Інститут кібернетики імені В. М. Глушкова
Національної академії наук України
Кам’янець-Подільський національний університет
імені Івана Огієнка

# МАТЕМАТИЧНЕ ТА КОМП’ЮТЕРНЕ МОДЕЛЮВАННЯ

**Серія: Технічні науки**

Збірник наукових праць

**Випуск 19**

Кам’янець-Подільський національний університет
імені Івана Огієнка
2019

УДК 004.94:53.072
ББК 30
М34

Свідоцтво про державну реєстрацію друкованого засобу масової інформації:
Серія КВ № 14522-3493Р від 25.06.2008 р.

Збірник наукових праць включено до Переліку наукових фахових видань ДАК Міністерства освіти і науки України з технічних наук (наказ №1021 від 07 жовтня 2015 р.)

Друкується згідно з рішенням вченої ради Кам'янець-Подільського національного університету імені Івана Огієнка, протокол № 6 від 23 травня 2019 року.

**Рецензенти:**

**І. В. Бейко,** доктор технічних наук, професор, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»;

**Р. Н. Квєтний,** доктор технічних наук, професор, завідувач кафедри Вінницького національного технічного університету.

**Редакційна колегія:**

**О. М. Хіміч,** член-кореспондент НАНУ, доктор фізико-математичних наук, професор (*відповідальний редактор*);
**А. Ф. Верлань,** член-кореспондент НАПНУ, доктор технічних наук, професор (*заст. відповідального редактор*а);
**В. А. Федорчук,** доктор технічних наук, професор (*відповідальний секретар*);
**Т. Бокалруд,** доктор філософії, професор, Норвегія;
**В. П. Боюн,** член-кореспондент НАНУ, доктор технічних наук, професор;
**В. В. Васильєв,** член-кореспондент НАНУ, доктор технічних наук, професор;
**А. А. Верлань,** доктор філософії, професор, Норвегія;
**В. К. Задірака,** академік НАНУ, доктор фізико-математичних наук, професор;
**І. М. Конет,** доктор фізико-математичних наук, професор;
**Б. Б. Нестеренко,** доктор технічних наук, професор;
**С. А. Положаєнко,** доктор технічних наук, професор.

**М34** **Математичне та комп'ютерне моделювання. Серія: Технічні науки** : зб. наук. праць / Інститут кібернетики імені В. М. Глушкова Національної академії наук України, Кам'янець-Подільський національний університет імені Івана Огієнка ; [редкол.: О. М. Хіміч (відп. ред.) та ін.]. — Кам'янець-Подільський : Кам'янець-Подільський національний університет імені Івана Огієнка, 2019. — Вип. 19. — 160 с.

У збірнику друкуються результати досліджень, що стосуються проблем застосування математичних моделей у різних галузях людської діяльності.

Збірник включений до бази даних наукових журналів Норвегії.

Для наукових та інженерно-технічних працівників, докторантів, аспірантів, студентів вищих навчальних закладів.

УДК 004.94:53.072
ББК 30

© Інститут кібернетики імені В. М. Глушкова НАН України, 2019
© Кам'янець-Подільський національний університет імені Івана Огієнка, 2019

**ISSN 2308-5916**
**DOI: 10.32626/2308-5916.2019-19**

V. M. Glushkov Institute of Cybernetics
of National Academy of Sciences of Ukraine
Kamianets-Podilskyi National Ivan Ohiienko University

# MATHEMATICAL AND COMPUTER MODELLING

**Series: Technical sciences**

Scientific journal

**ISSUE 19**

Kamianets-Podilskyi National Ivan Ohiienko University
2019

**Critics:**

**I. Beyko,** Doctor of Technical Science, Professor,
National Technical University of Ukraine
«Igor Sikorsky Kyiv Polytechnic Institute»;
**R. Kvyetnyy,** Doctor of Technical Science, Professor,
Head of department Vinnytsia national technical university.

**Editorial board:**

**O. Himich,** Corresponding Member of the NAS of Ukraine, Doctor of Physical and Mathematical Sciences, Professor (*Executive Editor*);
**A. F. Verlan,** Corresponding Member of the NAPS of Ukraine, Doctor of Technical Science, Professor (*Vice Executive Editor*);
**V. Fedorchuk,** Doctor of Technical Science, Professor (*Responsible Secretary*);
**T. Bokalrud,** Associate Professor, Norway;
**V. Boyun,** Corresponding Member of the NAS of Ukraine, Doctor of Technical Science, Professor;
**I. Konet,** Doctor of Physical and Mathematical Sciences, Professor;
**B. Nesterenko,** Doctor of Technical Science, Professor;
**S. Polozhaenko,** Doctor of Technical Science, Professor;
**V. Vasiliev,** Corresponding Member of the NAS of Ukraine, Doctor of Technical Science, Professor;
**A. A. Verlan,** Ph. D., Professor, Norway;
**V. Zadiraka,** Academician of the NAS of Ukraine, Doctor of Physical and Mathematical Sciences, Professor.

**Mathematical and computer modelling. Series: Technical sciences:** scientific journal / V. M. Glushkov Institute of Cybernetics of the National Academy of Sciences of Ukraine, Kamianets-Podilskyi National Ivan Ohiienko University ; [Editorial Board: O. Himich (Executive Editor) and others]. — Kamianets-Podilskyi : Kamianets-Podilskyi National Ivan Ohiienko University, 2019. — ISSUE 19. — 160 p.

The journal publishes results of studies on the mathematical models' application problems in various areas of human activity.

Joint with NTNU the journal has been included to the database of Norwegian Register for Scientific Journals, Series and Publishers.

Intended for scientific and engineering staff, researchers, undergraduate, graduate and Ph. D. students, post-graduates.

© V. M. Glushkov Institute of Cybernetics of NAS of Ukraine, 2019
© Kamianets-Podilskyi National Ivan Ohiienko University, 2019

**ISSN 2308-5916**
**DOI: 10.32626/2308-5916.2019-19**

УДК 517.9:519.6
DOI: 10.32626/2308-5916.2019-19.5-10

**В. А. Богаєнко,** канд. техн. наук,
**В. М. Булавацький,** д-р техн. наук,
**А. В. Гладкий,** д-р фіз.-мат. наук
Інститут кібернетики імені В. М. Глушкова НАН України, м. Київ

# ІДЕНТИФІКАЦІЯ ПАРАМЕТРІВ ОДНІЄЇ ДРОБОВО-ДИФЕРЕНЦІАЛЬНОЇ МОДЕЛІ МІГРАЦІЇ РОЗЧИННИХ РЕЧОВИН

Розглядається задача ідентифікації параметрів моделі у випадку математичного моделювання дробово-диференціальної динаміки аномального процесу конвективної дифузії розчинних речовин при профільній усталеній фільтрації ґрунтових вод з вільною поверхнею. При цьому, процес масопереносу описується моделлю, що містить узагальнену похідну дробового порядку Капуто–Герасимова за часовою змінною, а процес фільтрації розглядається у потенціальному полі швидкостей. Оскільки область фільтрації є областю з частково невідомою межею, розв’язання поставленої задачі виконується шляхом попереднього переходу до області комплексного потенціалу при відомій характеристичній функції течії. Ставиться задача ідентифікації значень параметрів узагальненої дробової похідної, виходячи з вимірів концентрації речовини. Такий підхід дозволяє більш адекватно описувати процеси масопереносу в середовищах із складною просторово-часовою структурою, у тому числі в ґрунтах у ситуації істотної затратності їх точного геофізичного аналізу. З огляду на складність вирішення обернених задач для диференціальних рівнянь з дробовими похідними, фіксовану кількість і неперервність параметрів, що визначаються, пропонується використовувати для їх ідентифікації метаевристичний алгоритм рою частинок. В роботі стисло викладена скінченно-різницева методика наближеного розв'язання прямої задачі, наведена постановка задачі ідентифікації параметрів, описана використовувана варіація алгоритму рою частинок. Наведено результати комп'ютерних експериментів, які показують ефективність алгоритму рою частинок для визначення параметрів похідної дробового порядку, а також те, що в залежності від вигляду функціонального параметра узагальненої дробової похідної, модель дозволяє описувати як «надповільні», так й «надшвидкі» дифузійні режими.

**Ключові слова:** *динаміка аномальних конвективно-дифузійних процесів, усталена профільна фільтрація ґрунтових вод, дробово-диференціальні математичні моделі перене-*

© В. А. Богаєнко, В. М. Булавацький, А. В. Гладкий, 2019

*сення, узагальнена похідна Капуто–Герасимова, ідентифікація параметрів моделі, метод рою частинок.*

**Вступ.** Відомо, що ефективні методи визначення параметрів технологічних процесів промивання ґрунтів і очищення засолених ґрунтових вод, а також вод, забруднених промисловими або побутовими стоками, базуються на використанні методів математичного моделювання [1–3]. У випадку складної просторово-часової структури середовища мають місце нелокальні процеси перенесення, що досить адекватно описуються дробово-диференціальними математичними моделями [4–7]. При цьому особливої актуальності набуває розробка комп'ютерних методів ідентифікації параметрів моделі.

У роботі з цією метою пропонується використання метаевристичного алгоритму рою частинок [8].

**Математична модель і чисельний метод розв'язання крайової задачі.** Розглянемо задачу моделювання динаміки аномального процесу конвективної дифузії домішок у випадку плоско-вертикальної усталеної фільтрації з вільною поверхнею з річок, каналів чи накопичувачів промислових стоків [7]. Математична модель процесу поширення забруднень описується наступною крайовою задачею:

$$\sigma D_{t,g}^{(\beta)} C = \frac{\partial}{\partial x}\left( D \frac{\partial C}{\partial x} \right) + \frac{\partial}{\partial y}\left( D \frac{\partial C}{\partial y} \right) - \upsilon_x \frac{\partial C}{\partial x} - \upsilon_y \frac{\partial C}{\partial y}, \qquad (1)$$

$$C\,|_{AC} = C_0,\ \frac{\partial C}{\partial n}\,|_{AB,\,CB} = 0,\ C\,|_{t=0} = 0, \qquad (2)$$

де $C(x, y, t)$ — концентрація речовини, $\sigma$ — пористість середовища, $\upsilon = (\upsilon_x, \upsilon_y)$ — швидкість фільтрації, $D(x, y)$ — коефіцієнт конвективної дифузії, $D_{t,g}^{(\beta)} C$ — похідна Капуто–Герасимова по змінній $t$ порядку $\beta\,(0 < \beta < 1)$ від функції $C$ за функцією $g$ [9], $C_0$ — концентрація на вході фільтраційного потоку $AC$, $n$ — зовнішня нормаль, $AB$ — вісь симетрії потоку, $CB$ — крива депресії [5].

Оскільки область фільтрації $G_z$ є областю з частково невідомою межею, розв'язок задачі (1), (2) будемо шукати в області комплексного потенціалу течії $G_\omega = \{(\varphi, \psi) : 0 < \varphi < +\infty,\ 0 < \psi < Q\}$ [5]. Тоді, крайова задача (1), (2) приймає вигляд

$$\sigma D_{t,g}^{(\beta)} C(\varphi, \psi, t) = \upsilon^2(\varphi, \psi)\left[ \frac{\partial}{\partial \varphi}\left( D \frac{\partial C}{\partial \varphi} \right) + \frac{\partial}{\partial \psi}\left( D \frac{\partial C}{\partial \psi} \right) - \frac{\partial C}{\partial \varphi} \right], \qquad (3)$$

$$((\varphi, \psi, t) \in G_\omega \times (0, +\infty)),$$

$$C\mid_{\varphi=0}= C_0,\ \frac{\partial C}{\partial \psi}\mid_{\psi=0,\,\psi=Q}= 0,\ C\mid_{t=0}= 0\ , \qquad (4)$$

де $\upsilon^2(\varphi,\psi)$ — відома функція, що визначається згідно [5, 10].

Ефективний чисельний метод розв'язання крайової задачі (3), (4) базується на використанні локально-одновимірної різницевої схеми [11] із відповідними граничними умовами:

$$\frac{\sigma}{2}\Delta_t^{(\beta)}C^{\,j+1/2} = \upsilon^2\left((aC_{\bar{\varphi}}^{\,j+1/2})_{\varphi} - C_{\overset{0}{\varphi}}^{\,j+1/2}\right),$$

$$\frac{\sigma}{2}\Delta_t^{(\beta)}C^{\,j+1} = \upsilon^2\left(aC_{\bar{\psi}}^{\,j+1}\right)_{\psi},$$

де $C$ — сіткова функція і використовуються загальноприйняті позначення теорії різницевих схем [11], $\Delta_t^{(\beta)}C$ — різницевий аналог похідної $D_{t,g}^{(\beta)}C$ [7].

Після отримання розв'язку задачі в області комплексного потенціалу, перехід у фізичну область здійснюється згідно [10].

**Задача ідентифікації параметрів і метод її розв'язання.** Подаючи пробну функцію $g(t)$ у визначенні дробової похідної Капуто–Герасимова в степеневому вигляді $g(t) = t^{\gamma}$, задачу ідентифікації параметрів $\beta, \gamma$ сформулюємо так.

Нехай відомі значення концентрації $C_i$, $i = 1,...,N$ в моменти часу $T_i$ в точках $(x_i, y_i)$.

Необхідно знайти значення параметрів $\beta, \gamma$, які мінімізують

$$F(C) = \sum_{i=1}^{N}\left(C(x_i, y_i, T_i) - C_i\right)^2,$$

де $C(x,y,t)$ — розв'язок крайової задачі (1), (2).

Враховуючи складність задачі, фіксовану кількість і неперервність параметрів, що визначаються, пропонується розв'язувати її метаевристичним алгоритмом рою частинок [8], який коротко може бути описаним наступним чином:

- позначимо як $S$ кількість частинок в рої; $\xi_k$, $k = 1,...,S$ — координати частинки $k$, значення яких відповідають значенням параметрів, що визначаються; $v_k$ — швидкість частинки $k$; $p_k$ — координати частинки $k$, для яких отримано мінімальне значення цільової функції $F(C)$; $\eta$ — координати, для яких отримано мінімальне значення цільової функції серед усіх частинок рою; $\omega, \varphi_p, \varphi_g$ — параметри алгоритму;

- на стадії ініціалізації початкові координати частинок генеруються випадковим чином, беручи до уваги обмеження щодо значень параметрів, що визначаються. Швидкості приймаються рівними нулю;
- поки не досягнуто заданого максимального числа ітерацій $N_m$, виконується умова $\eta > \varepsilon_1$, де $\varepsilon_1$ — задана константа, а різниця між найбільшим і найменшим значеннями цільової функції для частинок рою перевищує задане число $\varepsilon_2$, на ітерації $j$ алгоритму для кожної частинки $k$
- генеруються випадкові значення $r_p, r_g \in [0,1]$;
- модифікується швидкість:
$$v_k^{(j+1)} = \omega \cdot v_k^{(j)} + \varphi_p r_p (p_k^{(j)} - \xi_k^{(j)}) + \varphi_g r_g (\eta^{(j)} - \xi_k^{(j)});$$
- модифікуються координати частинки: $\xi_k^{(j+1)} = \xi_k^{(j)} + v_k^{(j)}$;
- обчислюється значення цільової функції й оновлюється $p_k$ та $\eta$.

**Обчислювальний експеримент** з ідентифікації параметрів моделі (1), (2) здійснювався наступним чином. Значення концентрації $C_i$, які використовувались для ідентифікації параметрів $\beta, \gamma$ дробової похідної при $g(t) = t^\gamma$, були отримані з розв'язку [7] прямої задачі (1), (2) для $t = 0.4$ при $\beta = 0.84, \gamma = 0.9$ і $\gamma = 1.0$ в точках (6.026, 3.151), (6.126, 5.502), (6.024, 7.940), що відповідають вузлам сітки (10, 28), (11, 21) і (12, 16). Параметри методу рою частинок приймалися наступними: $S = 20$, $\omega = \varphi_p = \varphi_g = 0.2$, $N_m = 25$, $\varepsilon_1 = 10^{-14}$, $\varepsilon_2 = 10^{-12}$, $\beta \in [0.8,1]$, $\gamma \in [0.1,1.9]$. Отримані результати ідентифікації параметрів для випадків, коли здійснювався пошук як обох параметрів $\beta, \gamma$, так і тільки порядку похідної $\beta$, наведені в таблиці.

Таблиця

*Результати ідентифікації параметрів моделі*

| $x$ | $y$ | $C_i$ отримані при $\beta = 0.84$, $\gamma = 0.9$ | | | $C_i$ отримані при $\beta = 0.84$, $\gamma = 1.0$ | | |
|---|---|---|---|---|---|---|---|
| | | $C_i$ | Пошук $\beta$ при $\gamma = 1.0$: $\beta = 0.96$ | Пошук $\beta, \gamma$: $\beta = 0.835$ $\gamma = 0.904$ | $C_i$ | Пошук $\beta$ при $\gamma = 1.0$: $\beta = 0.96$ | Пошук $\beta, \gamma$: $\beta = 0.86$ $\gamma = 0.96$ |
| 6.026 | 3.151 | 7.98e-2 | 8.00e-2 | 7.97e-2 | 5.70e-2 | 5.69e-2 | 5.69e-2 |
| 6.126 | 5.502 | 7.77e-4 | 5.14e-4 | 6.30e-4 | 4.60e-4 | 4.79e-4 | 4.42e-4 |
| 6.024 | 7.940 | 6.71e-5 | 3.96e-5 | 5.13e-5 | 3.79e-5 | 4.00e-5 | 3.61e-5 |

Продовження таблиці

| | | | | | | |
|---|---|---|---|---|---|---|
| Значення цільової функції $F(C)$ | – | 9.90e-8 | 3.18e-8 | – | 4.13e-10 | 6.44e-10 |
| Середня відносна похибка | – | 24.9 % | 14.1 % | – | 3.2 % | 2.8 % |

Отримані результати ідентифікації параметрів розглядуваної моделі демонструють адекватність запропонованої методики. У випадку, коли методом рою частинок відбувається пошук $\beta$ при фіксованому $\gamma = 1.0$, що не відповідає значенню $\gamma = 0.9$, при якому були отримані значення $C_i$, знайдене значення $\beta$ істотно відрізняється від вихідного. Мінімальне знайдене значення цільової функції і середня відносна похибка в цьому випадку в ~ 2 рази вище, ніж при пошуку обох параметрів розглядуваної дробової похідної. Це показує некоректність опису за допомогою класичної похідної Капуто–Герасимова динаміки процесу, аналогічного представленому крайовою задачею (1), (2).

При збільшенні кількості параметрів, що ідентифікуються, якість отриманого розв'язку погіршується при незмінних значеннях параметрів алгоритму рою частинок.

**Висновки.** Таким чином, для адаптації моделі до реальних умов, значення її параметрів можуть бути ідентифіковані на основі вимірів концентрації речовини методом рою частинок. Проведені обчислювальні експерименти підтверджують на прикладі модельної задачі ефективність даного алгоритму для визначення параметрів похідних дробового порядку в дробово-диференціальних моделях перенесення.

**Список використаних джерел:**


1. Гладкий А. В., Ляшко И. И., Мистецкий Г. Е. Алгоритмизация и численный расчёт фильтрационных схем. Киев : Вища школа, 1981. 288 с.
2. Ляшко И. И., Демченко Л. И., Мистецкий Г. Е. Численное решение задач тепло- и массопереноса в пористых средах. Киев : Наукова думка, 1991. 264 с.
3. Мистецкий Г. Е. Гидростроительство. Автоматизация расчета массопереноса в почвогрунтах. Киев : Будівельник, 1985. 136 с.
4. Kilbas A. A., Srivastava H. M., Trujillo J. J. Theory and applications of fractional differential equations. Amsterdam : Elsevier, 2006. 523 p.
5. Bulavatsky V. M. Mathematical modeling of dynamics of the process of filtration convection diffusion under the condition of time nonlocality. *Journal of Automation and Information Science.* 2012. 44, N 2. P. 13–22.
6. Булавацкий В. М., Кривонос Ю. Г. Математические модели с функцией контроля для исследования дробно-дифференциальной динамики геомиграционных процессов. *Проблемы управления и информатики.* 2014. № 3. С. 138–147.

7. Богаенко В. А., Булавацкий В. М. Компьютерное моделирование динамики процесса миграции растворимых веществ при фильтрации грунтовых вод со свободной поверхностью на основе дробно-дифференциального подхода. *Доповіді НАНУ.* 2018. № 12. С. 21–29.
8. Zhang Y. A. Comprehensive Survey on Particle Swarm Optimization Algorithm and Its Applications. *Mathematical Problems in Engineering.* 2015. 931256.
9. Almeida R. A. Caputo fractional derivative of a function with respect to another function. *Communications in Nonlinear Science and Numerical Simulation.* 2017. № 44. P. 460–481.
10. Полубаринова-Кочина П. Я. Теория движения грунтовых вод. М. : Наука, 1977. 664 с.
11. Самарський А. А., Вабищевич П. Н. Вычислительная теплопередача. М. : Едиториал УРСС. 2003. 784 с.

## IDENTIFICATION OF PARAMETERS OF ONE FRACTIONAL MODEL OF SOLUBLE SUBSTANCES MIGRATION

The paper deals with the problem of identification of model parameters in the case of mathematical modeling of fractional-differential dynamics of anomalous process of convective diffusion of soluble substances under steady-state profile groundwater filtration with a free surface. We describe the process of mass transfer using a model containing a generalized fractional derivative of Caputo-Gerasimov with respect to the time variable while the filtration process is considered in the potential velocity field. Since the filtration domain is a domain with a partially unknown boundary, the solution of the problem is performed using an anticipatory transition to a completely determined complex potential domain with a known characteristic flow function. We pose the problem of identification of the values of the parameters of a generalized fractional derivative based on the measurements of substance concentration. Such an approach allows us to more adequately describe the processes of mass transfer in environments with a complex spatial and temporal structure, including soils, in the situation of significant costs needed for their exact geophysical analysis. Taking into account the complexity of the solution of inverse problems for differential equations with fractional derivatives, the fixed quantity and continuity of optimized parameters, it is proposed to use a meta-heuristic particle swarm optimization algorithm for their identification. The paper briefly describes the finite-difference method of the approximate solution of the direct problem, poses the problem of parameters identification, and describes the modification of the used particle swarm optimization algorithm. We present the results of computer experiments that show the efficiency of the particle swarm optimization algorithm for determining the parameters of the fractional derivative, as well as the fact that, depending on the type of functional parameter of the generalized fractional derivative, the model allows describing both «ultra-slow» and «ultra-fast» diffusion modes.

**Key words:** *anomalous convective-diffusion processes dynamics, steady-state profile groundwater filtration, fractional differential mathematical models, generalized Caputo-Gerasimov derivative, identification of parameters, particle swarm optimization.*

Одержано 04.02.2019

UDC 519.6
DOI: 10.32626/2308-5916.2019-19.11-17

**A. Ya. Bomba**, Doct. of Techn. Sciences,
**M. V. Boichura**
Rivne State Humanitarian University, Rivne

# NUMERICAL COMPLEX ANALYSIS METHOD FOR PARAMETERS IDENTIFICATION OF ANISOTROPIC MEDIA USING APPLIED QUASIPOTENTIAL TOMOGRAPHIC DATA. PART 2: ALGORITHM AND NUMERICAL EXPERIMENT

An algorithm, which lies in the sequential iterative applying of numerical quasiconformal mapping methods for constructing a series of dynamic meshes using different boundary conditions (that determined by experimental data) and solving the problem of parameter identification for each of these meshes is developed. It is based on the proposed approach to the solving of gradient problems of parameters identification of quasiideal fields with using applied quasipotential tomographic data in cases of anisotropic media and applying the ideas of the block iteration method. The reconstructed image of the distribution of conductivity tensor inside the investigated object, obtained as a result of numerical calculations performed on the basis of the developed algorithm with a sufficient accuracy corresponds to the etalon. The method is characterized by comparatively fast computer convergence (since, unlike many used methods, it does not require finding derivatives of the conductivity tensor distribution function at certain points and refining the boundary nodes at each iteration step). Its significant feature is the possibility of comparatively easy its paralleling and stopping the calculation procedure when some conditions for finishing the process are complete with simultaneous automatic determination the areas of the physical domain where have place large errors of the calculations, which makes it possible to use the machine time more economically. The algorithm for image reconstruction could be extended not only for the medium with a known sum of eigenvalues of the conductivity tensor, but also to cases of other rather wide dependencies between them. In particular, this approach provides an opportunity to represent it as some complex function as required by biomedical practice.

**Key words**: *applied Quasipotential Tomography, Quasiconformal Mappings, Anisotropy, Identification, Nonlinear Problems.*

**Introduction.** In the paper [1], the approach to the solving of gradient problems of parameters identification of quasiideal fields with using applied quasipotential tomographic data based on numerical complex analysis methods is transferred to cases of anisotropic media. In this, the

© A. Ya. Bomba, M. V. Boichura, 2019 

additional information about the nature of the conductivity distribution inside the domain (research object) is considered a priori known. However, in opposite to the traditional approaches to the statement and solving the problems of electrical impedance tomography, here set the local velocities distribution of a substance (liquid, current) in addition to the averaged potential at the contact sections of plate and body and at other sections (stream lines) here set the potential distribution (according to experimental data). Generation of initial data at the boundary of the investigated object is carried out in accordance with the polar model of current injection when eigenvalues sum of the conductivity tensor (CT) of the media is given. The corresponding problem is reduced to the iterative solving of a series of problems for Laplace type equations, where instead of «boundary numerical analogues of the Cauchy–Riemann type equations» appear the ratio of quasiorthogonality with using special types of optimization conditions. This work is devoted to the construction of an appropriate algorithm and conducting computer experiments.

**The algorithm.** Algorithm for solving the input problem lies in rotational parametrization of internal nodes of the mesh domains $G_z^{\gamma(p)}$, CT and using an ideas of block iteration method [5, 6]. In particular: we set the number of injections $\tilde{p}$, bound of domains $G_z^{(p)}$ (by the functions $x = \tilde{x}(\tau)$, $y = \tilde{y}(\tau)$), parameters $\tau_A^{(p)}$, $\tau_B^{(p)}$, $\tau_C^{(p)}$, $\tau_D^{(p)}$ and $\varepsilon_1$, $\varepsilon_2$ (of accuracy), $q$ ($q > 1$ is responsible for the number of iterations for correct of internal nodes having specific CT), quasipotentials $\varphi_*^{(p)}$, $\varphi^{*(p)}$ and discharges $Q^{(p)}$, parameters $m^{(p)}$, $n^{(p)}$ of $G_\omega^{\gamma(p)}$ partition (it is desirable to select this values so that $\dfrac{Q^{(p)}}{\varphi^{*(p)} - \varphi_*^{(p)}} \dfrac{m^{(p)}+1}{n^{(p)}+1} \approx 1$ in order to improve the accuracy of the calculations) [3, 5], constants of functional (18) [1] $\mu$ and $\eta$, distribution of the eigenvalues sum $\lambda = \lambda(x, y)$ and parameters $\alpha_k$ ($1 \le k \le 4$) for inequalities-restrictions (19) [1]. Along with this we calculate the coordinates of the angular points $A_p = \left(\tilde{x}(\tau_A^{(p)}), \tilde{y}(\tau_A^{(p)})\right)$, $B_p = \left(\tilde{x}(\tau_B^{(p)}), \tilde{y}(\tau_B^{(p)})\right)$, $C_p = \left(\tilde{x}(\tau_C^{(p)}), \tilde{y}(\tau_C^{(p)})\right)$, $C_p = \left(\tilde{x}(\tau_C^{(p)}), \tilde{y}(\tau_C^{(p)})\right)$, $D_p = \left(\tilde{x}(\tau_D^{(p)}), \tilde{y}(\tau_D^{(p)})\right)$ on $\partial G_z^{(p)}$, $\Delta\varphi^{(p)} = (\varphi^{*(p)} - \varphi_*^{(p)}) / (m^{(p)} + 1)$, $\Delta\psi^{(p)} = Q^{(p)} / (n^{(p)} + 1)$ and values of quasiconformal invariants $\gamma^{(p)} = \Delta\varphi^{(p)} / \Delta\psi^{(p)}$.

Then we set the values of local velocities $\Psi_{*j}^{(p)}$, $\Psi_j^{(p)}$ (and therefore, stream functions $\psi_{*j}^{(p)}$, $\psi_j^{*(p)}$) and potentials $\overline{\varphi}_i^{(p)}$, $\underline{\varphi}_i^{(p)}$ having some arguments $\tau = \tau_{*j}^{(p)}$, $\tau_j^{*(p)}$, $\overline{\tau}_i^{(p)}$, $\underline{\varphi}_i^{(p)}$ (results of physical measurements), respectively, after which we calculate (10) [1] using interpolation and finally we find the coordinates of $x_{0,j}^{(p)}$, $y_{0,j}^{(p)}$, $x_{i,0}^{(p)}$, $y_{i,0}^{(p)}$, $x_{i,n^{(p)}+1}^{(p)}$, $y_{i,n^{(p)}+1}^{(p)}$, $x_{m^{(p)}+1,j}^{(p)}$, $y_{m^{(p)}+1,j}^{(p)}$ $(1 \le p \le \tilde{p},\ 0 \le i \le m^{(p)}+1,\ 0 \le j \le n^{(p)}+1)$ on $\partial G_z^{\gamma(p)}$. Then we form the initial approximations of the nodes $x_{i,j}^{(p,0)}$, $y_{i,j}^{(p,0)}$ and list of parameters $a_{k_a-r_a,r_a}^{(0)}$, $b_{k_b-r_b,r_b}^{(0)}$, $c_{k_c-r_c,r_c}^{(0)}$, which define CT. After that we start the iterative process of reconstruction, which consists of the following steps: we apply the difference representation of Laplace type equations (14) [1] (with consider «injectivity») for search the coordinates of internal nodes when $1 \le p \le \tilde{p}$, $1 \le i \le m^{(p)}$, $1 \le j \le n^{(p)}$ $q$ times; we solve the functional minimizing problem (18) [1] under conditions (19) [1] relative $a_{k_a-r_a,r_a}^{(l)}$, $b_{k_b-r_b,r_b}^{(l)}$, $c_{k_c-r_c,r_c}^{(l)}$ (here $l = 0,1,...$ is the iterative step number, $k_a = \overline{1,s_a}$, $r_a = \overline{0,k_a}$, $k_b = \overline{1,s_b}$, $r_b = \overline{0,k_b}$, $k_c = \overline{0,s_c}$, $r_c = \overline{0,k_c}$); check the conditions for the completion of the iterative process, among which may be [5]: stabilizing of near-boundary nodes, CT, the quasiconformal degree parameter, the values of discharges, etc. $(1 \le p \le \tilde{p},\ 1 \le i \le m^{(p)},\ 1 \le j \le n^{(p)})$. In the cases when one of these conditions is not satisfied the iterative process begins again, otherwise we build the corresponding reconstructed image and, if it's necessary, the electrodynamical mesh, the complex quasipotential domains or calculate the velocity fields etc.

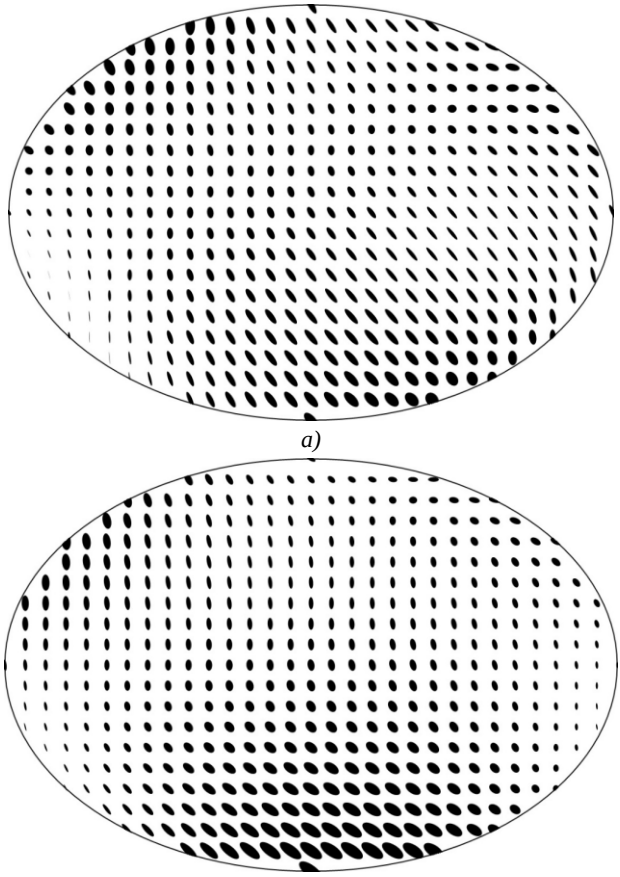
Note that the algorithm will be identical if instead of eigenvalues sum (4) [1], it is known the distribution either $\lambda_1$ or $\lambda_2$. In first case the term $\tilde{\mu}(\lambda_{i,j}^{\gamma(p)} - \sigma_{11_{i,j}}^{\gamma(p)} - \sigma_{22_{i,j}}^{\gamma(p)})^2$ of functional (18) [1] is replaced by $\tilde{\mu}\left(\lambda_{1_{i,j}}^{\gamma(p)} - 0.5\left(\sigma_{11_{i,j}}^{\gamma(p)} + \sigma_{22_{i,j}}^{\gamma(p)} + \sqrt{(\sigma_{11_{i,j}}^{\gamma(p)} - \sigma_{22_{i,j}}^{\gamma(p)})^2 + 4\sigma_{12_{i,j}}^{\gamma(p)2}}\right)\right)^2$, in the second it is replaced by $\tilde{\mu}\left(\lambda_{2_{i,j}}^{\gamma(p)} - 0.5\left(\sigma_{11_{i,j}}^{\gamma(p)} + \sigma_{22_{i,j}}^{\gamma(p)} - \right.\right.$ $\left.\left. - \sqrt{(\sigma_{11_{i,j}}^{\gamma(p)} - \sigma_{22_{i,j}}^{\gamma(p)})^2 + 4\sigma_{12_{i,j}}^{\gamma(p)2}}\right)\right)^2$. However, the solving of the nonlinear

programming problem thus created will require the using of the global optimization method.

