцій. І на сьогодні розроблені механізми настільки підвищують та спрощують якість таких втручань, що деякі операції без них неможливі, або достатньо ризиковані.

Проблема забезпечення стерильності в медицині є досить актуальною, оскільки наявність інфекційних агентів у медичних установах може призвести до розвитку небажаних побічних ефектів у пацієнтів, ускладнень у процесі лікування та збільшення витрат на медичну допомогу. Зокрема, використання медичних маніпуляторів для роботи зі стерильними боксами може допомогти вирішити проблему забезпечення стерильності.

Актуальність дослідження полягає у розробці медичного маніпулятора, який допоможе ефективно та безпечно працювати зі стерильними боксами, забезпечуючи дотримання вимог стерильності.

Подібні системи уже наявні, наприклад [1 – 4], але їх використання чітко визначене виробником і має не весь необхідний персоналу функціонал, або у певних моментах може бути незручним у користуванні. Окрім того саме застосування керованих маніпуляторів у стерильному боксі має зараз найбільшу перспективу у клітинній інженерії та створенні штучних органів. Орієнтуватися необхідно на варіант, котрий буде відповідати максимальній кількості вимог як для хірургічного втручання, так і для автоматизованих процесів усередині стерильних боксів. Тому розробка має відповідати наступним критеріям: невеликі розміри; зручність застосування; можливість автоматизувати певні процеси; можливість віддаленого доступу; модульність, простота заміни компонентів; гнучкість, простота налаштування.

Вибір прототипу

Досягнення у галузі застосування роботів значно просувають як усю медицину, так і технології оперування. Розглянемо найвідоміші роботи-хірурги.

Роботизований комплекс Da Vinci [1] – це передова технологія в галузі хірургії. Це робот, яким керує хірург, він підвищує можливості лікаря, «поліпшує» його зір і точність рухів. При використанні такої системи хірург проводить операцію, сидячи за пультом. Він бачить об'ємне 3D зображення у десятикратному збільшенні та управляє роботом за допомогою маніпуляторів, що передають інструменту мінімальні рухи пальців хірурга.

Робочих «кінцівок» у робота цілих чотири, і всі вони мають рухливість майже на 360°. Роботична хірургія – це сім площин руху хірургічного інструмента, що дозволяє хірургу з максимальною точністю зберігати нервові волокна та кровоносні судини. У чоловіків це дозволяє зберегти еректильну функцію та утримання сечі; у жінок – зберегти нормальні функції тазових органів, чутливість, секреторну функцію залоз піхви. При операціях на кишківнику дозволяє зберегти функції зовнішнього та внутрішнього сфінктеру прямої кишки.



Рис. 1. Комплекс Da Vinci

ROBODOC – унікальна комп'ютеризована система-робот для проведення операцій на суглобі [2].

Під час операції з встановлення імплантатів потрібна дуже висока точність, а при протезуванні штучним суглобом руками хірурга через "людський фактор" значно знижується точність проведення операції, виникають помилки, які можуть викликати ускладнення на суглобі. Використання ROBODOC зводить до нуля помилки, викликані "людським фактором", операція від початку до її закінчення прораховується комп'ютером з високою точністю, що допомагає мінімізувати болючі відчуття під час і після операції.



Рис. 2. Система ROBODOC

SMR Surgical Versius. Ця система [3] призначена для загальних хірургічних операцій, торакальних, гінекологічних та колоректальних процедур, а також для втручань на верхніх відділах шлунково-кишкового тракту. Рішення успішно застосовується в лікарні Galaxy Care в Пуні (Індія) при різних хірургічних операціях, що включають трансторакальні процедури, гістеректомію та міомектомію.

Оскільки система Versius є модульною, її можна легко та швидко переміщати між операційними залами, що розширює можливості використання та рентабельність платформи. Очікується, що робот-хірург скоротить тривалість хірургічного втручання та одночасно покращить результати лікування. І на сьогодні це найменший робот-хірург.



Рис. 3. Модульна система Versius

Проаналізуємо ці системи за наведеними вище критеріями.

1. Розміри. Тут виділяється Versius, оскільки має найменші розміри маніпуляторів і при цьому у функціональності не поступається Da Vinci. Роботизована система маніпулятора може займати небагато місця і не потребує дуже тонких налаштувань (вони можуть бути скориговані оператором під час операції).

2. Зручність застосування. Серед усіх можливих варіантів краще ніж Da Vinci поки що жодна система себе не показала. Зручність консолі хірурга дозволяє йому проводити найскладніші операції у набагато більшому комфорті, ніж звичайне втручання, що підвищує ефективність хірурга та швидкість відновлення пацієнта після операції

3. Можливість автоматизувати певні процеси. Оскільки ROBODOC знаходиться на ринку довше всіх, їй вдалося автоматизувати велику кількість процесів та створити інтуїтивний інтерфейс між комп'ютером та системою, що дозволяє завантажувати нові параметри та вносити їх до вже готового автоматизованого процесу.

4. Можливість віддаленого доступу. Da Vinci подолав цей бар'єр з великою перевагою, коли дозволив не просто віддалено керувати роботом-хірургом, але й віддалено асистувати хірургу, що відкриває нові можливості для навчання та дозволить передавати досвід молодим фахівцям.

5. Модульність, простота заміни компонентів. Тут найкращою виступає модульна система Versius. Це є однією з найбільших переваг як економічно, так і в плані ремонту та підтримки таких систем, відкриває новий рівень операцій для клінік середнього розміру.

6. Гнучкість, простота налаштування. Систему ROBODOC можливо відкалібрувати автоматизовано, що спрощує її подальше налаштування, але гнучкістю ця система не володіє. Натомість нова модульна система Versius пропонує цікаві рішення та може бути досить швидко налаштована під конкретну особу.

Одним з напрямків є створення альтернативи для сумісних маніпуляторів, бо зазвичай вони або надто дорогі, або не мають необхідних можливостей. У [4, 5] наведено повністю реалізовану парадигму недорогого маніпулятора з квазіпрямим приводом (Quasi-Direct Drive (QDD)) і показано технічні рішення при проектуванні цієї системи. Нас цікавить кожен сегмент.

На рис. 4 відображено, як два протилежно влаштовані мотори керують кінцевою передачею, що забезпечує не лише зміщення, але й обертальні рухи.

Застосування подібної схеми дозволяє збільшити кількість ступенів свободи, що для медичного маніпулятора є вкрай важливим, проте при такій конфігурації розміри будуть наближатись до категорії промислових роботів. Так, наприклад, у Blue розмір одного сегменту 110x110x220 мм, що робить його занадто великим для високоточних міні-маніпуляцій. Тож можемо зробити висновок – основним нюансом при створенні невеликого за розмірами маніпулятора є кількість та розміри компонентів.

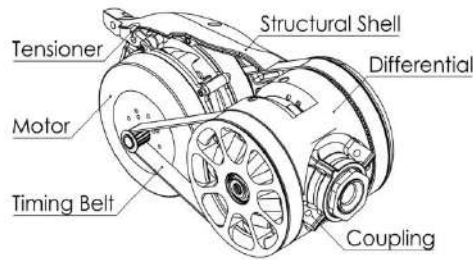


Рис. 4. Сегмент маніпулятора руки робота Blue



Рис. 5. Конічна передача

У більшості маніпуляторів застосовано крокові двигуни безпосередньо у конструкції руки, а їх розміри не можуть бути зменшені, окрім того, сам механізм може не передбачати такої можливості. Подолати обмеження розмірів маніпулятора – це непроста задача, зазвичай у таких випадках поступаються у потужності двигунів або змінюють конструкцію сегменту таким чином, щоб вдалося вмістити всі необхідні компоненти. У промислових роботів для різних складальних робіт такі складнощі зазвичай не виникають, але для невеликих маніпуляторів подібні технічні рішення досить обмежені, а для малих конструкція напряму залежить від мінімального можливого крокового двигуна, що відповідає потребам. Рішення, які застосовують у таких випадках, – винесення окремо механізму від керованого елемента (рис. 6). Таким чином, розмір конструкції маніпулятора можна значно скоротити, а також зробити складання та ремонт маніпулятора значно простішим та дешевшим.

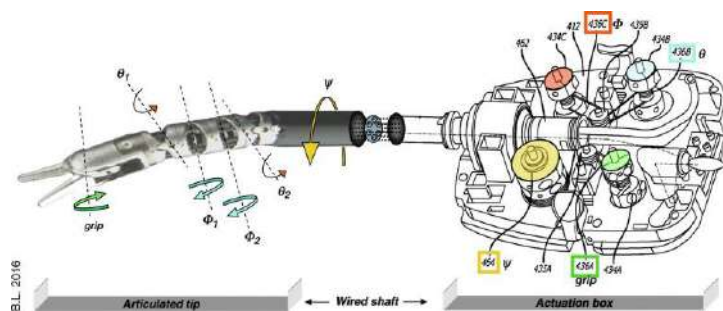


Рис. 6. Розділення маніпулятора на дві частини – маніпуляційна частина та тяговий механізм

Тяговий механізм розташований в окремому блоці. Подібна реалізація зустрічається у великій кількості маніпуляторів, наприклад шупи хірургічного робота Da Vinci. Це дозволяє максимально зменшити розміри маніпулюючих сегментів і все зайве винести окремо та проводити оперативні втручання у розрізі менше 2 см.

На рис. 7 показана схема, за якою працює велика кількість медичних маніпуляторів. Вдосконалення робота Da Vinci тривало 24 роки перед випуском на ринок і продовжується й досі, але є кілька недоліків, викликаних саме такою конструкцією, – це низька точність та невисока зносостійкість тросів. Окрім того така конструкція унеможливує процес автоматизації через постійну похибку. За даними [6, 7] приводиться похибка у сантиметр після декількох рухів, тому подібний механізм ідеальний для втручання з оператором, але неможливий у автоматизації.

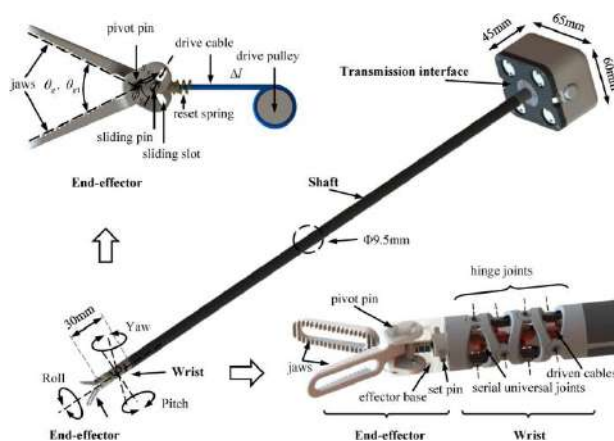


Рис. 7. Видовжений хірургічний щуп з тяговим механізмом

Невисока зносостійкість тросів змушує проводити заміну кожного щупа після десяти хірургічних втручань, що робить підтримку робочого стану маніпулятора досить коштовним. При недотриманні таких умов Da Vinci просто заблокує консольні команди і не буде слухати оператора.

Технічні рішення

Дослідження можливих варіантів передачі руху на сегменти маніпулюючої частини дозволило знайти наступну технологію. Її принципова відмінність – у невикористанні тяги на тросах, а передача руху через конічні шестерні. Тобто конструкція передбачає конічний центр з двигунами у самій основі маніпулятора, котрі передають рух сегментам (рис. 8).



Рис. 8. Конічний центр з двигунами

Над конічним центром розташовується конічний суглоб маніпулятора, де кожна шестерня матиме обертальний рух від окремого двигуна. Це дозволить максимально спростити обслуговування електронної та моторної частин. Загальний принцип роботи конічного суглобу показано на рис. 9.

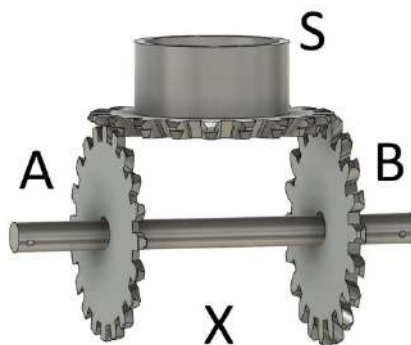


Рис. 9. Конічний суглоб

Розглядаючи даний приклад, можна побачити таку залежність.

Якщо шестерні А та В рухаються за годинниковою стрілкою відносно осі (тобто А до нас, а В від нас), то ми отримаємо обертальний рух шестерні S у праву сторону.

Якщо шестерні А та В рухаються проти годинникової стрілки відносно осі, то ми отримаємо обертальний рух у ліву сторону.

Якщо шестерні А та В будуть обертатися до нас, то ми отримаємо зміщення шестерні S відносно осі у нашу сторону прямо пропорційно оберту шестерень А та В.

Якщо шестерні А та В будуть обертатися від нас, то ми отримаємо зміщення шестерні S відносно осі від нас прямо пропорційно до оберту шестерень А та В.

Якщо шестерні А та В матимуть різну швидкість оберту, ми отримаємо зміщення та обертання прямо пропорційне коефіцієнту різностей швидкостей, чим більша різниця тим більше коефіцієнт обертання і менше коефіцієнт зміщення, і навпаки.

Для досягнення такого ефекту зі сторони X потрібно встановити відповідно дві шестерні окремо для А та В і тоді можливо буде керування у зазначених вище параметрах. Якщо брати до уваги, що це один з декількох сегментів і нам потрібно крізь нього передати оберт на наступні сполучення сегментів, то постає питання, як саме це можливо зробити. Для цього нам знадобляться внутрішня конусна передача, тобто для проведення маніпуляцій ми будемо застосовувати вісь Z та передавати обертання так само і для усіх наступних сполучень. Тобто кількість шестерень у сполученні з передачею оберту для кінцевої частини буде відповідати закономірності:

$$X = 2C + 1.$$

А без передачі оберту кінцевій частині відповідно

$$X = 2C.$$

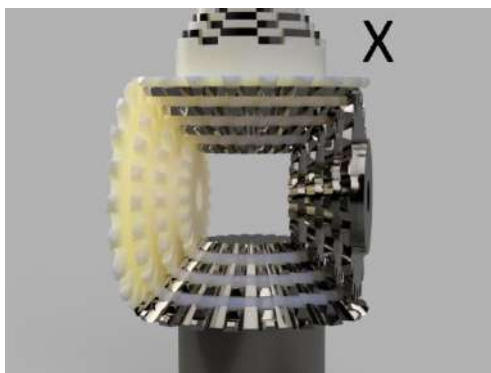


Рис. 10. Цільний кіничний суглоб

Наприклад, якщо розглядати даний механізм передачі, можна порахувати, що кількість передаючих шестерень X (а саме – вісім) матиме відповідно чотири сполучення, отже над цією частиною знаходяться чотири сегменти керування, до яких і передається у даному сполученні, або три сполучення, і на кінцевіку встановлений керований щуп. Застосовуючи подібний механізм, можна без втрат точності та потужності значно зменшити маніпулятори, а також винести електроніку та механізм керування поза маніпулятор. Це підвищить точність і, оскільки вага двигунів буде винесена, додасть потужності. При цьому налагодження, ремонт та будь-яке інше втручання буде значно простішим ніж у більшості інших маніпуляторів. Зносостійкість модульних сегментів та сполучень залежить лише від матеріалів та кількості сполучень. Через те, що сегменти та деталі сполучень можна цілком друкувати на 3D-принтері, питання зносостійкості розглядається не як для маніпулятора у цілому, а як для модульної частини маніпулятора.