In order to use the machine time more frugally, it is also possible to apply formulas (18) [1] and (19) [1] only for selected points. In particular (if it allows the chosen optimization algorithm) the fulfillment of conditions (19) [1] should not be required in all nodes of the $\tilde{p}$ meshes, but only in the coordinates of the extreme values of the functions (4) [1] instead. It makes sense to set a series of control points inside the investigated domain in other cases. Such in some cases may be nodes of meshes from arbitrary injection.

Also note, that instead of the procedure for determining the coordinates of the boundary nodes using formula (16) [1] (by interpolating the results of physical measurements), we can immediately select them so that the local differences in the values of the function of flow or potential between them at the corresponding neighboring points to be constant within the injection.

**Numerical calculations.** We represent the results of numerical calculations for the following input data: $s_a = 2,\ s_b = s_c = 3,\ \tilde{p} = 20,\ \tilde{x}(\tau) = 150\cos\tau,\ \tilde{y}(\tau) = 100\sin\tau,\ a_{k_a - r_a, r_a} = b_{k_b - r_b, r_b} = c_{k_c - r_c, r_c} = 0\ \ (k_a = \overline{1, s_a},\ r_a = \overline{0, k_a},\ k_b = \overline{1, s_b},\ r_b = \overline{0, k_b},\ k_c = \overline{0, s_c},\ r_c = \overline{0, k_c}),\ a_{0,0} = b_{0,0} = 1,\ \mu = 0.1,\ \eta = 0.01,\ \alpha_1 = \alpha_2 = 0.01,\ \alpha_3 = \alpha_4 = 4,\ q = 200,\ \varepsilon_1 = \varepsilon_2 = 10^{-2},\ m^{(p)} = 100,\ \varphi_*^{(p)} = 0,\ \varphi^{*(p)} = 1,\ \tau_A^{(p)} = 9\pi/8 + (p-1)\pi/\tilde{p},\ \tau_B^{(p)} = \tau_A^{(p)} - \pi/4,\ \tau_C^{(p)} = \tau_A^{(p)} - \pi,\ \tau_D^{(p)} = \tau_C^{(p)} - \pi/4,\ Q^{(p)},\ \Psi_{*j}^{(p)},\ \Psi_j^{*(p)},\ \bar{\varphi}_i^{(p)},\ \underset{-i}{\varphi^{(p)}}\ (1 \le p \le \tilde{p}),\ \lambda(x, y)$. Visual representation of the received CT distribution is carried out using a specially developed procedure similar to [4]. According to this, the investigated domain is divided into square sections by lines parallel to the axes of coordinates. The CT is characterized in the center of each of them as an ellipse (its directions of axes and radiuses are corresponds to the directions of eigenvectors and proportional to the eigenvalues, respectively) by the formula $\kappa_{11}x^2 + \kappa_{22}y^2 + 2\kappa_{12}xy = 1,$ where $\kappa_{11} = \sin^2\theta/\lambda_2^2 + \cos^2\theta/\lambda_1^2,$ $\kappa_{22} = \cos^2\theta/\lambda_2^2 + \sin^2\theta/\lambda_1^2,\ \kappa_{12} = (\lambda_1^{-2} - \lambda_2^{-2})sin\theta cos\theta,$ the angle $\theta$ of rotation of the ellipse must satisfy the conditions $2\sigma_{12} = (\lambda_1 - \lambda_2)sin2\theta,$ $\sigma_{11} = (\lambda_1 - \lambda_2)cos^2\theta + \lambda_2$. Figura, b presents the reconstructed image of the CT distribution in comparison to the given theoretically (Figura, a).



*a)*

*b)*

***Figura.*** *CT distribution: exact (when* $\lambda(x, y) = 1.9 - 5 \cdot 10^{-4} x + 0.01y +$
$+10^{-7}(-145x^2 + 600xy + 850y^2 + 2x^3 - 0.3x^2 y - 4.5xy^2 - 5y^3))$ *(a), approximated solution* (*b*)

**Conclusions.** The algorithm for solving the problem of image reconstruction of the CT of anisotropic media given in [1] is developed. It is characterized by comparatively fast computer convergence (since, unlike many used methods, it does not require finding derivatives of the CT distribution function at certain points and refining the boundary nodes at each iteration step).

The significant feature of developed algorithm is the possibility of detection of so-named «stagnant zones» and «zones of large gradients», which appears near the especial points of non-smooth boundary lines and critical points inside the respective domains. We also note that the considerably new in algo-

rithm is considering the conditions of «anisotropic quasiorthogonality» along the boundary equipotentials and current lines (instead of orthogonality in cases of isotropic media), which requires additional substantially new constructions. Also, the anisotropy tensor affects the decrease in accuracy by orders of magnitude and stability, which in particular requires the creation of new structures-procedures for Tikhonov-type regularization.

We plan to extend the proposed algorithm to the following cases: when have place other rather wide dependencies between eigenvalues of the CT, spatial resolution, applying the quasipotential of the initial stream to several sections.

**References:**


1. Bomba A. Ya., Boichura M. V. Numerical Complex Analysis Method for Parameters Identification of Anisotropic Media using Applied Quasipotential Tomographic Data. Part 1: Problem Statement and its Approximation. *Mathematical and computer modelling. Series: Physical and mathematical sciences.* 2018. Vol. 18. P. 14–24.
2. Bomba A. Ya., Kroka L. L. Numerical Methods of Quasiconformal Mappings for Solving Problems of Identifying of Electrical Conductivity Coefficient in an Applied Potential Tomography. *Volyn Mathematical Bulletin. Applied Mathematics Series*. Rivne : RSHU, 2014. Vol. 11 (20). P. 24–33. (Ukr).
3. Bomba A. Ya., Boichura M. V. Applied Quasipotenrial Method for Solving Coefficient Problems of Parametric Identification. *Bulletin of NUWEE. Technical Sciences Series*. Rivne : NUWEE, 2017. Vol. 4 (76). P. 163–177. (Ukr).
4. Martins T. C., Tsuzuki M. S. G. Investigating Anisotropic EIT with Simulated Annealing. *IFAC-PapersOnLine*. 2017. Vol. 50 (1). P. 9961–9966.
5. Bomba A. Ya., Kashtan S. S., Pryhornytskyi D. O., Yaroshchak S. V. Complex analysis methods. Rivne : Editorial and Publishing Department of NUWEE, 2013. 415 p. (Ukr).
6. Ortega J. M., Rheinboldt W. C. Iterative Solution of Nonlinear Equations in Several Variables. San Diego : Academic Press, 1970. 572 p.


## ЧИСЛОВИЙ МЕТОД КОМПЛЕКСНОГО АНАЛІЗУ ІДЕНТИФІКАЦІЇ ПАРАМЕТРІВ АНІЗОТРОПНИХ СЕРЕДОВИЩ ЗА ДАНИМИ ТОМОГРАФІЇ ПРИКЛАДЕНИХ КВАЗІПОТЕНЦІАЛІВ. ЧАСТИНА 2: АЛГОРИТМ ТА КОМП'ЮТЕРНИЙ ЕКСПЕРИМЕНТ

На основі запропонованого підходу до розв'язання градієнтних задач ідентифікації параметрів квазіідеальних полів за даними томографії прикладених квазіпотенціалів у випадках анізотропних середовищ та ідеях методу блочної ітерації, розроблено алгоритм, який полягає у послідовному ітераційному застосуванні числових методів квазіконформних відображень для побудови серії динамічних сіток при різних заданнях крайових умов (що визначаються експериментальними даними) та розв'язанні

задачі параметричної ідентифікації для кожної з цих сіток. Реконструйоване зображення розподілу тензора провідності у внутрішності досліджуваного об'єкта, отримане в результаті числових розрахунків, проведених на основі розробленого алгоритму, з достатньою точністю відповідає еталонному. Метод характеризується порівняно швидкою комп'ютерною збіжністю (оскільки, на відміну від багатьох використовуваних методів, не потребує знаходження похідних функції розподілу тензора провідності у визначених точках та уточнення граничних вузлів на кожному ітераційному кроці). Суттєвою його особливістю є можливість порівняно легкого його розпаралелення та зупинки процедури обчислення за умови виконання лише деяких із умов закінчення процесу з автоматичним визначенням тих ділянок фізичної області, де мають місце великі похибки обчислень, що дає змогу економніше використовувати машинний час. Розроблений алгоритм реконструкції зображення може бути поширений не тільки на середовища з відомою сумою власних значень тензора провідності, але й на випадки досить широких інших залежностей між ними. Зокрема підхід забезпечує можливість представлення його деякою комплексно значною функцією як це вимагає біомедична практика.

**Ключові слова:** *томографія прикладених квазіпотенціалів, квазіконформні відображення, анізотропія, ідентифікація, нелінійні задачі.*

Data received 30.01.2019

УДК 519.6:004.02
DOI: 10.32626/2308-5916.2019-19.17-24

**Л. П. Вакал*,** канд. техн. наук,
**Є. С. Вакал**,** канд. фіз.-мат. наук

*Інститут кібернетики імені В. М. Глушкова НАН України, м. Київ,
**Київський національний університет імені Тараса Шевченка, м. Київ

# НАЙКРАЩЕ РІВНОМІРНЕ НАБЛИЖЕННЯ СПЛАЙНАМИ З ВИКОРИСТАННЯМ ДИФЕРЕНЦІАЛЬНОЇ ЕВОЛЮЦІЇ

Розглянуто задачу найкращого рівномірного наближення функцій поліноміальними сплайнами з фіксованими вузлами. Для її розв'язання запропоновано підхід на основі еволюційних алгоритмів — потужного класу стохастичних пошукових методів оптимізації. Для знаходження сплайна найкращого рівномірного наближення адаптовано алгоритм диференціальної еволюції. Це один із кращих еволюційних алгоритмів, який стабільно знаходить глобальний оптимум цільової функції (критерію оптимізації) за мінімальний час. Еволюційний процес в алгоритмі починається з генерації популяції випадкових векторів, координати яких представляють собою можливі значення коефіцієнтів сплайна. Далі вектори постійно модифікуються за допомогою операцій мутації, схрещування та селекції з метою змен-

© Л. П. Вакал, Є. С. Вакал, 2019

шення значення цільової функції (похибки наближення сплайном). Алгоритм завершується, якщо вичерпано задане максимальне число популяцій або відбувається стагнація еволюційного процесу. Алгоритм диференціальної еволюції простий у програмній реалізації й використанні (містить мало параметрів, що потребують підбору), легко розпаралелюється. Розроблені рекомендації щодо вибору оптимальних значень основних параметрів алгоритму: розміру популяції, коефіцієнта мутації, ймовірності схрещування. Для низки тестових функцій виконано порівняння похибок наближення, отриманих за стохастичним алгоритмом диференціальної еволюції та за іншими (детерміністичними) алгоритмами. Результати порівняння показали, що точність наближення функцій сплайнами з використанням алгоритму диференціальної еволюції не гірше, ніж при застосуванні значно складніших детерміністичних алгоритмів рівномірного наближення. Це свідчить про ефективність алгоритму диференціальної еволюції. Він може використовуватись як альтернатива відомим детерміністичним алгоритмам наближення сплайнами.

**Ключові слова:** *сплайн, фіксовані вузли, найкраще рівномірне наближення, диференціальна еволюція, стохастичний метод.*

**Вступ.** Останнім часом для наближення функціональних залежностей складної структури, які виникають при розв'язанні різноманітних прикладних задач, широко використовуються поліноміальні сплайни. Найбільш популярними є інтерполяційні сплайни степеня не вище трьох, параметри яких легко обчислюються. На практиці також застосовують сплайни найкращого наближення. При тому ж числі параметрів сплайн найкращого наближення апроксимує функцію не гірше, ніж інтерполяційний. Крім того, для побудови інтерполяційного сплайна звичайно потрібно задавати ще деякі граничні умови [1, с. 24]. Тому в багатьох випадках доцільнішим є використання сплайнів найкращого наближення, зокрема, у рівномірній (чебишовській) нормі [2, 3].

Алгоритми найкращого рівномірного наближення функцій поліноміальними сплайнами з фіксованими вузлами поділяються на дві основні групи. До першої належать алгоритми [4–6], в яких використовується зведення задачі найкращого наближення до задачі лінійного програмування (ЛП). Алгоритми другої групи є узагальненням на випадок сплайнів методу послідовних чебишовських інтерполяцій Ремеза [7, 8]. Складність і громіздкість вказаних алгоритмів, а також їхня недостатня реалізація у загальнодоступних математичних пакетах [9, 10] перешкоджають більш широкому застосуванню сплайнів найкращого рівномірного наближення на практиці.

**Мета роботи** — розробка нескладного в реалізації й водночас ефективного алгоритму для найкращого рівномірного наближення функцій поліноміальними сплайнами з фіксованими вуздами.

**Постановка задачі.** Нехай на відрізку $[\alpha, \beta]$ задані дві сітки:

$$\Delta_m: \alpha = x_1 < x_2 < \ldots < x_m = \beta ,$$

$$\Delta_k : \alpha < \tilde{x}_1 < \ldots < \tilde{x}_k < \beta$$

і множина $S_{n,k}$ сплайнів $s(x)$ степеня $n$ ($n \geq 1$) дефекту 1 з вузлами $\Delta_k$. Надалі будемо вважати, що $m > n + k$ і на кожному з проміжків $[\tilde{x}_{i-1}, \tilde{x}_i]$ ($i = 1, 2, \ldots, k+1, \tilde{x}_0 = \alpha, \tilde{x}_{k+1} = \beta$) є щонайменше дві точки сітки $\Delta_m$. Будь-який сплайн $s(x) \in S_{n,k}$ можна записати у вигляді [1]

$$s(x) = \sum_{i=1}^{n+1} a_i (x - \alpha)^{i-1} + \sum_{i=1}^{k} a_{n+1+i} (x - \tilde{x}_i)_+^n , \qquad (1)$$

де $a_i$ — дійсні числа і

$$(x - \tilde{x}_i)_+^n = \begin{cases} (x - \tilde{x}_i)^n, & x > \tilde{x}_i \\ 0, & x \leq \tilde{x}_i \end{cases} .$$

Задача найкращого рівномірного наближення функції $f(x)$ на сітці $\Delta_m$ сплайном вигляду (1) з фіксованими вузлами $\Delta_k$ полягає у знаходженні сплайна $s^*(x) \in S_{n,k}$, що задовольняє умову

$$\max_{1 \leq i \leq m} \left| f(x_i) - s^*(x_i) \right| \equiv \rho = \min_{s(x) \in S_{n,k}} \max_{1 \leq i \leq m} \left| f(x_i) - s(x_i) \right| . \qquad (2)$$

Величина $\rho$ називається похибкою найкращого наближення.

Для розв'язання задачі (2) пропонується застосувати підхід, що ґрунтується на використанні еволюційних алгоритмів (ЕА) — потужного класу стохастичних пошукових методів оптимізації. Для знаходження оптимуму функції ЕА використовують випадково породжену популяцію розв'язків, яка покращується шляхом еволюційного процесу з використанням операцій схрещування, мутації та селекції, поки не виконається умова завершення еволюції (наприклад, досягнуто задане граничне число популяцій). ЕА включають генетичний алгоритм, диференціальну еволюцію, алгоритм рою часток, алгоритм оптимізації мурашиної колонії та ін.

**Алгоритм знаходження сплайна найкращого рівномірного наближення.** Для розв'язання задачі (2) пропонується адаптувати диференціальну еволюцію (ДЕ) [11]. Алгоритм ДЕ успішно використовувався авторами для розв'язання низки задач наближення [12–15]. Це один з кращих ЕА, який стабільно знаходить глобальний оптимум функції за мінімальний час. Крім того, він простий у реалізації та використанні (містить мало варійованих параметрів), легко розпаралелюється.

На кожній ітерації еволюційного процесу операції мутації, схрещування та селекції в алгоритмі ДЕ застосовуються до популяції

$P_G = \{B_{1,G}, \ldots, B_{NP,G}\}$, що складається з $D$-мірних векторів $B_{i,G} = (b_{i,1,G}, \ldots, b_{i,D,G})$, $i = 1, \ldots NP$, де $NP$ — розмір популяції, $G$ — номер популяції, $G = 0, 1, \ldots, G_{\max}$. У випадку задачі (2) $D = n + k + 1$, а координати $b_{i,1,G}, \ldots, b_{i,n+k+1,G}$ векторів $B_{i,G}$ представляють собою можливі значення коефіцієнтів $a_1, \ldots, a_{n+k+1}$ сплайна $s^*(x)$.

Далі наведено покроковий опис алгоритму.

1. Покладається лічильник числа популяції $G = 0$, і створюється початкова популяція $P_G = \{B_{1,G}, \ldots, B_{NP,G}\}$, в якій координати векторів $B_{i,G} = (b_{i,1,G}, \ldots, b_{i,n+k+1,G})$, $i = 1, \ldots NP$, генеруються за допомогою датчика випадкових чисел із заданого діапазону $ID$.

Далі на кроках 2–4 формується нова популяція.

2. Мутація. Для кожного вектора $B_{i,G}$ із старої популяції (цей вектор називається базовим) за допомогою трьох інших випадкових векторів $B_{r_1,G}$, $B_{r_2,G}$, $B_{r_3,G}$ ($r_1 \neq r_2 \neq r_3 \neq i$) створюється мутантний вектор $V_{i,G}$ за формулою

$$V_{i,G} = B_{r_1,G} + FM \cdot (B_{r_2,G} - B_{r_3,G}),$$

де коефіцієнт $FM$ — задана додатна дійсна стала з проміжку $(0, 2]$.

3. Над векторами $B_{i,G}$ і $V_{i,G}$ виконується операція схрещування, результатом якої є вектор $U_{i,G}$ з координатами

$$u_{i,j,G} = \begin{cases} v_{i,j,G}, \text{ якщо } \text{rand}(0,1) \le CR \text{ або } j = j_{rand}, \\ b_{i,j,G} \text{ в іншому випадку,} \end{cases} \quad j = 1, \ldots, n + k + 1,$$

де $rand(0,1)$ — випадкове дійсне число з інтервалу $(0,1)$, $CR$ — задана ймовірність схрещування, $j_{rand}$ — випадкове ціле число в діапазоні $[1, n + k + 1]$.

4. Селекція. До нової популяції з номером $G+1$ переходить той з векторів $B_{i,G}$ і $U_{i,G}$, значення цільової функції $F$ якого менше

$$B_{i,G+1} = \begin{cases} U_{i,G}, \text{ якщо } F(U_{i,G}) \le F(B_{i,G}), \\ B_{i,G} \text{ в іншому випадку.} \end{cases}$$

Цільова функція $F$ (критерій оптимізації) обчислюється за формулою:

$$\mathrm{F}(B_{i,G}) = \max_{1 \le l \le m} \left| \sum_{j=1}^{n+1} b_{i,j,G} (x_l - \alpha)^{j-1} + \sum_{j=1}^{k} b_{i,n+1+j,G} (x_l - \tilde{x}_j)_+^n \right|.$$

5. Якщо вичерпано задане максимальне число популяцій $G_{\max}$ або відносний розкид значень цільової функції найгіршого і найкращого векторів популяції менше деякого заданого $\delta$ (умова стагнації), то еволюційний процес завершується, інакше — перехід до п. 2.

Через стохастичний характер алгоритму ДЕ для отримання прийнятного результату потрібно зробити декілька його пусків. Розмір популяції *NP*, коефіцієнт мутації *FM* та ймовірність схрещування *CR* є основними параметрами налаштування алгоритму. За результатами проведеного дослідження рекомендовано такі значення параметрів: $5(n+k+1) \le NP \le 10(n+k+1)$, $0.4 \le FM \le 0.6$, $0.8 \le CR \le 1$.

**Результати обчислювальних експериментів.** За допомогою описаного вище алгоритму ДЕ виконано серію обчислювальних експериментів з наближення низки тестових функцій. У табл. 1 і 2 наведено результати наближення відповідно функції $f_1(x) = (1+x)^{-1}$ на відрізку $[0,1]$ сплайнами з рівновіддаленими вузлами та функції $f_2(x) = \sqrt{x}$ на відрізку $[0,2]$ сплайном 3-го степеня. Перше число в комірках табл. 1 — похибка наближення $\rho$ за алгоритмом типу Ремеза [8], друге — за алгоритмом ЛП [6], третє — за алгоритмом ДЕ. Зазначимо, що експерименти виконувались при таких налаштуваннях алгоритму ДЕ: $NP = 10(n+k+1)$, $FM = 0.5$, $CR = 1$, $G_{\max} = 250$, $\delta = 10^{-4}$, $m = 1001$, число пусків — 10, $ID = [-1,1]$ для функції $f_1(x)$ та $ID = [-100,100]$ для функції $f_2(x)$.

Таблиця 1

*Апроксимація сплайнами функції* $f_1(x) = (1+x)^{-1}$ *на* $[0,1]$

| **Степінь сплайна *n*** | **Число вузлів сплайна *k*** | | | |
|---|---|---|---|---|
| | 1 | 2 | 3 | 4 |
| 3 | $3.85\cdot10^{-4}$<br>$3.249\cdot10^{-4}$<br>$3.249\cdot10^{-4}$ | $8.9\cdot10^{-5}$<br>$8.635\cdot10^{-5}$<br>$8.635\cdot10^{-5}$ | $3.3\cdot10^{-5}$<br>$3.328\cdot10^{-5}$<br>$3.328\cdot10^{-5}$ | $1.5\cdot10^{-5}$<br>$1.505\cdot10^{-5}$<br>$1.505\cdot10^{-5}$ |
| 4 | $5.1\cdot10^{-5}$<br>$5.115\cdot10^{-5}$<br>$5.115\cdot10^{-5}$ | $10.0\cdot10^{-6}$<br>$9.898\cdot10^{-6}$<br>$9.898\cdot10^{-6}$ | $3.6\cdot10^{-6}$<br>$3.611\cdot10^{-6}$<br>$3.616\cdot10^{-6}$ | $1.7\cdot10^{-6}$<br>$1.696\cdot10^{-6}$<br>$1.698\cdot10^{-6}$ |
| 5 | $8.2\cdot10^{-6}$<br>$8.281\cdot10^{-6}$<br>$8.282\cdot10^{-6}$ | $1.3\cdot10^{-6}$<br>$1.462\cdot10^{-6}$<br>$1.464\cdot10^{-6}$ | $6\cdot10^{-7}$<br>$6.108\cdot10^{-7}$<br>$6.194\cdot10^{-7}$ | $3\cdot10^{-7}$<br>$2.509\cdot10^{-7}$<br>$2.564\cdot10^{-7}$ |

Таблиця 2

*Апроксимація функції* $f_2(x) = \sqrt{x}$ *на* $[0, 2]$ *кубічним сплайном*

| **Вузли сплайна** | **Число коефіцієнтів** | **Похибка наближення за алгоритмом** | | |
|---|---|---|---|---|
| | | **типу Ремеза** | **ЛП** | **ДЕ** |
| 0.04 | 5 | 0.02524 | 0.025216 | 0.025238 |
| 0.0065, 0.108 | 6 | 0.01380 | 0.013789 | 0.013790 |
| 0.002, 0.02, 0.15 | 7 | 0.01034 | 0.010337 | 0.010338 |
| 0.0015, 0.02, 0.1, 0.3 | 8 | 0.00448 | 0.004471 | 0.004474 |
| 0.001, 0.015, 0.06, 0.2, 0.35 | 9 | 0.00338 | 0.003372 | 0.003387 |

Як свідчать наведені в табл. 1 і 2 результати, точність наближення функцій сплайнами з використанням стохастичного алгоритму ДЕ не гірше, ніж при застосуванні значно складніших детерміністичних алгоритмів найкращого рівномірного наближення.

**Висновки.** Представлено алгоритм ДЕ, адаптований для знаходження поліноміального сплайна найкращого рівномірного наближення для функцій, заданих на сітці. Алгоритм простий у програмній реалізації й використанні (містить мало параметрів, що потребують налаштування) і водночас достатньо ефективний. Результати обчислювальних експериментів показали, що точність наближення функцій сплайнами з використанням алгоритму ДЕ не гірше, ніж при застосуванні значно складніших алгоритмів рівномірного наближення. У подальшому планується дослідити ефективність використання ДЕ для найкращого наближення сплайнами з вільними вузлами, де потрібно визначати як коефіцієнти сплайна, так і його вузли.

## Список використаних джерел:


1. Стечкин С. Б., Субботин Ю. Н. Сплайны в вычислительной математике. М. : Наука, 1976. 248 с.
2. Попов Б. А. Равномерное приближение сплайнами. Киев : Наук. думка, 1989. 272 с.
3. Малачівський П. С., Скопецький В. В. Неперервне й гладке мінімаксне сплайн-наближення. Київ : Наук. думка, 2013. 270 с.
4. Barrodale J., Young A. A note on numerical procedures for approximation by spline functions. *Comput. J.* 1966. Vol. 9. P. 318–320.
5. Esch R. E., Eastman W. L. Computational methods for the best spline function approximation. *J. Approx. Theory*. 1969. Vol. 2. P. 85–96.
6. Вакал Л. П. Побудова найкращих чебишовських наближень сплайнами. Штучний інтелект. 2017. № 2 (76). С. 94–100.
7. Schumaker L. L. Some algorithms for the computation of interpolating and approximating spline functions. *Theory and applications of spline functions.* New York : Academic Press, 1969. P. 87–102.

8. Nürnberger G., Sommer M. A Remez type algorithm for spline functions. *Numer. Math.* 1983. Vol. 41, № 1. P. 117–146.
9. Каленчук-Порханова А. А., Вакал Л. П. Пакет программ аппроксимации функций. *Комп'ютерні засоби, мережі та системи*. 2008. № 7. С. 32–38.
10. Каленчук-Порханова А. А., Вакал Л. П. Аппарат аппроксимации в составе программного обеспечения суперкомпьютера с кластерной архитектурой. *Искусственный интеллект*. 2009. № 1. С. 158–165.
11. Storn R., Price K. Differential evolution — a simple and efficient heuristic for global optimization over continuous spaces. *Journal of Global Optimization*. 1997. Vol. 11. P. 341–359.
12. Vakal L. P. Seeking optimal knots for segment approximation. *Journal of Automation and Information Sciences*. 2016. Vol. 48, № 11. P. 68–75.
13. Вакал Л. П. Апроксимація функцій багатьох змінних із застосуванням алгоритму диференціальної еволюції. *Математичні машини і системи*. 2017. № 1. С. 90–96.
14. Vakal L. P., Kalenchuk-Porkhanova A. A., Vakal E. S. Increasing the efficiency of Chebyshev segment fractional rational approximation. *Cybernetics and Systems Analysis*. 2017. Vol. 53, № 5. P. 759–765.
15. Вакал Л. П., Вакал Є. С. Розв'язання перевизначеної системи трансцендентних рівнянь з використанням диференціальної еволюції. *Математичне та комп'ютерне моделювання. Серія: Технічні науки : зб. наук. пр.* Кам'янець-Подільський : Кам'янець-Подільськ. нац. ун-т, 2017. Вип. 15. С. 24–30.

## BEST UNIFORM SPLINE APPROXIMATION USING DIFFERENTIAL EVOLUTION

It is considered a problem of the best uniform approximation of functions by polynomial splines with fixed knots. It is proposed an approach based on evolutionary algorithms — a powerful class of stochastic search optimization methods — for its solution. To find a spline of the best uniform approximation, a differential evolution algorithm is adapted. It is one of the best evolutionary algorithms that consistently finds a global optimum of a target function (optimization criterion) in a minimal time. An evolutionary process in the algorithm begins with a generation of random vectors, coordinates of which are possible values of spline coefficients. Further, the vectors are constantly modified by mutation, crossover and selection operations in order to reduce a value of the target function (spline approximation error). The algorithm is completed if a specified maximum number of populations is exhausted or a stagnation of the evolutionary process takes place. The differential evolution algorithm is simple in program realization and using (it contains few varied parameters that need to be selected). It is easily paralleled. Recommendations for choosing optimal values of main parameters of the algorithm such as a population size, a mutation factor, a crossover probability are developed. A comparison of the approximation errors obtained by the stochastic differential evolution algorithm and by other (deterministic) algorithms is made for a series of test functions. Results of the comparison showed that an accuracy of the functions approximation by splines using the

differential evolution is not worse than using much more complicated deterministic algorithms of the best uniform approximation. This testifies about the effectiveness of the differential evolution algorithm. It can be used as an alternative for known deterministic algorithms of spline approximation.

**Key words:** *spline, fixed knots, best uniform approximation, differential evolution, stochastic method.*

Одержано 27.01.2019

УДК 004.94
DOI: 10.32626/2308-5916.2019-19.24-30

**А. Ф. Верлань*,** д-р техн. наук, професор,
**В. А. Федорчук**,** д-р техн. наук, професор,
**В. А. Іванюк**,** канд. техн. наук, доцент

*Інститут проблем моделювання в енергетиці
імені Г.Є. Пухова НАН України, м. Київ,
**Кам'янець-Подільський національний університет
імені Івана Огієнка, м. Кам'янець-Подільський

## ІНТЕГРАЛЬНІ МОДЕЛІ НЕСТАЦІОНАРНИХ ЗАДАЧ ТЕПЛОПРОВІДНОСТІ НА ОСНОВІ МЕТОДУ ТЕПЛОВИХ ПОТЕНЦІАЛІВ

Розглядається підхід до побудови інтегральних моделей нестаціонарних задач теплопровідності на основі застосування методу теплових потенціалів. Можливість побудови інтегральних моделей розглядається на конкретних прикладах із використанням різних теплових потенціалів: одновимірна задача теплопровідності із різною постановкою крайової задачі (умови першого та другого роду), двовимірна задача теплообміну, задача теплообміну із рухомою границею. Пропонується застосування комбінації точних та чисельних методів, що дає змогу враховувати переваги різних підходів. Застосування методу теплових потенціалів до моделей у формі диференціальних рівнянь із частинними похідними дозволило отримати загальний розв'язок у вигляді оператора Вольтерри, який залежить від функцій, що визначаються із крайових умов, тобто поставлена задача зводиться до розв'язання інтегральних рівнянь Вольтерри II роду або їх систем. Особливістю отриманих моделей є те, що ядра інтегральних моделей є сингулярними у кінцевій точці інтегрування. Розв'язування таких рівнянь пропонується здійснювати за допомогою обчислювальних методів, основаних на методі квадратур. Для уникнення особливостей в ядрі застосовується метод зсуву. Врахувавши властивості ядр, пропонується застосовувати метод лівих прямокутників, що дозволить уникнути сингуляр-


© А. Ф. Верлань, В. А. Федорчук, В. А. Іванюк, 2019

ності. Для підвищення точності побудови розв'язку пропонується застосовувати адаптивний алгоритм ущільнення кроку моделювання в околі сингулярної точки. Запропонований підхід до розв'язування нестаціонарних задач теплопровідності враховує переваги точних (метод теплових потенціалів) і обчислювальних методів (метод квадратур) та дає змогу підвищити ефективність обчислень на основі розпаралелення задачі.

**Ключові слова:** *нестаціонарна задача теплопровідності, метод потенціалів, інтегральні рівняння, метод квадратур, сингулярні інтегральні рівняння.*

**Вступ.** При розв'язуванні прикладних задач теплообміну виникають труднощі ефективного застосування стандартних методів, які можна розділити на чисельні, аналітичні та наближені аналітичні.

Сучасні чисельні методи (скінченних різниць, скінченних елементів, граничних елементів та ін.) не завжди можуть ефективно використовуватись в силу складності і великих часових затрат, які збільшуються при зменшенні кроку сітки [5, 6]. Точні аналітичні методи (метод інтегральних перетворень, метод функції Гріна, метод інтегральних представлень, теплових потенціалів та ін. [1, 2, 4, 5, 8]) потребують від дослідника високої математичної підготовки та можуть бути застосовані до обмеженого числа крайових задач. Одним із основних недоліків наближених методів (методи Рітца, Треффтца, Канторовича, Гальоркіна, зважених нев'язок, колокацій та ін.) є те, що при малих значеннях кроку дискретизації часової координати отримуються великі системи лінійних алгебраїчних рівнянь, матриці коефіцієнтів яких, зазвичай, погано обумовлені [4]. Тому вдосконалення методів моделювання процесів теплообміну шляхом комбінування аналітичних, наближених та обчислювальних методів, які можна реалізувати в сучасних засобах комп'ютерного моделювання є актуальною задачею.

Пропонується підхід, який дозволяє розв'язувати нестаціонарні задачі теплопровідності при застосуванні методу теплових потенціалів та методу квадратур, що дає змогу підвищити ефективність обчислень за рахунок можливості розпаралелення задачі.

Розглянемо методи отримання інтегральних моделей на основі методу теплових потенціалів.

*Одновимірний випадок*. Методику отримання математичних моделей у формі інтегральних операторів на основі методу теплових потенціалів розглянемо на конкретних прикладах [2]. Розглянемо одновимірне рівняння теплопровідності

$$u_t = a^2 u_{xx} \tag{1}$$

і покладемо, що для проміжку $0 \le x \le l$ поставлена крайова задача з умовами

$$u\big|_{x=0} = \omega_1(t),\ u\big|_{x=l} = \omega_2(t) \tag{2}$$

і початковою умовою

$$u\big|_{t=0} = 0\ \ (0 \le x \le l). \tag{3}$$

Шукаємо розв'язок у вигляді суми двох потенціалів, заданих у точці $x = 0$ і в точці $x = l$ (шукану інтенсивність у першій точці позначимо $\varphi(\tau)$, у другій — $\psi(\tau)$):

$$u(x,t) = \int_0^t \frac{\varphi(\tau) e^{-\frac{x^2}{4a^2(t-\tau)}}}{2a\sqrt{\pi}(t-\tau)^{3/2}} x\,d\tau + \int_0^t \frac{\psi(\tau) e^{-\frac{(l-x)^2}{4a^2(t-\tau)}}}{2a\sqrt{\pi}(t-\tau)^{3/2}} (x-l)\,d\tau. \tag{4}$$

Крайові умови (2), в силу (4), запишемо у вигляді:

$$\begin{cases} \varphi(t) - l\int_0^t \dfrac{\psi(\tau)}{2a\sqrt{\pi}(t-\tau)^{3/2}} e^{-\frac{l^2}{4a^2(t-\tau)}} d\tau = \omega_1(t), \\ -\psi(t) + l\int_0^t \dfrac{\varphi(\tau)}{2a\sqrt{\pi}(t-\tau)^{3/2}} e^{-\frac{l^2}{4a^2(t-\tau)}} d\tau = \omega_2(t). \end{cases} \tag{5}$$

Таким чином, для визначення інтенсивності потенціалів отримано систему інтегральних рівнянь.

Розглянемо випадок, коли крайові умови мають вигляд

$$u\big|_{x=0} = \omega_1(t),\ \frac{\partial u}{\partial x}\Big|_{x=l} = \omega_2(t) \tag{6}$$

і початкові умови, як і вище, мають вигляд (3). Тоді розв'язок можна записати у вигляді

$$u(x,t) = \int_0^t \frac{\varphi(\tau)}{2a\sqrt{\pi}(t-\tau)^{3/2}} x e^{-\frac{x^2}{4a^2(t-\tau)}} d\tau + \int_0^t \frac{a\psi(\tau)}{\sqrt{\pi}\sqrt{t-\tau}} e^{-\frac{(l-x)^2}{4a^2(t-\tau)}} d\tau. \tag{7}$$

Використавши умови (6) та розв'язок (7), матимемо

$$\begin{cases} \varphi(t) + \int_0^t \dfrac{a}{\sqrt{\pi}\sqrt{t-\tau}} \psi(\tau) e^{-\frac{l^2}{4a^2(t-\tau)}} d\tau = \omega_1(t), \\ \psi(t) + \int_0^t \dfrac{e^{-\frac{l^2}{4a^2(t-\tau)}}}{2a\sqrt{\pi}(t-\tau)^{3/2}} \varphi(t)\,d\tau - l^2 \int_0^t \dfrac{e^{-\frac{l^2}{4a^2(t-\tau)}}}{4a^3(t-\tau)^{5/2}} \varphi(\tau)\,d\tau = \omega_2(t). \end{cases} \tag{8}$$

В результаті знову отримується система інтегральних рівнянь відносно $\varphi(t)$ і $\psi(t)$.

*Двовимірний випадок*. Ідея потенціалу може застосовуватись і до багатовимірних задач теплопровідності [2]. Розглянемо двовимірний випадок, тобто рівняння

$$u_t = a^2(u_{xx} + u_{yy}). \tag{9}$$

Аналог потенціалу простого шару визначається формулою:

$$u(x,y,t) = \frac{1}{2\pi}\int_0^t d\tau \int_l \frac{a(\sigma,\tau)}{(t-\tau)} e^{-\frac{r^2}{4a^2(t-\tau)}} d\sigma, \tag{10}$$

де $\sigma$ — довжина дуги контуру $l$ і $a(\sigma,\tau)$ — функція змінної контуру $\sigma$ і часового параметра $\tau$, $r^2 = (\xi - x)^2 + (\eta - y)^2$, $r$ — відстань від точки $(x,y)$ до змінної $\sigma$ контуру $l$. Тепловий потенціал подвійного шару представляється формулою

$$v(x,y,t) = \int_0^t d\tau \int_l \frac{b(\sigma,\tau)}{4\pi a^2 (t-\tau)^2} e^{-\frac{r^2}{4a^2(t-\tau)}} r\cos(r,n)\, d\sigma, \tag{11}$$

де $n$ — напрям зовнішньої нормалі в точці інтегрування.

Шукана функція $v(x,y,t)$ задовольняє рівняння (9), яке має на контурі $l$ задані крайові умови:

$$v\big|_l = \omega(s,t), \tag{12}$$

де $s$ — координата точки контуру, що визначається довжиною дуги $s$, яка відраховується від деякої точки. Початкові умови вважаються рівними нулю. Шукаючи розв'язок у вигляді подвійного шару (11) отримуємо інтегральні рівняння для функції $b(\sigma,\tau)$:

$$-b(s,t) + \int_0^t d\tau \int_l \frac{b(\sigma,\tau)}{4\pi a^2 (t-\tau)^2} e^{-\frac{r^2}{4a^2(t-\tau)}} r\cos(r,n)\, d\sigma = \omega(s,t). \tag{13}$$

У даному рівнянні інтегрування по $\sigma$ здійснюється за фіксованим проміжком $(0,L)$, де $L$ — довжина контуру $l$, і по $\tau$, де верхня границя є змінною. Іншими словами, отримане інтегральне рівняння має характер рівнянь Фредгольма за відношенням до змінної $\sigma$ і характер рівнянь Вольтерри за відношенням до змінної $\tau$.

*Задача теплопровідності з рухомою границею*. Розглянемо на прикладі застосування методу теплових потенціалів до задач із рухомою границею. Задача формулюється наступним чином: знайти розв'язок рівнянь

$$\frac{\partial u_1}{\partial t} = a_1^2 \frac{\partial^2 u_1}{\partial x^2}, \quad 0 < x < a\sqrt{t}, \quad t > 0, \tag{14}$$

$$\frac{\partial u_2}{\partial t} = a_2^2 \frac{\partial^2 u_2}{\partial x^2}, \quad a\sqrt{t} < x < \infty, \quad t > 0, \tag{15}$$

з крайовими умовами

$$\begin{cases} u_1(0,t) = \varphi(t), \quad 0 < t < \infty, \\ u_1(a\sqrt{t},t) = u_2(a\sqrt{t},t) = \psi(t), \quad 0 < t < \infty, \\ u_2(\infty,t) = 0, \quad 0 < t < \infty, \\ u_2(x,0) = 0, \quad 0 < x < \infty, \end{cases} \tag{16}$$

та умовою узгодження

$$\varphi(0) = \psi(0). \tag{17}$$

Розв'язок шукаємо у вигляді теплових потенціалів подвійного шару:

$$u_1(x,t) = \int_0^t \frac{x e^{-\frac{x^2}{4a_1^2(t-\tau)}} \mu_1(\tau)}{2a_1\sqrt{\pi}(t-\tau)^{3/2}} d\tau + \int_0^t \frac{\left(x - a\sqrt{\tau}\right) e^{-\frac{\left(x-a\sqrt{\tau}\right)^2}{4a_2^2(t-\tau)}} \mu_2(\tau)}{2a_1\sqrt{\pi}(t-\tau)^{3/2}} d\tau, \tag{18}$$

$$u_2(x,t) = \int_0^t \frac{x - a\sqrt{\tau}}{2a_2\sqrt{\pi}(t-\tau)^{3/2}} e^{-\frac{\left(x-a\sqrt{\tau}\right)^2}{4a_2^2(t-\tau)}} v(\tau)\, d\tau. \tag{19}$$

Для виконання граничних умов отримуємо систему двох інтегральних рівнянь відносно $\mu_1(t)$ і $\mu_2(t)$ та одне рівняння відносно $v(t)$:

$$\begin{cases} \varphi(t) = -\frac{k_1}{\pi} \int_0^t \frac{\tau^{1/2}}{(t-\tau)^{3/2}} e^{-\frac{k_1^2\tau}{t-\tau}} \mu_2(\tau)\, d\tau + \mu_1(t), \\ \psi(t) = \int_0^t \frac{k_1\zeta\mu_2(\tau) e^{-\frac{k_1^2\zeta^2}{t-\tau}}}{\sqrt{\pi}(t-\tau)^{3/2}} d\tau + \int_0^t \frac{k_1\sqrt{t} e^{-\frac{k_1^2 t}{t-\tau}} \mu_1(\tau)}{\sqrt{\pi}(t-\tau)^{3/2}} d\tau - \mu_2(t), \end{cases} \tag{20}$$

$$\psi(t) = v(t) + \frac{k_2}{\sqrt{\pi}} \int_0^t \frac{\zeta}{(t-\tau)^{3/2}} e^{-\frac{k_2^2\zeta^2}{t-\tau}} v(\tau)\, d\tau, \tag{21}$$

де $k_1 = \alpha / 2a_l$, $l = 1,2$, $\zeta = \left(\sqrt{t} - \sqrt{\tau}\right)$.

Розглянуті вище приклади показали, що розв'язок поставленої задачі задається у вигляді інтегральних операторів Вольтерри або їх сум (4), (7), (11), (18), (19) в яких присутня невідома функція, що визначається із крайових умов, які задаються інтегральними рівняннями Вольтерри II роду або їх системами (5), (8), (13), (20), (21) відповідно.

Підхід до розв'язування сингулярних інтегральних рівнянь і їх систем може полягати в наступному. Для розв'язування даних рівнянь пропонується застосовувати чисельні методи, основані на методі квадратур [3]. При побудові алгоритмів розв'язування таких систем необхідно враховувати сингулярність ядер інтегральних моделей у точці $\tau = t$. Застосування методу зсуву сітки на $h/2$ ($h$ — крок моделювання) дозволяє уникнути сингулярності [7]. Оскільки в даних моделях особливою є кінцева точка інтегрування, то для апроксимації інтегралів квадратурними сумами доцільно застосовувати метод лівих прямокутників. Компенсувати втрату точності методу квадратур можна шляхом застосування адаптивного методу зміни кроку моделювання в околі особливої точки.

**Висновки.** Запропонований метод розв'язування нестаціонарних задач теплопровідності дає змогу враховувати особливість та використати переваги як аналітичного методу теплових потенціалів, так і обчислювальних квадратурних методів. Така постановка задачі дозволяє знаходити розв'язки в необхідних точках, не шукаючи розв'язки у всіх точках просторової координати. Крім того, оскільки розв'язки в кожній точці є незалежними один від одного і можуть обчислюватись у різних потоках, то є можливість підвищення ефективності обчислень на основі застосування паралельних алгоритмів.

## Список використаних джерел:


1. Carslaw H. S., Jaeger J. C. Conduction of Haet in Solids. *Oxford Science Publications*. Oxford University Press, 1986. 520 p.
2. Белоносов С. М., Овсиенко В. Г., Карачун В. Я. Применение интегральных представлений к решениям задач теплопроводности и динамики вязкой жидкости. Київ : Вища школа, 1989. 163 с.
3. Верлань А. Ф., Сизиков В. С. Интегральные уравнения: методы, алгоритмы, программы. Киев : Наук. думка, 1986. 542 с.
4. Карташов Э. М., Кудинов В. А., Калашников В. В. Теория тепломассопереноса: решение задач для многослойных конструкций : учеб. пособ. для бакалавриата, специалитета и магистратуры. М. : Издательство Юрайт, 2018. 435 с.
5. Пилипенко Н. В. Методы и приборы нестационарной теплометрии на основе решения задач теплопроводности. Санкт-Петербург : СПбГУ ИТМО, 2011. 180 с.
6. Самарский А. А., Вабищевич П. Н. Вычислительная теплопередача. М. : Едиториал УРСС, 2003. 784 с.
7. Сизиков В. С., Смирнов А. В., Федоров Б. А. Численное решение сингулярного интегрального уравнения Абеля обобщенным методом квадратур. *Изв. вузов. Матем.* 2004. № 8. С. 62–70.
8. Скопецький В. В., Стоян В. А., Кривонос Ю. Г. Математичне моделювання прямих та обернених задач динаміки систем з розподіленими параметрами. Київ : Наукова думка, 2002. 361 с.

# INTEGRAL MODELS OF NON-STATIONARY HEAT CONDUCTION PROBLEMS BASED ON THE METHOD OF THERMAL POTENTIALS

The article discusses the approach to the construction of integral models of non-stationary problems of heat conduction based on the application of the method of thermal potentials. The possibility of constructing integral models is considered on specific examples using different thermal potentials: a one-dimensional heat conduction problem with different formulation of a boundary value problem (conditions of the first and second kind), the two-dimensional problem of heat exchange, the problem of heat exchange with a moving boundary. It is proposed to use a combination of exact and numerical methods, which allows to take into account the advantages of various approaches. The application of the method of thermal potentials to models in the form of partial differential equations allowed us to obtain a general solution in the form of the Volterra operator, which depends on the functions that are determined from the boundary conditions. That is, the task is reduced to solving the Volterra integral equations of the second kind or their systems. A feature of the models obtained is that the cores of integral models are singular at the end point of integration. It is proposed to solve such equations using computational methods that are based on the quadrature method. To avoid features in the kernel, the offset method is used. Taking into account the properties of the core, it is proposed to apply the method of left rectangles, which will avoid the singularity. To improve the accuracy of building a solution, it is proposed to apply the adaptive algorithm for compaction of simulation step in the vicinity of a singular point. The proposed approach to solving non-stationary problems of heat conduction takes into account the advantages of exact (thermal potential method) and computational methods (quadrature method) and allows to increase the efficiency of calculations based on the parallelization of the problem.

**Key words:** *nonstationary heat conduction problem, potential method, integral equations, quadrature method, singular integral equations.*

Одержано 15.02.2019

УДК 519.8
DOI: 10.32626/2308-5916.2019-19.31-37

**В. М. Горбачук*,** д-р фіз.-мат. наук,
**М. С. Дунаєвський*,** магістр,
**О. О. Морозов**,** магістр

*Інститут кібернетики імені В.М. Глушкова НАН України, м. Київ,
**Науково-виробниче приватне підприємство «Гіперон», м. Київ

# ХАРАКТЕРИСТИКИ РІВНОВАГ ЛАНЦЮГІВ ПОСТАЧАННЯ

Мета роботи — розробити базову теорію глобальних ланцюгів постачання. Нехай світова економіка складається з довільної кількості країн, які мають один виробничий фактор (фактор праці) і виробляють один кінцевий продукт, що потребує континуум проміжних продуктів. Кінцевий продукт є результатом послідовних стадій виробництва проміжних продуктів, у процесі якого трапляється брак. Можна довести, що існує єдина рівновага вільної торгівлі, в якій країни з нижчими ймовірностями браку на всіх стадіях спеціалізуються на пізніших стадіях виробництва. Спираючись на цю просту теоретичну базу, можна запропонувати форму вертикальної спеціалізації взаємозалежних країн.

Явище вертикальної спеціалізації привертає в однаковій мірі увагу розробників стратегій, ділових лідерів, економістів. Можливість транскордонної фрагментації виробничих процесів впливає на обсяги, риси і наслідки міжнародної торгівлі. Залишаються відкритими питання механізмів впливу глобальних і локальних технологічних змін на участь різних країн в одному й тому самому ланцюгу постачання, а також механізмів впливу вертикальної спеціалізації на взаємозалежність держав.

Оскільки в моделях загальної рівноваги з довільною (великою) кількістю товарів і країн, незалежно від наявності послідовного виробництва, важко отримати зрозумілі передбачення порівняльної статики, то потрібна проста теорія торгівлі з послідовним виробництвом. Для цього потрібні деякі ідеї щодо ієрархій у моделях часткової рівноваги для закритої економіки. Зосередимося на середовищі, в якому виробництво є послідовним і може містити брак. Моделі ієрархій застосовувалися до вивчення питань міжнародної торгівлі. Наприклад, модель знаннєвої економіки використовується для дослідження транскордонних парос получень між агентами з неоднорідними здібностями і відповідних наслідків для нерівності у даній державі. Нерівність у державі внаслідок ієрархій при торгівлі досліджувалася також в інших моделях. Припускається, що все населення даної держави має однакові здібності.

**Ключові слова**: *рівновага, ланцюги постачання, стадії виробництва, кінцевий продукт, проміжні продукти.*

© В. М. Горбачук, М. С. Дунаєвський, О. О. Морозов, 2019

**Вступ.** Нехай організаційна проблема фірми при виробництві кінцевого товару полягає у виконанні виробничих стадій $j \in [0,1]$, де більший індекс відповідає більшій близькості до кінцевого продукту (нижчій стадії течії ланцюга постачання) [1]. Позначимо $x(j)$ вхідний обсяг (вхід) сумісних (з фірмою) проміжних послуг, які надає фірмі постачальник на стадії $j$ (якщо ці послуги несумісні, то $x(j) = 0$) [2]. Тоді обсяг (quantity) випуску кінцевого товару з урахуванням його якості становить

$$q(m=1) = \theta\left(\int_0^{m=1} [x(j)]^{\alpha} I(j)dj\right)^{1/\alpha}, \qquad (1)$$

де $\theta$ — параметр продуктивності, $\alpha \in (0,1)$ — параметр симетричного ступеня заміни серед входів стадій, $I(j)$ — індикаторна функція, значення якої дорівнює 1 при виконанні всіх попередніх стадій $i \in [0, j)$ і дорівнює 0 в решті випадків. Хоча виробництво вимагає виконання всіх стадій, додатність $\alpha$ гарантує додатність випуску при несумісності входів на деяких стадіях: незважаючи на важливість усіх стадій з інженерної точки зору, можна допускати їх деяку замінюваність через те, що характеристики входів формують обсяг кінцевого продукту з урахуванням його якості [3]. Наприклад, виробництво автомобіля вимагає чотири колеса, дві фари, одне кермо тощо, але цінність цього автомобіля для споживачів типово залежатиме від послуг, отриманих від цих різних компонентів, де вища якість певних частин означатиме гіршу якість інших.

Виробнича функція (1) схожа на звичайну функцію з постійною еластичністю заміни (constant elasticity of substitution, CES) з нескінченною кількістю входів, але індикаторна функція $I(j)$ породжує, по суті, послідовну технологію виробництва тому, що нижчі стадії течії є марними при невиконанні вищих стадій.

Технологію (1) можна виразити у диференціальній формі, застосовуючи правило Лейбніца (Leibniz):

$$\alpha [q(m)]^{\alpha-1} q'(m) = \frac{d}{d\,m},$$

$$[q(m)]^{\alpha} = \frac{d}{d\,m}\theta^{\alpha}\left(\int_0^{m} [x(j)]^{\alpha} I(j)dj\right) = \theta^{\alpha}[x(m)]^{\alpha} I(m),$$

$$q'(m) = \frac{1}{\alpha}\theta^{\alpha}[x(m)]^{\alpha}[q(m)]^{1-\alpha} I(m).$$

Отже, граничне підвищення випуску, внесене постачальником на стадії $m$ процесу виробництва, задається простою функцією Кобба–Дугласа, залежною від сумісного входу цього постачальника й обсягу випуску з урахуванням якості, виробленого до цієї стадії (проміжного входу до стадії $m$).

Припускаємо, що є велика кількість постачальників, які максимізують свої прибутки [4]. Вони можуть залучатися до виробництва проміжних входів фірми або альтернативної діяльності, що не стосується кінцевого товару фірми [5]. Нехай кожному проміжному входу (продукту) взаємно однозначно відповідає свій постачальник, з яким фірма повинна укласти контракт [6]. Кожний постачальник має здійснити певну інвестицію у взаємозв'язки ланцюга постачання для виробництва сумісного входу. Якщо вхід налаштований виключно під виробника кінцевого товару, то цінність цього входу для альтернативних покупців рівна 0. Хоча послідовність виробництва породжує асиметрії, всі стадії виробництва (всіх постачальників) вважаємо симетричними за граничними витратами (cost) на інвестиції, рівними $c$: одиниця інвестицій генерує одиницю послуг сумісного входу стадії $j$ для поєднання з входами постачальників вищих стадій течії. Несумісні входи можуть вироблятися всіма учасниками (включаючи фірму) з нульовими граничними витратами, без вартості для виробництва кінцевого товару і без шкоди для продовження виробничого процесу.

З точки зору споживачів кінцевий товар є диференційованим, бо належить до галузі, в якій фірми виробляють континуум товарів, а споживчі переваги мають властивість CES з еластичністю $\frac{1}{1-\rho}$ поміж цих товарів ($\rho \in (0,1)$). Нехай нарахована субкорисність (sub-utility) від споживання товарів галузі дорівнює

$$U = \left( \int\limits_{\omega \in \Omega} [\varphi(\omega)\tilde{q}(\omega)]^{\rho} d\omega \right)^{\frac{1}{\rho}}, \qquad (2)$$

де $\tilde{q}(\omega)$ — обсяг споживання товару $\omega$ (у фізичних одиницях) якості $\varphi(\omega)$, $\Omega$ — множина товарів. Можна довести, що максимізація функції (2) при бюджетному обмеженні

$$\int\limits_{\omega \in \Omega} p(\omega)\tilde{q}(\omega) d\omega = E$$

дає споживчий попит, який має властивість CES з еластичністю $\frac{1}{1-\rho}$ ($E$ позначено витрати (expenditure), а $p(\omega)$ — ціну (price) товару). Крім того, неявна функція виручки фірми, що продає товар, є увігну-

тою за обсягом випуску $q(\omega) = \tilde{q}(\omega)\varphi(\omega)$ з урахуванням якості. Тоді виручка (revenue) від виробництва кінцевого товару рівна

$$r = A^{1-\rho}[q(m=1)]^{\rho} = A^{1-\rho}\theta^{\rho}\left(\int_0^{m=1}[x(j)]^{\alpha} I(j)dj\right)^{\frac{\rho}{\alpha}},$$

де $A$ — деякий параметр зсуву попиту галузі, екзогенний для фірми.

Спочатку розглянемо повні контракти, в яких фірма має повний контроль над усіма інвестиціями, а так над вхідними послугами на всіх стадіях: для кожного входу $j \in [0,1]$ фірма здійснює контрактну пропозицію $[x(j), s(j)]$, за якою постачальник зобов'язаний надати обсяг $x(j)$ сумісних входів, як передбачено у контракті, в обмін на платіж $s(j)$. Оскільки фірма має стимул дотримуватися природної послідовності виробництва, то $I(j) = 1 \ \ \forall j$, а фірма, шукаючи оптимальний повний контракт, максимізує за всіма допустимими контрактними пропозиціями $[x(j), s(j)] \ \ \forall \ \ j \in [0,1]$ свій прибуток

$$\pi = r - \int_0^1 s(j)dj = A^{1-\rho}\theta^{\rho}\left(\int_0^1 [x(j)]^{\alpha} dj\right)^{\frac{\rho}{\alpha}} - \int_0^1 s(j)dj$$

при обмеженнях $s(j) \geq c\,x(j)$. Розв'язання цієї задачі оптимізації дає однакові для всіх проміжних входів рівні інвестицій $x(j)$ і платежів $s(j) = c\,x(j) \ \ \forall j$ (звідки чистий виграш постачальників є нульовим).

Для втілення повних контрактів важливо, щоб судовий порядок був здатним верифікувати точну вартість вхідних послуг, які надаються постачальниками різних стадій. Однак на практиці суд загалом не є здатним верифікувати те, є входи сумісними чи ні, відповідають надані сумісними входами послуги записаним у контракті положенням чи ні. Водночас зазначимо, що фірма не є схильною укладати зв'язуючі (юридично обов'язкові) контракти, які залежать від обсягу входів і не залежать від їх сумісності, бо постачальники можуть мати стимул до дешевого виробництва несумісних (з фірмою) входів і вимагати від фірми платежі [7]. Можна уявити, що контракти, залежні від загальної виручки, забезпечуватимуть інвестиційні стимули для постачальників, але у даній постановці з континуумом постачальників подібні контракти не матимуть цінності, бо зводитимуться до нульових інвестиційних рівнів. Тому природно вивчати ситуації, в яких умови обміну між фірмою і постачальниками не є жорсткими у втілюваному ex-ante контракті [6–8]. Фактично вважається, що початковий контракт лише вказує те, є постачальники вертикально інтегрованими з фірмою чи ні (залишаючись незалежними).

Згаданий недолік зв'язуючого контракту породжує відому проблему затримки (holdup). Фактичний платіж конкретному постачальнику (скажімо, стадії $m$) є предметом двосторонніх переговорів лише після виробництва входу стадії $m$ й отримання можливості фірми інспектувати результат цього виробництва. Нехай ці переговори не залежать від двосторонніх переговорів на інших стадіях. Оскільки проміжний вхід вважається сумісним тільки з випуском фірми, то решта можливостей постачальника на стадії переговорів зводиться до нуля. Тому квазіренти у переговори між фірмою і постачальником задаються приростом внеску в загальну виручку, породженим постачальником $m$ на стадії переговорів. При обчисленні цього внеску зазначимо, що фірма спілкується з постачальниками виключно з міркувань технологічної послідовності виробництва і завжди може в односторонньому порядку виконати дану стадію шляхом власного виробництва несумісного входу. Таке жорстке припущення можна послабити можливістю часткових контрактів: коли частка інвестицій постачальників верифікується і визначається контрактом, то фірма може скористатися формальним контрактом для забезпечення мінімального обсягу сумісних вхідних послуг постачальника, достатнього для продовження виробничого процесу. Як наслідок, $I(j)=1 \quad \forall j < m$, а вартість виробництва кінцевого товару, гарантована до стадії $m$, задається

$$r(m) = A^{1-\rho}\theta^{\rho}\left(\int_0^m [x(j)]^{\alpha}\,dj\right)^{\frac{\rho}{\alpha}},$$

звідки правило Лейбніца дає

$$\frac{\alpha}{\rho}[r(m)]^{\frac{\alpha}{\rho}-1} r'(m) = \frac{d}{d\,m},$$

$$[r(m)]^{\frac{\alpha}{\rho}} = \frac{d}{d\,m}(A^{1-\rho}\theta^{\rho})^{\frac{\alpha}{\rho}}\left(\int_0^m [x(j)]^{\alpha}\,dj\right) = (A^{1-\rho}\theta^{\rho})^{\frac{\alpha}{\rho}}[x(m)]^{\alpha},$$

$$r'(m) = \frac{\rho}{\alpha}(A^{1-\rho}\theta^{\rho})^{\frac{\alpha}{\rho}}[x(m)]^{\alpha}[r(m)]^{1-\frac{\alpha}{\rho}}. \qquad (3)$$

За теорією прав власності для меж фірми, ефективна переговорна сила фірми стосовно конкретного постачальника залежить від того, володіє фірма цим постачальником чи ні. Можна припустити, що власність постачальників є джерелом ринкової влади у сенсі здатності фірми діставати більшу частку ринкового надлишку від інтегрованих постачальників порівняно з не інтегрованими [6–8]. Коли контракти є неповними, то факт контролю інтегратором (фірмою) фізичних активів виробництва дозволятиме інтегратору диктувати використання цих активів, яке схи-

лятиме поділ ринкового надлишку на свою користь. Для простоти не деталізуватимемо природу таких переговорів ex-post і припускатимемо, що фірма отримуватиме частку $\beta_V$ додаткового внеску у вартість (value) (3), коли постачальник є інтегрованим, і меншу частку $\beta_O < \beta_V$ цього внеску, коли постачальник є неінтегрованим.

Модель з континуумом постачальників відповідає граничному випадку $\varepsilon \to 0$ дискретної моделі з $M$ постачальниками, кожний з яких контролює частину $\varepsilon = \frac{1}{M}$ континууму проміжних входів.

**Висновки.** Стимул фірми до інтеграції постачальників виявляє систематичну мінливість залежно від відносного положення (вище чи нижче течії ланцюга постачання) постачальника у виробництві. Така залежність визначається еластичністю попиту на кінцевий товар. Можна враховувати різні джерела асиметрії поміж виробників кінцевих товарів і постачальників [8].

**Список використаних джерел:**


1. Costinot A., Vogel J., Wang S. An elementary theory of global supply chains. *Review of economic studies.* 2013. 80(1). P. 109–144.
2. Морозов А. А. Сравнительный анализ способов управления цепочками поставок. *Економіка та управління АПК*. 2009. Вип. 1. С. 90–94.
3. Морозов А. А. Аналіз моделей ризик-орієнтованого аутсорсингу в системі управління ланцюгами постачання. *Компьютерная математика.* 2014. № 2. С. 64–73.
4. Nagurney A., Dong I., Zhang D. A supply chain network equilibrium model. *Transportation research. Part E: Logistics and transportation review*. 2002. № 38 (5). P. 281–303.
5. Горбачук В. М., Дунаєвський М. С., Морозов О. О. Рівноважні інвестиції у кібербезпеку мережі ланцюгів постачання. *Вісник Київського університету.* Серія: фізико-математичні науки. 2017. № 2. С. 47–52.
6. Морозов А. А. Приложения теории цепочек снабжения. *Теорія оптимальних рішень*. 2015. С. 119–125.
7. Морозов А. А. Реализация модели интеграции цепи поставок в агромашиностроении. *Компьютерная математика*. 2016. № 1. С. 20–27.
8. Горбачук В. М. Дослідження операцій і ланцюгів постачання для досягнення корпоративної порівняльної переваги. *Науковий вісник Херсонського державного університету*. Серія: економічні науки. 2014. Вип. 7. Ч. 5. С. 178–183.


## THE CHARACTERISTICS OF SUPPLY CHAIN EQUILIBRIA


The goal of this work is to develop a basic theory of global supply chains. Let the world economy consist of an arbitrary number of countries having the only production factor (labor) and producing the only final good requiring continuum of intermediate products. The final good is the result of consequtive stages for production of intermediate products where mistakes occur during the production processes. One can prove there is the only free trade equilibrium

where the countries with lower probabilities of mistakes on all stages are specialized on the later stages of production. Using the simple theoretical basis, one may suggest a form of vertical specialization for interdependent countries.

Policy makers, business leaders, economists equally pay attention to the phenomenon of vertical specialization. The option of transboundary fragmentation for production processes affects amounts, features, and consequences of international trade. The issues how global and local technology changes influnce on participation of various countries in the same supply chain, how vertical specialization influence on interdependence of countries remain opened.

As the general equilibrium models with an arbitrary (large) number of products and countries, regardless of sequential production presence, do not give clear comparative static predictions, a simple trade theory with sequential production is needed. It requires some ideas about hierarchies in partial equilibrium models of a closed economy. The environment where production may contain mistakes is the focus. Models of hierarchies have been applied to the international trade questions. For instance, the kowledge economy model is used for research of transboundary matching between agents with nonuniform abilities and corresponding consequences for inequality in a given country. Inequality in a country due to hierarchies at trade has been investigated by other models as well. It is assumed all people of a given country have equal abilities.