Що стосується електронної складової, то для абсолютно різних моделей з різною кількістю сегментів можна застосовувати плати NodeMcu v3. Цей вибір обумовлений невеликими розмірами, чудовими характеристиками мікроконтролера та достатнім об'ємом пам'яті і

вбудованою Esp8266. Від кожної плати можна розвести керування на п'ять крокових двигунів. Загальний порядок такий: головна плата отримує сигнал або напрям з комп'ютеру, або через wifi-мережу і передає його усім дочірнім. Кожна плата має свої номери двигунів, і тому розповсюдження усіх сигналів жодним чином не впливає на інші: якщо у плати є відповідний номер двигуна – рух відбудеться, а в іншому випадку просто буде проігнорований. Це дозволяє забезпечити необхідну модульність, тобто у будь-який момент можна буде додати кілька сегментів та ще одну плату керування до існуючого маніпулятора. Окрім того можливо підключити необмежену кількість маніпуляторів послідовно і керувати ними з одного комп'ютера.

Перевірка технічних рішень

Прототип, розроблений за даною технологією, показав повну відповідність виставленим вимогам. У перспективі робот матиме вигляд кварто-маніпулятора (чотири руки), що дозволить проводити хірургічні втручання (кількість обумовлена потребами операційного втручання). Зазвичай хірург використовує декілька інструментів одразу, одні необхідні для маніпуляцій, інші – для фіксації. Це дозволяє асистувати хірургу, тобто першими двома маніпуляторами керує сам хірург, а асистент – двома іншими.

Що стосується розмірів такого робота, то розміри прототипу складають 324x324x620 мм, але можуть бути зменшені чи збільшені в залежності від потреб. До того ж ця характеристика цілком залежить від кількості сегментів. Так, наприклад, 620 мм висоти – це три сегменти (що забезпечує сім ступенів свободи), кожен з сегментів має довжину 180 мм плюс конічний центр передачі висотою 80 мм. Це значно менше ніж у будь-якого існуючого на разі робота-хірурга. На виробництві розміри та кількість сегментів можна варіювати у значних проміжках.

З таким підходом механізм стане універсальним та незамінним у областях з невеликими за розмірами маніпуляторами. До того ж, виробництво може бути значно дешевшим за інші. Вартість прототипу одного маніпулятора складає близько 200 \$, якщо замінити пластик на метал, то ціна виросте до 1000 \$, відповідно загальна вартість робота-хірурга складатиме 800 – 4000 \$, що значно дешевше за всі аналоги.

Подібне обладнання може бути застосоване у місцях, де потрібно забезпечити високу планку оперативного втручання та надійну медичну допомогу від найкваліфікованіших осіб, зокрема у зонах бойових дій. Питання віддаленого доступу для хірургів не стоїть так гостро, як 20 років тому. Наразі у більшості українських батальйонів наявні станції starlink з швидкісним інтернетом, саме тому подібна революція серед медичних маніпуляторів відбувається сьогодні.

Для медичних боксів маніпулятор має володіти додатковими функціоналом для автоматизації. Тому блок конічного центру передачі додатково оснащується міні-комп'ютером для обчислень та програмування нових дій, що додає у вартості 200 \$, тобто загальна вартість маніпулятора складатиме від 400 до 1200 \$ за штуку (три сегменти). І при цьому це модульне устаткування, тому вартість ремонту значно нижча (30 – 90 \$ за заміну сегмента).

Висновки

У роботі представлений спосіб підвищення якості маніпулятора для стерильних боксів. У розробленому прототипі вдосконаленню підлягали дві основні характеристики: розмір та точність маніпулювання. Винесення всіх електронних компонент та двигунів поза сегменти маніпулятора дозволило без зменшення кількості двигунів, тобто без втрати потужності, зменшити розміри конструкції. Підвищення точності було досягнуто за рахунок використання у механізмі крокових двигунів.

Розглянуті технічні рішення дозволять автоматизувати роботу у стерильних боксах, забезпечивши максимальну надійність та захист від потрапляння зовнішніх факторів. Запропонована схема матиме значні переваги завдяки своїй модульності, розмірам, вартості виробництва та можливості автоматизації.

Список літератури:

1. Da Vinci (робот-хірург). <https://biokurs.com.ua/ua/news-biokurs-view/161/>
2. Система вирівнювання поверхні бедра ROBODOC. <https://www.medicaexpo.ru/prod/kaiser-precision-co/product-102760-868119.html>
3. Ibrahim Alkatout, Hamid Salehiniya, Leila Allahqoli. Assessment of the Versius Robotic Surgical System in Minimal Access Surgery: A Systematic Review. <https://www.medicaexpo.ru/prod/kaiser-precision-co/product-102760-868119.html>
4. Project Blue. <https://rl.berkeley.edu/blue/>
5. Karl Khandalavala, Tim Shimon, Laura Flores, Priscila Rodrigues Armijo, Dmitry Oleynikov. Emerging surgical robotic technology: a progression toward microbots. <https://ales.amegroups.com/article/view/5499/html>
6. Хірургічні операції роботом DaVinci. <https://uamt.com.ua/RU/robot-da-vinchi.html>
7. Innomed oncology. <https://davinci.innomed.ua>

Надійшла до редколегії 27.11.2023

Відомості про авторів:

Довнар Олександр Йосипович – канд. техн. наук, доц., Національний аерокосмічний університет ім. М.Є Жуковського «Харківський авіаційний інститут», доц. кафедри радіоелектронних та медичних комп'ютеризованих засобів та технологій; Україна; email: a.dovnar@khai.edu; ORCID: <https://orcid.org/0000-0001-7171-0024>

Черкіс Владислав Ігорович – студент, Національний аерокосмічний університет ім. М.Є Жуковського «Харківський авіаційний інститут»; Україна; email: v.i.cherkis@student.khai.edu

Зінченко Олександр Миколайович – аспірант, Національний аерокосмічний університет ім. М.Є Жуковського «Харківський авіаційний інститут», асистент кафедри радіоелектронних та медичних комп'ютеризованих засобів та технологій; Україна; email: a.zinchenko@khai.edu; ORCID: <https://orcid.org/0000-0001-5651-8931>

Каданер Олександр Олександрович – асистент кафедри радіоелектронних та медичних комп'ютеризованих засобів та технологій; Національний аерокосмічний університет ім. М.Є Жуковського «Харківський авіаційний інститут»; Україна; email: o.kadanner@khai.edu

**INFORMATION METHODS OF RADIO ENGINEERING,
SIGNAL PROCESSING**
ІНФОРМАЦІЙНІ МЕТОДИ РАДІОТЕХНІКИ, ОБРОБКА СИГНАЛІВ

УДК 615.472.03

DOI:10.30837/rt.2023.4.215.11

*В.І. ЛЕОНІДОВ, канд. техн. наук, В.В. СЕМЕНЕЦЬ, д-р техн. наук,
О.В. ГРИГОР'ЄВ, канд. техн. наук*

**АНАЛІЗ ЧАСТОТНО-ЧАСОВОЇ СТРУКТУРИ АКУСТИЧНИХ ШУМІВ
БЕЗПЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ В СЕРЕДОВИЩІ STM32 CubeIDE**

Вступ

Область застосування сучасних безпілотних літальних апаратів (БПЛА) безперервно розширюється. Дослідження акустичного шуму, створюваного БПЛА, почалося практично одночасно з їх створенням. Стимулом до проведення цих досліджень служить область практичного застосування БПЛА [1 – 3].

Шум БПЛА вивчають при їх використанні в біології для спостереження за поведінкою тварин і комах у різних ситуаціях, так як при цьому шум дронів може впливати на досліджувані види фауни [4, 5]. Схожі явища виникають при використанні дронів у сільському господарстві та в проблемах екології [6, 7].

Крім того, БПЛА можуть використовуватися для несанкціонованого моніторингу різних об'єктів [8, 9]. У зв'язку з цим виникає також завдання розробки правил своєчасного виявлення БПЛА.

Використання відомих методів виявлення повітряних цілей для виявлення БПЛА має ряд особливостей.

Для радіолокаційних засобів виявлення, що працюють у сантиметровому та міліметровому діапазонах електромагнітних хвиль, БПЛА є малопомітними цілями, тому що для їх виготовлення, як правило, використовуються радіопрозорі матеріали і, отже, ці об'єкти мають малу ефективну поверхню розсіювання (ЕПР).

Виявлення БПЛА у діапазоні видимого світла за допомогою відеокамер обмежено денним часом доби або потребує додаткового підсвічування за допомогою прожекторів. Цей метод може бути використаний й у умовах виникнення туману.

У більшості випадків БПЛА є дуже слабкими джерелами інфрачервоного випромінювання, тому їх виявлення за допомогою засобів пасивної локації в інфрачервоному діапазоні електромагнітних хвиль також малоперспективне.

Виявлення цих об'єктів за сигналами їх зв'язку з командним пунктом може бути можливим тільки в тому випадку, якщо в системі не використовується повністю автономний режим виконання польотного завдання з одноразовим режимом передачі отриманих даних в кінці польоту.

Одним із напрямків вирішення завдання виявлення БПЛА може бути реєстрація акустичного сигналу (шуму), створюваного їх силовими установками. Однак при використанні цього методу слід враховувати низку особливостей.

Зовнішні по відношенню до БПЛА акустичні поля, які створюються турбулентністю атмосфери і різними технічними засобами, відносяться до нестаціонарних випадкових процесів і за потужністю можуть значно перевищувати потужність акустичного сигналу, що генерується БПЛА. У цьому часова амплітудно-частотна структура сигналів БПЛА не є заданою априорі (на відміну від радіолокації).

Виявлення акустичних сигналів БПЛА має здійснюватися в безперервному режимі методом пасивної акустичної локації. У цьому випадку завдання виявлення нестаціонарного

випадкового процесу, до яких відноситься сигнал БПЛА, на тлі нестационарного фонового шуму, стає в загальному випадку невизначеним.

У зв'язку з наведеними особливостями для вирішення задачі виявлення БПЛА необхідно враховувати два положення:

- енергетичне виявлення цілі можливе лише за наявності інформація про потужності фонового шуму в реальному часі;
- звести задачу виявлення цілі до виявлення відомого сигналу можливо лише за відомої часової амплітудно-частотної структури акустичного сигналу БПЛА.

У даному разі поняття «фоновий шум» означає композицію будь-яких джерел акустичних сигналів крім шуму дронів. У загальному випадку фоновий шум є процесом нестационарним, тому використання апріорних даних про рівень фонового шуму, отриманих при гарантованій відсутності шуму БПЛА, для вирішення завдання виявлення в реальному часі призводить до невизначеності, оскільки розрахований за апріорними даними пороговий рівень сигналу може бути перевищений будь-яким випадковим джерелом, що включилося в даний момент.

Отже, у разі рішення завдання виявлення сигналів БПЛА зводиться до розв'язання задачі розпізнавання сигналів.

Мета роботи – виявлення інформативних ознак тимчасової амплітудно-частотної структури сигналів БПЛА (дронів) за допомогою середовища STM32CubeIDE, які характеризуються стійкою повторюваністю від досліду до досліду, і, отже, можуть бути використані для надійного розпізнавання об'єктів БПЛА.

Основні положення

Вочевидь, що при пілотуванні дрона діапазон девіації частоти кожної групи двигун–пропелер є близькі за значенням величини, різниця між якими при необмеженому збільшенні часу спостереження прагне до нуля. Однак у межах кожного малого фіксованого інтервалу часу різниця частот цих сигналів є випадкова величина, яка залежить від заданого режиму руху і турбулентного процесу в атмосфері.

Отже, модель акустичного сигналу дрону можна представити як суперпозицію кількох (за кількістю двигунів і повітряних гвинтів) частотних складових – гармонік, кожна з яких модульована за частотою сигналом управління, що забезпечує підтримку заданого режиму руху в умовах випадкових (турбулентних) атмосферних збурень, що впливають на дрон.

Можна припустити існування ще однієї складової акустичного сигналу дрону. Це комбінаційні частоти, що виникають в результаті нелінійних процесів розповсюдження вібрацій уздовж конструкції дрону, які порушуються системою двигун–пропелер. Інтенсивність цієї складової визначається резонансними властивостями конструкції БПЛА, а частота – сумою та різницею частот, що генеруються встановленими системами двигун–пропелер.

У роботах [10 – 12] розглянуто один з можливих підходів до аналізу комбінаційних сигналів, при якому використовується аналіз залежностей зміни періодів, тобто аналіз на малих інтервалах часу, при яких тривалість періоду гармонік не встигає істотно змінитися. У цьому випадку сигнал, який аналізується, можна представити як адитивну суміш низки дискретних гармонік.

Розподіл за тривалістю періоду характеризує діапазон зміни режимів роботи пристрою загалом і, отже, дає «портрети», індивідуальні для кожного з джерел шуму.

Отже, для виявлення інформативних ознак акустичних сигналів дрону доцільно зіставити акустичний сигнал дрону і фоновий акустичний шум, що існує в середовищі мегаполісу.

Проведені експериментальні дослідження дають необхідні вихідні дані для розробки вимірювального пристрою та алгоритму його функціонування.

У відповідність до розробленого алгоритму програмна частина пристрою працює у режимі моніторингу. Після старту програми відбувається ініціалізація портів вводу-виводу інформації, підключення стандартних бібліотек, які забезпечують роботу ЖК індикатору та інтерфейсу USB [13 – 18]. Аналогові входи мікроконтролера підключені до схеми виміру. Аналогові сигнали перетворюються в цифрові за допомогою АЦП. Значення змінних виводяться на ЖК індикатор і відправляються або в комп'ютер, або флешку для обробки і прий-

няття рішення. В процесі роботи буде задіяно інтерфейс SPI1. Включимо SPI1 в режим Full-Duplex Master (рис. 1).

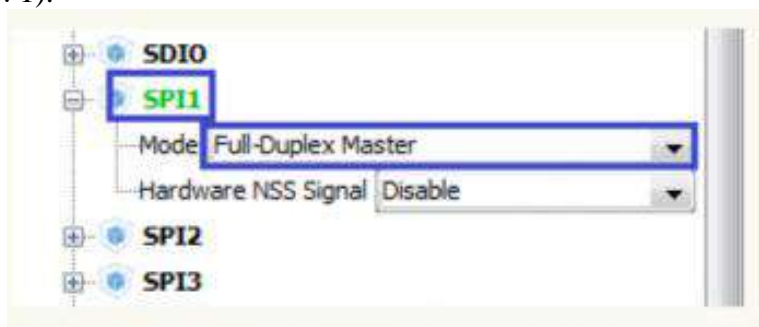


Рис.1. Підключення SPI1

Ніжки мікроконтролера для інтерфейсу SPI залишимо за замовчуванням (рис. 2).

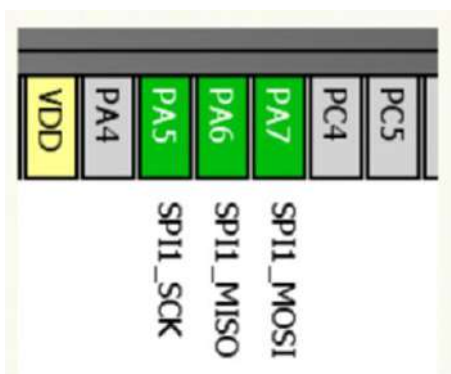


Рис. 2. Контакти мікроконтролера для SPI

Включимо ще три ніжки. Одну – для вибору чіпа (CS), інші дві – для виявлення переривань (рис. 3). Можливо, останні нам не знадобляться, але для порядку включимо, щоб помилково їх не задіяти згодом на щось ще.

Також увімкнемо на вихід ніжки портів для керування різнокольоровими світлодіодами на платі (рис. 4).

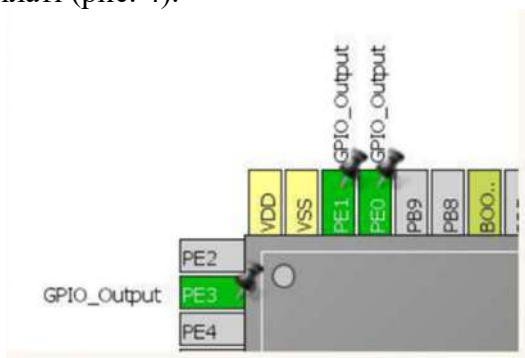


Рис. 3. Контакти мікроконтролера для чіпа

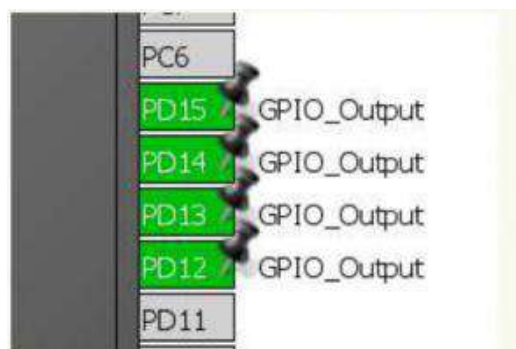


Рис. 4. Контакти мікроконтролера для керування різнокольоровими світлодіодами на платі

Розроблено наступні функції для обробки даних:

`void Zvyk_Ini(void)` – функція ініціалізації;

`void Zvyk_ReadAcc(void)` – функція читання даних;

`static void Error (void)` – функція обробки помилок;

`uint8_t Zvyk IO_Read(uint16_t DeviceAddr, uint8_t RegisterAddr)` – функція читання даних з регістрів сенсора;

`void Zvyk _IO_Write(uint16_t DeviceAddr, uint8_t RegisterAddr, uint8_t Value)` – функція запису даних в регістри сенсора;

`uint8_t Zvyk _ReadID(void)` – функція читання ID адреси;

`void Zvyk _AccFilterConfig(uint8_t FilterStruct)` – функція фільтрації даних ;

`void Zvyk Init(uint16_t InitStruct)` – функція ініціалізації інтерфейсу;

`void Zvyk _GetXYZ(int16_t* pData)` – функція обробки вихідних даних.

Сучасні мікроконтролери мають високу частоту ядра, що формується із значно меншої частоти опорного генератора шляхом множення опорної частоти на фіксований коефіцієнт. У мікроконтролері STM32F407VG максимальна частота ядра до 168 МГц. У якості опорного генератора може бути використаний зовнішній кварцовий резонатор HSE або вбудований RC – HIS. Функціональна організація системи тактування STM32F407VG наведена на рис. 5.

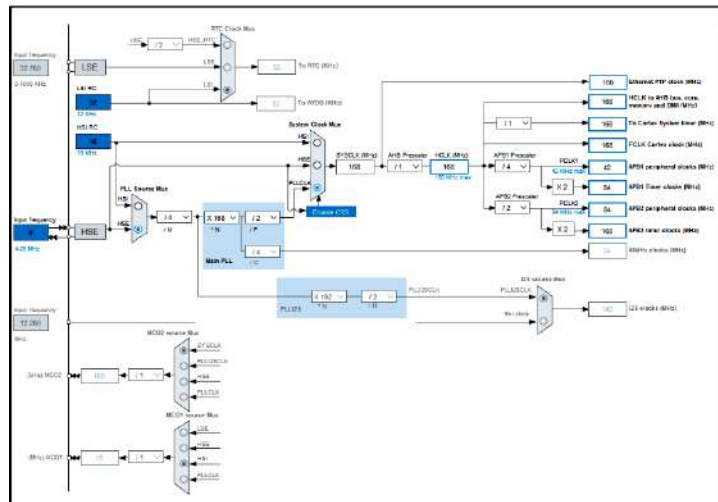


Рис. 5. Система тактування мікроконтролера STM32F407VG

Зовнішній кварцовий резонатор HSE може мати частоту від 4 до 26 МГц. Він має високу стабільність. Його відносна нестабільність частоти $2 \cdot 10^{-6}$, що при стандартному значенні частоти кварцового резонатора 8 МГц складає ± 16 Гц. Внутрішній HIS генератор має частоту 16 МГц та дуже низьку стабільність. Його частота може змінюватись в межах від -2 % до +2,5% в температурному діапазоні від -40 до +85°C. В більшості інтерфейсів передавання даних (USB, USART й т.і.) це призводить до виникнення помилок при передаванні інформації, що є недопустимим. Також виникають помилки при рахуванні часу за допомогою таймерів. Тому, практично в усіх електронних пристроях використовуються зовнішні кварцові резонатори.

Для підключення у середовищі STM32CubeIDE зовнішнього кварцового резонатора відкриваємо на вкладці Pinout&Configuration в розділі System Core підрозділ RCC та обираємо High Speed Clock (HSE) → Crystal/Ceramic Resonator (рис. 6).

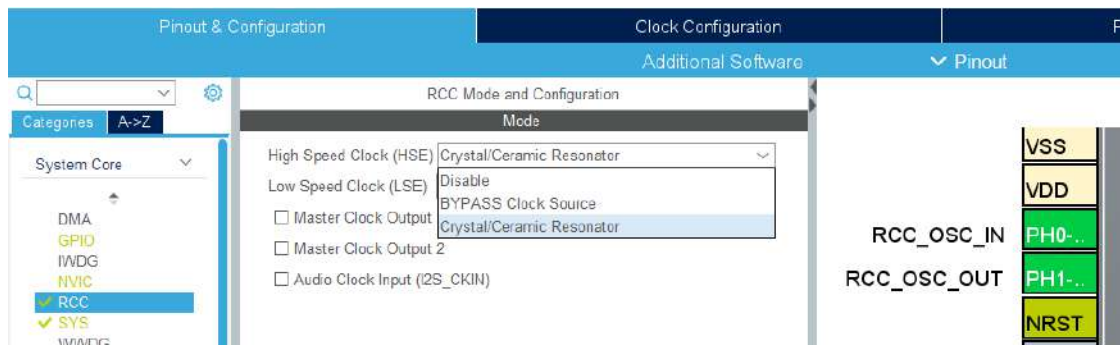


Рис. 6. Налаштування підключення кварцового резонатора до HSE

Після цього автоматично виводи мікроконтролера РН0, РН1 виділяються для підключення кварцового резонатора.

Результати обробки та аналізу даних експериментальних спостережень

Натурні дослідження, проведені авторами, дозволили отримати великий експериментальний матеріал акустичних сигналів БПЛА.

На рис. 7, 8 наведено приклади результатів модельно-кореляційної обробки сигналів БПЛА та фонового шуму, отримані у вигляді тривимірної модельно-кореляційної структури періодів акустичного сигналу. Обробка виконана за методикою, наведеною в [10 – 12].

Завданням аналізу сигналів є перевірка гіпотези, яка полягає у тому, що розробка системи інформативних ознак на основі часового аналізу дозволить створити надійну систему розпізнавання сигналів БПЛА.

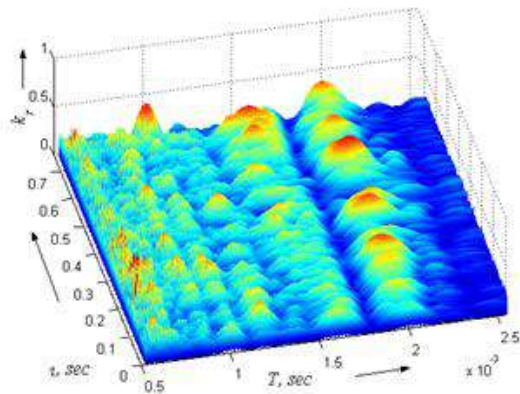


Рис. 7. Модельно-кореляційна структура

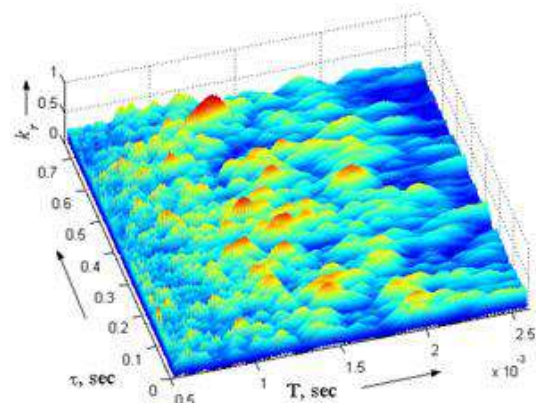


Рис. 8. Модельно-кореляційна структура фонового шуму

Тоді мета обробки полягає у приведенні вибірок сигналів до виду, зручному для дослідження флуктуації періоду акустичного сигналу БПЛА на малих інтервалах часу. Виходячи з поставленої мети, методика обробки акустичних шумоподібних сигналів полягає в записі вибірки S_v акустичного сигналу БПЛА тривалістю t_v в пам'ять мікроконтролеру, а потім у послідовному виявленні присутності в досліджуваній вибірці коротких фрагментів синусоїдального сигналу:

$$S_{ai} = \sin\left(\frac{x \cdot 2\pi}{T_{ai}}\right),$$

де T_{ai} – період шуканої складової сигналу; $t_{pi} = pT_{ai}$ – тривалість фрагменту; $x = [0 : (p \cdot T_i)]$; p – ціле число періодів в моделі фрагменту сигналу; $p = 10$ згідно з [11].

Потрібні фрагменти сигналу при вибраному періоді T_i виявляються шляхом розрахунку коефіцієнта кореляції k_r між моделлю S_{Mi} фрагменту сигналу $S_{Mi} = \sin\left(\frac{x \cdot 2\pi}{T_{Mi}}\right)$ з встановленими періодом T_{Mi} і тривалістю $t_{Mi} = t_{pi}$, і фрагментом записаного сигналу $S_{ai}(x)$. Причому коефіцієнти кореляції обчислюються послідовно при зрушенні моделі S_{Mi} сигналу вздовж часової осі τ на величину $\Delta\tau$ при $T_{Mi} = const$. При цьому виконується умова: $t_M \ll t_e$ – де тривалість моделі набагато менша за тривалість записаної вибірки. Операція розрахунку проводиться для кожного значення T_M із заздалегідь встановленого ряду дискретних значень $T_M(i) = T_0 + i \cdot \Delta t$ при $i = (1 \dots n)$, де $T_0 = 0,52 \cdot 10^{-3} s$ або еквівалент частоти $F_s = [385 \dots 2000] Гц$ при $\Delta t = 2,083 \cdot 10^{-5} s$ і $n = 100$. Отже, за одну операцію повного зсуву виявляється наявність однієї компоненти шуканої складової сигналу при одному із заданих

значень періоду моделі T_{Mi} , при цьому число операцій повного зсуву моделі вздовж вибірки сигналу дорівнює кількості заданих значень T_{Mi} періоду моделі (в даному випадку $n = 100$).

В результаті отримуємо ряд залежностей $k_{ri}(\tau, T_{Mi})$, які організуються в матрицю $(m \times n)$. При цьому приймається умова, якщо $k_r \geq k_{st}$ шуканий фрагмент присутній у сигналі БПЛА, при $k_r < k_{st}$ приймається альтернативне рішення.

Члени матриці M_{kr} вздовж стовпців є коефіцієнти кореляції k_{ri} , отримані при одному із заданих значень періоду моделі T_{Mi} та розраховані в залежності від зсуву моделі вздовж осі часу вибірки.

Члени вздовж строк є значення коефіцієнтів кореляції, полученні при одной и той же величине сдвига модели вздовж осі времени выборки, то есть каждая строка есть зависимость коэффициента корреляции от периода модели при данном сдвиге.

Члени вздовж рядків є значення коефіцієнтів кореляції, отримані при одній і тій же величині зсуву моделі вздовж осі часу вибірки, тобто кожен рядок є залежність коефіцієнта кореляції від періоду моделі при даному зсуві.

Візуальний аналіз рис. 7 показує, що сигнал МАА на малих інтервалах часу $t_M = 10T_M$ представлений рядом дискретних складових при $T_M = [2; 1,5; 1,25; 1]ms$. Видно також, що амплітуда цих складових істотно флукує.

Компоненти при $T_M < 1ms$ слабо помітні як дискретні складові. Їх амплітуда істотно знижена по відношенню до складових при $T_M = [2; 1,5]ms$.

Як впливає з рис. 8, у структурі «період – час» сигналів фонового шуму повністю відсутня стійка повторюваність, тобто сигнали мають суто випадковий характер.

Для формалізації візуального аналізу на рис. 9 наведено залежності нормованого коефіцієнта кореляції в діапазоні періодів моделі $T_M = [0,5 \dots 2,5] \cdot 10^{-3}c$ (еквівалентні частоти $F_{se} = [400 \dots 2000]Гц$) в структурі сигналу дрону і фонового шуму. Ці залежності отримані шляхом усереднення значень матриці вздовж стовпчиків.

Залежність, представлена суцільною лінією, отримана з матриці сигналу БПЛА, дві інші (пунктир) отримані аналогічним розрахунком по двох вибірках одного запису шуму вулиць мегаполісу.

Як впливає з наведених графіків, у двох реалізаціях сигналу фонового шуму відсутні повторювані області гармонійних складових. Ці залежності характеризують суто випадковий характер спостережуваного процесу.

Залежність, отримана із сигналів БПЛА, дозволяє визначити число гармонік та діапазон флукуації їх періодів. Вигляд цієї залежності формалізує властивість структурованості періодів сигналу БПЛА. На цій залежності спостерігаються дві області, розділені глибокими мінімумами при періоді $T_M = 1,3ms$ і $T_M = 1,83ms$, що свідчить про існування двох основних процесів генерації акустичного сигналу.

Полученная структура позволяет выдвинуть предположение о существовании корреляционной связи между строками полученной матрицы M_{kr} коэффициентов корреляции.

На рис. 10 наведено графіки залежностей коефіцієнтів кореляції між рядками матриці M_{kr} , причому розрахунок коефіцієнтів кореляції ведеться між початковим рядком і всіма наступними рядками, включаючи початковий рядок.

Номери початкових рядків встановлюються з ряду $N_{0str} = [1, 100, 200, 300, 400, 500, 600]$. Розмір $N_{str\max} = 600$ вибрано з умови $\Delta\tau_{N_{\max}} \geq 0,01s$.

У результаті кожної ітерації N_{0str} маємо послідовність коефіцієнтів кореляції $k_{rNi} = [k_{ri} \dots k_{rm}]^i$, де $i = N_i \dots m$, де m – число рядків M_{kr} . Кожне значення залежностей на рис. 10 отримано шляхом усереднення розрахованих послідовностей $k_{rNi} = [k_{ri} \dots k_{rm}]$.