**Key words:** *equilibrium, supply chains, production stages, final good, intermediate products.*

Одержано 15.02.2019

УДК 004.728:004.728.3,004.056.055
DOI: 10.32626/2308-5916.2019-19.37-43

**І. Д. Горбенко*,****, д-р техн. наук,
**О. А. Замула***, д-р техн. наук,
**Хо Чі Лик****

*Харківський національний університет імені В. Н. Каразіна, м. Харків,
******АТ «Інститут інформаційних технологій», м. Харків

# ОПТИМІЗАЦІЯ ПОШУКУ ДИСКРЕТНИХ СКЛАДНИХ СИГНАЛІВ З НЕОБХІДНИМИ ВЛАСТИВОСТЯМИ ДЛЯ ЗАСТОСУВАННЯ У СУЧАСНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Серед основних напрямків покращення показників ефективності функціонування інформаційно-комунікаційних систем (ІКС), зокрема, завадозахищеності, скритності, інформаційної безпеки, можна виділити напрямки, пов'язані із застосуванням фазоманіпульованих широкосмугових сигналів (ФМ ШПС) і частотно-фазоманіпульованих (ЧФМ) сигналів. Оскільки в багатокористувачевих системах, кодовий поділ каналів ґрунтується на відмінності сигналів, то побудова ІКС і показ-

© І. Д. Горбенко, О. А. Замула, Хо Чі Лик, 2019

ники ефективності зазначених систем визначаються вибором сигналів і їх властивостями. При цьому, як дискретні послідовності (ДП), які розширюють спектр (маніпулюють несучу частоту), повинні бути використані ДП, які засновані на нелінійних правилах побудови і мають покращені кореляційні, ансамблеві і структурні властивості. Зокрема, при використанні таких сигналів як фізичного переносника інформації або сигналів синхронізації часові витрати на розкриття структури використовуваних сигналів зростають і постановка «оптимальних», з точки зору станції протидії, перешкод стає проблематичною. Складні сигнали, отримані на основі таких послідовностей, володіють, з одного боку, структурними властивостями, аналогічними властивостям випадкових (псевдовипадкових) послідовностей, а з іншого — необхідними ансамблевими і кореляційними властивостями. Мінімізація рівня бічних пелюсток АКФ має найбільше значення при конструюванні сигналу для таких додатків як вимір часу запізнювання, часовий дозвіл й ін. У даній роботі сформульована і вирішена задача оптимізації синтезу нелінійних дискретних послідовностей, які мають покращені ансамблеві, структурні і автокореляційні властивості. Застосування нелінійних дискретних сигналів, які утворені на основі таких послідовностей, дозволить забезпечити необхідні значення завадозахищеності, інформаційної та структурної скритності функціонування ІКС.

**Ключові слова:** *дискретна послідовність, криптографічний сигнал, функція кореляції, ізоморфізм, кінцеве поле.*

**Вступ.** До інформаційно-комунікаційних систем (ІКС), особливо, критичного призначення, пред'являються все більш жорсткі вимоги щодо забезпечення ефективності їх функціонування (продуктивності, достовірності передавання інформації, живучості, завадозахищеності, інформаційної безпеки) [1, с. 154–156]. Існує протиріччя між жорсткими вимогами щодо забезпечення зазначених показників, з одного боку, і існуючими моделями, методами і технологіями керування ІКС, інформаційною безпекою, з іншого боку. Основними шляхами вирішення зазначеного протиріччя є підвищення завадозахищеності та інформаційної безпеки ІКС на основі розробки методів синтезу нових класів сигналів — переносників даних з необхідними ансамблевими, кореляційними і структурними властивостями.

**Синтез систем сигналів із заданими кореляційними властивостями.** В роботі [2] показано, що процес вибору раціональних по тих чи інших критеріях дискретних сигналів (ДС) тотожний синтезу відповідних дискретних послідовностей (ДП), за допомогою яких маніпулюють, наприклад, фазу несучої частоти. Як критерій вибору класу ДС (як правило), орієнтуються на мінімаксний критерій. Такий критерій має на

увазі побудову ансамблів сигналів, які як можна помітніше відрізняються один від одного. Кількісною мірою відмінності ДП служать максимальні рівні бічних пелюсток функції автокореляції в аперіодичному (АФАК) і періодичному режимах передачі (ПФАК).

Виходячи з цього широкосмугові сигнали (ШСС), повинні володіти такими кореляційними властивостями, коли бічні піки кореляційних функцій ШСС є якомога меншими, тобто в ідеальному випадку повинні прагнути до нуля. У теорії складних сигналів відомий ряд інтегральних рівності [2]. Нехай $C$ множина комплексних чисел, а $C^N$ множина векторів з комплексними компонентами. Елементи множини $w, x, y, z \in C^N$ довільні вектори, а $w, x, y, z$ відповідні їм дискретні послідовності. Чотири взаємно-кореляційні функції $R_{w,x}$, $R_{y,z}$, $R_{w,y}$, $R_{x,z}$ пов'язані співвідношенням

$$\sum_{l=0}^{N-1} R_{w,y}(l)[R_{x,z}(l+n)]^* = \sum_{l=0}^{N-1} R_{w,x}(l)[R_{y,z}(l+n)]^* . \quad (1)$$

Поклавши в (1) $z = y$, отримаємо

$$\sum_{l=0}^{N-1} R_{w,y}(l)[R_{x,y}(l+n)]^* = \sum_{l=0}^{N-1} R_{w,x}(l)[R_{y}(l+n)]^* . \quad (2)$$

Поклавши в (2) $w = x$, отримаємо

$$\sum_{l=0}^{N-1} R_{x,y}(l)[R_{x,y}(l+n)]^* = \sum_{l=0}^{N-1} R_{x}(l)[R_{y}(l+n)]^* . \quad (3)$$

Нарешті, поклавши в (5) $n = 0$, отримаємо

$$\sum_{l=0}^{N-1} \left|R_{x,y}(l)\right|^2 = \sum_{l=0}^{N-1} R_{x}(l)[R_{y}(l)]^* . \quad (4)$$

За допомогою (1)–(4) отримано ряд важливих границь оцінки кореляційних функцій. Рівність (3) означає, що автокореляційна функція (АКФ) послідовності $R_{x,y}$ збігається з взаємно-кореляційною функцією (ВКФ) послідовностей $R_x$ і $R_y$. Крім того, з (4) слід, що середнє значення квадрата модуля функції взаємної кореляції сигналів $x$ і $y$ дорівнює середньому значенню твору їх АКФ. Фактично це означає, що сигнали, що володіють хорошими автокореляційними властивостями будуть володіти і хорошими властивостями ВКФ. ПФАК послідовності $\{a_0, a_1, \ldots . a_{N-1}\}$ має вид [3, с. 141–143]:

$$\rho_p(m) = \frac{1}{\left\|a^2\right\|} \sum_{i=m}^{N-1} a_i \cdot a_{i-m}^* + \frac{1}{\left\|a^2\right\|} \sum_{i=0}^{m-1} a_i \cdot a_{i-m}^* , m \geq 0 . \quad (5)$$

Перший доданок у виразі (5) є АФАК, тоді як другий — дорівнює $p_a(m-N)$. В результаті отримуємо співвідношення, що зв'язує ПФАК із своїм аперіодичним аналогом:

$$\rho_p(m) = \rho(m) + \rho_a(m-N), m = 0,1,....N\ . \quad (6)$$

Рівність нулю всіх бічних пелюсток неможливо для аперіодичних ФМ сигналів. Тоді крайній правий боковий пік нормованої АФАК ДП сигналу буде:

$$P_a(N-1) = \frac{a_0 a_{N-1}}{\|a\|^2} \neq 0\ . \quad (7)$$

Останнє співвідношення призводить до застосування мінімаксного критерію при синтезі сигналів. Формальна запис даного критерію має вигляд:

$$\rho_{a,\max} = \max_{m\neq 0}\left\{\left|\rho_a(m)\right|\right\} = \min. \quad (8)$$

Таким чином вимоги, що пред'являються до найкращого сигналу, можуть бути сформульовані у вигляді такої оптимізаційної задачі: на безлічі всіх можливих послідовностей довжини $N$ з символами з обраного алфавіту знайти послідовності з мінімальною величиною максимального бічного пелюстка АФАК. Загальна ідея алгоритмів, спрямованих на вирішення цієї задачі, полягає у попередньому відборі деякої обмеженої множини послідовностей, і подальшому пошуку послідовностей з мінімальним значенням серед послідовностей, які увійшли у зазначену множину. Одним із прикладів такої стратегії, є використання співвідношення (6). Позначаючи $\rho_{p,\max}$, максимальний бічний пелюсток ПФАК: $\rho_{p,\max} = \max_{m=1,2,...n-1}\left\{\left|\rho_p(m)\right|\right\}$, і використовуючи нерівність: $\max\left\{|x+y|\right\} \le \max\left\{|x|+|y|\right\} \le \max\left\{|x|\right\} + \max\left\{|y|\right\}$, приходимо до оцінки $\rho_{p,\max} \le \rho_{a,\max}$ або:

$$\rho_{a,\max} \ge \frac{1}{2}\rho_{p,\max}\ . \quad (9)$$

Випливає, що ДП з хорошою АФАК можуть бути знайдені серед послідовностей з хорошими характеристиками ПФАК.

Таким чином, ДП з відповідними значеннями бокових піків АФАК, можуть бути відібрані з множини ДП, значення бокових піків ПФАК яких є оптимальними. Саме ці обставини були застосовані для проведення оптимізації пошуку ДС з покращеними характеристиками АФАК. До оптимальних (з точки зору ПФАК) за мінімаксним критерієм відносяться нелінійні характеристичні дискретні сигналів (ХДС) [4, с. 125–129]. Досліджені автокореляційні властивості даного

класу сигналів у аперіодичному режимі передачі. Зокрема, встановлено, що для періоду ДП 256 елементів існує 56 ДП, для яких значення максимальних бічних піків АФАК не перевищує значення 18 (1,1√N). Було синтезовано 470 ХДС, нормовані значення максимальних бічних піків АФАК яких, не перевищують величини 20/256. У стандарті системи з кодовим поділом UMTS як код первинної синхронізації використовується бінарна синхропослідовність (СП) з періодом 256 елементів, які володіють $\rho_{a,\max}$ аж до ¼, тобто $\rho_{a,\max}$ = 64. При виборі ХДС як СП, у порівнянні з сигналами, що застосовуються в стандарті UMTS, виграш, з точки зору завадостійкості прийому сигналів, складе більше 4 дБ. В роботах [5–7] показано, що застосування криптографічних сигналів (КС) дозволить суттєво покращити показники інформаційної безпеки, скритності функціонування ІКС. З метою підвищення завадостійкості прийому сигналів була висунута гіпотеза щодо можливості застосування саме КС як фізичних переносників даних, а також як СП. Для перевірки гіпотези синтезовано 680 КС, $\rho_{a,\max}$ АФАК для яких, не перевищує значень 33. В цьому випадку, як показали розрахунки, виграш з точки зору завадостійкості прийому СП у порівнянні з використання ДП, що застосовуються в стандарті UMTS, складає 3 дБ. Якщо висуваються більш жорсткі умови до завадозахищеності прийому сигналів в ІКС, можна запропонувати застосовувати КС, для яких $\rho_{a,\max}$ АФАК менше ніж 33. В таблиці наведено дані щодо деяких КС, для яких $\rho_{a,\max}$ не перевищують значення 26, а на рисунку показано вид АФАК для одного з таких КС.

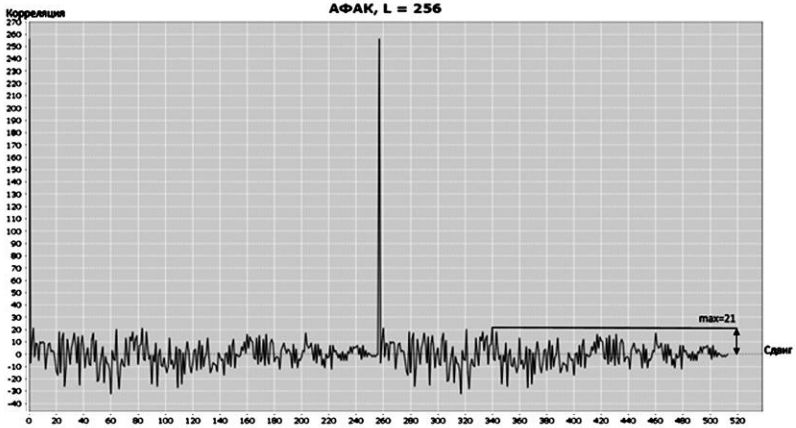



***Рисунок.*** *АФАК КС для N = 256. Циклічний зсув* {83}

Таблиця

*КС для N = 256 з найменшими бічними пелюстками АФАК*

| Сигнал № | Значення максимальних бокових піків АФАК | Відповідні зсуви КС |
|---|---|---|
| 1 | 25 | {31} |
| 2 | 25 | {61} |
| 3 | 26 | {60} |
| 4 | 26 | {10,22} |
| 5 | 24 | {212} |
| 6 | 26 | {48} |
| 7 | 21 | {3,83} |
| 8 | 26 | {66} |

**Висновки.** На основі застосування мінімаксного критерію та рівностей, що встановлюють залежність авто- і взаємно-кореляційних функцій ДС, вирішена задача оптимізації пошуку нелінійних ДС з покращеними властивостями. Показано, що застосування синтезованих систем сигналів дозволить підвищити завадостійкість прийому сигналів, показники інформаційної безпеки та скритності функціонування ІКС в умовах кібератак, дії природніх та організованих, у тому числі, структурних, ретрансльованих й інших завад.

## Список використаних джерел:


1. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія. Теорія. Практика. Застосування : монографія. Харків : Форт, 2012. 880 с.
2. Sarvate D. V., Pursley M. V. Crosleration Properties of Pseudorandom and Related Sequences. *IEEE Trans. Commun.* 1980. Vol. 68. P. 59–90.
3. Ipatov Valery P. Spread Spectrum and CDMA. Principles and Applications. University of Turku, Finland and St. Petersburg Electro technical University «LETI», Russia. John Wiley & Sons Ltd, The Atrium, Southern Gate, Chi Chester, West Sussex PO19 8SQ, England.
4. Свердлик М. Б. Оптимальные дискретные сигналы. М. : Сов. радио, 1975. 200 с.
5. Горбенко І. Д., Замула О. А. Моделі та методи синтезу криптографічних сигналів та їх оптимізація за критерієм часової складності. *Математичне та комп'ютерне моделювання.* Серія: Фізико-математичні науки : зб. наук. праць. Інститут кібернетики імені В. М. Глушкова Національної академії наук України, 2017. Вип. 15. 272 с.
6. Gorbenko I. D., Zamula A. A. Cryptographic signals: requirements, methods of synthesis, properties, application in telecommunication systems. *Telecommunications and Radio Engineering*. 2017. Vol. 76, Issue 12. P. 1079–1100. DOI: 10.1615/TelecomRadEng.v76.i12.50.
7. Gorbenko D., Zamula A. A., Semenko A. E., Morozov V. L. Method for synthesis of performed signals systems based on cryptographic discrete sequences of symbols. *Telecommunications and Radio Engineering.* 2017. Vol. 76, Issue 17. P. 1523–1533.

# OPTIMIZATION OF DISCREET COMPLEX SIGNALS SEARCH WITH NECESSARY PROPERTIES FOR APPLICATION IN MODERN INFORMATION AND COMMUNICATION SYSTEMS

Among the main areas of the performance indicators improvement of information and communication systems (ICS), in particular, noise immunity, secrecy, and information security, it is possible to identify the areas associated with the use of phase-manipulated broadband signals and frequency-phase-manipulated signals. Since in multi-user systems, the code division of channels is based on the difference in signals, then the construction of ICS and performance indicators of these systems are determined by the choice of signals and their properties. In this case, discrete sequences (DS), that extend the spectrum (manipulate carrier frequency), should be based on nonlinear construction rules and have improved correlation, ensemble and structural properties. In particular, when using signals such as the physical carrier of information or synchronization signals, the time expenditures on the disclosure of the structure of the signals used are increasing and the setting of «optimal», from the standpoint of the counter-station, obstacles becomes problematic. Complex signals obtained on the basis of such sequences, possess, on the one hand, structural properties, similar to the properties of random (pseudorandom) sequences, and on the other hand, necessary ensemble and correlation properties. The side petals minimization levels of the ACF is of greatest importance when designing a signal for such applications as measuring the lag time, time resolution, etc. In this paper, the problem of optimizing the synthesis of nonlinear discrete sequences, which have improved ensemble, structural and autocorrelation properties, is formulated and solved. The use of non-linear discrete signals, which are formed on the basis of such sequences, will provide the necessary values of impedance protection, information and structural secrecy of the ICS operation.

**Key words:** *discrete sequence, cryptographic signal, correlation function, isomorphism, finite field.*

Одержано 08.02.2019

УДК 519.9
DOI: 10.32626/2308-5916.2019-19.44-49

**Ю. І. Горбенко*,** канд. техн. наук,
**О. С. Акользіна**,**
**В. О. Подгайко**,** магістр

*АТ «Інститут інформаційних технологій», м. Харків,
**Національний університет імені В. Н. Каразіна, м. Харків

# АНАЛІЗ АКТУАЛЬНИХ ПРОБЛЕМНИХ ПИТАНЬ ЩОДО ПЕРСПЕКТИВНОЇ АСИМЕТРИЧНОЇ КРИПТОГРАФІЇ

Наведений аналіз актуальних досліджень щодо криптографії на решітках. Аналіз відбувається відповідно до найбільш актуальних алгоритмів, що пройшли до другого етапу конкурсу NIST США. Деякі з них комбіновані — включають в себе декілька схожих алгоритмів з минулого етапу. Для детального їх розгляду приведено ряд актуальних тем дослідження для пост-квантових алгоритмів, що дозволяє описувати та класифікувати їх більш суттєво.

**Ключові слова**: *решітка, постквантовий алгоритм, LWE, кільце, інкапсуляція.*

**Вступ.** Нині на світовому рівні проводяться дослідження проблеми створення перспективних стандартів асиметричної криптографії — асиметричних шифрів (АСШ), протоколів інкапсуляціє ключів (ПІК) та електронного підпису (ЕП).

Попередні дослідження та перший етап їх суспільного обговорення показали, що певні переваги для реалізації стандартів щодо асиметричної криптографії має математичний апарат криптографічних перетворень у кільцях поліномів [1, 2]. Нині його називають крипто перетвореннями на алгебраїчних решітках, це пов'язане з тим, що доведення його стійкості ґрунтувалось на методах алгебраїчних решіток. На наш погляд, важливим є аналіз цього напрямку з токи зору створення перспективних стандартів асиметричної криптографії у кільцях поліномів з додатковими перетвореннями. Аналіз даних таблиці показує, що всього до 2 раунду конкурсу пройшло 17 кандидатів (із 40). Також, як видно із даних таблиці пройшли у 2 раунд 14 кандидатів, що ґрунтуються на математичних кодах та 4 на мультиваріативних перетвореннях. Серед інших необхідно виділити SIKE та SPHINCK+. Тому важливим завданням другого етапу конкурсу NIST США є подальше порівняння кандидатів.

**Мета даної роботи** — систематизація знань відносно процесу постквантової стандартизації, аналізу стану, основних властивостей кандидатів та конкретизація напрямку подальших досліджень із створення перспективних АСШ, ПІК та ЕП та їх порівняння.

 © Ю. І. Горбенко, О. С. Акользіна, В. О. Подгайко, 2019

Таблиця

| Механізм | Математичні методи | Назви алгоритмів | Кіль-кість |
|---|---|---|---|
| Направлене шифрування | Решітки | CRYSTALS-KYBER, LAC, NTRU, Round5, SABER, Three Bears | 7 |
| | Коди | Classic McEliece, HQC, ROLLO, LEDAcrypt, RQC | 6 |
| | Інше | SIKE | 1 |
| | Усього кандидатів | | 14 |
| Протоколи обміну ключами | Алгебраїчні решітки | CRYSTALS-KYBER, LAC, FrodoKEM, NewHope, NTRU, NTRU Prime, SABER, Three Bears | 8 |
| | Коди | BIKE, Classic McEliece, HQC, LEDAcrypt, NTS-KEM, ROLLO, RQC | 8 |
| | Інше | SIKE | 1 |
| | Усього кандидатів | | 17 |
| Електронний підпис | Алгебраїчні решітки | CRYSTALS-DILITHIUM, FALCON, qTesla | 3 |
| | Мультиваріативні перетворення | GeMSS, LUOV, MQDSS, Rainbow | 4 |
| | Геш-перетворення | SPHINCK+ | 1 |
| | Інше | Picnic | 1 |
| | Усього кандидатів | | 9 |

1. Аналіз стану створення стандартів асиметричної криптографії. Проведений аналіз показав, що до першого раунду конкурсу NIST США було допущено 69 кандидатів, 31 січня 2019 року інститутом NIST опубліковано перелік заявок, які пройшли до другого раунду конкурсу пост-квантової стандартизації [1]. Цей раунд, як повідомив представник NIST США Дастін Муді, буде тривати від 12 до 18 місяців. Деякі з них були об'єднані та автори об’єднаних проектів сформували комбіновані криптосистеми. Серед комбінованих заявок наступні [1]: LEDAcrypt (поєднання LEDAkem та LEDApkc), NTRU (поєднання NTRUEncrypt та NTRU-HRSS-KEM), ROLLO (поєднання LAKE, LOCKER та Ouroboros-R), Round5 (поєднання HILA5 та Round2). У таблиці наведена класифікація алгоритмів другого раунду за математикою та механізмами, що були застосованими.

Таким чином, із 69 проектів на другий етап рекомендовано 40 кандидатів на стандарти асиметричної криптографії — АСШ, ПІК та ЕП.

Попередні дослідження [3] дозволили визначити важливі та проблемні питання подальших досліджень. Основними з них є такі як:

- класичний та квантовий криптоаналіз кандидатів, включаючи криптоаналіз спрощених та демо-версій;

- аналіз відносної швидкодії або ресурсних вимог до кандидатів;
- оцінка класичної та квантової стійкості кандидатів;
- систематизація знань відносно процесу стандартизації NIST PQC;
- істотне покращення реалізації алгоритмів;
- вдосконалення аналізу або доведення властивостей кандидатів, навіть якщо це не призводить до якоїсь атаки;
- пропозиції критеріїв для вибору алгоритмів для стандартизації;
- вплив на існуючі додатки та протоколи. Наприклад, які зміни необхідні для впровадження конкретних кандидатів;
- підготовчі кроки або стратегії для організацій до майбутнього переходу на пост квантову криптографію.

2. Огляд та попередній аналіз деяких кандидатів на стандарти перспективних асиметричних крипто перетворень. Попередній аналіз та дослідження практичних реалізацій дозволили виділити такі проекти [1]: NTRU Prime, ThreeBears, Saber, Round5, CRYSTALS-Kyber та SPHINCS +. Розглянемо їх та проведемо попередній аналіз.

2.1. Проект NTRU Prime. Модернізований NTRU Prime [2] розроблений з метою забезпечити IND-CCA2 стійкості, тобто стійкості проти атак з адаптивно-підібраним шифртекстом. При реалізації такої моделі безпеки, сервер може повторно використовувати відкриті ключі будь-яку кількість разів, що спрощує вартість генерації та узгодження ключа. Для встановлення нового сеансового ключа, включаючи постквантовий сервер автентифікації, необхідне лише одне зашифрування для клієнта та одне розшифрування для серверу. Тому в модернізований NTRU Prime має важливі переваги у швидкодії при виконанні механізму обміну. Інші властивості NTRU Prime можна знайти в [2].

2.2. ThreeBears. Криптосистема ThreeBears [4] заснована на криптосистемах навчання з помилками у кільці (RLWE) Lyubashevsky-Peikert-Regev [5] та Ding [6]. Більш точно, вона заснована на NewHope [7] та Kyber [8], остання з яких використовує модульне навчання з помилками (MLWE). Автори ThreeBears замінили кільце поліномів, що лежить в основі цього модуля, на цілий модуль, узагальнене число Мерсена, за рахунок цього з'являється цілий модуль навчання з помилками (I-MLWE).

ThreeBears названа таким чином, через те, що її модуль має однакову форму «золотого співвідношення Солінас», та насправді деякий арифметичний код з її реалізації отриманий з арифметичного коду Goldilocks.

Одна з цілей ThreeBears — сприяти дослідженню потенційно бажаних, але менш традиційних систем. Через це ThreeBears використовує I-MLWE замість MLWE, через це особистий ключ є лише рядком, через це використовується явне відхилення, і через це відсутнє гешування Targhi-Unruh.

2.3. Saber. Saber представляє собою родину криптопримітивів, які засновані на складності Задачі Модульного навчання з округленням (Module Learning With Rounding problem — Mod-LWR) [9]. Спершу описується Saber.PKE — IND-CPA стійка схема шифрування, та її перетворення в Saber.KEM, IND-CCA стійкий механізм інкапсуляції ключа, з використанням перетворення Fujisaki-Okamoto. Цілями розробки були простота, швидкодія та гнучкість, які спричинили наступні рішення: усі цілі модулі є степенями 2, що дозволяє повністю уникнути зведення за модулем та вибірку з відхиленням; використання LWR зменшує вдвічі розмір необхідної випадковості у порівнянні з LWE-схемами та знижує пропускну здатність; модульна структура забезпечує гнучкість за рахунок повторного використання одного кореневого компоненту для багатьох рівнів стійкості.

2.4. Round5. Заявка Round5 складається з заявок Round2 та Hila5 [10]. Ключовою характеристикою Round2 є те, що він був розроблений, щоб визначити задачу навчання з округленням (Learning with Roundings — LWR) та Ring LWR задачу однаковим чином. Це досягається за рахунок Загальної LWR задачі, на якій заснований Round2, який може визначити LWR або RLWR в залежності від вхідних параметрів. Причини такого вибору наступні.

Round2 є адаптивним та може бути застосований до багатьох середовищ. З іншого боку, алгоритми на основі LWR є бажаними у тих середовищах, в яких швидкодія — найменша проблема, а стійкість — першочергова. В таких випадках бажано, щоб були відсутні додаткові кільцеві структури (як у ідеальних решітках [4, 5]). З іншого боку, алгоритми на основі RLWR забезпечують кращу швидкодію для пропускної здатності та обчислень, тож вони краще підходять для обмежених середовищ з вимогами обмеження пропускної здатності, наприклад, через складність фрагментації повідомлення.

Round2 зменшує аналіз коду та керування, так як єдине визначення для схем Round2.KEM та Round2.PKE визначають різні задачі, LWR та RLWR з одним кодом.

HILA5 використовує новий метод узгодження для Ring-LWE, який має значно меншу швидкість відмови, ніж попередні пропозиції, одночасно зменшуючи розмір шифртексту і кількість обов'язкової випадковості. Вона заснована на простому, детерміністичному варіанті погодження Peikert, який працює з нашим новим вибором «безпечних бітів» та методами корекції помилок постійного часу. Новий метод не потребує рандомізованого згладжування для досягнення необмежених секретів. Автори виконують аналіз комбінаторних відмов, використовуючи повні вірогідні згортки, що веде до точного розуміння умов відмови розшифрування на рівні бітів. Навіть із додатковими заходами безпеки та безпечності, нова схема, як і раніше, настільки ж швидко, як New Hope, але

має трохи коротші повідомлення. Нові методи були інсценировані та впроваджені як механізм інкапсуляції ключа (KEM) та схема шифрування відкритого ключа, розроблена для задоволення вимог постквантової криптографії NIST на найвищому рівні безпеки.

2.5. CRYSTALS-Kyber. Kyber — це IND-CCA2 безпечний механізм інкапсуляції ключів (KEM) [8]. Безпека Kyber заснована на складності вирішення проблеми навчання-з-помилками в модульних решітках (проблема MLWE). Побудова Kyber відбувається за двоетапним підходом: спочатку автори представляють схему шифрування загальнодоступного ключа INDCPA безпеки, що шифрує повідомлення фіксованої довжини 32 байтів, яка називається Kyber.CPAPKE. Потім використовується злегка змінене перетворення Fujisaki-Okamoto (FO), щоб побудувати IND-CCA2 безпечний KEM.

2.6. SPHINCS +. На високому рівні, SPHINCS + працює як SPHINCS [11]. Основна ідея полягає в автентифікації великої кількості ключових пар багаторазового підпису (FTS), використовуючи так зване гіпердерево. Схеми FTS — схеми підпису, які дозволяють парі ключів виготовити невелику кількість підписів, наприклад, порядку десяти для наших наборів параметрів.

Для кожного нового повідомлення ключова пара (псевдовипадкових) FTS підбирається для підпису повідомлення. Підпис складається, таким чином, з підпису FTS та інформації про автентифікацію для цієї ключової пари FTS. Інформація про автентифікацію приблизно є підписом гіпердерева, тобто підписом використовується дерево сертифікації підписів дерева Мерклі.

**Висновки.** 1. Попередній аналіз, результати якого наведені в таблиці, показав, що до 2 раунду конкурсу пройшло 17 кандидатів (із 40), що засновані та перетвореннях у кільцях поліномів. Також, як видно із даних таблиці, у другий раунд пройшли 14 кандидатів, що ґрунтуються на математичних кодах та 4 на мультиваріативних перетвореннях. Серед інших необхідно виділити SIKE та SPHINCK+.

2. Якщо розглядати АСШ як складову ПІК, то тоді до другого раунду процесу постквантової стандартизації пройшло усього 26 криптосистем (9 алгоритмів ЕП, 17 АСШ та ПІК).

3. Необхідно проводити подальші дослідження основних властивостей кандидатів та провести їх порівняння за прийнятими критеріями. На наш погляд для цього необхідно застосовувати обґрунтовану методику з відповідними критеріями.

4. В процесі попередніх досліджень визначені проблемні питання та пріоритетні напрямки досліджень, вони стосуються таких питань: оцінювання алгоритмів, формування критеріїв, класичний і квантовий криптоаналіз, вдосконалення аналізу та визначення необхідних змін для практичного впровадження постквантових алгоритмів.

**Список використаних джерел:**

1. URL: https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions.
2. URL: https://ntruprime.cr.yp.to.
3. URL: https://groups.google.com/a/list.nist.gov/forum/#!forum/pqc-forum.
4. URL: https://sourceforge.net/ projects/threebears/
5. URL: https://eprint.iacr.org/2012/230.pdf.
6. URL: https://eprint.iacr.org/2012/688.
7. URL: https://newhopecrypto.org.
8. URL: https://eprint.iacr.org/2017/634.pdf.
9. URL: https://eprint.iacr.org/2018/230.pdf.
10. URL: https://round5.org.
11. URL: https://cryptojedi.org/papers/sphincs-20141001.pdf.

## ACTUAL ISSUES ANALYSIS REGARDING PERSPECTIVE PUBLIC-KEY CRYPTOGRAPHY

An analysis of current research on cryptography on lattices is given. The analysis takes place in accordance with the most relevant algorithms that have gone through the second stage of the US NIST competition. Some of them are combined — include several similar algorithms from the past stage. For a detailed consideration of them, a number of relevant topics for post-quantum algorithms are presented, which allows them to be described and categorized more substantially.

**Key words:** *lattice, post-quantum algorithm, LWE, ring, encapsulation.*

Одержано 02.12.2018

УДК 004.056.55
DOI: 10.32626/2308-5916.2019-19.49-55

**М. В. Єсіна,** канд. техн. наук

АТ «Інститут інформаційних технологій»,
Харківський національний університет імені В. Н. Каразіна, м. Харків

## МОДЕЛІ БЕЗПЕКИ ПОСТКВАНТОВИХ КРИПТОГРАФІЧНИХ ПРИМІТИВІВ

У даній роботі розглядається сутність та досліджуються моделі безпеки щодо асиметричних постквантових криптографічних примітивів різного типу. За основу взяті моделі безпеки, які рекомендовані NIST США у вимогах конкурсу PQC до кандидатів на постквантові криптографічні примітиви. До таких алгоритмів відносяться асиметричні криптографічні перетворення типу асиметричне шифрування, цифровий підпис та механізм інкапсуляції ключів. Рекомендованими є наступні моделі безпеки, які стосуються: щодо асиметричного шифрування — IND-CCA2 (IND-CPA, IND-CCA); щодо цифрового підпису — EUF-CMA (та її варіації); щодо механізмів інкапсуляції ключів —

© М. В. Єсіна, 2019

СК-модель. У роботі розглядається основна сутність таких моделей безпеки. Використання моделей безпеки при дослідженнях криптографічних примітивів є відносно новим. Потрібне узагальнення щодо кожної із вказаних моделей та визначення необхідності та умов, і наслідків їх застосування. У таких моделях враховується середовище застосування, в якому може діяти неавтентифікований чи автентифікований порушник. У роботі розглядається поняття нерозрізнюваності (невизначеності) та моделі безпеки постквантових асиметричних шифрів на її основі. Визначається властивість нерозрізнюваності (невизначеності) при атаці на основі підібраного (вибраного) відкритого тексту. Розглядається поняття семантичної безпеки. Наводяться види найпоширеніших атак на основі нерозрізнюваності (невизначеності). Розглядаються існуючі різновиди моделі безпеки EUF-CMA — SUF-CMA і т. д. Даються визначення понять «пряма секретність» (forward security, forward secrecy) та «досконала пряма секретність» (perfect forward secrecy (PFS)). Також у роботі розглядаються особливості застосування щодо перспективних асиметричних перетворень «теорії ігор». Надається визначення поняття «теорія ігор».

**Ключові слова**: *атака, інкапсуляція ключів, модель безпеки, семантична безпека, шифротекст, електронний підпис.*

**Вступ.** У критеріях відбору, які висуваються NIST США до кандидатів на постквантові стандарти криптографічного захисту інформації [1], визначено моделі безпеки, яким повинні відповідати кандидати. Відповідно до трьох кандидатів — асиметричний шифр (АСШ), цифровий підпис та протокол інкапсуляції ключів (ПІК), визначено три моделі безпеки. Стосовно АСШ — IND-CCA2 (IND-CPA, IND-CCA), для підпису — EUF-CMA-модель та для ПІК — СК-модель [1].