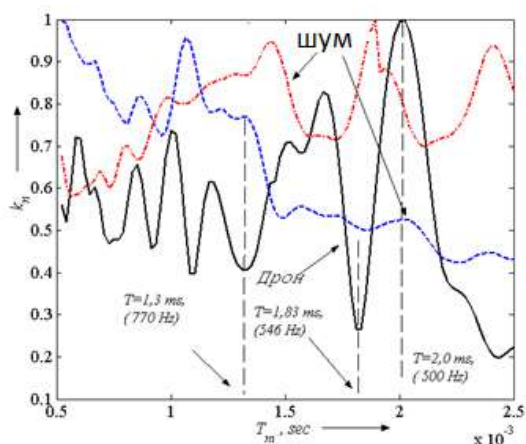
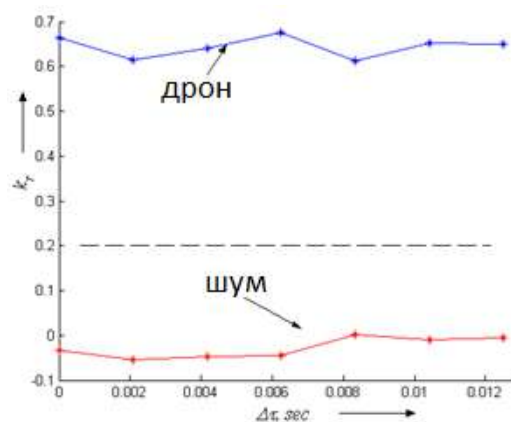


Рис. 9. Залежність нормованого коефіцієнту кореляції від періоду моделі в структурі сигналу дрону та фонового шуму вулиці



10. Залежність коефіцієнта кореляції БПЛА та фонового шуму

На рис. 10 наведено дві залежності. Перша отримана із сигналів БПЛА (позначено дрон), друга – із сигналів фонового шуму вулиці мегаполісу (позначено шум).

З отриманого результату випливає, що залежності на рис. 10 не перетинаються, між їх значеннями є суттєва та стійка відмінність. Отже, отриманий результат дозволяє запровадити ознаку як умови:

$$H = 1 \quad \text{при} \quad k_r > k_{cl}$$

$$H = 0 \quad \text{при} \quad k_r < k_{cl}$$

де H – подія, що визначає приналежність аналізованого сигналу, значення "1" – означає, що подія H полягає у правильному виявленні сигналу БПЛА, значення "0" – означає, що подія H полягає у виявленні сигналу фонового шуму, k_{cl} – граничне значення ознаки, в даному випадку можна прийняти $k_{cl} = 0,3$.

Висновки

Основним результатом є обґрунтування доцільності використання аналізу «час – період» на малих інтервалах часу. Показано, що цей підхід дозволяє отримати інформативну ознаку для розпізнавання акустичних сигналів БПЛА на тлі зовнішніх шумів.

Сформульовано постановку завдання виявлення БПЛА щодо реєстрації та аналізу акустичних сигналів за допомогою середовища STM32CubeIDE, які генеруються БПЛА в процесі польоту, визначено фактори, що впливають на часову структуру флуктуацій періоду сигналів БПЛА.

Список літератури:

1. Kloet N. et al. Acoustic signature measurement of small multi-rotor unmanned aircraft systems // International Journal of Micro Air Vehicles. 2017. 9(1). P.3–14.
2. Stimpson A. et al. Small UAV Noise Analysis. Humans and Autonomy Laboratory, Duke University, Durham, NC, USA. 2017. April 26, 12 pp. Available at https://hal.pratt.duke.edu/sites/hal.pratt.duke.edu/files/u24/Small_UAV_Noise_Analysis_rqi.pdf.

3. Leslie A. et al. Broadband noise reduction on a mini-UAV propeller // 14th AIAA/CEAS aeroacoustic conference, Geelong, Victoria, Australia, 2008. Available at <https://www.semanticscholar.org/paper/Broadband-Noise-reduction-from-a-mini-UAV-propeller-Auld-Leslie/aa8f1514d96bd711bea00880afdb8050800037bc>.
4. Brown J. What Is A Drone: Main Features and Applications of Today's Drones. Available at <https://www.mydronelab.com/blog/what-is-a-drone.html>.
5. King E., et al. Bee threat elicits alarm call in African elephants // PLoS One. 2010. vol. 5, no. 4. P. e10346. Available at <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0010346>
6. Anderson K., Gaston K. Lightweight unmanned aerial vehicles will revolutionize spatial ecology // Frontiers in Ecology and the Environment. 2013. vol. 11, no. 3. P. 138146.
7. Feight J. (2017). Characterization of a Multi-Rotor SUAS as a First Step Towards Detection and Identification via Acoust. Available at <https://shareok.org/handle/11244/300026>.
8. Карташов В. М. Информационные характеристики звукового излучения малых беспилотных летательных аппаратов / В.М. Карташов, С.А. Шейко, С.И. Бабкин, И.В. Корытцев, О.В. Зубков // Радиотехника. 2017. Вып. 191. С. 181–187.
9. Козерук С. О., Коржик О. В. Виявлення малих літальних апаратів за акустичним випромінюванням // Visnyk NTUU KPI Seriya – Radiotekhnika Radioaparatabuduvannia. 2019. Iss. 76. P. 15–20.
10. Semenetz V.V., Leonidov V.I. Model-structural analysis of combination interference in the problems acoustic sounding of the atmosphere // Telecommunications and Radio Engineering. 2019. Vol. 78, Issue 12. P. 1078-1095. DOI: 10.1615/TelecomRadEng.v78.i12.60, pages 1087–1095, 2019.
11. Леонідов В.І., Семенець В.В. Особенности амплитудно-временной структуры помех в системах акустического зондирования атмосферы // Радиотехника: 2019. Вып. 197. С. 93–99.
12. Leonidov V.I. Analysis of the models and structure of echo signals of the atmospheric acoustic sounding // Telecommunications and Radio Engineering. 2014. 73(16). P. 1497–1502.
13. Семенець В.В., Леонідов В.І. Використання мікроконтролера stm32f407vg для дослідження амплітудно-частотних характеристик біологічних тканин // Радиотехніка: 2023. Вып. 214. С. 94–101.
14. Програмування мікроконтролерів STM32 в середовищі STM32CubeIDE в прикладах і задачах : навч. посіб. / О. В. Зубков, І. В. Свид, О. В. Воргуль, В. В. Семенець. Дніпро : ЛІРА ЛТД, 2022. 144 с.
15. В.В. Семенець, В.І. Леонідов. Исследование амплитудно-частотных характеристик биологических тканей // Радиотехніка.зб. 2020. Вып. 203. С. 186–190.
16. В.В. Семенець, В.І. Леонідов. Аналіз частотно-часової структури акустичних шумів малих автоматичних аеросистем // Радиотехніка. 2020. Вып. 202. С. 147–152. DOI:10.30837/rt.2020.3.202.15.
17. Аврунін О.Г., Запорожець О.В., Носова Т.В., Семенець В.В // Микропроцессоры в информационно-измерительных системах : навч. посібник. Харків : ХНУРЕ, 2015. 180с. <http://openarchive.nure.ua/handle/document/5291>.
18. Основи реєстрації та аналізу біосигналів : навч. посіб. / О.Г. Аврунін, В.Г. Абакумов, З.Ю. Готра, С.М. Злепко, А.В. Кіпенський, С.В. Павлов, В. В. Семенець. Харків : ХНУРЕ, 2019. 400 с. <https://doi.org/10.30837/978-966-659-257-9>.

Надійшла до редколегії 09.11.2023

Відомості про авторів:

Леонідов Володимир Іванович – канд. техн. наук, Харківський національний університет радіоелектроніки, с. н. с. кафедри біомедичної інженерії, Україна; e-mail: volodymyr.leonidov@nure.ua; ORCID: <https://orcid.org/0000-0001-5218-3177>

Семенець Валерій Васильович – д-р техн. наук, професор. Харківський національний університет радіоелектроніки, професор кафедри біомедичної інженерії, Україна; e-mail: valery.semenets@nure.ua; ORCID: <https://orcid.org/0000-0001-8969-2143>

Григор'єв Олександр Вікторович – канд. техн. наук, доц., Харківський національний університет радіоелектроніки; Україна; e-mail: oleksandr.hryhoryev@nure.ua; ORCID: <https://orcid.org/0000-0001-6467-7983>

І.В. СВИД, канд. техн. наук, Д.О. СУХОПУКОВ, О.В. КОРОТІЧ, Т.С. МАЧОНІС

МЕТОД ПІДВИЩЕННЯ ЯКОСТІ ОБСЛУГОВУВАННЯ СИГНАЛІВ ЗАПИТУ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Вступ

Запитальні інформаційні системи є важливою складовою інформаційного забезпечення управління повітряного руху і системи контролю повітряного простору. До запитальних інформаційних систем відносяться системи вторинної радіолокації [1 – 5], системи радіолокаційної ідентифікації державної приналежності [6 – 10] та радіосистеми ближньої навігації [11 – 14].

Слід зазначити, що основним елементом досліджуваної системи, який суттєво знижує якість інформаційного забезпечення, є літаковий відповідач (ЛВ) [15 – 17]. Ця обставина зумовлена принципом побудови літакового відповідача як відкритої одноканальної системи масового обслуговування з відмовами [18]. Така побудова зазначеної інформаційної радіолокаційної системи дозволяє зацікавленій стороні здійснювати несанкціоноване отримання польотної інформації від літакового відповідача, що розглядається, і, також, здійснювати паралізацію літакового відповідача постановкою навмисних корельованих завад необхідної інтенсивності. При цьому слід зазначити, що у існуючих літакових відповідачах запитальних інформаційних систем, зазвичай, реалізується квазіоптимальний виявлювач сигналів запиту при багатоканальному прийомі з об'єднанням каналних рішень виявлення сигналів запиту. Однак це призводить до енергетичних втрат при прийомі сигналів запиту і, як наслідок, зниження якості обслуговування сигналів запиту.

Метою запропонованої роботи є підвищення якості обслуговування сигналів запиту в запитальних інформаційних системах за рахунок управління потоками сигналів запиту.

Управління потоками сигналів запиту

Як видно з моделі літакового відповідача несинхронної запитальної інформаційної системи [19, 20], сигнали запиту, що надходять на його вхід, обслуговуються з відмовами. Ця обставина дозволяє стверджувати, що характеристики процесу обслуговування сигналів запиту в літаковому відповідачі істотно впливають на статистичні властивості потоку сигналу відповіді, що в підсумку, як наслідок, відображається на ефективності роботи всього радіолокаційного каналу передачі сигналів відповіді з активною відповіддю. При цьому слід зазначити, що однією з важливих характеристик процесу обслуговування сигналів запиту в літаковому відповідачі є його кореляційна функція $R(t)$, на основі аналізу якої можливо зробити висновок щодо вибору типу потоку сигналів відповіді та структури літакового відповідача. Ця обставина дозволяє, за інших рівних умов, досягти підвищення ймовірності обслуговування, збільшення ймовірності виявлення повітряного об'єкта, зменшення середньоквадратичної помилки оцінки азимуту повітряного об'єкта та підвищення достовірності передачі польотної інформації з борту повітряного об'єкту, що спостерігається.

При цьому слід зазначити, що процес обслуговування сигналів запиту літаковим відповідачем можливо представити у вигляді деякої часової функції $Q(t)$, яка приймає значення "одиниця", якщо літаковий відповідач вільний та "нуль" – у протилежному випадку.

Зазначену часову функцію $Q(t)$, яка слідує з моделі літакового відповідача [21], можливо отримати з потоку сигналів відповіді, коли провести розширення кожного сигналу відповіді вліво за віссю часу на ширину $T_i - t_{o(i-1)}$, при обслуговуванні сигналів відповіді, випромінюваних основним променем діаграми спрямованості антени запитувача, та $T_i - t_{p(i-1)}$ при обслуговуванні сигналів відповіді, випромінюваними за боковими пелюстками діаграми

спрямованості антени запитувача, де T_i – часовий інтервал між моментами появи $(i-1)$ та i -го сигналу відповіді, $t_{o(i-1)}$ – час обслуговування $(i-1)$ -го сигналу запиту, випромінюваного основним променем діаграми спрямованості антени запитувача, $t_{p(i-1)}$ – час паралізації літакового відповідача при прийманні сигналів відповіді, які випромінені боковими пелюстками діаграми спрямованості антени запитувача.

Зазначимо, так як потік сигналів відповіді визначається потоком сигналів запиту та коефіцієнтом готовності літакового відповідача, то можливо стверджувати, що управлінням потоком сигналів відповіді в мережі запитальних інформаційних систем можливо підвищити за рахунок підвищення імовірності обслуговування сигналів запиту літаковим відповідачем, а отже і всією запитальною інформаційною системою.

Таким чином, виходячи з викладеного – підвищення якості обслуговування сигналів запиту запитальних несинхронних інформаційних систем можливо досягнути за рахунок:

- управління потоком сигналів запиту в мережі вторинних радіолокаторів;
- зниження сумарної інтенсивності потоку сигналів запиту;
- зниження сумарної інтенсивності потоку сигналів відповіді.

При цьому слід зазначити, що відомі різні методи підвищення завадостійкості зазначених запитальних інформаційних систем [1 – 3]. Більшість з зазначених методів ґрунтується на зниженні рівня внутрісистемних завад, що, як відомо, веде до підвищення завадостійкості.

В цій роботі досліджується варіант зниження потоку внутрісистемних завад за рахунок управління потоками сигналів запиту в запитальних інформаційних системах, що дозволяє підвищити завадостійкість зазначених інформаційних систем.

Слід зазначити, що потік сигналів запиту на вході літакового відповідача є сумою потоків сигналів запиту $\lambda_i(t)$ $(N-1)$ запитувачів, в зоні дії яких знаходиться літаковий відповідач. Цей потік сигналів запиту може бути записано в наступному виді:

$$\lambda_s = \sum_{i=1}^{N-1} \alpha_i(t) \beta_i(t),$$

де

$$\alpha_i(t) = \begin{cases} 1, & \text{при } \xi_i + mT_{zi} \leq T(t) < \xi_i + mT_{zi} + \tau_0; \\ 0, & \text{при інших } T(t); \end{cases}$$

ξ_i – початкова фаза потоку; $\alpha_i(t)$ – випадкова величина з рівномірною щільністю розподілення на часовому інтервалі $[0, T_{zi}]$, τ_0 – тривалість імпульсів потоку сигналів запиту;

$$\beta_i(t) = \begin{cases} 1, & \text{при } \mu_i + sT_{oi} \leq T(t) < \mu_i + sT_{oi} + \Delta t_i; \\ 0, & \text{при інших } T(t); \end{cases}$$

Δt_i – тривалість пачки сигналів запиту.

З зазначеного вище можливо зробити висновок, що інтенсивність потоку сигналів запиту $\lambda_s(t)$ повністю визначається параметрами чотирьох типів N_i, t_i, T_{zi}, T_{oi} . Число запитальних інформаційних систем N та ширина діаграми спрямованості антен запитальних інформаційних систем, як правило, відомі. Таким чином, залишаються два параметри, змінюючи які, можна проводити зміну властивості потоку сигналів запиту в потрібному напрямку, використовуючи певні інформаційні критерії. Так, в якості такого критерію може бути використана дисперсія числа сигналів відповіді у пачці сигналів відповіді. Дійсно, мінімум цієї дисперсії виконується в тому випадку, коли сума кореляційних моментів дорівнює нулю, що вказує на незалежність або некорельованість станів літакового відповідача запитальної інформаційної системи у моменти надходження на його вхід i -го та j -го сигналів запиту

конкретного запитувача. При цьому слід зазначити, що умова некорельованості виконується у тому випадку, якщо період слідування сигналів запиту запитувачів інформаційної системи, що розглядається, обраний так, що $\tau = kT_{z0}$ потрапляють у проміжки між пелюстками кореляційної функції процесу обслуговування сигналів запиту. Так як кожний з N вторинних інформаційних радіолокаторів може вважатися визначеним, то періоди слідування сигналів запиту кожної запитальної інформаційної системи повинні задовольняти умові збереження незалежності потоків сигналів запиту $\lambda_i(t)$, для чого повинні бути виконані наступні умови:

$$\begin{aligned} m_r T_{zr} &= m_s T_{zs}, \quad s, r = 1, 2, \dots, N, \quad s \neq r, \\ m_r T_{zr} &= m_0 T_{z0} \quad \text{та} \quad |T_{zt} - T_{z0}| > 2t_0, \end{aligned}$$

де m_r, m_s – цілі нескорочувані числа; t_0 – час обслуговування сигналів запиту у літаковому відповідачі; T_{z0} – період повторення сигналів запиту запитувача, що розглядається.

Таким чином, наведений спосіб управління потоками сигналів запиту в мережі запитальних інформаційних систем не передбачає взаємодії потоків сигналів запиту. Однак, як впливає із процесу функціонування існуючих вторинних радіолокаторів, які розглядаються, вище наведені умови незалежності потоків сигналів запиту можна дещо послабити. Це обумовлено тим, що для роботи систем радіолокаційної ідентифікації за ознакою свій-чужий достатньо обслуговування тільки певної кількості сигналів запиту [1].

Будемо вважати, що набір періодів слідування сигналів запиту запитальної інформаційної системи, що розглядається, та інших вторинних радіолокаторів задовольняє критерію обмеженої взаємодії, якщо виконується рівність

$$r_m = m - k.$$

Як слідує з цього виразу, обмежена взаємодія обрана так, що за всю пачку сигналів запиту виявиться така частина сигналів відповіді літакового відповідача, що у запитувачі відбудеться виконання критерію початку пачки сигналів.

Визначимо вимоги, у яких набір періодів повторення сигналів запиту задовольняє критерію обмеженої взаємодії. Для цього розглянемо найпростіший випадок – взаємодія двох запитальних послідовностей. Нехай на вхід літакового відповідача з кінцевим часом обслуговування одночасно надходять послідовності сигналів запиту двох радіолокаторів.

Назвемо інтервалом взаємодії i -ї та j -ї послідовностей число V_{ij} – це число періодів повторення між можливими втратами сигналів запиту i -ї послідовності внаслідок зайнятості літакового відповідача обслуговуванням j -ї послідовності. Очевидно, що при однакових періодах повторення $V_{12} - V_{21} = 1$ можливо показати, що для $V_{12} = k'$ при деякому цілому числі n' маємо

$$k'T - t_0 < n'(T + \Delta T) < k'T + t_0, \quad (1)$$

де $T, \Delta T, t_0$ – в загальному випадку довільні позитивні дійсні числа, що визначаються обраною одиницею виміру часу.

З другої сторони, якщо послідовність сигналів запиту, що аналізується, є послідовністю з періодом $T + \Delta T$, то $V_{21} = n''$ і деякого цілого числа k'' , то маємо

$$n''(T + \Delta T) - t_0 < k''T < n''(T + \Delta T) + t_0. \quad (2)$$

Кожне з співвідношень (1) та (2) визначає можливі інтервали взаємодії V_{12} і V_{21} та є еквівалентним сукупності рівнянь виду

$$n(T + \Delta T) - kT = \xi, \quad (3)$$

де ξ приймає значення з наступного інтервалу:

$$\overline{-t_0, +t_0}; n = n' = n'' = V_{21}; k = k' = k'' = V_{12}.$$

Здійснимо перехід від сукупності (3) до аналогічної сукупності в цілих числах. Коли позначити $[a]$ як цілу частину числа a , ввести позначення $T - [T] = \alpha$; $\Delta T - [\Delta T] = \beta$; $\xi - |\xi| = \gamma$ та коли для деяких n^*, k^*, ξ^* задовольняється одне з рівнянь сукупності (3), то маємо

$$n^* (|T| + \alpha + |\Delta T| + \beta) - k^* (|T| + \alpha) = |\xi^*| + \gamma$$

або

$$n^* (|T| + |\Delta T|) - k^* (|T|) = |\xi^*| - \Theta, \quad (4)$$

де $\Theta = \{n^* (\alpha + \beta) - k^* \alpha - \gamma^*\}$ – ціле число.

Так як значення n^* та k^* фіксовані, то при виборі достатньо малої одиниці вимірювання часу маємо наступну нерівність $\Theta \ll t_0$. Звідси з точністю для всіх $[\xi] < [t_0] - \Theta$ множини рішень рівнянь із сукупності (3) збігаються з рішеннями рівнянь сукупності

$$n(|T| + |\Delta T|) - k(|T|) = \xi, \quad (5)$$

для кожного цілого ξ з інтервалу $-t_0, +t_0$.

Таким чином, множину інтервалів взаємодії може бути знайдено рішенням рівняння виду (5). При цьому слід зазначити, що для досліджень становлять інтерес лише рішення, яким відповідають мінімальні значення інтервалів взаємодії. Далі будемо використовувати лише цілі числа.

Відомо, що рівняння виду

$$n(T + \Delta T) - kT = \xi \quad (6)$$

вирішуються тільки тоді, коли найбільший спільний дільник $(T, \Delta T)$ чисел T та ΔT ділить ξ .

В залежності від значення $(T, \Delta T)$ кількість розв'язних рівнянь сукупності (6) дорівнює одному при $(T, \Delta T) > t_0$ та не більше $2t_0 + 1$ при $(T, \Delta T) < t_0$.

Будемо вважати, що n^* та k^* є найменші позитивні рішення рівняння (6). Тоді n^* задовольняє співвідношенню

$$n\Delta T / (T, \Delta T) = \frac{\xi}{(T, \Delta T)} \bmod \frac{T}{(T, \Delta T)}. \quad (7)$$

При цьому слід зазначити, що k^* можливо визначити за виразом

$$k^* = \frac{|\xi - n^* (T + \Delta T)|}{T}. \quad (8)$$

Серед різних способів розв'язання виразу (7) у нашому випадку найбільш зручним способом може бути перетворення коефіцієнтів. У цьому способі перебуває найменше позитивне число s , таке, що ΔT ділить $\xi + sT$, тоді

$$n^* = (\xi + sT) / \Delta T. \quad (9)$$

Необхідна кількість випробувань вибирається з числа елементів повної системи відрахувань за модулем $\Delta T / (T, \Delta T)$. Крім того, коли виконується умова

$$\Delta T / (T, \Delta T) = \eta \bmod \{\Delta T / T, \Delta T\},$$

то для шуканого s число $\xi + s\eta$ ділиться на ΔT .

З урахуванням викладеного та відповідно до виразу (9) за $s = \Delta T / (T, \Delta T)$ та умови (8), отримуємо

$$n^* = \frac{T}{(T, \Delta T)}; k^* = n^* + \frac{\Delta T}{(T, \Delta T)}. \quad (10)$$

Розглянемо вибір періодів повторення сигналів запиту в мережі із двох радіолокаторів. Для того щоб набір періодів слідування $T_1 = T$ й $T_2 = T + \Delta T$ задовольняв критерію обмеженої взаємодії, необхідно T і ΔT вибрати так, щоб мінімальні значення інтервалів взаємодії перевищували число $m - k$. Зазвичай, значення ΔT бажано вибрати мінімально можливим. Якщо $\Delta T = t_0 + 1$, то найкращим вибором відповідають значення T_1 , що дорівнюють

$$T_1 = T = a(t_0 + 1),$$

де a – будь-яке ціле число, яке більше за число $m - k$.

Так, у разі $(T, \Delta T) = t_0 + 1$ і відповідно до виразу (10) отримуємо єдине значення V_{12} , що дорівнює $n^* = T / (t_0 + 1) = a$.

При практичному виборі періодів повторення сигналів запиту мережі запитальних інформаційних систем з обмеженою взаємодією потоків сигналів запиту можливо використовувати наступний алгоритм, що дозволяє просто визначити набір періодів повторення. Дійсно, при заданому часі обслуговування сигналів запиту вибирається період повторення першого вторинного радіолокатора так, що

$$T_1 = a(t_0 + 1),$$

де $a > m - k$. Тоді періоди слідування сигналів запиту інших запитальних інформаційних систем можливо вважаємо рівними

$$T_i = T_1 + (i - 1)(t_0 + 1), \quad i = 2, 3, \dots, N.$$

Таким чином, правильний вибір періодів повторення сигналів запиту в районі спільної дії запитальних інформаційних систем дозволяє значно зменшити ймовірність взаємодії окремих сигналів запиту і, як наслідок, дозволяє підвищити завадостійкість всіх запитальних інформаційних систем, що входять до зазначеної інформаційної системи.

Висновки

Отримані результати дозволяють зробити наступні висновки:

- правильний вибір періодів повторення сигналів запиту в районі спільної дії запитувачів інформаційних систем, що розглядаються, дозволяє зменшити ймовірність взаємодії окремих сигналів запиту і, як наслідок, дозволяє підвищити завадостійкість запитальних інформаційних систем, які входять до зазначеної інформаційної системи;
- при управлінні потоками сигналів запиту в мережі запитальних інформаційних систем можливо підвищити імовірність якості обслуговування сигналів запиту літаковим відповідачем, а отже, і всією запитальною інформаційною системою.

Список літератури:

1. Свид І.В., Обод І.І. Завадостійкість радіолокаційних систем ідентифікації за ознакою «свій-чужий»: монографія. Харків: Друкарня Мадрид, 2021. 254 с.

2. Васишин В.І., Лебедєв В.О., Висоцький О.В., Коцюба В.П. Вторинна радіолокація як основа сучасних систем спостереження за повітряною обстановкою // Наука і техніка Повітряних Сил Збройних Сил України. 2021. № 2(43). С. 94–103. <https://doi.org/10.30748/nitps.2021.43.13>.
3. Обод І.І., Свид І.В. Порівняльний аналіз якості виявлення повітряних об'єктів запитальними системами спостереження // Системи обробки інформації. 2010. Вип. 9 (90). С. 74–76.
4. Svyd I. V. Comparative analysis of the quality of detection of air objects by secondary radar systems // Radiotekhnika. 2023. No. 213. P. 78–87. doi:10.30837/rt.2023.2.213.09.
5. Обод І.І., Шевцова В.В. Порівняльний аналіз запитальних систем передачі інформації системи контролю повітряного простору // Зб. наук. пр. Харк. нац. ун-ту Повітряних Сил. 2013. № 1(34). С. 123–125.
6. Svyd I. V. et al. Optimal measurement of signal data parameters of requesting radar systems // 2021 IEEE 3rd Ukraine Conference on Electrical and Computer Engineering (UKRCON), 2021. doi:10.1109/ukrcon53503.2021.9575235
7. Obod I. I. Integrated coordinate-and-time support for the Address Inquiry in the secondary radar systems // Telecommunications and Radio Engineering. 1999. Vol. 53, no. 3. P. 54–56, doi:10.1615/telecomradeng.v53.i3.100
8. Свид І.В. Показники якості інформаційного забезпечення користувачів сполученими системами спостереження повітряного простору // Радіотехніка. 2011. Вип. 165. 2011. С. 157–160.
9. Beel J. J. Anti-UAV Defense For Ground Forces and Hypervelocity Rocket Lethality Models. Monterey, California : Naval Postgraduate School, 1992. pp. 36–46.
10. Moses A., Rutherford M. J. and Valavanis K. P. Radar-based detection and identification for Miniature Air Vehicles // 2011 IEEE International Conference on Control Applications (CCA), 2011. doi:10.1109/csa.2011.6044363
11. Sadasivan S., Gurubasavaraj M., Sekar S.R. Acoustic signature of an unmanned air vehicle – exploitation for aircraft localisation and parameter estimation // Eronautical DEF SCI J. 2001. Vol. 51, № 3. P. 279–283.
12. Обод І.І., Стрельницький О.О., Андрусевич В.А. Структура та показники якості обробки інформації систем спостереження повітряного простору // Системи обробки інформації. 2013. № 8(115). С. 80–83.
13. Svyd I. et al. Optimizing the request signals detection of aircraft secondary radar system transponders // 2022 IEEE 41st International Conference on Electronics and Nanotechnology (ELNANO), 2022. doi:10.1109/elnano54667.2022.9926991
14. Обод І.І., Стрельницький О.О. Інформаційна безпека інформаційної мережі систем спостереження повітряного простору // Системи обробки інформації. 2015. № 9(134). С. 96–98.
15. Свид І.В., Обод А.І. Інформаційні технології обробки даних систем спостереження // Системи управління, навігації та зв'язку. Полтава : Полтав. нац. техн. ун-т ім. Юрія Кондратюка. 2016. Вип. 4 (40). С. 91–93.
16. Обод І.І., Шевцова В.В. Пропускна спроможність відповідачів запитальних систем передачі польотної інформації // Системи обробки інформації. 2013. № 1(108). С. 105–108.
17. Andrusевич V., Obod I. Assessment of the quality of information support by air radar surveillance systems // Advanced Information Systems. 2021. Vol. 5, No. 2, s.78–82. DOI: <https://doi.org/10.20998/2522-9052.2021.2.10>.
18. Semenets V. et al. Method of increasing the relative throughput of requesting radar systems // Przegląd Elektrotechniczny. 2022. Vol. 1, no. 11. P. 99–103. doi: 10.15199/48.2022.11.17.
19. Обод І.І., Стрельницький О.О., Андрусевич В.А. Методи підвищення якості інформаційного забезпечення системами спостереження повітряного простору // Системи обробки інформації. 2014. № 4(120). С. 53–55.
20. Pavlova D. B. et al., Comparative analysis of data consolidation in Surveillance Networks // 2019 10th International Conference on Dependable Systems, Services and Technologies (DESSERT), 2019. doi:10.1109/dessert.2019.8770008.
21. Obod I. et al., Optimization of the quality of information support for consumers of Cooperative Surveillance Systems // Data-Centric Business and Applications. 2020. P. 133–155, doi:10.1007/978-3-030-43070-2_8.

Надійшла до редколегії 26.08.2023

Відомості про авторів:

Свид Ірина Вікторівна – канд. техн. наук, доц., завідувач кафедри мікропроцесорних технологій і систем, Харківський національний університет радіоелектроніки, Україна; email: iryna.svyd@nure.ua; ORCID: <http://orcid.org/0000-0002-4635-6542>

Сухоруков Дмитро Олексійович – аспірант кафедри мікропроцесорних технологій і систем, Харківський національний університет радіоелектроніки, Україна; email: dmytro.sukhorukov@nure.ua; ORCID: <https://orcid.org/0000-0002-5772-286X>

Коротіч Олексій Віталійович – аспірант кафедри мікропроцесорних технологій і систем, Харківський національний університет радіоелектроніки, Україна; email: oleksii.korotich@nure.ua; ORCID: <https://orcid.org/0000-0002-7213-6666>

Мачоніс Тадас Сігігасович – аспірант кафедри мікропроцесорних технологій і систем, Харківський національний університет радіоелектроніки, Україна; email: tadas.machonis@nure.ua; ORCID: <https://orcid.org/0000-0001-7656-2948>

SYSTEMS AND METHODS OF INFORMATION PROTECTION
СИСТЕМИ І МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

UDC 004.056.5

Comparative analysis of artificial intelligence based on existing chatbots / Yu.L. Golikov, M.V. Yesina, O.A. Kobylanska // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2023. №215. P. 7 – 12.