На наш погляд, на сьогоднішній день проблемними є питання, що стосуються узагальненого визначення та дослідження моделей безпеки постквантових криптопримітивів різного типу, але з урахуванням основних положень та пропозицій, що викладені у [2–5]. На відміну від традиційного застосування тільки моделей порушника та загроз, при створенні кандидатів на перспективні асиметричні криптографічні перетворення запропоновано використовувати моделі безпеки. Але, ні досвіду, ні рекомендацій щодо їх застосування практично немає чи вони є формальними. Тому, на наш погляд, актуальною є проблема узагальненого визначення та дослідження моделей безпеки взагалі, в першу чергу на рівні сутності, умов та можливостей застосування при оцінці кандидатів щодо їх вразливості щодо класичного та квантового криптоаналізу.

**Мета цієї роботи** — узагальнене визначення, класифікація та попереднє дослідження моделей безпеки, зокрема, визначення можливостей та умов застосування постквантових криптопримітивів при протидії із сторони класичного чи квантового порушника [2–5].

**Модель безпеки постквантових алгоритмів асиметричного шифрування.** Нерозрізнюваність (невизначеність) зашифрованого тексту — це важлива властивість безпеки багатьох схем шифрування. Якщо криптосистема володіє властивістю нерозрізнюваності, то зловмисник не зможе відрізнити пари шифрованих текстів на основі повідомлення, що вони шифрують [6].

Властивість нерозрізнюваності при атаці на основі підібраного відкритого тексту вважається основною вимогою для більшості достовірно захищених криптосистем з відкритим ключем, хоча деякі схеми також забезпечують нерозрізнюваність при атаці на основі підібраного зашифрованого тексту та атаці на основі адаптивно підібраного зашифрованого тексту. Нерозрізнюваність при атаці на основі підібраного відкритого тексту еквівалентна властивості семантичної безпеки, і багато криптографічних доказів використовують ці визначення як еквівалентні [6].

Криптосистема вважається «безпечною з точки зору нерозрізнюваності», якщо жоден зловмисник $A$, отримавши зашифроване повідомлення, довільно вибране з двоелементного простору повідомлень, визначеного зловмисником, не може ідентифікувати вибір повідомлення з ймовірністю значно краще, ніж при випадкових вгадуваннях (½). Якщо будь-який зловмисник може вдало відрізнити вибраний шифрований текст з ймовірністю значно більше, ніж ½, тоді цей зловмисник вважається таким, що має «перевагу» в розрізнені шифрованого тексту, і схема «не» вважається безпечною з точки зору нерозрізнюваності [6].

Безпека з точки зору нерозрізнюваності представляється як гра, де криптосистема вважається безпечною, якщо жоден із зловмисників не може виграти гру зі значно більшою ймовірністю, ніж зловмисник, який повинен вгадати випадковим чином. Найпоширеніші визначення, що використовуються у криптографії [6, 7]: нерозрізнюваність при атаці на основі підібраного відкритого тексту (IND-CPA безпека); нерозрізнюваність при атаці на основі підібраного шифртексту (IND-CCA безпека); нерозрізнюваність при атаці на основі адаптивно підібраного шифртексту (IND-CCA2 безпека).

Безпека за будь-яким з останніх визначень означає безпеку за попередніми [6]: схема, яка є IND-CCA безпечною, також є IND-CPA безпечною; схема, яка є IND-CCA2 безпечною, є як IND-CCA безпечною, так і IND-CPA безпечною. Таким чином, IND-CCA2 є найстрогішим з цих трьох визначень безпеки.

Семантична безпека — поняття, яке описує безпеку схеми шифрування, позначається як SEM-CPA та фіксує ідею, що безпечна схема шифрування повинна приховувати всю інформацію про невідомий відкритий текст. Зловмиснику дозволяється вибирати між двома відкритими текстами $m_0$ та $m_1$, і він отримує зашифрування будь-якого з відкритих текстів. Схема шифрування є семантично безпечною, якщо

зловмисник не може здогадуватися з кращою ймовірністю, ніж ½, чи даний шифртекст є зашифруванням повідомлення $m_0$ або $m_1$. Семантична безпека вимагає, щоб те, що можна ефективно обчислювати щодо деяких відкритих текстів з їх шифртекстів, можна обчислювати так само легко за відсутності цих шифртекстів [8].

**Модель безпеки постквантових цифрових підписів.** Сьогодні пропонується як модель безпеки стосовно постквантових підписів застосовувати EUF-CMA модель. EUF-CMA визначає екзистенційну непідроблюваність від атак на основі адаптивно вибраних повідомлень. Зокрема, безпека в сенсі EUF-CMA не дозволяє криптоаналітику виробляти підпис для повідомлень, що залежать від ключів, наприклад, підпис при застосуванні повного особистого *sk* ключа. Якщо є хоча б один запит повідомлення, що залежить від ключів, безпека механізму підпису порушується [9–12].

Існує два загальних формальних визначення для забезпечення безпеки схеми цифрового підпису. Кожне з цих визначень представлено як «гра», або експеримент, який виконується між атакуючим (attacker) та деяким чесним претендентом (challenger).

Теорія ігор — теорія математичних моделей прийняття оптимальних рішень в умовах конфлікту. Оскільки сторони, що беруть участь у більшості конфліктів, зацікавлені в тому, щоб приховати від противника власні наміри, прийняття рішень в умовах конфлікту, зазвичай, відбувається в умовах невизначеності.

Неформально, експеримент EUF-CMA працює так [9–12]:

1. Претендент генерує дійсну пару ключів (*pk, sk*) і надає *pk* атакуючому.
2. Атакуючий тепер може повторно запросити підписи на підібраних повідомленнях ($M_1$,...,$M_q$) за своїм вибором, і отримує дійсні підписи ($\sigma_1$,...., $\sigma_q$) у відповідь.
3. По завершенню експерименту зловмисник повинен вивести повідомлення та підпис $M^*$, $\sigma^*$ такі, що (1) повідомлення було не одним із повідомлень, які вимагали попереднього кроку, і (2) повідомлення/підпис перевіряється правильно з відкритим ключем.

Схема вважається безпечною, якщо жоден зловмисник не має ні найменшої переваги у виконанні вищезазначених умов. Зазвичай кількість повідомлень $q$ обмежується лише часом виконання атакуючого, однак для спеціального випадку одноразових підписів, зловмисник обмежується запитом лише одного підпису на кроці (2).

Це визначення досить сильне, але не настільки сильне, наскільки це можливо. Дещо сильнішим є визначення SUF-CMA.

Неформально, експеримент SUF-CMA працює так [9–12]:

1. Аналогічно попередньому експерименту.

2. Аналогічно попередньому експерименту.
3. Після завершення експерименту, атакуючий повинен вивести повідомлення та підпис $M^*$, $\sigma^*$ такі, що (1) пара ($M^*$, $\sigma^*$) не була одним із запитаних повідомлень, а підпис повернувся на попередньому кроці, (2) повідомлення/підпис перевіряється на відкритому ключі.

Головна відмінність полягає у тому, що це більш сильне визначення гарантує, що атакуючий не зможе підібрати підпис [8].

**Модель безпеки постквантових протоколів інкапсуляції ключів.** Модель СК включає у себе три основні компоненти: модель неавтентифікованого порушника (UM), модель автентифікованого порушника (AM) та механізм автентифікації (автентифікатор) (MT). Модель безпеки СК використовується для автентифікації обміну ключами (AKE) [2]. СК-модель стосується безпеки ключа сеансу, що використовується на сеансі зв'язку. При її оцінці використовується формальна модель для протоколів обміну ключами та можливостей криптоаналітика. Поняття безпеки, яке називається безпекою ключа сеансу (або SK-безпека), направлене на забезпечення безпеки окремих ключів сеансу. Її порушення являє собою компрометацію сеансового ключа. У випадку безпечності ключа, зловмисник «нічого не дізнається про значення ключа», коли він перехвачує дані протоколу обміну ключами та здійснює атаки на інші сеанси та сторони, що взаємодіють. Такий підхід є стандартним для моделі семантичної безпеки, коли криптоаналітик не може відрізнити реальне значення ключа від незалежного випадкового значення [2].

Поняття досконалої прямої безпеки (PFS) відноситься до властивості протоколів обміну ключами (KE), за допомогою якої розкриття довгострокових ключів, що використовується у протоколі для автентифікації та узгодження ключів сеансу, не ставить під загрозу секретність ключів сеансу, встановлених до розкриття [2].

**Висновки.** 1. На сьогодні запропоновано три моделі безпеки: асиметричне шифрування — IND-CPA, IND-CCA/CCA2, цифровий підпис — EUF-CMA, та механізми інкапсуляції ключів — СК. Моделі безпеки усіх асиметричних криптоперетворень засновуються на понятті «теорії ігор».

2. Сьогодні актуальна — проблема узагальненого визначення та дослідження моделей безпеки, визначення сутності, умов їх застосування при криптоаналізі та використання при оцінці захищеності від відомих класичних та квантових атак.

3. Відповідно до моделі безпеки на основі нерозрізнюваності, безпека за будь-яким з наступних визначень означає безпеку за попередніми, тобто: схема, яка є IND-CCA безпечною, є IND-CPA безпечною; схема, яка є IND-CCA2 безпечною, є як IND-CCA безпечною,

так і IND-CPA безпечною. Тобто, IND-CCA2 є найстрогішим з цих трьох визначень безпеки. Нерозрізнюваність при атаці на основі підібраного відкритого тексту (IND-CPA) еквівалентна властивості семантичної безпеки (SEM-CPA).

4. Як модель безпеки щодо постквантових криптоперетворень типу підпис застосовується EUF-CMA-модель. EUF-CMA-модель визначає екзистенційну непідроблюваність від атак на основі адаптивно вибраних повідомлень. Зокрема, безпека в сенсі EUF-CMA не дозволяє зловмиснику виробляти підписи для повідомлень, що залежать від ключів, наприклад, підпис при застосуванні повного особистого *sk* ключа. При наявності хоча б одного запиту повідомлення, що залежить від ключів, безпека механізму підпису порушується.

5. CK модель безпеки включає у себе три основні складові компоненти: модель неавтентифікованого порушника (UM), модель автентифікованого порушника (AM) та механізм автентифікації (автентифікатор) (MT). Як правило модель безпеки CK використовується для автентифікації обміну ключами (AKE).

6. Модель безпеки CK стосується безпеки ключа сеансу, що використовується на сеансі зв'язку. При оцінці протоколів обміну ключами та можливостей криптоаналітика використовується формальна модель. Поняття безпеки, яке називається безпекою ключа сеансу (або SK-безпека), направлене на забезпечення безпеки окремих ключів сеансу. Її порушення може призвести до компрометації ключа сеансу.

**Список використаних джерел:**


1. Post-Quantum Cryptography. URL: https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions.
2. Ran Canetti, Hugo Krawczyk Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels. URL: http://iacr.org/archive/eurocrypt2001/20450451.pdf.
3. Shoup V. On Formal Models for Secure Key Exchange, Theory of Cryptography Library, 1999. URL: http://philby.ucsd. edu/cryptolib/1999/9912.html.
4. Yoshida Y., Morozov K., Tanaka K. CCA2 Key-Privacy for Code-Based Encryption in the Standard Model. Post-Quantum Cryptography. PQCrypto 2017. Lecture Notes in Computer Science, Vol. 10346. Springer, Cham.
5. Bellare M., Boldyreva A., Desai A., Pointcheval D. Key-privacy in public-key encryption. ASIACRYPT 2001. LNCS. Vol. 2248. P. 566–582. Springer, Heidelberg (2001). doi:10.1007/3-540-45682-1 33.
6. Ciphertext indistinguishability. URL: http://cse.iitkgp.ac.in/~debdeep/-courses_iitkgp/FCrypto/scribes/scribe8.pdf.
7. Henk C.A. van Tilborg, Sushil Jajodia (Eds.) Encyclopedia of Cryptography and Security Springer, 2011. 1416 p.
8. Bellare M. Symmetric encryption. URL: https://cseweb.ucsd.edu/~mihir/-cse207/w-se.pdf.

9. EUF-CMA and SUF-CMA. URL: https://blog.cryptographyengineering.com/-euf-cma-and-suf-cma.
10. Haitner I., Holensteiny T. On the (im) possibility of key dependent encryption, in: TCC'09 — Theory of Cryptography, 6th Theory of Cryptography Conference, San Francisco, CA, USA, 2009, Lecture Notes in Comput. Sci. Vol. 5444, Springer, Berlin, 2009, P. 202–219.
11. Hofheinz D., Unruh D. Towards key-dependent message security in the standard model. *EUROCRYPT'08 — Advances in Cryptology*, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, 2008, Lecture Notes in Comput. Sci., Vol. 4965, Springer, Berlin, 2008. P. 108–126.
12. Applebaum B., Cash D., Peikert C., Sahai A. Fast cryptographic primitives and circular-secure encryption based on hard learning problems. *Advances in Cryptology — CRYPTO'09*, 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, 2009. Lecture Notes in Comput. Sci. Vol. 5677, Springer, Berlin, 2009. P. 595–618.

## SECURITY MODELS OF POST-QUANTUM CRYPTOGRAPHIC PRIMITIVES

In this paper, the essence is considered and security models of asymmetric post-quantum cryptographic primitives of different types are investigated. The basis taken security models that are recommended by NIST USA in the requirements of the PQC competition for candidates for post-quantum cryptographic primitives. Such algorithms include asymmetric cryptographic transformations such as asymmetric encryption, digital signature, and key encapsulation mechanism. The following security models are recommended, which are related to: the asymmetric encryption — IND-CCA2 (IND-CPA, IND-CCA); the digital signature — EUF-CMA (and its variations); the key encapsulation mechanisms — CK-model. In this paper, the basic essence of such security models is considered. The use of security models in research of cryptographic primitives is relatively new. A generalization of each of these models and a definition of the necessity and conditions, and the consequences of their application are required. Such models take into account the application environment in which an unauthenticated-links adversarial model and authenticated-links adversarial model can operate. The paper considers the concept of indistinguishability and security model of post-quantum asymmetric ciphers on its basis. The property of indistinguishability under chosen plaintext attack is determined. The concept of semantic security is considered. The types of most common attacks based on indistinguishability are given. Existing versions of the EUF-CMA security model — SUF-CMA, etc. are considered. Definitions of «forward security, forward secrecy» and «perfect forward secrecy (PFS)» are given. In addition, the paper considers the peculiarities of the application regarding to perspective asymmetric transformations of the «game theory». The definition of concept «game theory» is given.

**Key words:** *attack, key encapsulation, security model, semantic security, ciphertext, signature.*

Одержано 26.01.2019

УДК 0681.3.06
DOI: 10.32626/2308-5916.2019-19.56-62

**Б. Я. Корнієнко*,** д-р техн. наук,
**Л. П. Галата****

*****Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського», м. Київ,
******Національний авіаційний університет, м. Київ

# ОПТИМІЗАЦІЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ КОРПОРАТИВНОЇ МЕРЕЖІ

Розглядаються основні підходи до розробки алгоритму оптимізації системи захисту інформації корпоративної мережі. Запропоновано перехід від багатокритеріальної задачі оптимізації, до однокритеріальної. При сформульованому понятті захищеності системи оптимізаційна задача полягає в забезпеченні максимального рівня захищеності (як функції вартості інформації, що захищається і ймовірності злому) при обмеженнях вартості системи захисту і впливу на продуктивність системи.

**Ключові слова:** *оптимізація, критерій, система, захист інформації, загроза, рівень захищеності.*

**Вступ.** Проблема побудови оптимальної системи захисту інформації у даний час — найбільш актуальна для більшості промислових підприємств. Мета будь-якої системи захисту визначається можливістю сталого функціонування системи в цілому, визначення та нейтралізації загроз безпеки, запобігання витоку інформації по різних каналах. Одною з головних задач стає оптимізація проектування системи захисту. Сьогодні для промислових підприємств інформація являє собою основний комерційний товар. З розвитком інформаційних технологій і доступу до ринків є потреба в її захисті для забезпечення конфіденційності, цілісності і доступності. Для багатьох промислових підприємств впровадження систем захисту є необхідним етапом на шляху до успішного розвитку, кожне з них має свою критичну інформацію, втрата якої може звести до мінімуму конкурентоспроможність і шанси на успішний розвиток на ринку. Поширення такої інформації може призвести до втрати репутації і завдати матеріальної шкоди. Слід зазначити, що активне запровадження автоматизованих інформаційних систем обумовлює виникнення проблем, пов'язаних з інформаційною безпекою. Рішення даних проблем може бути реалізовано з застосуванням спеціальних автоматизованих програмно-технічних засобів [1–4].

**Мета роботи** — запропоновано алгоритм оптимізації системи захисту інформації корпоративної мережі.

 © Б. Я. Корнієнко, Л. П. Галата, 2019

У будь-якій галузі діяльності для вибору ефективної системи, ця система має характеризуватися деякими параметрами, на підставі яких і робиться вибір. Як такі параметри для системи захисту інформації можна виділити наступні: продуктивність, вартість, керованість, сумісність, захищеність тощо. Як зазначено вище, вибір оптимальної системи за такою множиною її характеристик є класичною задачею оптимізації і не завжди може мати ефективне рішення. Тим більше що багато параметрів є суперечливими: із зростанням рівня захищеності, наприклад, зростає вартість, складність настройки, водночас падає продуктивність.

Можна записати критерій якості за вартістю інформації, що захищається, за ймовірністю злому, за вартістю системи захисту інформації, за продуктивністю системи, за захищеністю. З урахуванням сказаного може бути зроблений висновок про багатокритеріальний характер завдання проектування системи захисту інформації. При цьому, крім забезпечуваного рівня захищеності, має враховуватися ще ряд найважливіших характеристик системи. Наприклад, обов'язково має враховуватися вплив системи захисту на завантаження обчислювального ресурсу, що захищається [5–8].

Кінцевою метою вирішення загальної задачі прийняття рішень є вибір з допустимої множини рішень $X$ єдиного найкращого, тобто екстремального за обраними окремими критеріями рішень

$$x^{opt} = \arg \underset{x \in X}{extr} \left\{ k_i \left( x \right) \right\}, \; i = 1, n. \qquad (1)$$

Задача багатокритеріальної оптимізації (1) є некоректною, оскільки в загальному випадку не забезпечує визначення єдиного оптимального рішення з допустимої множини X. Ця некоректність може бути усунена шляхом регуляризації задачі, тобто введенням деякої додаткової інформації, математичних співвідношень або правил, що дозволяють забезпечити вибір єдиного рішення [1].

Одним із шляхів розв’язку багатокритеріальної задачі оптимізації полягає у формуванні зведеного критерію оптимальності, коли використовується згортка частинних критеріїв, чи використання нормативних показників, чи справедливий компроміс, чи оптимальність за Парето.

Інший підхід базується на виділенні головного критерію та перетворення всіх інших критеріїв у обмеження. Для цього проводиться аналіз конкретних особливостей багатокритеріальної задачі, з множини окремих критеріїв вибирається один — найважливіший, і він приймається як єдиний критерій оптимізації. Для кожного з інших окремих критеріїв призначається граничне значення, нижче якого він не може опускатися.

Тому в нашому алгоритмі буде проводитися оцінка ефективності системи за параметром захищеності, як основним показником, що характеризує рівень забезпечення захисту системи захисту інформації, а на інші характеристики вводяться обмеження. Будемо оцінюва-

ти захищеність системи ($Z$) кількісно залежно від вартості інформації, що захищається, ймовірності злому, вартості самої системи захисту, продуктивності системи:

$$Z = f\left(C_{інф}, p_{зл}, B_{сзі}, П\right),$$

де $C_{інф}$ — вартість інформації, що захищається; $p_{зл}$ — ймовірність злому; $B_{сзі}$ — вартість системи захисту інформації; $П$ — продуктивність системи.

З урахуванням введеного поняття захищеності системи оптимізаційна задача полягає у забезпеченні максимального рівня захищеності (як функції вартості інформації, що захищається і ймовірності злому) при обмеженнях вартості системи захисту і впливу на продуктивність системи:

$$Z^{opt} = \max Z(C_{інф}, p_{зл}, B_{сзі}, П).$$

Таким чином, всі окремі критерії, крім одного перетворюються на обмеження, додатково звужують область допустимих рішень $X$. Тоді вихідна багатокритеріальна задача (1) перетворюється в однокритеріальну вигляду

$$\begin{aligned} x^{opt} &= \arg \underset{x \in X}{extr}\, k^*(x), \\ k_i(x) &\geq (\leq) k_i^B(x), i = 1, n-1, \end{aligned} \qquad (2)$$

де $k^*(x)$ — оптимізаційний скалярний критерій; $k_i^B(x)$ — найгірші допустимі значення окремих критеріїв-обмежень; знак «>» використовується для критеріїв, які необхідно максимізувати, а знак «<» — мінімізувати.

Виведення головного (оптимізаційного) критерію і рівнів обмежень для $k_i^B(x)$ всіх інших критеріїв — суб'єктивна операція, здійснювана експертами. Слід зазначити, що можна розглянути декілька різних варіантів і порівняти результати.

Розглянемо захищеність системи з точки зору ризику. Зауважимо, що використання теорії ризиків для оцінки рівня захищеності на сьогоднішній день є підходом, який найбільш часто використовується на практиці. Ризик ($R$) — це потенційні втрати від загроз захищеності:

$$R(p) = C_{інф} \cdot p_{зл}.$$

За суттю, параметр ризику тут вводиться як мультиплікативна згортка двох основних параметрів захищеності.

З іншого боку, можна розглядати ризик як втрати в одиницю часу:

$$R(\lambda) = C_{інф} \cdot \lambda_{зл},$$

де $\lambda_{зл}$ — інтенсивність потоку зломів (під зломом будемо розуміти вдалу спробу реалізації загрози інформації).

Ці дві формули пов'язані наступним співвідношенням:

$$p_{зл} = \frac{\lambda_{зл}}{\Lambda},$$

де $\Lambda$ — загальна інтенсивність потоку несанкціонованих спроб порушення основних властивостей інформації зловмисниками.

Як основний критерій захищеності будемо використовувати коефіцієнт захищеності ($D$), що показує відносне зменшення ризику в захищеній системі в порівнянні з незахищеною системою:

$$D = \left(1 - \frac{R_{зах}}{R_{нез}}\right) \cdot 100\%, \qquad (3)$$

де $R_{зах}$ — ризик в захищеній системі; $R_{нез}$ — ризик у незахищеній системі.

Для вирішення цієї задачі зведемо її до однокритеріальної за допомогою введення обмежень. В результаті отримаємо:

$$\begin{cases} D(C_{інф}, p_{зл}) \to \max; \\ B_{сзі} \le B_{зад}; \\ П_{сзі} \ge П_{зад}, \end{cases}$$

де $B_{зад}$ і $П_{зад}$ — задані обмеження на вартість системи захисту і продуктивність системи.

Цільова функція обрана виходячи з того, що саме вона відображає основне функціональне призначення системи захисту — забезпечення безпеки інформації [9].

Тепер виразимо коефіцієнт захищеності через параметри загроз. У загальному випадку в системі присутня безліч видів загроз. У цих умовах задамо такі величини: $W$ — кількість видів загроз, що впливають на систему; $C_i (i = 1, w)$ — вартість втрати від злому і-го вигляду; $\lambda_i (i = 1, w)$ — інтенсивність потоку зломів і-го вигляду, відповідно; $Q_i (i = 1, w)$ — ймовірність появи загроз і-го вигляду в загальному потоці спроб реалізації загроз, причому $Q_i = \frac{\lambda_i}{\Lambda}$; $p_i (i = 1, w)$ — ймовірність відбиття загроз і-го вигляду системою захисту. Відповідно, для коефіцієнта втрат від зломів системи захисту маємо:

$$R(p) = \sum R_i(p) = \sum C_i \cdot p_{зл\_i};$$

де $R_i(p)$ — коефіцієнт втрат від злому і-го типу; показує, які в середньому втрати припадають на один злом і-го типу. Для незахищеною системи $P_{загр\_i} = Q_i$, для захищеної системи

$$P_{загр\_i} = Q_i \cdot (1 - p_i).$$

Відповідно, для коефіцієнта втрат від зломів системи захисту в одиницю часу маємо:

$$R(\lambda) = \sum_1^w R_i(\lambda) = \sum_1^w C_i \cdot \lambda_{загр\_i},$$

де $R_i(\lambda)$ — коефіцієнт втрат від зломів і-го типу в одиницю часу.

Для незахищеною системи $\lambda_{загр\_i} = \lambda_i$, для захищеної системи $\lambda_{загр\_i} = \lambda_i \cdot (1 - p_i)$. Відповідно, з (3) маємо:

$$D = 1 - \frac{\sum_1^w C_i \cdot Q_i \cdot (1 - p_i)}{\sum_1^w C_i \cdot Q_i} = 1 - \frac{\sum_1^w C_i \cdot \lambda_i \cdot (1 - p_i)}{\sum_1^w C_i \cdot \lambda_i}. \qquad (4)$$

Розглянуту інформаційну систему можна інтерпретувати як систему масового обслуговування, в яку надходять загрози (заявки). Спочатку розглянемо ситуацію, коли на вхід системи надходить загроза одного типу, припускаючи при цьому, що ця загроза не може бути реалізована або наступити кілька разів в один і той же момент часу. Якщо виконані зазначені припущення, то система може перебувати в трьох різних станах:

1) загроза не надходила, а значить, не була реалізована;
2) загроза надходила, але не була реалізована;
3) загроза надходила і була реалізована.

Елементи матриці інтенсивностей переходів можуть бути знайдені за допомогою імітаційної моделі. Для визначення ймовірностей $p_0(t),\ p_1(t),\ p_2(t)$ маємо систему диференціальних рівнянь

$$\begin{cases} \dfrac{dp_0(t)}{dt} = p_0(t) \cdot \lambda_{11} + p_1(t) \cdot \lambda_{21} + p_2(t) \cdot \lambda_{31}, \\ \dfrac{dp_1(t)}{dt} = p_0(t) \cdot \lambda_{12} + p_1(t) \cdot \lambda_{22} + p_2(t) \cdot \lambda_{32}, \\ \dfrac{dp_2(t)}{dt} = p_1(t) \cdot \lambda_{23} + p_2(t) \cdot \lambda_{33} \end{cases} \qquad (5)$$

з початковими умовами

$$p_0(0) = 1;\ p_1(0) = 0;\ p_2(0) = 0.$$

Для оптимізації використовуються кінцеві усталені значення $p_i$.

Оцінка захищеності з урахуванням наведених вище розрахункових формул і вибір оптимального варіанту системи захисту (необхідного набору механізмів захисту) здійснюється наступним чином.

1. Розрахунок параметрів $C_i$, $\lambda_i$, $p_i$ для оцінки захищеності за вихідними даними.
2. Розрахунок критеріїв захищеності $D$, $B_{СЗІ}$, $П_{СЗІ}$ ($dП_{СЗІ}$) для кожного варіанту системи захисту (набору механізмів захисту).
3. Вибір системи захисту (набору механізмів захисту при розробці системи) з максимальним коефіцієнтом захищеності $D$, що задовольняє обмеженням по вартості $B_{СЗІ}$ і продуктивності $П_{СЗІ}$.

**Висновки.** Запропоновано алгоритм оптимізації системи захисту інформації корпоративної мережі. Здійснено перехід від багатокритеріальної задачі оптимізації, до однокритеріальної. При сформульованому понятті захищеності системи оптимізаційна задача полягає у забезпеченні максимального рівня захищеності (як функції вартості інформації, що захищається і ймовірності злому) при обмеженнях вартості системи захисту і впливу на продуктивність системи.

## Список використаних джерел:


1. Korniyenko B. Y., Galata L. P. Design and research of mathematical model for information security system in computer network. *Науковий журнал «Наукоємні технології».* 2017. № 2 (34). С. 114–118.
2. Корнієнко Б.Я. Дослідження моделі взаємодії відкритих систем з погляду інформаційної безпеки. *Наукоємні технології.* 2012. № 3 (15). С. 83–89. doi.org/10.18372/2310-5461.15.5120 (ukr).
3. Korniyenko B. Y., Yudin O., Novizkij E. Open systems interconnection model investigation from the viewpoint of information security. *The Advanced Science Journal*. 2013. Issue 8. P. 53–56.
4. Корниенко Б. Я. Информационная безопасность и технологии компьютерных сетей: монография. ISBN 978-3-330-02028-3, LAMBERT Academic Publishing, Saarbrucken, Deutschland. 2016. 102 с.
5. Korniyenko B., Galata L., Kozuberda O. Modeling of security and risk assessment in information and communication system. *Sciences of Europe*. 2016. Vol. 2. № 2 (2). P. 61–63.
6. Korniyenko B., Yudin A., Galata L. Risk estimation of information system. *Wschodnioeuropejskie Czasopismo Naukowe*. 2016. № 5. P. 35–40.
7. Корнієнко Б. Я., Юдін О. К., Снігур О. С. Безпека аутентифікації у web-ресурсах. *Науково-практичний журнал «Захист інформації».* 2012. № 1 (54). С. 20–25. doi.org/10.18372/2410-7840.14.2056 (ukr).
8. Корнієнко Б. Я., Максімов Ю. О., Марутовська Н. М. Прикладні програми управління інформаційними ризиками. *Науково-практичний журнал «Захист інформації»*. 2012. № 4 (57). С. 60–64. doi.org/10.18372/2410-7840.14.3493 (ukr).
9. Корниенко Б. Я. Кибернетическая безопасность — операционные системы и протоколы. ISBN 978-3-330-08397-4, LAMBERT Academic Publishing, Saarbrucken, Deutschland. 2017. 122 с.

## OPTIMIZATION OF THE INFORMATION SYSTEM OF THE CORPORATE NETWORK

The main approaches to the algorithm of optimization of the information security system of the corporate network are considered. The transition from the multicriterion optimization problem to the one-criterion is proposed. With the formulation of the concept of system security optimization problem is to provide the maximum level of security (as a function of the value of information, protects and probability of breaking) with the limitations of the value of the system of protection and impact onproductivity of the system.

**Key words:** *optimization, criterion, system, information protection, threat, security level.*

Одержано 31.01.2019

УДК 681.3:519.72:003.26:004.056
DOI: 10.32626/2308-5916.2019-19.62-68

**А. М. Кудін***, **, д-р техн. наук,
**Л. В. Ковальчук***, д-р техн. наук,
**Б. А. Коваленко*****

*Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського», м. Київ,
**Національний банк України, м. Київ,
***ООО «GlobalLogic Ukraine», м. Київ

## ТЕОРЕТИЧНІ ЗАСАДИ ТА ЗАСТОСУВАННЯ БЛОКЧЕЙН-ТЕХНОЛОГІЙ: ІМПЛЕМЕНТАЦІЯ НОВИХ ПРОТОКОЛІВ КОНСЕНСУСУ ТА КРАУДСОРСІНГ ОБЧИСЛЕНЬ

Наведено аналіз існуючих блокчейн-технологій, їх алгоритмів консенсусу та стійкості до відомих атак підміни блоку. Наведені основні ідеї та варіанти практичних реалізацій нового протоколу консенсусу «Proof-of-accuracy», розробленого авторами. Наведено проект блокчейн-системи, яка надає послуги обчислень в режимі краудсорсінгу.

**Ключові слова**: *блокчейн, протоколи консенсусу, атаки подміни блоку, краудсорсінг.*

**Вступ.** Сталою сучасною тенденцією розвитку IT-технологій є зростання частки децентралізованих систем зберігання та обробки даних, що визначає актуальність дослідження блокчейн-технології. Важливою складовою технології є протоколи узгодження. В роботі вирішено задачу вдосконалення протоколів узгодження в розподілених системах за рахунок застосування принципово нових схем залу-


© А. М. Кудін, Л. В. Ковальчук, Б. А. Коваленко, 2019

чення майнерів до генерації нового блоку. Наведено опис нового варіанту протоколу консенсусу «proof-of-accuracy (PoAcc)», основні ідеї і положення якого вперше були описані в роботі [1]. Наведено результати строго математичного обґрунтування вибору параметрів протоколу, при яких можна забезпечити його стійкість до різних атак на блокчейн (зокрема, атаки, яка в криптовалютних блокчейнах називається атакою «подвійної витрати монети» (double spend attack) [2–5]). Аналог такої атаки будемо називати атакою підміни блоку, що в точності відображає її сутність. Авторами також пропонуються ідеї побудови схем застосування блокчейн-технології для здійснення обчислень.