Today, artificial intelligence (AI) is rapidly gaining popularity in various sectors, including the corporate world, business circles, and people's daily lives. The application of artificial intelligence in such fields as medicine, banking and government structures is becoming more frequent. Artificial intelligence facilitates data processing, as it occurs without the intervention of human labor and usually ensures the accuracy of the tasks performed. According to statistics, the number of companies using artificial intelligence in their operations is increasing, and many organizations consider artificial intelligence as an important technology to achieve competitive advantage. This scientific study presents a comprehensive analysis of two leading artificial intelligence systems – ChatGPT-4 from the OpenAI company and Bard from the Google AI company. The work also provides an overview of the development of artificial intelligence in various fields and its impact on everyday human life, especially in such vital areas as medicine, finance, public administration, etc. The paper delves into a detailed comparison of different versions of ChatGPT (GPT-3 and GPT-4) by discussing and analyzing their capabilities, improvements, and limitations. The article also discusses the integration of the Bard system with Google services, its unique functionality and recent updates. The purpose of this study is to compare the capabilities of the artificial intelligence systems ChatGP-4T and Bard, highlight their strengths and weaknesses, as well as their practical application. The paper presents the results of comparative testing to evaluate the performance of each model (system) in various tasks, including solving a logical task, writing an essay, analyzing with subsequent suggestions for improving the web-site, and writing HTML/CSS code for a web-page. The results highlight the fact that, despite the recognized advantages of these models, their functional characteristics may sometimes be limited or not meet expectations when performing specific tasks and the choice of system (model) will be adjusted depending on the needs of users.

Key words: ChatGPT-4; Bard, OpenAI; GoogleAI; comparative analysis.

2 tabl. 3 fig. Ref: 4 items.

УДК 004.056.5

Порівняльний аналіз штучного інтелекту на основі існуючих чат-ботів / Ю.Л. Голіков, М.В. Єсіна, О.А. Кобилянська // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2023. Вип. 215. С. 7 – 12.

Штучний інтелект (ШІ, AI) набуває популярності у різних секторах, включаючи корпоративний світ, бізнес-кола та повсякденне життя людей. Застосування штучного інтелекту в медицині, банківській сфері та урядових структурах стає все частішим. Штучний інтелект полегшує обробку даних, оскільки вона відбувається без втручання людської праці та забезпечує точність виконаних завдань. Згідно зі статистикою зростає кількість компаній, які використовують штучний інтелект у своїй діяльності, а багато організацій вважають штучний інтелект важливою технологією для досягнення конкурентних переваг. У дослідженні представлено комплексний аналіз двох провідних систем штучного інтелекту – ChatGPT-4 від компанії OpenAI та Bard від компанії Google AI. Наведено огляд розвитку штучного інтелекту в різних галузях та його впливу на повсякденне життя людини, особливо в таких життєво важливих сферах, як медицина, фінанси, державне управління тощо. Детально порівняно різні версії ChatGPT (GPT-3 та GPT-4) шляхом обговорення та аналізу їхніх можливостей, вдосконалення та обмежень. Розглянуто інтеграцію системи Bard із сервісами Google, її унікальні функціональні можливості та останні оновлення. Мета дослідження – порівняння можливостей систем штучного інтелекту ChatGP-4T і Bard, висвітлення їхніх сильних і слабких сторін, а також їх практичного застосування. Наведено результати порівняльного тестування для оцінки продуктивності кожної моделі (системи) в різних завданнях, включаючи розв'язання логічного завдання, написання есе, аналіз із подальшим внесенням пропозицій щодо покращення веб-сайту та написання коду HTML/CSS для веб-сторінки. Результати підкреслюють, що, незважаючи на визнані переваги цих моделей, їхні функціональні характеристики можуть бути обмежені або не відповідати очікуванням при виконанні специфічних завдань, а вибір системи (моделі) буде коригуватися у залежності від потреб користувачів.

Ключові слова: ChatGPT-4; Bard; OpenAI; GoogleAI; порівняльний аналіз.

Табл. 2. Іл. 3. Бібліогр.: 4 назв.

UDC 004.056.5

Analysis of methods for detecting attacks on facial biometric authentication in mobile devices / O.D. Dolhanenko, O.V. Sievierinov, D.O. Viukhin, V.P. Kotsiuba, A.V. Krepko // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2023. №215. P. 13 – 21.

The object of the research is facial biometric authentication in the context of mobile devices (financial and government applications, etc.) of the Android and IOS platforms. The subject of the research is methods of detecting attacks on biometric authentication by face in mobile devices. The purpose of the work is to investigate the methods of

creating and recognizing Deepfake videos, to evaluate the possibility of local recognition of fakes within applications in mobile devices of the Android and IOS platforms.

As a result, the vulnerability of biometric authentication to Deepfake technology was confirmed, methods for recognizing fakes were analyzed, and the effectiveness of using a neural network model for local recognition of Deepfake in a mobile device was experimentally confirmed. Conclusions are drawn about possible ways to optimize the size of the model with an emphasis on maintaining accuracy.

Key words: attack; biometric authentication; protection; camera; face; neural network; Android; Deepfake; GAN; PyTorch Mobile; TensorFlow Lite.

2 tabl. 6 fig. Ref: 5 items.

УДК 004.056.5

Аналіз методів виявлення атак біометричної автентифікації за обличчям у мобільних пристроях / О.Д. Долганенко, О.В. Северінов, Д.О. В'юхін, В.П. Коцюба, А.В. Крепко // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2023. Вип. 215. С. 13 – 21.

Об'єкт дослідження – біометрична автентифікація за обличчям в контексті мобільних пристроїв (фінансових та державних додатків, тощо) платформи Android та IOS. Предмет дослідження – методи виявлення атак на біометричну автентифікацію за обличчям на мобільних пристроях. Мета роботи – дослідити методи створення та розпізнавання Deepfake відео, оцінити можливість локального розпізнавання підробок у межах додатків на мобільному пристрої платформи Android та IOS.

Підтверджено вразливість біометричної автентифікації до технології Deepfake, проаналізовано методи розпізнавання підробок та експериментально підтверджено ефективність застосування моделі нейронної мережі для локального розпізнавання Deepfake на мобільному пристрої. Зроблено висновки щодо можливих способів оптимізації розміру моделі з акцентом на збереження точності.

Ключові слова: атака; біометрична автентифікація; захист; камера; нейронна мережа; обличчя; Android; Deepfake; GAN; PyTorch Mobile; TensorFlow Lite.

Табл. 2. Л. 6. Бібліогр.: 5 назв.

UDC 004.056:519.2

A method for recovering linear block codes over an arbitrary finite field from sets of distorted code words / A.N. Alekseychuk, O.S. Shevchuk // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2023. №215. P. 22 – 30.

The article is devoted to one of the practically important problems of information security and cryptanalysis, which consists in recovering an unknown linear block code over an arbitrary field from a set of distorted code words. This is a hard computational problem, and the known problem-solving methods are proposed only for codes over the field of two elements and are based on the algorithms for searching words of small weight in (undistorted) linear block codes.

The main result of the article is a method for solving the problem posed, which differs in essence from the known ones and consists in recovering the desired code by solving the LPN (Learning Parity with Noise) problem, namely, recovering the solutions of systems of linear equations with distorted right-hand sides and a random equally probable matrix of coefficients over specified field. The LPN problem is well known from the Theory of Computational Algorithms and Cryptanalysis. It is equivalent to the problem of random linear block code decoding, and the security of many modern post-quantum cryptosystems are based on its hardness.

The proposed method provides an opportunity to apply a wider class of algorithms for recovering linear block codes in comparison with the previously known methods, in particular, algorithms like BKW and also the low weight words search algorithms in co-sets of linear block codes. Moreover, in contrast to previously known ones, the complexity of the proposed method depends linearly on the length of the required code (and increases with increasing of its dimension according to which algorithm for the LPN problem-solving is applied). Thus, the basic parameter determined the complexity of recovering a linear block code is its dimension (not its length), which, in principle, makes it possible to speed up known algorithms for recovering linear block codes from a set of corrupted code words.

Key words: information security; learning of information; code-based cryptography; linear block code recovering; LPN problem.

2 fig. Ref: 26 items.

УДК 004.056:519.2

Метод відновлення лінійних блокових кодів над довільним скінченним полем за наборами спотворених кодових слів / А.М. Олексійчук, О.С. Шевчук // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2023. Вип. 215. С. 22 – 30.

Присвячено задачі інформаційної безпеки та криптоаналізу, яка полягає у відновленні невідомого лінійного блокового коду над довільним полем за набором спотворених кодових слів. Ця задача є обчислювально складною, а відомі методи її розв'язання запропоновано лише для кодів над полем з двох елементів та базуються на застосуванні алгоритмів пошуку слів малої ваги у (неспотворених) лінійних блокових кодах.

Основним результатом статті є метод розв'язання поставленої задачі, який відрізняється за сутністю від відомих і полягає у відновленні шуканого коду шляхом розв'язання задачі LPN (Learning Parity with Noise), а саме, відновленні істинного розв'язку системи лінійних рівнянь зі спотвореними правими частинами та

випадковою рівномірною матрицею коефіцієнтів над заданим полем. Задача LPN добре відома в теорії обчислювальних алгоритмів і криптоаналізі. Вона еквівалентна задачі декодування випадкового лінійного блокового коду, а на її складності базується стійкість багатьох сучасних постквантових криптосистем.

Запропонований метод дозволяє застосовувати для відновлення лінійних блокових кодів більш широкий клас алгоритмів в порівнянні з раніше відомими, зокрема алгоритми типу ВКВ, а також алгоритми пошуку слів малої ваги у суміжних класах двійкових лінійних кодів. На відміну від раніше відомих трудомісткості запропонованого методу залежить лінійно від довжини шуканого коду (і зростає з ростом його вимірності відповідно до того, який алгоритм розв'язання задачі LPN застосовується). Таким чином, основним параметром, від якого залежить складність відновлення лінійного блокового коду, є його вимірність (а не довжина), що, в принципі, надає можливість пришвидшити відомі алгоритми відновлення лінійних блокових кодів за наборами спотворених кодових слів.

Ключові слова: інформаційна безпека; вивідування інформації; кодова криптографія; відновлення спотворених лінійних блокових кодів; задача LPN.

Лл. 2. Бібліогр.: 26 назв.

UDC 004.056.5

Analysis and comparison of the security of electronic signatures based on new quantum-resistant problems

/ I.D. Gorbenko, Ye.Yu. Kaptol // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2023. №215. P. 31 – 45.

Due to the development of quantum computers and quantum methods and algorithms, in order to ensure the security of information after the development of cryptographically relevant quantum computers, NIST conducted the NIST PQC competition. As a result of conducting three rounds of NIST PQC, NIST selected 4 candidates for standardization and four candidates for the fourth round (key encapsulation mechanisms BIKE, Classic McEliece, HQC, and SIKE (which the developers considered unreliable)). Due to the fact that selected algorithms are based on the use of lattices and to add diversity to this list through the use of general-purpose signatures, the process of standardizing additional digital signatures for quantum-resistant cryptography has been initiated.

The following types of signatures are considered for the first round of this standardization process: code-based signatures, isogeny signatures, multivariate signatures, symmetric signatures, MPC-in-the-head, and NIST-defined "other" signatures. These "other" digital signatures are mostly based on new and promising post-quantum (quantum-resistant) problems.

The purpose of the work is to analyze and compare candidates for quantum-resistant digital signatures, based on new and promising quantum-resistant problems, resistant to classical and quantum attacks and side-channel attacks. The paper provides comparison of four digital signatures classified by NIST as "other", namely: ALTEQ, eMLE-Sig 2.0, KAZ-SIGN, Xifrat1-Sign.I. For this purpose, the paper presents the basic principles of each of these digital signatures, their main parameters and available at the time of consideration attack vectors. The paper also provides unconditional criteria necessary for comparison. Digital signatures were compared according to such unconditional criteria as: possible lengths of the public key, possible lengths of the personal (secret) key, length of the result of cryptographic algorithm; and conclusions are made regarding the completeness of given comparison and the possibility of further research is highlighted.

Key words: quantum-resistant cryptography; digital signature; ALTEQ; eMLE-Sig 2.0; KAZ-SIGN; Xifrat1-Sign.I; standardization, NIST.

5 tabl. 10 fig. Ref: 18 items.

УДК 004.056.5

Аналіз та порівняння безпеки електронних підписів, що ґрунтуються на нових квантовостійких проблемах / I.D. Gorbenko, Є.Ю. Каптьол // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2023. Вип. 215. С. 31 – 45.

У зв'язку з розвитком квантових комп'ютерів та квантових методів та алгоритмів, з метою забезпечення захищеності інформації після розробки криптографічно-релевантних квантових комп'ютерів з боку NIST було проведено конкурс NIST PQC. В результаті проведення трьох раундів NIST PQC було обрано для стандартизації чотири кандидати та визначено кандидатів для проведення четвертого раунду (механізми інкапсуляції ключів BIKE, Classic McEliece, HQC та SIKE (котрий розробники визнали ненадійним)). Через те, що обрані алгоритми засновані на використанні решіток, для внесення до цього переліку різноманіття за рахунок підписів загального призначення було розпочато процес стандартизації додаткових ЕП для квантовостійкої криптографії.

Серед поданих на розгляд до першого раунду цього процесу стандартизації наявні наступні види підписів: підписи, засновані на кодах; підписи на ізогеніях; мультіваріативні підписи; симетричні підписи; MPC-in-the-head та підписи визначені NIST як «інші». Саме ці «інші» ЕП здебільшого ґрунтуються на нових та перспективних постквантових (квантовостійких) проблемах.

Мета роботи – аналіз та порівняння кандидатів на квантовостійкий ЕП, що ґрунтуються на нових та перспективних квантовостійких проблемах, стійких до класичних та квантових атак та атак бічними каналами. В роботі наведено порівняння чотирьох ЕП, віднесених NIST до категорії «інші», а саме: ALTEQ, eMLE-Sig 2.0, KAZ-SIGN, Xifrat1-Sign.I. Наведено основні засади кожного з цих ЕП, їх основні параметри та наявні на момент розгляду вектори атак. Наведено безумовні критерії, необхідні для проведення порівняння. Проведено порів-

няння ЕП за такими безумовними критеріями, як: можливі довжини відкритого ключа, можливі довжини особистого (секретного) ключа, довжина результату криптоперетворення (збитковість), та зроблено висновки щодо повноти наведеного порівняння та можливості подальших досліджень.

Ключові слова: квантовостійка криптографія; електронний підпис; ALTEQ; eMLE-Sig 2.0; KAZ-SIGN; Xifrat1-Sign.I; стандартизація; NIST.

Табл. 5. Лл. 10. Бібліогр.: 18 назв.

UDC 621.391:519.2

Method of encryption in the MST3 cryptosystem based on Automorphisms group of Suzuki's functional field / Y. Kotukh, G. Khalimov, M. Korobchinskyi // Radiotekhnika: All-Ukr. Sci. Interdep. Mag. 2023. No 215. P. 46 – 59.

This article presents a new implementation of encryption based on MST, focused on generalized Suzuki 2-groups. The well-known MST cryptosystem, based on Suzuki groups, is constructed using a logarithmic signature at the center of the group, leading to a large array of logarithmic signatures. The proposed encryption is based on multi-parameter noncommutative groups, with a focus on the generalized multi-parameter Suzuki 2-group. This approach responds to the progress in the development of quantum computers, which may pose a threat to the security of many open cryptosystems, especially those based on factorization problems and discrete logarithms, such as RSA or ECC. The use of noncommutative groups to create quantum-resistant cryptosystems has been a known approach for the last two decades.