**Ідеї нових протоколів консенсусу.** За основу ідеї побудови нового протоколу пропонується взяти найкращі ідеї від протоколів типу «доказу роботи» та «доказу частки володіння», зокрема від протоколів типу «доказу роботи» — ідею змагання між майнерами за якнайшвидше вирішення складної обчислювальної задачі, від протоколів типу «доказу частки володіння» — залежність виграшу майнеру в змаганні за право генерації наступного блоку від наявної у майнера інформації, необхідної для генерації блоку (далі — «вихідної інформації»). Ця інформація пов’язана із деяким цінним ресурсом реального світу, довільне накопичення якого є непростою задачею. Для обчислення рейтингу учасника протоколу в змаганні за генерацію нового блоку важливим є не тільки певні обчислювальні ресурси для вирішення задачі, але і вихідна інформація, яка дозволяє вирішити обчислювальну задачу з певною точністю. Для неможливості згенерувати довільну кількість цінних ресурсів для учасника протоколу, до початку протоколу застосовується такі обмеження: по-перше, регулюється чисельність учасників, які можуть прийняти участь в протоколі; по-друге, окремі дані рейтингу учасників формуються тільки на поточний сеанс протоколу (як сеансові ключі в схемі Діффі–Геллмана), по-третє, винагорода за участь у генерації нового блоку не прямо пов’язана із цінним ресурсом, який застосовується при обчисленні рейтингу учасника. Визначається наступний підхід до побудови протоколу узгодження: пропонується змінити обчислення алгоритму додавання нового блоку в блокчейн при застосуванні протоколу угоди «proof-of-works» таким чином, щоб необхідна для роботи алгоритму вихідна інформація була задані неповно і неточно. Значення, яке обчислюється алгоритмом і яке може бути перевірено іншими учасниками протоколу, визначається з точністю, що задається деяким порогом. Вихідна інформація розташовуються на декількох ресурсах за доступ до яких конкурують учасники протоколу угоди. Цінним ресурсом може бути IP-адреса абонента. Теоретичною основою протоколу пропонується вибрати загальну теорію оптимальних алгоритмів [6], яка пов'язує існування і складність алгоритмів з

точністю задання вхідних даних. Розглянемо один з практичних реалізацій протоколу «доказу точності».

**Варіант протоколу консенсусу «proof-of-accuracy».** Наведемо покроковий опис протоколу, який реалізує зазначені вище ідеї.

1. Етап ініціалізації.

A. Беруть участь усі активні на даний час вузли мережі зі своїми IP-адресами $n$ вузлів — $IP_1, \ldots, IP_n$.

B. Всі учасники протоколу генерують сумісно випадкове число $m$ за допомогою схеми Діффі–Геллмана для групи абонентів [7]. Випадкове число $m$ є невідомим для всіх учасників протоколу до кроку E.

C. За допомогою $s$ — того вектора ініціації $IV_s$, поточне значення якого зберігається в блокчейні, кожен учасник протоколу генерує випадкове число $R_{si}$ (різне для кожного учасника). Начальне значення вектора ініціалізації $IV_0$ формується при ініціалізації блокчейну за допомогою генерації випадкового 256-бітного числа.

D. Кожен учасник мережі обчислює геш-код $H\left(IV_s, IP_i, R_{si}\right)$, $i = \overline{1,n}$. Ці геш-коди будуть коефіцієнтами многочленів степеня $k$. Всього можна побудувати $A_n^k$ таких многочленів, враховуючи різні перестановки коефіцієнтів. Вибір значення $k$ здійснюється з урахуванням середньої кількості кроків до знаходження всіх значень поліному $\frac{k}{n}$, ймовірностей доступності вузлів мережі, можливостей атак на мережу та імовірності розгалуження. Всі коефіцієнти розміщуються у блокчейні.

E. Обираємо за протоколом «гри в покер» [8] $m$ учасників II етапу. Вибір значення $m$ здійснюється із врахуванням виконання приблизної рівності $\frac{m}{n} \approx 1$. Учасники етапу маркуються як «активні» учасники. Інші учасники («наглядачі») випадково обирають з блокчейну один з поліномів, побудованих на попередньому кроці.

F. За допомогою протоколу захищених багатосторонніх обчислень [9] «наглядачами» значення $y_1, ..., y_k$ обраного поліному в деяких точках $x_1, ..., x_k$ (наприклад, у точках 1, 2, …, $k$), після чого обрані значення випадково розподіляються між всіма вузлами мережі з використанням $(k, m)$ — порогового протоколу розподілу секрету (деякі вузли мережи не будуть містити жодного значення, але в кожному вузлі не більше одного значення).

2. Етап збору. $m$ активних учасників протоколу збирають по всім вузлам мережі $k$ значень поліному. Перший, хто зібрав всі значення вважається переможцем та формує наступний блок транзакцій. Для зменшення ймовірності виникнення «розгалужень» можна використовувати складність задачі відновлення коефіцієнтів поліному. Величину імовірності виникнення розгалужень можна регулювати за допомогою складності задачі відновлення коефіцієнтів поліному.

3. Етап верифікації. Використовуються протокол з доведення знань секрету «наглядачам» [9].

4. Етап ре-ініціалізації. Генеруємо наступне значення вектора ініціалізації вектора ініціації $IV_{s+1}$ для захисту від атак повтору шляхом обчислення геш-коду за алгоритмом SHA256 від конкатенації сумісно згенерованого випадкового число $m'$ за допомогою схеми Діффі–Геллмана для групи абонентів та збільшеного на одиницю попереднього значення, а саме: $IV_{s+1} = SHA256\,((IV_s + 1) \,||\, m')$.

**Оцінка стійкості протоколу консенсусу до атак.** Знайдемо точні аналітичні вирази, які пов'язують, з одного боку, імовірність атаки з підміною блоку, а з іншого — параметри мережі, такі як час синхронізації, інтенсивність генерації блоків та частку гешрейту зловмисника.

Введемо позначення. HMs — множина чесних майнерів, MMs — множина зловмисників, $T_H$ та $T_H'$ ($T_M$ та $T_M'$) — випадкові величини часу, які HMs (MMs) витрачають на створення одного блоку та створення і розповсюдження блоку по всім вузлам мережі. За умов експоненційного розподілу цих величин [5], $\alpha = \alpha_H + \alpha_M$ — загальна інтенсивність генерації блоків у мережі, $D_H\,(D_M)$ — верхні межі часу розповсюдження блоків між чесними майнерами (зловмисниками), $p_H\,(p_M = 1 - p_H)$ — ймовірність того, що HMs згенерують наступний блок раніше, ніж MMs. Ми будемо вважати, що $\Delta D = D_M - D_H > 0$. За заданих параметрам мережі $\Delta D$ та $\alpha$ межою безпеки (security threshold) для протоколу консенсусу PoAcc є найменше значення $p_0$, таке що при умові $p_M \geq p_0$ ймовірність успіху атаки підміни блоку дорівнює 1, незважаючи на кількість блоків підтвердження. Доведена наступна теорема.

**Теорема 1.** За заданих параметрам мережі ΔD та α межа безпеки $p_0$ може бути знайдена як рішення рівняння $2(1 - p_0) = e^{\alpha p_0 \Delta D}$.

У таблиці наведено значення границі безпеки протоколу при різних параметрах мережі.

Таблиця

*Значення границі безпеки протоколу PoAcc при різних параметрах мережі*

| $\alpha$ \ $D_H$ | $D_H = 2$ | $D_H = 5$ | $D_H = 10$ | $D_H = 20$ | $D_H = 60$ |
|---|---|---|---|---|---|
| $1/600$ | 0.49917 | 0.49792 | 0.49585 | 0.49174 | 0.47564 |
| $1/60$ | 0.49174 | 0.47961 | 0.460146 | 0.42408 | 0.31492 |
| $1/6$ | 0.42408 | 0.33757 | 0.24626 | 0.15678 | 0.06283 |

**Блокчейн обчислювальна система, що надає послуги за принципом краудсорсінгу.** Якщо порівнювати обчислювальні потужності найвідомішої з блокчейн платформ Bitcoin ($5 \times 10^{19}$ гешів за секунду) з потужністю сучасних суперкомп'ютерів, то перший з них, Тянхе-2, може обчислювати приблизно $2{,}6 \times 10^{12}$ гешів на секунду, що на 7 порядків менше кількості обчислених гешів мережею Bitcoin, причому у блокчейн мережах вона витрачається даремно. Ідея даної концепції — використання обчислювальних можливостей мережі блокчейн для виконання практичних (наукових або інженерних) обчислень у режимі краудсорсінгу, що дозволяє побудувати відносно дешеву розподілену гнучку та масштабовану систему виконання складних обчислень, без використання додаткової інфраструктури. Запропонована схема є блокчейн мережею, вузли якої можуть пропонувати свої обчислювальні ресурси і отримувати винагороду за виконані обчислення. При цьому архітектура системи надає гарантії проведення чесних обчислень та отримання очікуваної суми винагороди. Кожен вузол мережі може виконувати одну з ролей. Замовник — подає заявку на обчислення певного складного алгоритму з вхідними даними. За отримання результату виплачує винагороду. Виконавець — виконує один із розміщених у блокчейні алгоритмів, за це отримує винагороду від замовника. Майстер-вузол — обирається відповідно до алгоритму консенсусу блокчейну, його задачею є перевірка множини транзакцій та підтвердження чергового блоку. Кожен з вузлів також має однакову бібліотеку з множиною допустимих алгоритмів, що можуть відправлятися на краудсорс Замовником / обчислюватися Виконавцем. Кожен алгоритм бібліотеки доповнюється алгоритмом оцінки обчислювальної складності (для визначення винагороди) та алгоритмом перевірки правильності обчислення (опціонально).

Протокол роботи системи складається з трьох етапів: подання запиту на виконання алгоритму Замовником, виконання алгоритму Виконавцем та підтвердження блоку з виплатою винагороди Майстер-

вузлом. На першому етапі Замовник обирає необхідний алгоритм з множини допустимих алгоритмів та оцінює складність алгоритму, визначає залежність значення винагороди від складності алгоритму, формує транзакцію, що містить власний ідентифікатор, ідентифікотор алгоритму, вхідні дані, серіалізовані у байтовий рядок, а також значення винагороди. На другому етапі Виконавець обирає з пулу транзакцій запит на виконання алгоритму, перевіряє платіжеспроможність Замовника, обчислює алгоритм за відомими вхідними даними. Після цього, посилає до блокчейну транзакцію, до якої включає власний ідентифікатор, ідентифікатор транзакції-запиту Замовника, $E_s(q)$ — результат $q$ обчислення алгоритму, зашифрований на спільному ключі $s$ Виконавця та Замовника (обчислюється за допомогою неінтерактивного протоколу Діффі–Хеллмана на основі пар власних ключів), а також $Proof(x_i, q)$ — доведення наявності результату без розголошення, що обчислюється на основі приватного ключа Виконавця та власне результату. На третьому етапі Майстер-вузол завантажує транзакції, відкидаються неплатоспроможні Замовники та Виконавці з балансом гаманця, що не дозволяє сплатити штраф у випадку необхідності, розглядаються запити на виконання, що мають невичерпаний термін дії. Для кожного такого запиту збираються відповіді Виконавців. Принцип перевірки правильності результату полягає у порівнянні всіх відповідей, той результат, який співпадає у більшості вважається найдостовірнішим. Для цього, Майстер попарно порівнює значення $Proof(x_i, q)$ за допомогою функції $Compare(\cdot)$ (перевірка відбувається без розкриття значення $q$ а також без можливості підробити значення без знання секретного ключа $x_i$ завдяки неінтерактивному протоколу доведення без розголошення). Далі, найбільша за сумою гаманців множина однакових результатів вважається найбільш достовірною та кожен її член має отримати винагороду пропорційно до свого балансу (конкретна функція розподілу виграшу може бути довільною, але обов'язкова умова $a(x+y) \geq a(x) + a(y)$, де $a(x)$ — винагорода Виконавця з балансом $x$). Решта Виконавців (відповіді яких є недостовірними) виплачують штраф на користь Майстер-вузла (функція нарахування штрафу $p(x)$ також довільна, але з додатковою умовою $p(x+y) \leq p(x) + p(y)$). Далі, Майстер вузол формує відповідні транзакції з винагородами та штрафами, перевіряє визначену кількість попередніх блоків (згідно з загальним процесом перевірки для даного блокчейну) та підписує новий блок.

### Список використаних джерел:


1. Кудин А. М. Блокчейн и криптовалюты на основаниии «доказательства точности». *Математичне та комп'ютерне моделювання.* Серія: Технічні науки : зб. наук. праць. Кам'янець-Подільський : Кам'янець-Подільський національний університет імені Івана Огієнка, 2017. Вип. 15. С. 104–108.
2. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2009. 9 p.
3. Rosenfeld M. Analysis of hashrate-based double-spending. 2014. 13 p.
4. Pinzon C., Rocha C. Double-Spend Attack Models with Time Advantage for Bitcoin. *Electronic Notes in Theoretical Computer Science.* 2016. Vol. 329. P. 9–103.
5. Pinson P., Lewenberg Y., Sompolinsky Y. Inclusive Block Chain Protocols. 20 p.
6. Grunspan C., Perez-Marco R. DOUBLE SPEND RACES. 35 p.
7. Трауб Д., Васильковский Г., Вожьняковский Х. Информация, неопределенность, сложность. М. : Мир, 1988. 184 с.
8. Steiner M., Tsudik G., Waidner M. Diffie-Hellman key distribution extended to groups, 1996.
9. Menezes A. J., van Oorschot P. C., Vanstone S. A. Handbook of Applied Cryptography. 816 p.
10. Ben-David A., Nisan N., Pinkas B. FairplayMP: a system for secure multi-party computation. *Computer and Communications Security — CCS 2008*, ACM. 2008. P. 257–266.


## THEORETICAL FOUNDATIONS AND APPLICATION OF BLOCKCHAIN: IMPLEMENTATION OF NEW PROTOCOLS OF CONSENSUS AND CROWDSOURCING COMPUTING


The analysis of existing blockade technologies, their algorithms of consensus and resistance to known block substitution attacks is given. The main ideas and variants of practical implementation of the new «Proof-of-accuracy» consensus protocol developed by the authors are presented. The project of BlockChein-system, which provides services of calculations in the mode of crowdsourcing, is presented.



**Key words:** *blockchain, consensus protocols, wrong block attack attacks, crowdsourcing.*

Одержано 01.02.2019

УДК 003.026:004.056
DOI: 10.32626/2308-5916.2019-19.69-74

**І. С. Кудряшов*,** студент,
**Г. А. Малєєва**,** аспірант

*Харківський національний університет імені В. Н. Каразіна, м. Харків,
**Харківський національний університет радіоелектроніки, м. Харків

# АНАЛІЗ ВЛАСТИВОСТЕЙ ЕЛЕКТРОННИХ ПІДПИСІВ НА БАЗІ MQ-ПЕРЕТВОРЕНЬ

Останнім часом найбільш важливими дослідженнями у сфері криптографічного захисту інформації є дослідження, які пов'язані з можливістю використання існуючих алгоритмів у пост квантовий період, а також дослідження, які спрямовані на пошуки перспективних алгоритмів які будуть стійкими до квантових атак, а отже відповідатимуть усім вимогам пост квантового світу. Стаття присвячена аналізу алгоритмів електронного підпису на базі MQ (Multivariate Quadratic Transformations — мультиваріативні квадратичні перетворення). У статті представлена загальна схема створення електронного підпису із застосуванням мультиваріативних перетворень. Наведені результати оцінки механізмів електронного підпису відносно загальноприйнятих критеріїв. Як основні умовні критерії використані довжини ключових даних та результату криптографічного перетворення, тобто електронного підпису, а також обчислювальна ефективність створення підпису та його перевірки. Порівняння проводилося щодо електронних підписів LUOV, Gui, Rainbow, MQDSS, TPSig, DualModeMS, HiMQ-3, DME та GeMSS. Під час аналізу використана методика порівняння криптографічних механізмів на основі експертних оцінок за сукупністю умовних та безумовних критеріїв методом вагових коефіцієнтів. На основі проведених досліджень обрані найбільш перспективні кандидати на пост квантовий стандарт електронного підпису, а також запропоновані рекомендації щодо їх застосування.

**Ключові слова:** *асиметричний ключ, асиметричні криптоперетворення, багатовимірні перетворення, електронний підпис, квадратичні поля, постквантові електронні підписи, MQ перетворення, пост квантовий алгоритм.*

**Вступ.** У 2016 році Національний інститут стандартів та технологій (NIST) США оголосив конкурс на пошук нових стандартів криптографічного захисту інформації, які будуть стійкими до пост-квантових атак [1]. Доведено, що більшість існуючих криптографічних стандартів не будуть стійкими до квантових атак [2]. У зв'язку з цими фактами був оголошений конкурс NIST PQC основне завдання якого пов'язано з від-

© І. С. Кудряшов, Г. А. Малєєва, 2019

бором алгоритмів, які планується прийняти в 2020–2022 рр. До таких віднесено стандарти електронного підпису (ЕП), стандарти направленого шифрування (НШ) та протоколи інкапсуляції ключів (ПІК).

Значна кількість механізмів запропонована на базі мультиваріативних квадратичних (MQ) перетворень — 13 з 71. На даний момент 2 кандидати відкликані, 3 кандидати атаковані, 2 з них вже запропонували шляхи усунення вразливостей. Таким чином з 13 запропонованих алгоритмів на даному етапі пропонується розглянути 9 алгоритмів електронного підпису — LUOV, Gui, Rainbow, MQDSS, TPSig, DualModeMS, HiMQ-3, DMT та GeMSS. У статті наводяться результати досліджень і порівнянь цих кандидатів відносно безумовних та умовних критеріїв та вимог технічних, техніко-економічних та техніко-експлуатаційних.

**Сутність MQ-перетворень.** Аналіз показує, що багатовимірна MQ криптографія ґрунтується на складності вирішення задач, що пов'язані з багатовимірними поліномами над кінцевими полями та вирішенням систем багатовимірних поліноміальних рівнянь. Основними особливостями MQ-перетворень є невеликі, у порівнянні з іншими, складність асиметричних перетворень та невеликі обчислювальні ресурси здійснення перетворень.

Детальний опис схеми електронного підпису на базі мультиваріативних перетворень описаний у [3]. У загальному випадку послідовність (схема) генерації та перевірки ЕП [4], що базується на MQ-перетвореннях, показано на рис. 1.

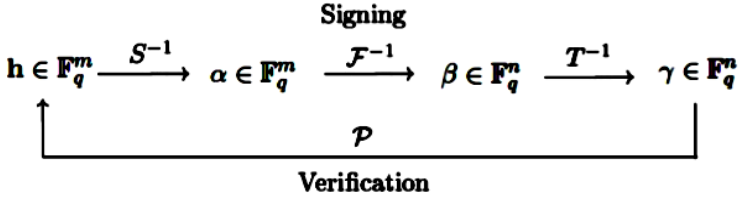



***Рис. 1.*** *Схеми створення та перевірки підпису на основі MQ-схеми*

де $F = (F^{(1)},...,F^{(m)}) : F_q^{\,n} \to F_q^{\,m}$ — секретна система, або центральне відображення, $S : F_q^{\,m} \to F_q^{\,m}$ та $T : F_q^{\,n} \to F_q^{\,n}$ — афінні відображення, а $P = (S \circ F \circ T)$ — публічний ключ.

Опис запропонованих алгоритмів. На конкурс NIST подано 8 кандидатів, що ґрунтуються на MQ — перетвореннях — LUOV [5], Gui [6], Rainbow [7], MQDSS [8], TPSig [9], DualModeMS [10], HIMQ-3 [4], DME [11] та GeMSS [12]. Більш детально ці алгоритми розглянуті у [3].

Схема підпису LUOV [5], (автор Ward Beullens) — Lifted Unbalanced Oil and Vinegar — це просте удосконалення схеми UOV, у якому значно зменшено розмір відкритих ключів. В ній використовуєть-

ся відображення публічного ключа (lifted — означає піднесений) у розширене поле, таким чином зменшується розмір ключа. Схема LUOV може бути використана в двох режимах: класичному, та режиму з відновленням повідомлення.

Схема підпису Gui [6] (автори — Ming-Shing Chen, Albrecht Petzoldt, Dieter Schmidt, Bo-Yin Yang) базується на HFEv — схемі ЕП, яку вперше запропонували Патарін, Куртуіз та Губін. В модифікованій схемі QUARTZ, як і в Gui, використовується спеціально розроблений процес вироблення ЕП за допомогою якого зменшується розмір самого підпису.

Схема підпису Rainbow [7] (автори — Ming-Shing Chen, Albrecht Petzoldt, Dieter Schmidt, Bo-Yin Yang) базується на добре відомій UOV схемі, яка була запропонована ще у 1999 році. Безпосередньо ЕП Rainbow розроблено у 2005 році, останні зміни вносилися до цього механізму ще у 2008 році, у зв'язку з існуючою на той час атакою. Варто зазначити що Rainbow має найбільш привабливі показники швидкодії.

Схема підпису MQDSS [8] (автори — Ming-Shing Chen, Andreas Husing, Joost Rijneveld, Simona Samardjiska, Peter Schwabe) є схемою ЕП, що ґрунтується на застосуванні до 5-крокової схеми ідентифікації перетворення Фіата–Шаміра (Fiat-Shamir transformation, FST).

Схема підпису TPSig [9] (автори — Yossi (Joseph) Peretz, Nerya Granot) — це схема ЕП, яка базується на рішенні MQ-проблеми та проблеми NSARE (асиметричні алгебраїчні рівняння Рікатті).

Схема підпису DualModeMS [10] (автори — J.-C. Faug`ere, L. Perret, J. Ryckeghem) — A Dual Mode for Multivariate-based Signature — ЕП, основна властивість якого є те, що при його застосуванні використовуються малі за розміром публічні ключі. Цей підпис базується на HFEv схемі, з модифікацією методом SBP, який дозволяє перетворити будь-який мультиваріативний підпис на основі MI на новий підпис, але з меншим публічним ключем, та більшим підписом.

Механізм HIMQ-3 [4] (автор — Kyung-Ah Shim ) — A High Speed Signature Scheme based on Multivariate Quadratic Equations — ЕП, що базується на модифікації стандартної MQ-схеми ЕП з парадигмою MQ+IP. Її сутність полягає у тому, що складність базується не тільки на вирішені MQ-проблеми, а також на проблемі невизначеності ізоморфізму поліномів (IP-problem).

Механізм DME [11] (автор — Ignacio Liengo) — a public key, signature and KEM system based on double exponentiation — ЕП, що базується на подвійному піднесенні з використанням матричних експонентів.

Механізм GeMSS [12] (автори — J.-C. Faug`ere, L. Perret, J. Ryckeghem, A. Casanova, G. Macario-Rat, J. Patarin) — Great Multivariate Signature Scheme — що має схожість з DualModeMS. Відмінність полягає у тому, що ЕП при використанні має малий розмір, водночас,

коли публічний ключ має великий розмір, а процес верифікації підпису доволі швидкий.

Аналіз механізмів відносно безумовних критеріїв. У роботі [13] проведено аналіз алгоритмів відносно безумовних критеріїв. Результати аналізу наведені у таблиці. За наведеними результатами були обрані механізми які, на наш погляд, задовольняють усім безумовним критеріям. Ця оцінка була спроектована у інтегральний безумовний критерій, який обчислюється наступним чином:

$$W_\delta = W_1 \wedge W_2 \wedge W_3 \wedge W_4 \wedge W_5 \wedge W_6 \wedge W_7$$

Якщо $W_\delta$ відповідає значенню 0, то приймається, що криптографічне перетворення не задовольняє безумовним критеріям, якщо 1 — задовольняє.

Таблиця

*Результати аналізу відповідності безумовним критеріям пост-квантових перетворень типу ЕП на базі MQ-перетворень*

| Scheme | $W_{\delta 1}$ | $W_{\delta 2}$ | $W_{\delta 3}$ | $W_{\delta 4}$ | $W_{\delta 5}$ | $W_{\delta 6}$ | $W_{\delta 7}$ | $W_\delta$ |
|---|---|---|---|---|---|---|---|---|
| TPSig | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 0 |
| HiMQ3 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 0 |
| DME | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 |
| LUOV | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| GUI | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Rainbow | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| MQDSS | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| DualModeMS | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| GeMSS | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |

Таким чином можна зробити висновок, що на даному етапі досліджень лише 6 алгоритмів відповідають безумовним критеріям і є потенційними кандидатами на пост-квантовий стандарт ЕП.

Порівняння алгоритмів відносно умовних критеріїв. У роботах [3, 13] наведені порівняння алгоритмів відносно технічних, техніко-економічних та техніко-експлуатаційних умов їх використання. Узагальнені результати оцінок показано на рис. 2.

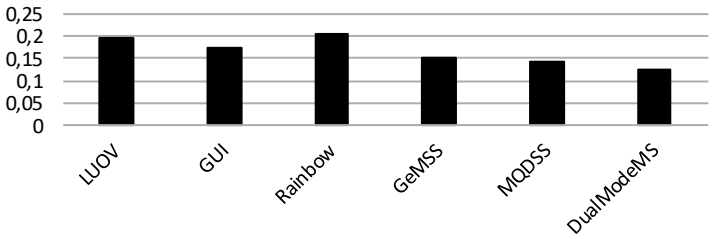



***Рис. 2.*** *Відносна перевага алгоритмів ЕП на базі MQ перетворень*

Відповідно до рис. 2, який узагальнює дослідження [3, 13], можна стверджувати, що найбільш перспективними алгоритмами ЕП на базі MQ-перетворень є Rainbow та LUOV. Також, варто зазначити, що у 2-й раунд [14] конкурсу NIST PQC пройшли 4 з 6 алгоритмів, які задовольняють безумовним критеріям: це LUOV, Rainbow, GeMSS, та MQDSS.

**Висновки.** Розглянуті алгоритми електронного підпису на базі мультиваріативних квадратичних перетворень, які подані як кандидати на пост-квантовий стандарт, на конкурс NIST PQC. Представлено результат їх аналізу при застосуванні безумовних та умовних технічних, техніко-економічних та техніко-експлуатаційних критеріїв. На основі отриманих результатів можна зробити висновок, що лише 6 з 9-ти представлених механізмів на базі MQ-перетворень відповідають усім безумовним критеріям. Як показали дослідження [3, 13], з цих 6 алгоритмів найбільш перспективними, на думку авторів, є Rainbow та LUOV [3, 13]. До значимих у цьому напрямку варто віднести аналіз стійкості наведених алгоритмів від різних видів атак. Перспективність дослідницьких робіт у напрямку MQ-перетворень підтверджує той факт, що 4 з 9 механізмів електронного підпису, які пройшли у 2-й раунд конкурсу — це підписи на базі MQ-перетворень.

**Список використаних джерел:**


1. Post-Quantum Cryptography, Round 1 Submissions, 2017. URL: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.
2. Горбенко Ю. І. Методи побудування та аналізу, стандартизація та застосування криптографічних систем : монографія. Харків : Форт, 2016. 959 с.
3. Горбенко І. Д., Кудряшов І. С., Онопрієнко В. В. Порівняльний аналіз пост квантових стандартів електронного підпису на основі мультиваріативних квадратичних перетворень. *Радиотехника* : всеукр. межвед. науч.-техн. сб. Харьков : ХТУРЕ. 2018. Вып. 195. С. 46–60.
4. Kyuang-Ah Shim, Cheol-Min Park, Aeyoung Kim. HiMQ-3: A High Speed Signature Scheme based on Multivariate Quadratic Equations, NIST Submission, 2017. URL: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/-Round-1-Submissions.
5. Ward Beullens, Bart Preneel, Alan Szepieniec, Frederik Vercauteren. LUOV: Lifted Unbalanced Oil and Vinegar, NIST Submission, 2017. URL: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.
6. Jintai Ding, Ming-Shen Chen, Albrecht Petzoldt, Dieter Schmidt, Bo-Yin Yang. Gui, NIST Submission, 2017. URL: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.
7. Jintai Ding, Ming-Shen Chen, Albrecht Petzoldt, Dieter Schmidt, Bo-Yin Yang. Rainbow. NIST Submission, 2017. URL: https://csrc.nist.gov/Projects/-Post-Quantum-Cryptography/Round-1-Submissions.
8. Simona Samardjiska, Ming-Shing Chen, Andreas Hulsing, Joost Rijneveld, Peter Schwabe. MQDSS, NIST Submission, 2017. URL: https://csrc.nist.gov/-Projects/Post-Quantum-Cryptography/Round-1-Submissions.

9. Joseph Peretz, Nerya Granot. TPSig, NIST Submission, 2017. URL: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.
10. Faugère J.-C., Perret L., Ryckeghem J. DualModeMS: A Dual Mode for Multivariate-based Signature, NIST Submission, 2017. URL: https://csrc.nist.gov/-Projects/Post-Quantum-Cryptography/Round-1-Submissions.
11. Ignacio Luengo, Martin Avendano, Michel Marco. DME: DME a public key, signature and KEM system based on double exponentiation, NIST Submission, 2017. URL: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/-Round-1-Submissions. unpublished.
12. Casanova A., Faugère J.-C., Macario-Rat G., Patarin J., Perret L., Ryckeghem J. GeMSS: A Great Multivariate Short Signature, NIST Submission, 2017. URL: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.
13. Post-Quantum Cryptography, Round 2 Submissions, 2019. URL: https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions.

## ANALYSIS OF OPPORTUNITIES OF THE DS BASED ON THE MQ-TRANSFORMATION

Recently, the most critical studies in the field of cryptographic information security are studies that relate to the possibility of using existing algorithms in the post quantum period, as well as studies that seek to find promising algorithms that will be resistant to quantum attacks, and therefore meet all requirements of the post. quantum world. The paper is devoted to the analysis of MQ-based electronic signature algorithms (Multivariate Quadratic Transformations) of transformations relative to the unconditional and conditional criteria that were proposed as candidates for the post-quantum standard of the NIST PQC competition. The paper presented the general scheme of creating an electronic signature using multivariate transformations. The analysis of candidates and their peculiarities was also conducted. The results of the evaluation of the electronic signature mechanisms in relation to generally accepted unconditional criteria, as well as regarding the conditional criteria based on the techno-economic and technical-operational requirements for nominated candidates for the post-quantum standard are presented. The main conditional criteria were the lengths of key data and the result of the cryptographic transformation, that is, the electronic signature, as well as the computational efficiency of signature creation and verification. The comparison was made on the electronic signatures of LUOV, Gui, Rainbow, MQDSS, TPSig, DualModeMS, HiMQ-3, DME and GeMSS. During the analysis, the technique of comparing cryptographic mechanisms on the basis of expert evaluations using a combination of conditional and unconditional criteria by weighting coefficients method was used. On the basis of the conducted researches, the most perspective candidates for the post quantum standard of electronic signature were selected, as well as recommendations for their application were proposed.

**Key words:** *asymmetric key, asymmetric cryptographic transformations, multivariate transformations, digital electronic signature, quadratic fields, post-quantum electronic signatures, MQ transformation, post quantum algorithm.*

Одержано 01.02.2019

УДК 519.65
DOI: 10.32626/2308-5916.2019-19.75-81

**П. С. Малачівський*,** д-р техн. наук,
**Б. Р. Монцібович*,** канд. фіз.-мат. наук,
**Я. В. Пізюр**,** канд. фіз.-мат. наук,
**Р. П. Малачівський**,** інженер

*Інституту прикладних проблем механіки і математики
імені Я. С. Підстригача НАН України, м. Львів,
**Національний університет «Львівська політехніка», м. Львів

# ЧЕБИШОВСЬКЕ НАБЛИЖЕННЯ РАЦІОНАЛЬНИМ ВИРАЗОМ ФУНКЦІЙ ДВОХ ЗМІННИХ

Запропоновано метод побудови чебишовського наближення раціональним виразом для функцій двох змінних. Ідея методу ґрунтується на побудові граничного середньостепеневого наближення у нормі простору $L^p$ при $p \to \infty$. Для побудови цього наближення використано метод найменших квадратів з двома змінними ваговими функціями. Одна вагова функція забезпечує побудову середньостепеневого наближення, а друга — уточнення параметрів раціонального виразу за схемою лінеаризації. Запропоновано спосіб послідовного уточнення значень вагових функцій. Результати розв'язування тестових прикладів підтверджують ефективність використання запропонованого методу.

**Ключові слова**: *чебишовське наближення раціональним виразом, функції двох змінних, середньостепеневе наближення, метод найменших квадратів.*

**Вступ.** Нехай неперервну функцію двох змінних $f(x, y)$ задану на множині точок $(x_i, y_j)$, $i = \overline{0, n}$, $j = \overline{0, m}$ необхідно наблизити нескорочуваним раціональним виразом

$$R_{k,l}(a,b;x,y) = \frac{\sum_{i=0}^{k} a_i \varphi_i(x,y)}{\sum_{i=0}^{l-1} b_i \varphi_i(x,y) + \varphi_l(x,y)}, \qquad (1)$$

де $\varphi_i(x,y)$, $i = \overline{0, k_m}$, $k_m = \max(k, l)$ — система базисних функцій, а $a_i$, $i = \overline{0, k}$ і $b_i$, $i = \overline{0, l-1}$ — невідомі параметри: $\{a_i\}_{i=0}^{k} \in A$, $A \subseteq R^k$, $\{b_i\}_{i=0}^{l-1} \in B$, $B \subseteq R^{l-1}$, $R^m$ — $m$-вимірний векторний простір.