The unsolvable word problem, proposed by Wagner and Magyarik, is used in the field of permutation groups and is key to the development of cryptosystems. Logarithmic signatures, introduced by Magliveras, represent a unique type of factorization suitable for finite groups. The latest version of such an implementation, known as MST3, is based on the Suzuki group. In 2008, Magliveras introduced the LS transitivity limit for the MST3 cryptosystem, and later Swaba proposed an improved version of the cryptosystem, eMST3. In 2018, T. van Trung suggested applying the MST3 approach using strong aperiodic logarithmic signatures for abelian p -groups. Kong and his colleagues conducted a deep analysis of MST3 and noted that due to the absence of publications on the quantum vulnerability of this algorithm, it can be considered a potential candidate for use in the post-quantum era.

The main distinction of the new system is the use of homomorphic encryption to construct logarithmic signature coverings for all group parameters, which improves the secrecy of the cryptosystem, particularly against brute-force attacks.

Key words: MST3; cryptosystem; word problem; logarithmic signature; homomorphic encryption; Suzuki 2-group.

10 tabl. Ref.: 28 items.

УДК 621.391:519.2

Метод направлено шифрування в криптосистемі MST3 на основі узагальненої Сузукі 2-групи та гомоморфного шифрування / С.В. Котух, Г.З. Халімов, М.В. Коробчинський // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2023. Вип. 215. С. 46 – 59.

Презентовано нову реалізацію шифрування на основі MST, зосереджену на узагальнених 2-групах Сузукі. Відома криптосистема MST, що базується на групах Сузукі, побудована з використанням логарифмічного підпису в центрі групи, що призводить до великої кількості логарифмічних підписів. Пропонується шифрування, засноване на багатопараметричних некомутативних групах, з акцентом на узагальнену багатопараметричну 2-групу Сузукі. Цей підхід реагує на прогрес у розвитку квантових комп'ютерів, які можуть становити загрозу для безпеки багатьох відкритих криптосистем, особливо тих, що базуються на проблемах факторизації та дискретного логарифмування, таких як RSA чи ECC. Використання некомутативних груп для створення квантовостійких криптосистем було відомим підходом протягом останніх двох десятиліть.

Нерозв'язна проблема слова, запропонована Вагнером і Магьяриком, використовується в сфері перестановочних груп і є ключовою для розвитку криптосистем. Логарифмічні підписи, введені Магліверасом, представляють собою унікальний тип факторизації, придатний для скінченних груп. Остання версія такої реалізації, відома як MST3, базується на групі Сузукі. Магліверас у 2008 р. представив ліміт LS транзитивності для криптосистеми MST3, а Сваба пізніше запропонував удосконалену версію криптосистеми eMST3. У 2018 р. Т. ван Трунг вніс пропозицію щодо застосування підходу MST3 з використанням міцних аперіодичних логарифмічних підписів для абелевих p -груп. Конг та його колеги провели глибокий аналіз MST3 і відзначили, що через відсутність публікацій про квантову вразливість цього алгоритму він може розглядатися як потенційний кандидат для використання в постквантову епоху.

Основною відмінністю нової системи є використання гомоморфного шифрування для побудови накріттів логарифмічних сигнатур для всіх параметрів групи, що покращує секретність криптосистеми, зокрема на рівні атаки грубої сили.

Ключові слова: MST3; криптосистема; проблема слова; логарифмічний підпис; гомоморфне шифрування; Сузукі 2-група.

Табл. 10. Бібліогр.: 28 назв.

UDC 621.357

New approaches for creating effective combined printed circuit boards on thermally conductive substrates with polyimide dielectrics / V.M. Borshchov, O.M. Listratenko, M.I. Slipchenko, M.A. Protsenko, I.T. Tymchuk, O.V. Kravchenko, I.V. Borshchov // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2023. №215. P. 60 – 68.

New approaches to manufacturing improved combined boards on aluminum bases with various thin polyimide dielectrics, including thermally conductive ones, foiled by copper or aluminum foil have been proposed.

Design and technological solutions and methods for manufacturing combined printed circuit boards on aluminum bases using industrial thin thermally conductive polyimide dielectric films with fluoropolymer coatings with thermal conductivity from 0,12 to 0,46 W/(m·K) have been developed. Design and technological solutions and methods for manufacturing combined printed circuit boards on thermally conductive aluminum bases using adhesive-free copper-polyimide and aluminum-polyimide lacquer foil dielectrics with thermal conductivity of varnish polyimide layers from 0,12 up to 1,0 W/(m·K) and more have been developed.

Main chemical, mechanical, electrical and thermal properties of various types of experimental combined printed circuit boards on aluminum bases with thin polyimide dielectrics for use in electronic modules and printed circuit assemblies (including with using Chip-on-board and Chip-on-flex technologies for assembling) have been studied.

Key words: constructive and technological solutions; combined printed circuit boards on aluminum bases; polyimide composites; quality test structures.

5 fig. Ref: 12 items.

УДК 621.357

Нові підходи для створення ефективних комбінованих друкованих плат на теплопровідних основах з діелектриками з полііміду / В.М. Борщов, О.М. Лістратенко, М.І. Сліпченко, М.А. Проценко, І.Т. Тимчук, О.В. Кравченко, І.В. Борщов // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2023. Вип. 215. С. 60 – 68.

Запропоновано нові підходи для виготовлення вдосконалених комбінованих плат на алюмінієвих основах з різними тонкими поліімідними діелектриками, у тому числі теплопровідними, які вкриті мідною або алюмінієвою фольгою.

Розроблено конструктивно-технологічні рішення та способи виготовлення комбінованих друкованих плат на алюмінієвих основах із застосуванням промислових тонких термозварюваних поліімідних діелектричних плівок з фторполімерними покриттями з теплопровідністю від 0,12 до 0,46 Вт/(м·К). Розроблено конструктивно-технологічні рішення та способи виготовлення комбінованих друкованих плат на теплопровідних алюмінієвих основах із застосуванням безадгезивних мідь-поліімідних та алюміній-поліімідних лакофольгових діелектриків з теплопровідністю лакових поліімідних шарів від 0,12 до 1,0 Вт/(м·К) та більше.

Досліджено основні хімічні, механічні, електричні та теплові властивості різних типів експериментальних комбінованих друкованих плат на алюмінієвих основах з тонкими поліімідними діелектриками для застосування в електронних модулях та друкованих вузлах (у тому числі із використанням Chip-on-board та Chip-on-flex технологій складання).

Ключові слова: конструктивно-технологічні рішення; комбіновані друковані плати на алюмінієвих основах; поліімідні композити; тестові структури якості.

Л. 5. Бібліогр.: 12 назв.

UDC 621.385.64

Comparison of the output spectrum for four models of devices with crossed fields / M.E. Alfeyorov, M.V. Volovenko, I.O. Moshchenko, O.M. Nikitenko // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2023. №215. P. 69 – 76.

This paper considers four models of crossed-field devices: cylindrical magnetron, cylindrical magnetron diode, planar magnetron diode and planar magnetron. As is known, in crossed-field devices electrons move by cycloid-like trajectories and induced current arises. The spectral components of the induced current for every of the models are calculated. It has been found that the components of the induced current spectrum contain from one (planar magnetron diode) to eight (cylindrical magnetron diode) components. The calculated spectral components have been compared to the spectral components of the generation spectrum of the real device.

Only one component whose frequency coincides with the cyclotron frequency was found in the induced current spectrum of the planar magnetron diode.

The induced current spectrum in a planar magnetron has three components. These frequencies have a large difference with the frequency of magnetron generation for a microwave oven. Therefore, the models of the planar magnetron diode and the planar magnetron are not very suitable for simulating the operation of crossed-field devices.

The induced current spectrum in a cylindrical magnetron diode contains eight components. The third harmonic is closest to the fundamental frequency of the microwave magnetron. In this case, the difference between the frequencies being compared is near 10 %. Therefore, the model of a cylindrical magnetron diode is not very suitable for modeling the operation of crossed-fields devices.

Two components were found in the induced current spectrum of a cylindrical magnetron. The first harmonic is the closest to the fundamental frequency of the microwave magnetron. In this case, the difference between the frequencies being compared does not exceed 3 %. Such a small discrepancy between the calculated and real frequencies can be explained by the presence of a spatially periodic distribution of the electrostatic field. Thus, the cylindrical magnetron model is well suited for simulating the operation of crossed-fields devices.

Key words: planar magnetron diode; planar magnetron; spectral component; induced current; cylindrical magnetron diode; cylindrical magnetron.

7 fig. Ref: 11 items.

УДК 621.385.64

Порівняння вихідного спектру для чотирьох моделей приладів зі схрещеними полями / М.С. Алфьоров, М.В. Воловенко, І.О. Моценко, О.М. Нікітенко // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2023. Вип. 215. С. 69 – 76.

Описано чотири моделі пристроїв зі схрещеним полем: циліндричний магнетрон, циліндричний магнетронний діод, площинний магнетронний діод і площинний магнетрон. Як відомо, в приладах зі схрещеним полем електрони рухаються за циклоїдальними траєкторіями і внаслідок цього руху виникає індукований струм. Обчислено спектральні складові індукованого струму для кожної з моделей. Виявлено, що складові спектра індукованого струму містять від однієї (площинний магнетронний діод) до восьми (циліндричний магнетронний діод) складових. Здійснено порівняння обчислених спектральних складових зі спектральними складовими спектру генерації реального приладу.

У спектрі індукованого струму площинного магнетронного діода виявлено лише одну компоненту, частота якою збігається з циклотронною частотою.

Спектр індукованого струму у площинному магнетроні має три компоненти. Ці частоти мають велику різницю з частотою генерації магнетрона для мікрохвильової пічки. Отже, моделі площинного магнетронного діода та магнетрона не дуже добре підходять для моделювання роботи приладів зі схрещеними полями.

Спектр індукованого струму у циліндричному магнетронному діоді містить вісім компонент. Найближчою до основної частоти магнетрона для мікрохвильової пічки є третя гармоніка. У цьому випадку розбіжність між частотами, які порівнюють, становить близько 10 %. Отже, модель циліндричного магнетронного діода не дуже добре підходить для моделювання роботи приладів зі схрещеними полями.

У спектрі індукованого струму циліндричного магнетрона виявлено дві складові. Найближчою до основної частоти магнетрона для мікрохвильової пічки є перша гармоніка. У цьому випадку розбіжність між частотами, які порівнюють, не перевищує 3 %. Таку невеличку розбіжність між обчисленою та реальною частотами можна пояснити наявністю просторово-періодичного розподілу електростатичного поля. Таким чином, модель циліндричного магнетрона добре підходить для моделювання роботи пристроїв зі схрещеними полями.

Ключові слова: площинний магнетронний діод; площинний магнетрон; спектральна складова; індукційний струм; циліндричний магнетронний діод; циліндричний магнетрон.

Л. 7. Бібліогр.: 11 назв.

MICROWAVE ANTENNAS AND DEVICES АНТЕНИ І ПРИСТРОЇ МІКРОХВИЛЬОВОЇ ТЕХНІКИ

UDC 621.396; 004.8

Application of artificial intelligence method in adaptive antenna system / M.V. Rozhnovskiy, I.Yu. Rozhnovska // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2023. №215. P. 77 – 85.

The requirements for adaptive antenna systems in modern and future wireless networks of the fifth (5G) and sixth (6G) generations are analyzed. The block diagram of the adaptive antenna system is presented and the basic principle of its operation is described. It is proposed to improve the block diagram of a modern adaptive antenna system by integrating an artificial intelligence module into it. The principle of interaction of the artificial intelligence module with the adaptive antenna system in the block diagram is shown and described. One of the methods of artificial intelligence (machine learning), the intelligent agent, is described and its mathematical model is presented. The possibility of applying the considered method in the cellular environment of a wireless communication network to improve the operation of an adaptive antenna system is shown. An example of the operation of an artificial intelligence module as part of an adaptive antenna system using an intelligent agent method is given. It is shown that, using the machine learning method, an intelligent agent within a single wireless communication cell can create a certain knowledge system capable of understanding and learning, taking into account the patterns of subscribers' movement within the cell and predicting the direction of movement of a particular subscriber terminal. The resulting knowledge system is formed in an artificial intelligence module, which is included in the block diagram of a modern adaptive antenna system proposed in this paper, and can potentially be used to more accurately control the directional pattern of an adaptive antenna system. The idea proposed in this paper potentially allows us to develop the concept of a smart antenna, as well as to improve the characteristics of adaptive antenna systems, namely, to increase the energy efficiency of these systems by more accurately realizing the directivity characteristics and intelligent control of the radiation pattern petals using artificial intelligence.

Key words: adaptive antenna system; artificial intelligence; intelligent agent; artificial intelligence module.

2 tabl. 6 fig. Ref.: 18 items.

УДК 621.396; 004.8

Застосування методу штучного інтелекту в адаптивній антенній системі / М.В. Рожновський, І.Ю. Рожновська // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2023. Вип. 215. С. 77 – 85.

Проаналізовано вимоги до адаптивних антенних систем у сучасних та майбутніх бездротових мережах п'ятого (5G) та шостого (6G) покоління. Наведено схему адаптивної антенної системи та описано основний принцип її роботи. Запропоновано вдосконалити схему сучасної адаптивної антенної системи шляхом інтеграції в неї модуля штучного інтелекту. Показано на схемі та описано принцип взаємодії модуля штучного інтелекту з адаптивною антенною системою. Описано один з методів штучного інтелекту (машинного навчання) – інтелектуальний агент та приведено його математичну модель. Показано можливість застосування розглянутого методу в середовищі стільника мережі безпроводового зв'язку для покращення роботи адаптивної антенної системи. Наведено приклад роботи модуля штучного інтелекту в складі адаптивної антенної системи з використанням методу штучного інтелекту – інтелектуальний агент. Показано, що за допомогою методу машинного навчання інтелектуальний агент в межах одного стільника безпроводового зв'язку можна створити деяку систему знань, здатну розуміти і навчатися, враховувати закономірності переміщення абонентів в стільнику і прогнозувати напрямок руху конкретного абонентського терміналу. Отримана система знань формується в модулі штучного інтелекту, який входить до запропонованої в даній роботі структурної схеми сучасної адаптивної антенної системи, і потенційно може бути використана для більш точного управління діаграмою спрямованості адаптивної антенної системи. Запропонована в роботі ідея потенційно дозволяє розвинути концепцію розумної антени, а також покращити характеристики адаптивних антенних систем, а саме – збільшити енергоефективність вказаних систем за рахунок більш точної реалізації характеристик направленості та інтелектуального керування пелюстками діаграми спрямованості із застосуванням штучного інтелекту.

Ключові слова: адаптивна антенна система; штучний інтелект; інтелектуальний агент; модуль штучного інтелекту.

Табл. 2. Іл. 6. Бібліогр.: 18 назв.

UDC 662.396.67: 621.314.6

Rectennas of electromagnetic power harvesting systems from the surrounding space / V.O. Alieksieiev, D.V. Gretsikh, D.S. Gavva, V.G. Lykhograi, I.A. Khan // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2023. №215. P. 86 – 105.

Progress in the development of rectenna systems for collecting/harvesting and converting the power of electromagnetic (EM) fields created by radio-electronic means of various classes and purposes into direct current (DC) are considered. The article consists of two parts, each of which highlights important aspects of this topic.

The main parameters of rectennas and the mechanisms of power loss in them are considered in the first part of the article. This allows us to understand the physical and technical limitations that have to be faced in the development of effective EM power harvesting systems.