© П. С. Малачівський, Б. Р. Монцібович, Я. В. Пізюр, Р. П. Малачівський, 2019 

Побудова чебишовського наближення раціональним виразом (1) для функції $f(x, y)$ на множині точок $(x_i, y_j)$, $i = \overline{0, n}$, $j = \overline{0, m}$ полягає в обчисленні таких значень параметрів $a^*$ та $b^*$, при яких досягається виконання умови

$$\max_{x_0 \le x \le x_n,\ y_0 \le y \le y_m} \left| f(x, y) - R_{k,l}(a^*, b^*; x, y) \right| = \min_{a \in A,\ b \in B} \max_{x_0 \le x \le x_n,\ y_0 \le y \le y_m} \left| f(x, y) - R_{k,l}(a, b; x, y) \right|. \quad (2)$$

На жаль, поки що немає ефективних алгоритмів для обчислення параметрів чебишовського наближення раціональним виразом [1]. Серед методів отримання чебишовського наближення функцій багатьох змінних раціональним виразом здебільшого застосовують зведення до послідовного розв'язування задачі лінійного програмування [2, 3], або метод нелінійної оптимізації [1, 4]. В працях [5, 6] описано алгоритми обчислення параметрів чебишовського наближення функцій однієї змінної на основі схеми Ремеза з використанням диференціальної корекції. Метод побудови чебишовського наближення раціональним виразом на основі обчислення середньостепеневих наближень функцій однієї змінної описано в [7].

Ми пропонуємо метод побудови чебишовського наближення функцій двох змінних раціональним виразом як граничного наближення у нормі простору $L^p$ при $p \to \infty$. Він ґрунтується на методі описаному в [8] і полягає у послідовній побудові середньостепеневих наближень. Останні раціональним виразом обчислюються за методом найменших квадратів з використанням двох змінних вагових функцій, значення яких уточнюються з урахуванням всіх попередніх наближень. Параметри раціонального наближення за методом найменших квадратів визначаємо з використанням лінеаризації [9, 10].

**1. Середньостепеневе наближення функцій раціональним виразом.** Для оцінки похибки середньостепеневого наближення функції $f(x, y)$, заданої на множині точок $(x_i, y_j)$, $i = \overline{0, n}$, $j = \overline{0, m}$, використовують норму евклідового простору $E^p$ $(1 \le p < \infty)$

$$\|\Delta\|_{E^p} = \left( \sum_{i=0}^{n} \sum_{j=0}^{m} \left| \Delta(x_i, y_j) \right|^p \right)^{1/p}, \quad (3)$$

де $\Delta(x, y) = f(x, y) - R_{k,l}(a, b; x, y)$. Граничне значення норми $\|\Delta\|_{E^p}$ при $p \to \infty$ відповідає нормі у просторі неперервних функцій $\|\Delta\|_C$ [1].

**2. Обчислення параметрів чебишовського наближення раціональним виразом.** Якщо неперервне чебишовське наближення

раціональним виразом $R_{k,l}(a,b;x,y)$ (1) для функції $f(x,y)$ на множині точок $(x_i, y_j)$, $i=\overline{0,n}$, $j=\overline{0,m}$ існує, то побудова такого наближення ґрунтується на ідеї послідовного обчислення середньостепеневих наближень при $p=2,3,4,\ldots$. Для побудови середньостепеневого наближення функції $f(x,y)$ раціональним виразом (1) в просторі $E^p$ використовуємо метод найменших квадратів [8]

$$\sum_{i=0}^{n}\sum_{j=0}^{m}\rho_r(x_i,y_j)\left(f(x_i,y_j)-R_{k,l}(a,b;x_i,y_j)\right)^2 \xrightarrow[a\in A,\ b\in B]{} \min, \quad (4)$$

$$r=0,1,\ \ldots,p-2$$

з послідовним уточненням значень вагової функції $\rho_r(x,y)$

$$\rho_0(x,y)=1,\ \rho_r(x,y)=\prod_{i=1}^{r}\left|\Delta_i(x,y)\right|,\ r=1,\ldots,p-2,\ p=3,4,\ldots, \quad (5)$$

де $\Delta_s(x,y)=f(x,y)-R_{k,l,s-1}(a,b;x,y)$, $s=\overline{1,r}$, $R_{k,l,s}(a,b;x,y)$ — наближення за методом найменших квадратів функції $f(x,y)$ з ваговою функцією $\rho_s(x,y)$. Наближення $R_{k,l,s}(a,b;x,y)$ відповідає середньостепеневому наближенню степеня $p=s+2$.

Побудова наближення раціональним виразом за методом найменших квадратів — це нелінійна задача. Для побудови такого наближення застосовано лінеаризацію з використанням змінної вагової функції [9, 10], яка полягає в ітераційному уточненні наближення раціональним виразом (1). Відповідно до цього методу лінеаризації для кожного фіксованого значення $p$ обчислюємо наближення функції $f(x,y)$ раціональним виразом $R_{k,l}(a,b;x,y)$ (1) за методом найменших квадратів

$$\sum_{i=0}^{n}\sum_{j=0}^{m}\rho_r(x_i,y_j)\upsilon_{r,t}(x_i,y_j)\left(\Phi_{r,t}(a,b;x_i,y_j)\right)^2 \xrightarrow[a\in A,\ b\in B]{} \min, \quad (6)$$

$$r=p-2,\ t=0,1,\ \ldots,$$

де

$$\Phi_{r,t}(a,b;x,y)=f(x,y)\left(\sum_{i=0}^{l-1}b_{i,r,t}\varphi_i(x,y)+\varphi_l(x,y)\right)-\sum_{i=0}^{k}a_{i,r,t}\varphi_i(x,y). \quad (7)$$

Значення вагової функції $\rho_r(x,y)$ обчислюємо за формулою (5), а вагової функції $\upsilon_{r,t}(x,y)$ — за формулою

$$\upsilon_{r,t}(x,y)=\begin{cases}1, \text{ якщо } & r=0,\ t=0,\\ \left(\sum_{i=0}^{l-1}b_{i,r,t-1}\varphi_i(x,y)+\varphi_l(x,y)\right)^{-2}, & \text{якщо } t>0.\end{cases} \quad (8)$$

Уточнення наближення раціональним виразом (1) за методом найменших квадратів (6), (8) можна контролювати точністю $\varepsilon_1$ виконання умови

$$\left| \eta_{r,t-1} - \eta_{r,t} \right| \le \varepsilon_1 \eta_{r,t}, \tag{9}$$

де

$$\eta_{r,t} = \sum_{i=0}^{n} \sum_{j=0}^{m} \rho_r(x_i, y_j) \upsilon_{r,t}(x_i, y_j) \left( \Phi_{r,t}(a,b; x_i, y_j) \right)^2 . \tag{10}$$

Під час тестування використовували значення $\varepsilon_1 = 0.003$, яке забезпечувало збіжність двох-трьох значущих цифр суми квадратів відхилень (10) на множині точок задання наближуваної функції. Виконання умови (9) означає, що середньостепеневе наближення степеня $p = r + 2$ раціональним виразом $R_{k,l,r}(a,b; x, y)$ обчислено з точністю $\varepsilon_1$. Значення параметрів наближення $R_{k,l,r}(a,b; x, y)$ такі:

$$a_{j,r} = a_{j,r,t} \quad (j = \overline{0, k}) \text{, а } b_{j,r} = b_{j,r,t} \quad (j = \overline{0, l-1}) . \tag{11}$$

Отже, побудова чебишовського наближення раціональним виразом (1) полягає у застосуванні двох ітераційних процесів: вкладених ітерацій (6)–(8) і зовнішніх (4), (5). Завершення ітерацій (4), (5) можна контролювати досягненням деякої заданої точності $\varepsilon$

$$\mu_{r-1} - \mu_r \le \varepsilon \mu_r , \tag{12}$$

де

$$\mu_r = \max_{x_0 \le x \le x_n,\ y_0 \le y \le y_m} \left| f(x,y) - R_{k,l,r}(a,b; x, y) \right| . \tag{13}$$

Під час розв'язування тестових прикладів досягнення точності $\varepsilon = 0.003$ спостерігалося за вісім-дванадцять ітерацій (4), (5). Ця точність забезпечувала збіжність двох-трьох значущих цифр похибки чебишовського наближення раціональним виразом. При цьому точність $\varepsilon_1 = 0.003$, визначення проміжних наближень раціональним виразом, досягалась за три-чотири внутрішні ітерації (6)–(8). Якщо для $r \ge 1$ значення вагової функції $\upsilon_{r,0}(x, y)$ не змінювати — залишити рівними попереднім $\upsilon_{r-1,t}(x, y)$, то для уточнення раціонального виразу достатньо було лише двох ітерацій (6), (8).

Для отриманого наближення раціональним виразом (1) проводимо симетризуюче коригування. Визначаємо значення адитивної поправки

$$\overline{a}_0 = \left( \mu_{\max} + \mu_{\min} \right) / 2 , \tag{14}$$

де

$$\mu_{\max} = \max_{x_0 \le x \le x_n,\ y_0 \le y \le y_m} \left( f(x, y) - R_{k,l}(a,b; x, y) \right) ,$$

$$\mu_{\min} = \min_{x_0 \le x \le x_n,\ y_0 \le y \le y_m} \left( f(x, y) - R_{k,l}(a,b; x, y) \right) .$$

В результаті шукане чебишовське наближення неперервної функції $f(x, y)$ раціональним виразом (1) буде мати вигляд

$$R_{k,l}\left(a,b;\, x, y\right) = R_{k,l}(a,b;\, x, y) + \overline{a}_0 . \qquad (15)$$

**Приклад.** Знайдемо чебишовське наближення функції $z(x, y) = e^{-(x^2+y^2)}$ заданої в точках $(x_i, y_j)$, $i = \overline{0,10}$, $j = \overline{0,10}$, де $x_i = -1 + 0.2i$, $y_j = -1 + 0.2\, j$, раціональним виразом $R_{2,2}(x, y)$, в якому чисельник і знаменник поліноми другого степеня за змінними *x* та *y*.

З використанням запропонованого методу при $\varepsilon = 0.003$ за сім ітерацій (4), (5) для функції $z(x, y)$ отримано раціональний вираз

$$R_{2,2}(x, y) = \frac{P_2(x, y)}{Q_2(x, y)}, \qquad (16)$$

в якому

$$P_2(x, y) = 1.007258776 - 0.115894128_{10}{}^{-8}\, x - 0.234478414_{10}{}^{-8}\, y -$$
$$-0.3393352184\, x^2 - 0.3393352234\, y^2 + 0.1445200801_{10}{}^{-9}\, xy,$$

$$Q_2\left(x, y\right) = 1 + 0.2634009507_{10}{}^{-8}\, x - 0.5167223229_{10}{}^{-8}\, y +$$
$$+0.7853630535\, x^2 + 0.7853630273\, y^2 + 0.4766678537_{10}{}^{-9}\, xy.$$

Раціональний вираз (16) з урахуванням коригуючої поправки $\overline{a}_0 = -0.00014942155$ забезпечує абсолютну похибку наближення — 0.007665. В процесі обчислення чебишовського наближення функції *z*(*x*, *y*) похибка наближення на ітераціях (5) набувала таких значень:

0.0153866457, 0.010443066, 0.009504082, 0.0085679,
0.007935789, 0.0078146481, 0.0078186119.

Поверхню похибки апроксимації раціональним виразом (16) показано на рисунку.

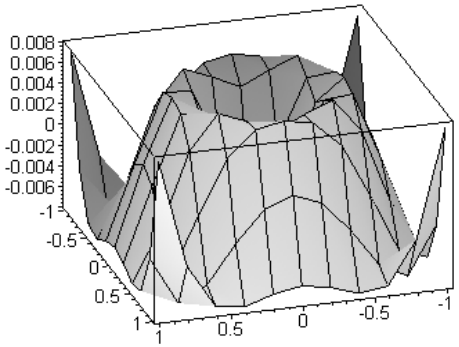



***Рисунок.*** *Поверхня похибки апроксимації функції* $z(x, y)$ *раціональним виразом (16)*

Цей приклад взято з праці Л. В. Петрак [7], в якій для отримання чебишовського наближення функції $z(x, y)$ використано метод зведення нелінійної задачі (2) до послідовного розв'язування задач лінійного програмування. Чебишовське наближення функції $z(x, y)$ в праці [7] отримано з похибкою 0.007666 за сім звертань до процедури розв'язування задачі лінійного програмування.

**Висновок.** Запропонований метод побудови чебишовського наближення раціональним виразом неперервних таблично-заданих функцій забезпечує можливість обчислення наближення з необхідною точністю. Метод простий для реалізації, надійний і ефективний. Результати розв'язування тестових прикладів підтверджують досить швидку збіжність запропонованого методу при наближенні раціональним виразом функцій однієї та двох змінних. Під час розв'язування тестових прикладів за цим методом збіжність двох-трьох значущих цифр похибки чебишовського наближення раціональним виразом досягалась з використанням від восьми до дванадцяти ітерацій (4), (5).

Ідея запропонованого методу допускає його використання для апроксимації раціональним виразом неперервних таблично-заданих функцій багатьох змінних.

**Список використаних джерел:**


1. Коллатц Л., Крабс В. Теория приближений. Чебышевские приближения и их приложения. М. : Наука, 1978. 272 с.
2. Каленчук-Порханова А. О., Вакал Л. П. Побудова найкращих рівномірних наближень функцій багатьох змінних. *Комп'ютерні засоби, мережі та системи.* 2007. № 6. С. 141–148.
3. Петрак Л. В. Приближение функций многих переменных рациональными дробями. *Программы оптимизации*. Свердловск : УНЦ АН СССР, 1975. Вып. 6. С. 130–144.
4. Malachivskyy P. S., Matviychuk Y. N., Pizyur Y. V., Malachivskyi R. P. Uniform Approximation of Functions of Two Variables. *Cybernetics and Systems Analysis.* N 3. May–June, 2017. P. 426–431.
5. Filip S.-I., Nakatsukasa Y., Trefethen L. N., Beckermann B. Rational minimax approximation via adaptive barycentric representations. URL: https://arxiv.org/-pdf/1705.10132. 2017. P. 1–29.
6. Nakatsukasa Y., Sete `O., Trefethen L. N. The AAA algorithm for rational approximation. *SIAM J. SCI. COMPUT.* 2018. Vol. 40, N 3. P. A1494–A1522.
7. Малачівський П. С., Пізюр Я. В., Малачівський Р. П. Рівномірне наближення раціональним виразом. *Комп'ютерні технології друкарства.* 2018. № 1 (39). С. 54–59.
8. Малачівський П. С., Пізюр Я. В., Малачівський Р. П. Обчислення чебишовського наближення функцій багатьох змінних. *Обчислювальні методи і системи перетворення інформації*: зб. праць V наук.-техн. конф., Львів, 4–5 жовтня 2018 р. Львів: ФМІ НАНУ, 2018. С. 35–38.
9. Калиткин Н. Н. Численные методы. М.: Наука, 1978. 512 с.

10. Малачівський П. С., Пізюр Я. В. Розв'язування задач в середовищі Maple. Львів : Видавництво «РАСТР–7». 2016. 282 с.

## CHEBYSHEV APPROXIMATION BY RATIONAL EXPRESSION FUNCTIONS OF TWO VARIABLES

The method for constructing of Chebyshev approximation by rational expression for function of two variables is proposed. Idea of the method is based on constructing the boundary power-average approximation in $L^p$ norm with $p \to \infty$. Least square method with two weight functions is used to construct of this approximation. One weight function ensures the construction of power-average approximation, and another refines parameters of rational expression by linearization scheme. Iterative refinement of weight functions values is proposed. Results of test examples solving confirm the effectivity of proposed method.

**Key words:** *Chebyshev approximation by rational expression, function of two variables, power-average approximation, least square method.*

Одержано 31.01.2019

УДК 621.391:519.2
DOI: 10.32626/2308-5916.2019-19.81-87

**А. А. Матійко**

Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського», м. Київ

## ПОРІВНЯЛЬНИЙ АНАЛІЗ АЛГОРИТМІВ ШИФРУВАННЯ NTRUENCRYPT ТА NTRUCIPHER

Асиметрична система шифрування NTRUEncrypt запропонована в 1996 р. та є однією з найшвидших постквантових шифросистем. Вона включена до стандарту ANSI X9.98-2010 та є прототипом широкого класу криптосистем з однойменною назвою, стійкість яких базується на складності знаходження коротких векторів в деяких решітках. Криптографічні властивості шифросистеми NTRUEncrypt достатньо повно досліджені, а її останні модифікації представлено на поточному конкурсі NIST із стандартизації постквантових асиметричних алгоритмів шифрування, інкапсуляції ключів та цифрового підпису.

Однією з актуальних задач у галузі криптології є створення симетричних шифросистем, стійкість яких, аналогічно асиметричним, базується на складності розв'язанні лише однієї конкретної задачі (наприклад, для RSA це — задача факторизації чисел). У зв'язку з цим в 2017 р. на базі NTRUEncrypt запропонована симетрична шифросистема NTRUCipher, для якої проведено попередній аналіз стійкості та запропоновано алгоритм вибору парамет-

© А. А. Матійко, 2019

рів. Поряд з тим, у доведенні CPA-стійкості алгоритму шифрування NTRUCipher містяться суттєві помилки; до того ж залишається не вирішеною задача порівняльного аналізу шифросистем NTRUCipher та NTRUEncrypt за стійкістю та практичністю.

Мета цієї роботи — проведення порівняльного аналізу зазначених шифросистем, а також коректне обґрунтування умов, що забезпечують CPA-стійкість шифросистеми NTRUCipher. Окремим результатом є аналітичні оцінки ймовірності помилкового розшифрування повідомлень для NTRUCipher, що є важливим для належного вибору параметрів шифросистеми при її практичному застосуванні. Показано, що значення ймовірності помилкового розшифрування повідомлень у шифросистемі NTRUCipher змінюється в межах від $2^{-357}$ до $2^{-157}$ водночас як значення цієї ймовірності для шифросистеми NTRUEncrypt змінюється в межах від $2^{-160}$ до $2^{-74}$. Крім того, отримані оцінки не базуються на жодних евристичних припущеннях.

**Ключові слова:** *постквантова криптографія, NTRUEncrypt, NTRUCipher, ймовірність помилкового розшифрування, CPA-стійкість.*

**Вступ.** Однією з актуальних задач у галузі криптології є створення симетричних шифросистем, стійкість яких базується на складності розв'язанні лише однієї конкретної обчислювальної задачі. Прикладом такої шифросистеми є NTRUCipher [1], що являє собою симетричний аналог відомої асиметричної шифросистеми NTRUEncrypt [2]. Попередній аналіз стійкості NTRUCipher, проведений в [1], містить суттєві помилки. Крім того, залишається не вирішеною задача порівняльного аналізу шифросистем NTRUCipher та NTRUEncrypt за стійкістю та практичністю.

**Мета роботи** — проведення порівняльного аналізу зазначених шифросистем, а також коректне обґрунтування умов, що забезпечують CPA-стійкість шифросистеми NTRUCipher. Окремим результатом є аналітичні оцінки ймовірності помилкового розшифрування повідомлень для NTRUCipher, які не базуються на жодних евристичних припущеннях.

**Означення основних понять та загальний опис шифросистем.** Нехай $n$ та $q$ — взаємно прості натуральні числа, $n, q > 3$, $q$ не ділиться на 3. Позначимо $Z_q$ кільце класів лишків за модулем $q$, елементи якого ототожнимо з цілими числами, що належать інтервалу $[-(q-1)/2, (q-1)/2]$ для непарного $q$ та інтервалу $[-q/2, q/2-1]$ для парного $q$. Позначимо $R_{n,q} = Z_q[x]/(x^n - 1)$ — кільце зрізаних поліно-

мів степеня не вище $n$ над кільцем $Z_q$, $R^*_{n,q}$ — множину оборотних елементів кільця $R_{n,q}$.

Нехай $S$ — множина всіх малих поліномів (коефіцієнти яких належать множині $\{-1, 0, 1\}$) степеня не вище $n$, $S_e$ — певна фіксована підмножина множини $S$. Для будь-яких натуральних чисел $d_1, d_2$ позначимо $S_{d_1,d_2}$ — множину всіх малих поліномів степеня не вище $n$, серед коефіцієнтів яких є точно $d_1$, що дорівнюють $1$, та точно $d_2$, що дорівнюють $-1$.

В табл. 1 наведено означення шифросистем NTRUCipher [1] та NTRUEncrypt [2]. Як видно з таблиці, обидві шифросистеми мають схожу будову. При цьому в NTRUCipher використовується тільки секретний ключ, що є у два рази коротше секретного ключа шифросистеми NTRUEncrypt. Отже, основними критеріями, за якими проведено порівняльний аналіз зазначених шифросистем, є:

1) малість ймовірності помилкового розшифрування повідомлень [3, 4];
2) умови стійкості відносно атак на основі підібраних відкритих повідомлень (CPA-стійкості) [5].

Таблиця 1

*Опис шифросистем NTRUEncrypt та NTRUCipher*

| **NTRUEncrypt** | **NTRUCipher** |
|---|---|
| асиметричний алгоритм шифрування | симетричний алгоритм шифрування |
| секретний ключ: $(F, g)$, де $F \in S_{d,d}$ є таким, що $f = 1 + 3F \in R^*_{n,q}$; $g \in S_{d'+1,d}$', де $d' = \lfloor n/3 \rfloor$ | секретний ключ: $F \in S_{d,d}$ є таким, що $f = 1 + 3F \in R^*_{n,q}$ |
| відкритий ключ: $h = 3g / f$ (обчислюється в кільці $R^*_{n,q}$) | — |
| алгоритм зашифровування: $\mathrm{E}_h(m, r) = (m + rh + 3e) \bmod q$, де $m \in S$ — відкритий текст, $r \in S_{d,d}$ та $e \in S_e$ — незалежні випадкові поліноми | алгоритм зашифровування: $\mathrm{E}_h(m, r) = (m + 3r / f + 3e) \bmod q$, де $m \in S$ — відкритий текст, $r \in S_{d,d}$ та $e \in S_e$ — незалежні випадкові поліноми |
| алгоритм розшифровування: $D_f(c) = cf \pmod q \bmod 3$, де $c \in R_{n,q}$ — шифротекст | алгоритм розшифровування: $D_f(c) = cf \pmod q \bmod 3$, де $c \in R_{n,q}$ — шифротекст |

Враховуючи обмеження щодо обсягу статті, доведення отриманих тверджень не наводяться.

**Ймовірність помилкового розшифрування повідомлень.** В роботі [4] для NTRUEncrypt отримано оцінку ймовірності $p_{er}(F,g) = \mathrm{P}_{m,r}\{D_f(E_h(m,r)) \neq m\}$ за умови, що $S_e = \{0\}$, поліноми $F \in S_{d,d}$ і $g \in S_{d'+1,d}$ є фіксованими, а коефіцієнти поліномів $m$, $r$ є незалежними випадковими величинами, розподіленими за законами

$$\mathrm{P}(g_i = 1) = \mathrm{P}(g_i = -1) = d'n^{-1},\ \mathrm{P}(g_i = 0) = 1 - 2d'n^{-1},$$

$$\mathrm{P}(m_i = 1) = \mathrm{P}(m_i = -1) = \mathrm{P}(m_i = 0) = 1/3, \quad (1)$$

$$\mathrm{P}(r_i = 1) = \mathrm{P}(r_i = -1) = dn^{-1},\ \mathrm{P}(r_i = 0) = 1 - 2dn^{-1}; \quad (2)$$

$$p_{er}(F,g) \le 2n \exp\{-\frac{(q-2)^2}{72(2d+2d'+1)}\}. \quad (3)$$

Для шифросистеми NTRUCipher має місце таке твердження.

**Твердження 1.** Нехай $F \in S_{d,d}$, $S_e = \{0\}$, а коефіцієнти поліномів $m$ і $r$ є незалежними випадковими величинами, розподіленими за законами (1) і (2) відповідно. Тоді для ймовірності $p_{er}(F) = \mathrm{P}_{m,r}\{D_f(E_h(m,r)) \neq m\}$ справедлива нерівність

$$p_{er}(F) \le 2n \exp\{-\frac{(q-8)^2}{72(2d+1)}\}. \quad (4)$$

В табл. 2 для низки пар $(n,d)$, перші п'ять з яких рекомендовано в [6], а дві останні — в [3], наведені значення $-\log_2 p_{er}$ для шифросистем NTRUEncrypt та NTRUCipher; при цьому $q = 2048$.

Таблиця 2

*Результати оцінювання параметрів, що характеризують частоту виникнення помилок розшифрування*

| $(n,d)$ | $-\log_2 p_{er}$ (NTRUEncrypt) | $-\log_2 p_{er}$ (NTRUCipher) |
|---|---|---|
| (401, 113) | 160,49 | 357,69 |
| (449, 134) | 138,12 | 300,18 |
| (677, 157) | 99,24 | 254,32 |
| (1087, 120) | 75,84 | 334,92 |
| (1171, 106) | 73,28 | 380,29 |
| (443, 143) | 134,58 | 280,76 |
| (743, 247) | 74,28 | 157,92 |

Як видно з даної таблиці, значення ймовірності помилкового розшифрування повідомлень шифросистеми NTRUCipher на декілька

порядків нижча і змінюється в межах від $2^{-357}$ до $2^{-157}$ водночас, коли значення цієї ймовірності для шифросистеми NTRUEncrypt змінюється в межах від $2^{-160}$ до $2^{-74}$. При $(n,d)=(401,113)$ в обох шифросистемах спостерігається найменша ймовірність виникнення помилок розшифрування повідомлень.

**Умови CPA-стійкості шифросистем.** Нагадаємо відоме означення CPA-стійкості симетричної шифросистеми (див., наприклад, [5]). Розглядається така «гра» між противником і дослідником:

1) дослідник генерує секретний ключ $k$;
2) противник може подавати на вхід оракула $E_k$, що здійснює зашифрування, будь-які відкриті та отримувати відповідні шифровані повідомлення;
3) противник подає дослідникові пару різних повідомлень $m_0$ та $m_1$ однакової довжини;
4) дослідник вибирає випадкове рівноймовірне число $b \in \{0,1\}$ та повертає противнику шифроване повідомлення $c = E_k(m_b)$;
5) противник може звертатися до оракула $E_k$ (як в п. 2)) і повинен відновити значення $b$.

Шифросистема називається $(T,\varepsilon)$-CPA-стійкою, якщо будь-який алгоритм відновлення значення $b$ з імовірністю $\varepsilon > 1/2$ у наведеній «грі» виконує не менше ніж $T$ операцій. CPA-стійкість асиметричних шифросистем визначається аналогічним чином.

Відомі наступні обчислювально складні задачі, пов'язані з NTRU-подібними шифросистемами [7].

**Задача 1 (NTRU Decision Key Craking Problem)** полягає у встановленні закону розподілу випадкового елемента $h$, який з імовірністю $1/2$:

- має рівномірний розподіл на множині $R_{n,q}$ (гіпотеза $H_0$);
- формується за правилом $h = 3r/f$, де $r$ і $f$ є незалежними випадковими елементами з рівно ймовірним розподілом на множинах $S$ і $S_{d,d} \cap R^*_{n,q}$ відповідно (гіпотеза $H_1$).

**Задача 2 (NTRU Search Key Craking Problem)** полягає у тому, щоби для заданої множини $S_e \subseteq S$ та згенерованого випадкового рівноймовірного елемента $h \in R_{n,q}$ встановити закону розподілу випадкового елемента $c$, який з імовірністю $1/2$:

- має рівномірний розподіл на множині $R_{n,q}$ (гіпотеза $H_0$);
- формується за правилом $c = 3(hr + e)$, де $r$ і $e$ є незалежними випадковими елементами з рівноймовірним розподілом на множинах $S$ і $S_e$ відповідно (гіпотеза $H_1$).

Відомо [7], що шифросистема NTRUEncrypt

- є CPA-стійкою лише за умови, що обидві задачі (1 і 2) є обчислювально складними;
- може не бути CPA-стійкою, якщо задача 2 не є обчислювально складною (наприклад, коли $S_e = \{0\}$).

Другим результатом цієї статті є наступне твердження.

**Твердження 2.** Нехай існує CP-атака на NTRUCipher зі складністю $T$ та ймовірністю успіху $\varepsilon > 1/2$. Тоді існує алгоритм розв'язання Задачі 1 зі складністю $T + c$ та ймовірністю успіху $1/2 \cdot (1 + \varepsilon)$, $c = \text{const}$. Іншими словами, шифросистема NTRUCipher є CPA-стійкою за умови високої обчислювальної складності лише задачі 1.

**Висновки.** Симетрична система шифрування NTRUCipher будується подібно до її асиметричного аналога NTRUEncrypt, але використовує секретний ключ, що має вдвічі меншу довжину. Значення ймовірності помилкового розшифрування повідомлень в NTRUCipher є на декілька порядків нижче і змінюється в межах від $2^{-357}$ до $2^{-157}$ водночас, як значення цієї ймовірності для NTRUEncrypt змінюється в межах від $2^{-160}$ до $2^{-74}$. Крім того, шифросистема NTRUCipher є CPA-стійкою за більш слабких умов в порівнянні з NTRUEncrypt. Для забезпечення стійкості першої шифросистеми достатньо лише високої обчислювальної складності задачі 1, в той час як друга шифросистем є стійкою за умови високої складності обох задач 1 і 2 (і може бути не стійкою у протилежному випадку).

**Список використаних джерел:**


1. Valluri M. R. NTRUCipher-lattice based secret key encryption. arXiv: 1710.01928V2. 6/10/2017
2. Hoffstein J., Pipher J., Silverman J.H. NTRU: a new high speed public key cryptosystem. Preprint, presented at the rump session of Crypto'96. 1996.
3. Hirschhorn P., Hoffstein J., Howgrave-Graham N., Whyte W. Choosing NTRU parameters in light of combined lattice reduction and MITM aproaches. Applied Cryptography and Network Security, LNCS. 2009. Vol. 5536. P. 437–455.
4. Олексійчук А. М., Матійко А. А. Оцінки ймовірності помилкового розшифрування повідомлень у шифросистемі NTRUEncrypt при фіксованому ключі. *Захист інформації.* 2018. № 2. С. 89–94.
5. Katz J., Lindell Y. Introduction to modern cryptography. CRC Press, 2015.

6. Chen C., Hoffstein J., Whyte W., Zhang Z. NIST PQ Submission: NTRUEncrypt. A lattice based algorithm. URL: https://cscr.nist.gov/Projects/-Post-Quantum-Cryptorraphy, 2017.
7. Steinfeld R. NTRU cryptosystem: resent developments and emerging mathematical problems in finite polynomial rings. URL: http://users.monach.edu.au/-~rste /NTRU_survey.pdf. 2014.

## THE COMPARATIVE ANALYSIS OF NTRUCIPHER AND NTRUENCRYPT ENCRYPTION SCHEMES

The asymmetric encryption scheme NTRUEncrypt proposed in 1996 and is one of the fastest post-quantum encryption schemes. It is included in the ANSI X9.98-2010 standard and is the prototype of cryptosystems' wide class with the same name, which security is based on the difficulty of finding short vectors in some lattices. The cryptographic properties of NTRUEncrypt encryption scheme are sufficiently explored and its latest modifications are presented at the current NIST competition to standardize post-quantum asymmetric encryption, key encapsulation and digital signature.

One of the most important problem in the field of cryptology is the design of symmetric encryption schemes, whose security, similarly to the asymmetric one, is based on the complexity of solving only one particular problem (for example, for RSA this is the problem of factorization of numbers). Due to this, in 2017 the symmetric encryption scheme NTRUCipher based on NTRUEncrypt was proposed. For it, a preliminary security analysis was performed and a parameter selection algorithm was proposed. At the same time, there are essential errors in the proof of CPA-security of the encryption algorithm NTRUCipher. Moreover, the problem of comparative analysis of NTRUCipher and NTRUEncrypt encryption schemes is not solved for security and practicality.

The purpose of this article is to conduct a comparative analysis of the abovementioned encryption schemes and to prove correctly the conditions that ensure the CPA-security of the NTRUCipher encryption scheme. A certain result is analytical bounds of decryption failure probability in NTRUCipher encryption scheme. This result is important for the proper parameters' choice of the encryption scheme in its practical implementation. It is shown that the decryption failure probability in the NTRUCipher varies from $2^{-357}$ to $2^{-157}$ while the value of this probability for the NTRUEncrypt encryption scheme varies from $2^{-160}$ to $2^{-74}$. In addition, the obtained bounds are not based on any heuristic assumptions.