The second part of the article considers typical schemes of rectennas for use in various applications. Features of the technical implementation of single-band rectennas, options for minimizing their dimensions and the construction of electrically small rectennas based on metasurfaces are given. Schemes of constructions of rectenna arrays and their advantages and disadvantages are also presented. Special attention in the article is paid to multi-band and wide-band rectennas. It is noted that such rectennas can store more energy and produce higher output DC power compared to narrowband rectennas. The design features of low-power rectifiers for rectennas of EM power harvesting systems from the surrounding space are considered.

It was determined that the energy characteristics of rectennas are characterized by numerous factors and there are three approaches to their improvement. The first approach is to improve the parameters of individual rectifier elements, the second is to optimize the parameters of individual rectenna elements and the third is to optimize the entire rectenna as a whole.

Key words: wireless power transmission (WPT); wireless power transmission technologies; wireless power transmission system; power harvesting from the surrounding space; rectenna; radiator; rectification scheme; metasurface.

30 fig. Ref: 78 items.

УДК 662.396.67: 621.314.6

Ректени систем збору електромагнітної енергії з навколишнього простору / В.О. Алексєєв, Д.В. Грецьких, Д.С. Гавва, В.Г. Лихограй, І.А. Хань // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2023. Вип. 215. С. 86 – 105.

Розглянуто досягнення в галузі розробки ректен систем збору та перетворення енергії електромагнітних полів, які створюються радіоелектронними засобами різного класу та призначення, в енергію постійного струму.

У першій частині статті наведено основні параметри ректен та розглянуто механізми втрат потужності у ректенах. Це дозволяє зрозуміти фізичні та технічні обмеження, з якими доводиться зіштовхуватися при розробці ефективних систем збору електромагнітної енергії.

Другу частину присвячено розгляду типових схем побудови ректен для використання їх в різних застосуваннях. Наведено особливості технічної реалізації однодіапазонних ректен, варіанти мінімізації їх габаритних розмірів та побудову електрично малих ректен на основі метаповерхонь. Наведено схеми побудови ректенних

решіток, подано їхні переваги та недоліки. Особливу увагу приділено багатосмуговим та широкосмуговим ректенам. Зазначається, що такі ректени можуть накопичувати більше енергії та виробляти більшу вихідну потужність, порівняно зі вузькосмуговими ректенами. Розглянуто особливості проєктування випрямлячів низької потужності для ректен систем збору електромагнітної енергії з навколишнього простору.

Визначено, що енергетичні характеристики ректен характеризуються численними факторами і є три підходи щодо їх вдосконалення. Перший підхід – поліпшення параметрів окремих випрямних елементів, другий – оптимізація параметрів окремих елементів ректени, третій – оптимізація усєї ректени в цілому.

Ключові слова: безпровідна передача енергії; технологія передачі енергії; система безпровідної передачі енергії; збір енергії з навколишнього простору; ректена; випромінювач; схема випрямлення; метаповерхня.

Лл. 30. Бібліоґр.: 78 назв.

APPLICATION OF RADIO ENGINEERING METHODS ЗАСТОСУВАННЯ МЕТОДІВ РАДІОТЕХНІКИ

UDC 621.865.8 (045)

One way to improve the quality of a medical manipulator for sterile boxes / O.I. Dovnar, V.I. Cherkis, O.M. Zinchenko, O.O. Kadaner // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2023. №215. P. 106 – 113.

Today, the advanced robot-surgeons and medical manipulators are managed by operators. Among the best recognized systems are: Da Vinci, Robodoc, SMR Surgical Versius. Further development of medical robotic surgery field requires new solutions in the engineering and software spheres. The main issues and directions are remote surgical operations online as well as automation of processes in sterile boxes. To overcome such limitations, the system must be of minimal size, but it should not lose its accuracy and power. A large number of solutions are aimed at a specific characteristic: Robodoc (accuracy and automation), Da Vinci (flexibility and remote control), SMR Surgical Versius (modularity and miniaturization). If the system has high accuracy, small dimensions and the possibility of automation, it will significantly accelerate the development of robotic surgery.

This task can be solved by removing all electronic components from the segments of the manipulator. Such a solution is already available in the robot surgeon Da Vinci, but a cable mechanism is used there at the base of the segments, which does not allow automating the process because of a low accuracy. The solution that will ensure sufficient accuracy and allow automating the processes is using a bevel gear inside the segments. In this way, it is possible to reduce significantly the size and to increase the accuracy (enlarging the number and type of motors), as well as to make the system as modular as possible, which in its turn will simplify the repair and maintenance.

A manipulator prototype was developed and printed on the NodeMcu hardware platform. The main functionality corresponds to the task. The dimensions of the prototype are 324x324x620 mm, but at the same time, like Da Vinci's robotic surgeon, 7 degrees of freedom remained. Nema17 motors have been used, the accuracy has increased significantly and reaches more than 0.01mm Automation research is still ongoing, but the vibration rate has been significantly reduced because all the motors are placed separately. Technical solutions will allow automating work in sterile boxes, ensuring maximum reliability.

Key words: manipulator; robot surgeon; sterile boxes; bevel gear; 3d printing.

10 fig. Ref.: 7 items.

УДК 621.865.8 (045)

Один спосіб підвищення якості медичного маніпулятора для стерильних боксів / О.І. Довнар, В.І. Черкіс, О.М. Зінченко, О.О. Каданер // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2023. Вип. 215. С. 106 – 113.

На сьогодні передовими роботами-хірургами та медичними маніпуляторами керують оператори. Найкращими системами визнані: Da Vinci, Robodoc, SMR Surgical Versius. Подальший розвиток галузі медичної роботохірургії потребує нових рішень у інженерній та програмній сферах. Одним з основних питань та напрямлень є віддаленні хірургічні операції в режимі онлайн та автоматизація процесів у стерильних боксах. Для подолання таких обмежень система має бути мінімальних розмірів, але не втратити своєї точності та потужності. Велика кількість рішень спрямована на конкретну характеристику: Robodoc (точність та автоматизація), Da Vinci (гнучкість та віддалене керування), SMR Surgical Versius (модульність та мініатюрність). Якщо система матиме високу точність, невеликі розміри та можливість автоматизації, це значно прискорить розвиток робохірургії.

Поставлена задача може бути вирішена шляхом винесення всіх електронних компонентів із сегментів маніпулятора. Таке рішення вже наявно у робота-хірурга Da Vinci, але там використовується тросовий механізм в основі сегментів, що не дозволяє автоматизувати процес через невисоку точність. Рішенням, котре забезпечить достатню точність та дозволить автоматизувати процеси, є використання конічної передачі всередині сегментів. Таким чином, можна значно зменшити розміри та підвищити точність (збільшити кількість та тип двигунів), а також зробити систему максимально модульною, а це спростить ремонт та обслуговування.

Розроблено та надруковано прототип маніпулятора на апаратній платформі NodeMcu. Основна функціональність відповідає поставленому завданню. Розміри прототипу складають 324x324x620мм, але при цьому, як і у робота-хірурга Da Vinci, лишилось сім ступенів свободи. Були використані двигуни Nema17, точність значно зросла та сягає понад 0,01 мм Дослідження автоматизації ще тривають, але значно знизився показник вібрацій,

оскільки всі двигуни винесені окремо. Технічні рішення дозволять автоматизувати роботу у стерильних боксах, забезпечивши максимальну надійність.

Ключові слова: маніпулятор; робот-хірург; стерильні бокси; конічна передача; 3d друк..

Лл. 10. Бібліогр.: 7 назв.

INFORMATION METHODS OF RADIO ENGINEERING, SIGNAL PROCESSING ІНФОРМАЦІЙНІ МЕТОДИ РАДІОТЕХНІКИ, ОБРОБКА СИГНАЛІВ

UDC 615.472.03

Analysis of the frequency-time structure of acoustic noises of unmanned aerial vehicles in the STM32 CubeIDE environment / V.I. Leonidov, V.V. Semenets, A.B. Grigoriev // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2023. №215. P. 114 – 121.

The formulation of the task of detecting small unmanned aerial vehicles (drones) is presented, the expediency of building a drone detection system in the stm32 cubeide environment based on the principle of reception and analysis of acoustic signals emitted by drones during their flight mission is substantiated.

The study of temporal fluctuations in the period of acoustic signals of a drone is carried out by the method of model-correlation analysis, as a result of which three-dimensional structures are formed: time – period – correlation coefficient of the acoustic signal with the model in the form of a time-limited sinusoidal function.

The resulting structures are formed as matrices of correlation coefficient values.

The members located along the columns are calculated by time shifting the model function along the signal sample. The members in each column are calculated with a constant period of the model function given from a series of values.

It is shown that the correlation coefficients between the rows of the matrices calculated from drone signals are significantly higher than the same values obtained from background noise measurements. The functions showing the change in time of the correlation coefficients between the rows of the time-period matrix structures for drone signals and background noise do not overlap and show a consistently larger difference in correlation coefficients, which allows us to use the correlation coefficient as a feature that classifies the presence of drone signals.

Key words: unmanned aerial vehicle; acoustic noise; correlation analysis; signal model; sign; microcontroller.

10 fig. Ref: 18 items.

УДК 615.472.03

Аналіз частотно-часової структури акустичних шумів безпілотних літальних апаратів в середовищі STM32 CubeIDE / В.І. Леонідов, В.В. Семенець, О.В. Григор'єв // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2023. Вип. 215. С. 114 – 121.

Наведено постановку задачі виявлення малих безпілотних літальних апаратів (дронів), обґрунтовано доцільність побудови системи виявлення дронів в середовищі stm32 cubeide на принципі прийому й аналізу акустичних сигналів, що випромінюються дронами під час виконання ними польотного завдання.

Дослідження часових флуктуацій періоду акустичних сигналів дрона проводиться методом модельно-кореляційного аналізу, у результаті якого формуються тривимірні структури: час – період – коефіцієнт кореляції акустичного сигналу з моделлю у вигляді обмеженої в часі синусоїдальної функції.

Отримані структури формуються у вигляді матриць значень коефіцієнта кореляції.

Члени, які розташовуються уздовж стовпців, розраховані при часовому зрушенні модельної функції уздовж вибірки сигналу. Члени в кожному стовпці розраховані при постійному, заданому з ряду значень, періоді модельної функції.

Показано, що коефіцієнти кореляції між рядками матриць, розрахованих по сигналах дрона, значно більші, ніж ті ж значення, що отримані по вимірах фонового шуму. Функції, що показують зміну в часі коефіцієнтів кореляції між рядками матриць структур час – період для сигналів дрона та фонового шуму, не перетинаються й показують стабільно більшу різницю коефіцієнтів кореляції, що дозволяє використати коефіцієнт кореляції як ознаку, що класифікує наявність сигналів від дрона.

Ключові слова: безпілотний літальний апарат; акустичний шум; кореляційний аналіз; модель сигналу; ознака; мікроконтролер.

Лл. 10. Бібліогр.: 18 назв.

UDC 621.396.96

Method for improving the quality of service of request signals in information systems / I.V. Syvd, D.O. Sukhorukov, O.V. Korotich, T.S. Machonis // Radiotekhnika : All-Ukr. Sci. Interdep. Mag. 2023. №215. P. 122 – 127.

The work notes that the request information systems are an important component of information support for air traffic control and airspace control systems. Interrogative information systems include: secondary radar systems, national identification radar systems and short-range navigation radio systems. It is shown that the characteristics of the process of servicing request signals in an aircraft transponder have a significant impact on the statistical properties of the response signal flow, which ultimately, as a consequence, affects the efficiency of the entire radar channel for

transmitting response signals with an active response. It is pointed out that one of the important characteristics of the process of servicing request signals in an aircraft transponder is its correlation function, based on the analysis of which one can conclude the choice of the type of response signal flow and the structure of the aircraft transponder. This makes it possible to achieve: increasing the probability of service, increasing the probability of detecting an air object, reducing the root-mean-square error in estimating the azimuth of an air object and increasing the reliability of the transmission of flight information from the observed board of an air object. The article analyzes the possibility of improving the quality of request service by managing the flow of request signals in a network of request information systems. It has been shown that the correct choice of repetition periods of request signals in the area of joint operation of request information systems makes it possible to reduce the likelihood of interaction between individual request signals. Also, as a consequence, it makes it possible to increase the noise immunity of the interrogative information systems under consideration that are part of the specified information system.

Key words: information system; radar system; questioning system; request signals; independence of signal flows; aircraft defendant; method; quality; signal flow; improvement of quality.

Ref: 21 items.

УДК 621.396.96

Метод підвищення якості обслуговування сигналів запиту в інформаційних системах / І.В. Свид, Д.О. Сухоруков, О.В. Коротіч, Т.С. Мачоніс // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2023. Вип. 215. С. 122 – 127.

Зазначено, що запитальні інформаційні системи є важливою складовою інформаційного забезпечення управління повітряного руху і системи контролю повітряного простору. До запитальних інформаційних систем відносяться: системи вторинної радіолокації, системи радіолокаційної ідентифікації державної приналежності та радіосистеми ближньої навігації. Показано, що характеристики процесу обслуговування сигналів запиту в літаковому відповідачі істотно впливають на статистичні властивості потоку сигналу відповіді, що, в підсумку, як наслідок, впливає на ефективність роботи всього радіолокаційного каналу передачі сигналів відповіді з активною відповіддю. Зазначено, що однією з важливих характеристик процесу обслуговування сигналів запиту в літаковому відповідачі є його кореляційна функція, на основі аналізу якої можливо зробити висновок щодо вибору типу потоку сигналів відповіді та структури літакового відповідача. Це дозволяє досягти: підвищення ймовірності обслуговування, збільшення ймовірності виявлення повітряного об'єкта, зменшення середньоквадратичної помилки оцінки азимуту повітряного об'єкта та підвищення достовірності передачі польотної інформації з борта повітряного об'єкта, що спостерігається. В статті проаналізовано можливість підвищення якості обслуговування сигналів запиту за рахунок управління потоками сигналів запиту в мережі запитальних інформаційних систем. Показано, що правильний вибір періодів повторення сигналів запиту в районі спільної дії запитальних інформаційних систем дозволяє зменшити ймовірність взаємодії окремих сигналів запиту і, як наслідок, підвищити завадостійкість запитальних інформаційних систем, що входять до зазначеної інформаційної системи.

Ключові слова: інформаційна система; радіолокаційна система; запитальна система; сигнали запиту; незалежність потоків сигналів; літаковий відповідач; метод; якість; потік сигналів; підвищення якості.

Бібліогр.: 21 назв.

COLLECTION OF SCIENTIFIC PAPERS
RADIOTEKHNIKA
Issue 215
In English and Ukrainian

ЗБІРНИК НАУКОВИХ ПРАЦЬ
РАДІОТЕХНІКА
Випуск 215
Англійською та українською мовами

Коректор Л.І. Сащенко

Підп. до друку 30.12.2023. Формат 60x90/8. Папір офсет. Гарнітура Таймс. Друк. ризограф.
Ум. друк. арк. 9,8. Обл.-вид. арк. 8,9 Тираж 300 прим. Зам. № 576. Ціна договір.

Харківський національний університет радіоелектроніки (ХНУРЕ)
Просп. Науки, 14, Харків, 61166.

Оригінал-макет підготовлено і збірник надруковано у ПФ „Колегіум”,
Свідоцтво про внесення суб’єкта видавничої діяльності до Державного реєстру видавців.
Сер. ДК №1722 від 23.03.2004.