**Key words:** *post-quantum cryptography, NTRUEncrypt, NTRUCipher, decryption failure probability, CPA-security.*

Одержано 21.01.2019

УДК 621.391:519.2
DOI: 10.32626/2308-5916.2019-19.88-94

**С. В. Мітін**

Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського», м. Київ

# ЗАСТОСУВАННЯ АЛГОРИТМУ BKW ДЛЯ ВІДНОВЛЕННЯ СИСТЕМАТИЧНИХ ЛІНІЙНИХ БЛОКОВИХ КОДІВ ЗА НАБОРАМИ СПОТВОРЕНИХ КОДОВИХ СЛІВ

Важливою практичною задачею у галузі інформаційної безпеки є розробка методів відновлення дискретних відображень, які використовуються в сучасних системах передачі, обробки та зберігання даних, за наборами спотворених значень цих відображень, що отримуються під впливом шумів (випадкових спотворень, навмисних перешкод, внутрішніх збоїв тощо). При розв'язанні цієї задачі додаткові складнощі виникають у разі відсутності повних відомостей про алгоритми, що визначають зазначені відображення, та використовуються для перетворення інформації. Окремим випадком поставленої задачі є відновлення систематичних лінійних блокових кодів з невідомими твірними матрицями за наборами спотворених кодових слів, що спостерігаються на виході двійкового симетричного каналу зв'язку. У даній статті запропоновано метод розв'язання останньої задачі, який базується на застосуванні алгоритму BKW, що використовується при побудові кореляційних атак на потокові шифри. Алгоритм застосовується для розв'язання не однієї, а (одночасно) багатьох систем лінійних рівнянь зі спотвореними правими частинами шляхом одноразового перетворення їх спільної матриці коефіцієнтів. Наведено обґрунтування коректності та отримано оцінку ефективності запропонованого методу. Здійснено його порівняння з раніше відомим методом. Показано, що запропонований метод має більшу ефективність за трудомісткістю та обсягом потрібної пам'яті, хоча й потребує більше спотворених кодових слів, які необхідні для відновлення твірної матриці коду. В залежності від параметрів кодів, що відновлюються, та ймовірності спотворення у каналі зв'язку, виграш у трудомісткості запропонованого методу в порівнянні з раніше відомим складає приблизно від $2^{36}$ до $2^{67}$ разів. Підтверджено також практичну застосовність запропонованого методу для випадків, коли раніше відомий метод є практично не реалізованим.

**Ключові слова:** *інформаційна безпека, вивідування інформації, відновлення дискретних відображень, лінійний блоковий код, система рівнянь зі спотвореними правими частинами, алгоритм BKW.*


© С. В. Мітін, 2019

**Вступ.** Важливою практичною задачею є відновлення невідомого лінійного блокового коду за набором спотворених кодових слів. Ця задача є NP-повною [1], а відомі алгоритми її розв'язання є практично застосовними лише у випадку помірної довжини кодів, що відновлюються, або малої ймовірності спотворень символів у каналі зв'язку [1, 2].

В роботі [3] запропоновано метод вирішення зазначеної задачі для систематичних лінійних блокових кодів з використанням методу максимуму правдоподібності, який за відомих умов характеризується найменшою ймовірністю помилки [4].

**Метою даної статті** є розробка методу, який удосконалює метод роботи [3] і має в порівнянні з ним більш високу ефективність.

**Постановка задачі та основні результати.** Використовуватиме такі позначення: $C$ — невідомий двійковий лінійний $(n, k)$-код з твірною матрицею $G = (I_k, X)$, де $I_k$ — одинична матриця порядку $k$, $X$ — матриця розміру $k \times (n-k)$ над полем з двох елементів.

Нехай $x_j$ $j$-й стовпець матриці $X$. Припустимо, що вага (число ненульових координат) вектора $x_j$ знаходиться в межах від 3 до $\rho$, де $\rho$ — ціле число, $\rho \geq 3$, $j \in \overline{1, n-k}$. Треба відновити матрицю $X$ за набором $m$ незалежних випадкових рівноймовірних слів коду $C$, спотворених у двійковому симетричному каналі (ДСК) зв'язку з імовірністю помилки $p \in (0, 1/2)$.

Поставлену задачу можна формулювати також наступним чином. Розглянемо лінійне відображення $L_C : \{0,1\}^k \to \{0,1\}^n$, що задається кодом $C$ зазначеного вигляду: $L_C(u) = uG$, $u \in \{0,1\}^k$. Спостерігається послідовність, яка складається з $m$ спотворених значень цього відображення:

$$Y_i = U_i G \oplus \eta_i, \ i \in \overline{1, m}, \qquad (1)$$

де $U_i$ — незалежні випадкові рівноймовірні вектори довжини $k$, $\eta_i = (\eta_{i,1}, \ldots, \eta_{i,n})$ — вектори спотворень, координати яких не залежать від $U_1, \ldots, U_m$ та є незалежними в сукупності випадковими величинами, що розподілені за законом

$$\mathbf{P}\{\eta_{i,s} = 1\} = 1 - \mathbf{P}\{\eta_{i,s} = 0\} \leq p \in (0, 1/2),$$

$s \in \overline{1, n}$, $i \in \overline{1, m}$. Треба відновити відображення $L_C$ (тобто матрицю $X$) за відомими значеннями $n, k, p, \rho$ та послідовністю (1).

Метод розв'язання поставленої задачі запропоновано в роботі [3]. Сутність методу полягає у складанні та розв'язанні за допомо-

гою методу максимуму правдоподібності [4] систем лінійних рівнянь (СЛР) із спотвореними правими частинами

$$Ax = b^{(j)} = Ax_j \oplus \xi^{(j)}, \ j \in \overline{1, n-k}, \tag{2}$$

де $A$ — відома реалізація випадкової рівноймовірної двійкової матриці розміру $m \times k$, $\xi^{(j)} = (\xi_{1,j}, \dots, \xi_{m,j})^{\mathrm{T}}$ — випадковий вектор з незалежними координатами, що розподілені за законом

$$\mathbf{P}\{\xi_{i,j} = 1\} = 1 - \mathbf{P}\{\xi_{i,j} = 0\} \le \tilde{p} = 1/2 \cdot (1 - (1-2p)^{\rho+1}), \tag{3}$$

$i \in \overline{1, m}$, $j \in \overline{1, n-k}$. В роботі [3] показано, що для відновлення матриці $X$ з імовірністю не менше $1-\delta$, $\delta \in (0, 1/2)$, потрібно не більше ніж

$$m_1 = \left\lceil 8(1-2\tilde{p})^{-2} \ln\left( (n-k)\delta^{-1} \sum_{i=3}^{\rho} \binom{k}{i} \right) \right\rceil \tag{4}$$

спотворених кодових слів. При цьому трудомісткість методу складає

$$T_1 = O\left( m_1 (n-k)(\rho+1) \sum_{i=3}^{\rho} \binom{k}{i} \right) \tag{5}$$

операцій.

Далі викладено метод відновлення матриці $X$, який удосконалює метод роботи [3] і дозволяє суттєво підвищити його ефективність шляхом одночасного розв'язання усіх СЛР (2) із застосуванням модифікованого алгоритму BKW [5].

Алгоритм реалізації методу (алгоритм **B**) залежить від натуральних параметрів $k_1$, $l$, $t$, де $1 \le k_1 \le k-3$, $m \ge lt$, та допоміжного алгоритму **A** розв'язання задачі про адитивне представлення з параметрами $k-k_1, r, l$. Останній являє собою відомий алгоритм BKW [6] і дозволяє знаходити для довільного списку $L$, що складається з $l$ випадкових незалежних рівноймовірних $(k-k_1)$-вимірних двійкових векторів $z_1, \dots, z_l$ $r$ (не обов'язково різних) номерів $\nu_1, \dots, \nu_r \in \{1, 2, \dots, l\}$ таких, що $z_{\nu_1} + \dots + z_{\nu_r} = 0$.

Алгоритм **B** складається з двох етапів і дозволяє відновлювати перші $k_1$ координат усіх стовпців матриці $X$ з ймовірністю помилки не вище ніж $\delta' = \delta \lceil k/k_1 \rceil^{-1}$. Застосовуючи цей алгоритм $\lceil k/k_1 \rceil$ разів до наборів координат (зазначених стовпців), що попарно не перетинаються, можна відновити матрицю $X$ в цілому з ймовірністю помилки не вище ніж $\delta$.

Для будь-якого $z \in R^k$ позначимо $z'$ та $z''$ підвектори вектора $z$, що складаються з його перших $k_1$ та останніх $k-k_1$ координат

відповідно. Далі, позначимо $A_i$ $i$-й рядок матриці $A$, $b_{ij}$ — $i$-ту координату вектора $b^{(j)}$ та запишемо системи рівнянь (2) у вигляді

$$A'_i x'_j \oplus A''_i x''_j = b_{ij},\ i = \overline{1,m},\ j \in \overline{1,n-k}.$$

**Алгоритм В** має такий вигляд.

1. Розіб'ємо систему рядків $A'_1, \dots, A''_m$ на $t$ списків $L_s$ довжини $l$ кожний та застосуємо для кожного $s \in \overline{1,t}$ алгоритм **А** до списку $L_s$. Якщо хоча б в одному випадку алгоритм **А** завершується неуспішно, то алгоритм **В** припиняє роботу. Інакше отримаємо рівності вигляду $A''_{\nu_1(s)} \oplus \dots \oplus A''_{\nu_r(s)} = 0$, де $A''_{\nu_1(s)}, \dots, A''_{\nu_r(s)} \in L_s$, $s \in \overline{1,t}$.

2. Складемо $n - k$ СЛР із спотвореними правими частинами

$$A'(s)x'_j = b(s,j),\ s \in \overline{1,t},\ j \in \overline{1,n-k}, \qquad (6)$$

де

$$A'(s) = A'_{\nu_1(s)} \oplus \dots \oplus A'_{\nu_r(s)},\ b(s,j) = b_{\nu_1(s),j} \oplus \dots \oplus b_{\nu_r(s),j} =$$
$$= A'(s)x'_j \oplus (\xi_{\nu_1(s),j} \oplus \dots \oplus \xi_{\nu_r(s),j})$$

та розв'яжемо їх методом максимуму правдоподібності.

Усі системи рівнянь (6) мають однакову матрицю коефіцієнтів, яка складається з $t$ рядків $A'(s)$ довжини $k_1$, $s \in \overline{1,t}$. Внаслідок незалежності випадкових величин $\xi_{i,j}$, $i \in \overline{1,m}$, $j \in \overline{1,n-k}$, та формули (3), спотворення у правих частинах рівнянь системи (6) є незалежними випадковими величинами, розподіленими за законом

$$\mathbf{P}\{\xi_{\nu_1(s),j} \oplus \dots \oplus \xi_{\nu_r(s),j} = 0\} =$$
$$= 1 - \mathbf{P}\{\xi_{\nu_1(s),j} \oplus \dots \oplus \xi_{\nu_r(s),j} = 1\} \le 1/2 \cdot (1 - (1-2p)^{(\rho+1)r}), \qquad (7)$$

де $s \in \overline{1,t}$, $j \in \overline{1,n-k}$.

Для обґрунтування коректності та оцінки ефективності запропонованого методу сформулюємо наступну теорему (доведення якої виходить за межі статті).

**Теорема.** Нехай $\delta' \in (0, 1/2)$, $k_1 \in \overline{1,k-3}$ і параметри алгоритму **В** визначаються наступним чином:

$$u = \left\lceil \frac{\log(k-k_1)}{2} \right\rceil,\ v = \left\lceil \frac{2(k-k_1)}{\log(k-k_1)} \right\rceil,\ r = 2^{u-1},$$

$$t = \left\lceil 2(1-2p)^{-2r(\rho+1)} \ln\left( 2(n-k)(\delta')^{-1} \sum_{i=0}^{\rho} \binom{k_1}{i} \right) \right\rceil,$$

$$l = (u + \left\lceil \ln(2t(\delta')^{-1}) \right\rceil - 1)2^v.$$

Алгоритм відновлює перші $k_1$ координат усіх стовпців матриці $X$ з ймовірністю помилки не вище ніж $\delta'$, використовуючи

$$T(k_1) = O\left( ult + (n-k)(\rho+1)t\sum_{i=0}^{\rho}\binom{k_1}{i} \right), \qquad (8)$$

операцій, $m(k_1) = lt$ спотворених кодових слів та $N(k_1) = O(l + t)$ біт пам'яті.

Зауважимо, що, згідно з формулою (8), трудомісткість (при заданій верхній межі ймовірності помилки) алгоритму **В** залежить від допоміжного параметра $k_1 \in \overline{1, k-3}$, який слід вибирати, виходячи з умови $T(k^*) = \min\{T(k_1) : k_1 \in \overline{1, k-3}\}$. Тоді обсяг пам'яті та число спотворених кодових слів, потрібних для виконання алгоритму, складає відповідно $N(k^*) = l(k^*) + t(k^*)$ та $m(k^*) = l(k^*)t(k^*)$.

В таблиці наведені значення (двійкових) логарифмів трудомісткості, обсягу пам'яті та числа спотворених кодових слів, яких достатньо для відновлення матриці $X$ з імовірністю не менше $1 - \delta$ за допомогою запропонованого методу. Значення $t$, $l$ та $m$ отримані з використанням теореми. В останніх двох колонках таблиці наведені значення параметрів (4), (5).

Таблиця

*Чисельні значення параметрів, що характеризують ефективність методів відновлення систематичних лінійних блокових кодів* ($n = 128$, $k = 80$, $\delta = \delta' = 0{,}1$)

| $p$ | $\rho$ | **Запропонований метод** | | | | **Метод роботи [3]** | |
|---|---|---|---|---|---|---|---|
| | | $k^*$ | $\log T(k^*)$ | $\log N(k^*)$ | $\log m(k^*)$ | $\log T_1$ | $m_1$ |
| 0,1000 | 20 | 18 | 88,42 | 59,36 | 85,91 | 94,29 | 4632991 |
| | 30 | 76 | 108,75 | 26,78 | 35,24 | 113,42 | 469177075 |
| | 50 | 76 | 126,99 | 39,73 | 48,69 | 133,03 | 3781005896745 |
| 0,0500 | 20 | 16 | 59,30 | 30,79 | 57,46 | 87,15 | 32920 |
| | 30 | 16 | 71,87 | 42,86 | 69,99 | 102,89 | 316141 |
| | 50 | 16 | 96,79 | 67,18 | 94,88 | 115,69 | 22911318 |
| 0,0300 | 20 | 16 | 48,35 | 26,27 | 46,41 | 84,52 | 5300 |
| | 30 | 16 | 55,88 | 27,99 | 53,89 | 99,00 | 21330 |
| | 50 | 16 | 70,72 | 41,58 | 68,68 | 109,29 | 271485 |
| 0,0100 | 20 | 16 | 37,76 | 25,58 | 35,65 | 81,99 | 921 |
| | 30 | 16 | 40,42 | 25,81 | 38,20 | 95,27 | 1611 |
| | 50 | 16 | 45,54 | 26,09 | 43,15 | 103,16 | 3871 |
| 0,0010 | 20 | 16 | 33,09 | 25,17 | 30,84 | 80,89 | 429 |
| | 30 | 16 | 33,64 | 25,32 | 31,23 | 93,64 | 521 |
| | 50 | 16 | 34,45 | 25,32 | 31,67 | 100,48 | 605 |
| 0,0001 | 20 | 14 | 32,63 | 25,32 | 30,49 | 80,78 | 398 |
| | 30 | 14 | 32,73 | 25,32 | 30,53 | 93,48 | 466 |
| | 50 | 14 | 32,95 | 25,32 | 30,64 | 100,22 | 504 |

**Висновки.** Отримані результати показують, що виграш у трудомісткості запропонованого методу в порівнянні з раніше відомим [3] складає приблизно від $2^{36}$ до $2^{67}$ разів в залежності від параметрів кодів, що відновлюються, та ймовірності спотворення у ДСК. Для забезпечення потрібної надійності відновлення кодів запропонований метод потребує більше спотворених слів у порівнянні з методом [3], але характеризується суттєво меншою трудомісткістю.

В окремих (визначених) випадках запропонований метод виявляється практично застосовним, водночас як раніше відомий метод є практично не реалізованим.

**Список використаних джерел:**


1. Valembios A. Detection and recognition of a binary linear code. Discrete Applied Mathematics. 2001. Vol. 111 (1-2). P. 199–218.
2. Cluzeau M., Finiasz M. Recovering a code's length and synchronization from a noisy intercepted bitstream. IEEE Conference ISIT'09. *Proc. IEEE Press.* 2009. P. 2737–2731.
3. Алексейчук А. Н., Грязнухин А. Ю. Метод восстановления систематических линейных кодов по наборам искаженных кодовых слов. *Прикладная радиоэлектроника*. 2013. Т. 12. № 2. С. 313–318.
4. Балакин Г. В. Введение в теорию случайных систем уравнений. *Труды по дискретной математике.* М. : ТВП. 1997. Т. 1. С. 1–18.
5. Zhang B., Xu C., Meier W. Fast correlation attacks over extension fields, large-unit linear approximation and cryptanalysis of SNOW 2.0. Cryptology ePrint Archive, Report 2016/311. URL: http://eprint.iacr.org/2016/311.
6. Blum A., Kalai A., Wasserman H. Noise-tolerant learning, the parity problem, and the statistical query model. J. ACM. 2003. Vol. 50, N 3. P. 506–519.


## APPLICATION OF BKW ALGORITHM FOR RECOVERING SYSTEMATIC LINEAR BLOCK CODES FROM SAMPLES OF NOISY CODEWORDS


The important practical problem in the information security sphere is the development of methods for recovering discrete mappings, which are used in modern systems for transmitting, processing and storing data, from samples of noisy values of these mappings caused by noise impact (random distortion, deliberate interference, internal faults, etc.). In solving this problem additional difficulties arise in the absence of complete information about the algorithms, which define these mappings and used to transform information. A special case of the problem is systematic linear block codes recovering with unknown generating matrix from samples of corrupted codewords observed at the output of a binary symmetric channel. In this paper, the problem-solving method, which based on the BKW algorithm application, which is used for building the correlation attack on streams ciphers, is suggested. The algorithm is applied for solving not one but (simultaneously) many systems of linear equations with noised right-hand sides by single transformation of their co-coefficients matrix. The justification for the correctness is given and

an estimation of the proposed method efficiency is obtained. Its comparison with the previously known method is made. It is shown that the proposed method has greater efficiency in terms of the complexity and volume of necessary memory, although it requires more noised codewords that are necessary for code generating matrix recovering. Depending on recovered codes parameters and the probabilities of distortion in the communication channel, benefits in terms of the complexity of the proposed method in comparison with the previously known is from $2^{36}$ up $2^{67}$ once. The practical applicability of the proposed method for cases, where the previously known method is practically not realizable, is confirmed.

**Key words:** *information security, deducing of information, discrete mappings recovering, linear block code, system of liner equations with noised right-hand sides, BKW algorithm.*

Одержано 21.01.2019

УДК 004.383.3:004.9.347
DOI: 10.32626/2308-5916.2019-19.94-100

**Л. М. Николайчук*,** канд. юрид. наук,
**А. Р. Воронич*,** канд. техн. наук,
**Т. О. Заведюк**,** канд. техн. наук

* Івано-Франківський національний
технічний університет нафти і газу м. Івано-Франківськ,
** Надвірнянський коледж Національного
транспортного університету м. Надвірна

## МЕТОДИ НЕЙРОПРОЦЕСОРНОГО ОПРАЦЮВАННЯ СИГНАЛІВ ТА КОМУНІКАЦІЙНИХ ВЗАЄМОДІЙ У СЕРЕДОВИЩІ СУБ'ЄКТІВ ПРАВА

Обгрунтована концепція адекватності моделей нейропроцесорного опрацювання сигналів та комунікаційних взаємодій в інформаційному середовищі суб'єктів права. Показано взаємозв'язок понять ймовірнісної та суб'єктивної ентропії в теорії інформації та юриспруденції. Запропоновані моделі імпульсно-квадратичного перетворення гармонічних сигналів на вході формального нейрона, модель аксона нейрона, рекурентного корелляційного нейрона та інформаційної нейромоделі суб'єкта права.

**Ключові слова**: *нейропроцесори, компоненти біологічних нейронів, ймовірнісна та суб'єктивна ентропія, моделі компонентів нейрона та суб'єктів права.*

**Вступ.** Широкомасштабне застосування ІТ-технологій та комп'ютеризованих систем керування є одним з істотних факторів соціально-економічного і технологічного розвитку. Комп'ютеризовані та хмарні

 © Л. М. Николайчук, А. Р. Воронич, Т. О. Заведюк, 2019

технології комунікаційної взаємодії суб'єктів права вже стали одним з найважливіших факторів, що інтенсивно впливають на розвиток науки та вдосконалення функцій інформаційного суспільства. Становлення, розвиток та цілеспрямоване вдосконалення в Україні функцій інформаційного суспільства [1] неможливе без широкого використання у всіх сферах комунікацій суб'єктів права нових ефективних інформаційних технологій, підвищення ролі інформаційних ресурсів, електронних даних, динамічного розвитку застосування мережі Інтернет та доступу до інформаційних ресурсів користувачів [2], особливо при виконанні ними обов'язків, які ідентифікують їх як суб'єктів права. Успішне рішення цієї проблеми може бути ефективно здійснене шляхом вдосконалення методів нейропроцесорного опрацювання сигналів [3] їх комунікаційних взаємодій та криптозахисту у середовищі суб'єктів права [4]. Крім того доцільно має бути обгрунтована концепція адекватності моделей нейропроцесорного опрацювання сигналів [4, 5] та комунікаційних взаємодій в інформаційному середовищі суб'єктів права, а також взаємозв'язок понять ймовірнісної та суб'єктивної ентропії у теорії інформації та юриспруденції [6].

**Аналіз останніх публікацій.** Сучасне суспільство стає інформаційним зростає роль інформації, інформаційних технологій і комп'ютерних знань, збільшується частка товарів у вигляді інформаційних продуктів та послуг, формується глобальний світовий інформаційний простір. Особливо це стосується ролі інформаційних суспільних відносин з урахуванням моделей ймовірнісної і суб'єктивної ентропії [6], стрімкого розвитку інформаційних технологій збору, формування, передавання, опрацювання, перетворення, криптозахисту та зберігання інформаційних даних у сучасному суспільстві [1, 2].

Відомі моделі формальних нейронів запропоновані в роботах Маккалоком–Пітсом, Хопфілда, Гросберга, моделі нейрона в дискретному часі [7], модель вейвлет-фаззі-нейрон Ванга–Менделя, модель прямої передачі сигналу Поморової О.В., модель Такагі–Сугено–Канга, адаптивні нейрон-фазі системи з W-нейронами [7], модель нейрона Девідсона–Сміта, модель динамічного рекурентного нейрона Николайчука–Заведюк [8]. Серед таких моделей найбільш адаптованою до опрацювання гармонічних сигналів на які найбільш адекватно реагують рецептори нейронів біологічних систем є модель динамічного рекурентного нейрона Николайчука–Заведюк [3]. Окремі розробки компонентів нейропроцесорів стосуються побудови моделі аксона нейрона [9].

Для успішної реалізації методів опрацювання сигналів на основі нейропроцесорів необхідна розробка теоретичних засад методів опрацювання сигналів а також оптимізації алгоритмів та структурних рішень компонентів нейропроцесорів.

**Характеристики реакції рецепторів біологічних нейронів та моделі порогових характеристик формальних нейронів.** На рис. 1

показано модель формування сигналів рецепторами нейронів, які найкраще реагують на сигнали $A\sin x$ та $A\sin^2 x$ [10].

На рис. 1 цифрами позначені частоти нервових імпульсів (імп/с) п'яти рецепторів, розміщених вздовж основної мембрани.

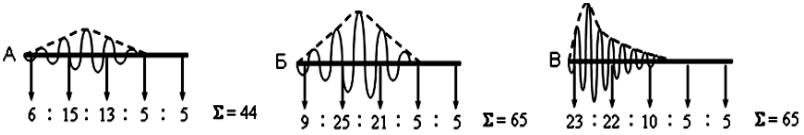



***Рис. 1.*** *Схема формування амплітудно-модульованих сигналів певної частоти на виході рецепторів*

Звуки А і Б будуть сприйматись, як одинакові по частоті, але різні по гучності, звуки Б і В — як однаково гучні, але різні по частоті, а звуки А і В — як різні і по частоті і по гучності.

Закономірності перетворення енергії різних подразників у серію нервових імпульсів різними типами нейронів показані на рис. 2 [10].


***Рис. 2.*** *Реакція різних первинних нейронів на тривалісний зовнішній подразник*

Відомі порогові сигмоїдні (*S*-подібні) вихідні сигнали формальних нейронів показані на рис. 3, які описуються наступним рівнянням:

$$y_j = \psi\left(u_j\right) = \psi\left(\sum_{i=0}^{n} G_{ji} x_i\right) \sum_{i=0}^{n} G_{ji} \qquad (1)$$

де $x_i$ ($i$ = 0, 1, 2,...,$n$) — вхідні напруги; $u_j$ — вхідна напруга $j$-го підсилювача; $y_j$ — вихідна напруга j-го нейрона; $\psi(\cdot)$ — сигмоїдна активаційна функція підсилювача; $G_{ji} = R_{ji}^{-1}$ — провідність резистора, який з'єднує $i$-й з $j$-м підсилювачем; $I_{ji}$ — струм, який тече через резистор $R_{ji}$ (від $i$-го до $j$-го нейрона).


***Рис. 3.*** *Типові функції нелінійності, які використовують у моделях штучних нейронів*

**Метод квадратично-імпульсного перетворення гармонічних сигналів на вході формального нейрона.** В основу запропонованого методу покладене квадратично-імпульсне перетворення гармонічного сигналу, яке забезпечує формування потоку імпульсів з адаптованим до особливих точок кроком дискретизації (рис. 4) згідно патенту України №100263 [11].

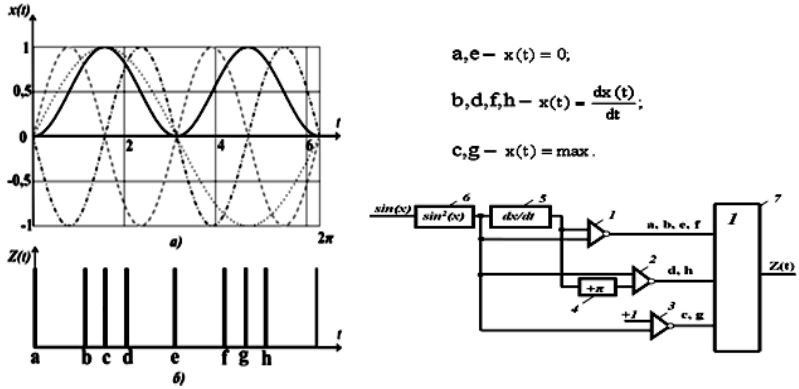



***Рис. 4.*** *Реалізація методу квадратично-імпульсного порогового перетворення гармонічного сигналу та структурна схема пристрою*

Структурна схема пристрою, який реалізує метод квадратично-імпульсного перетворення містить наступні компоненти: 1, 2 і 3 — імпульсні компаратори, 4 — фазоповертач на кут π, 5 — схема диференціювання, 6 — схема піднесення вхідного сигналу до квадрату, 7 — логічний елемент АБО.

Отриманий результат показує, що в нейронних структурах гармонічний синусоїдальний сигнал на вході нейрона трансформується у квадратичний простір, що відповідає оцінці та реакції нейрона на потужність вхідного сигналу $0 \le \sin^2 x \le +1$. Це добре узгоджується з макромоделями біонейронних структур, де показано, що сигнали $\sin^2 x$ є енергетично оптимальними імпульсами активації нейронів [10].

У результаті виконання перетворень згідно послідовності функціоналів $F_1$, $F_2$,… на інтервалі кожного періоду вхідного гармонічного сигналу на виході формується біт-орієнтований вектор його еталонної моделі наступного виду:

11100100111001001110010011100100111001001110010011100100…

Даний вектор характеризується особливими кореляційними властивостями, які аналогічні М-послідовностям та кодам Баркера.

В роботі [8] запропонована модель динамічного рекурентного нейрона, яка показана на рис. 5.

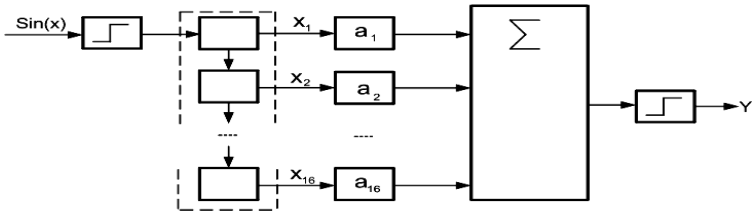



***Рис. 5.*** *Структура динамічного рекурентного нейрона опрацювання гармонічного сигналу*

В роботі [9] запропоновано реалізацію моделі аксона нейрона на основі мікро- та нанотехнологій. Структура мікроелектронної реалізації моделі аксона нейрона показана на рис. 6.

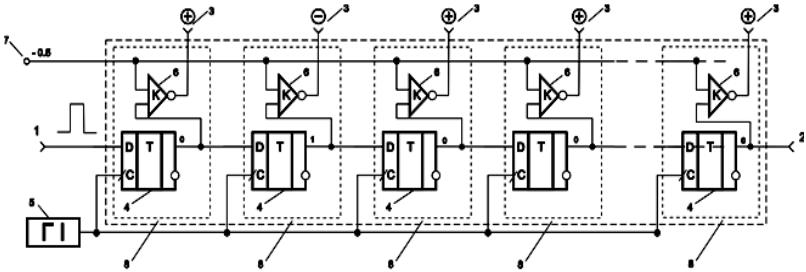



***Рис. 6.*** *Структура мікроелектронної моделі аксона нейрона на дискретних мікроелементах*

Запропонований пристрій містить: 1 — вхід, 2 — вихід; 3 — сигнальні виходи; 4 — D-тригери; 5 — генератор імпульсів; 6 — імпульсний компаратор; 7 — від'ємний потенціал; 8 — компоненти.

Інформаційна нейромодель оператора комп'ютеризованої системи (суб'єкта права) запропонована В. Касьяновим в роботі [6], яка показана на рис. 7.

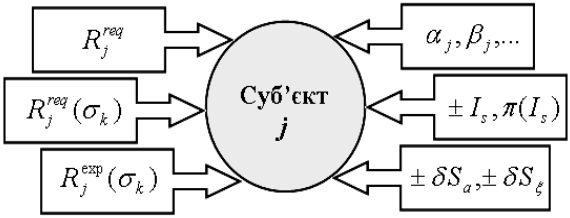



***Рис. 7.*** *Інформаційна нейромодель оператора комп'ютеризованої системи* (*суб'єкта права*)

Недоліком такої інформаційної моделі суб'єкта є обмежені функціональні можливості, які обумовлені відсутністю вихідних інформаційних комунікаційних зв'язків суб'єкта з зовнішнім інформацій-

ним середовищем, відсутністю внутрішніх інтелектуальних впливів на формування реакції суб'єкта.

В роботі [12] Николайчук Л. М. запропонована інформаційна нейромодель суб'єкта права, яка характеризується розширеними функціональними можливостями порогової нейровзаємодії з інформаційними потоками зовнішнього середовища, яка представлена на рис. 8.

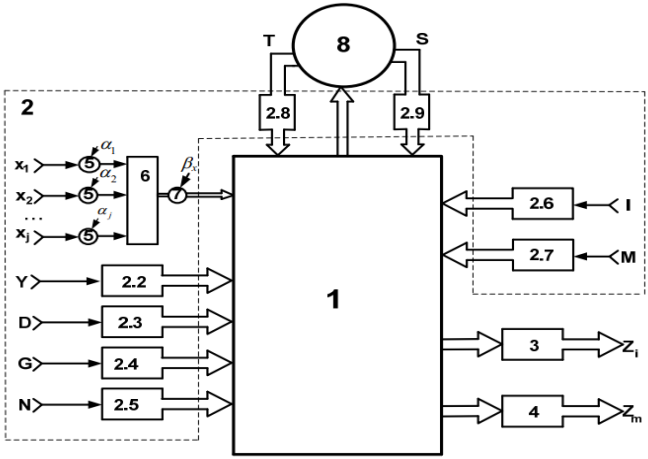



***Рис. 8.*** *Інформаційна нейромодель суб'єкта права*

**Висновки.** Виконані дослідження теоретичних засад та структурних рішень опрацювання сигналів на основі спецпроцесорів з нейрокомпонентами. Показаний взаємозв'язок цифрового опрацювання інформаційних потоків у комп'ютерних системах компонентами яких є біологічні об'єкти — суб'єкти права, які реалізують принципи опрацювання даних на основі оцінок ймовірнісної і суб'єктивної ентропії. Запропонований метод квадратично-імпульсного перетворення гармонічних сигналів на вході динамічного рекурентного нейрона. Розроблені моделі аксона нейрона та інформаційна нейромодель суб'єкта права. Виконані дослідження створюють передумови розвитку теорії нейропроцесорного опрацювання сигналів та її ефективного застосування для вирішення широкого класу прикладних задач оптимізації обчислень та формалізації комунікаційних взаємодій суб'єктів у процесі розвитку комп'ютеризованих систем та хмарних технологій в сучасному інформаційному суспільстві.

## Список використаних джерел:

1. Сергієнко І. В. Інформатика в Україні: становлення, розвиток, проблеми. НАН України. Ін-т кібернетики ім. В. М. Глушкова. Київ : Наук. думка, 1999. 354 с.

2. Палагин А. В., Яковлев Ю. С. Системная интеграция средств компьютерной техники : монографія. Вінниця : УНИВЕРСУМ, 2005. 680 с.
3. Заведюк Т. О. Методи опрацювання гармонічних сигналів на основі спец процесорів з негроподібними компонентами. *Вісник національного університету «Львівська політехніка». Комп'ютерні науки та інформаційні технології.* Львів. 2013. № 751. С. 18–28.
4. Николайчук Л. М. Дослідження впливу відео-, аудіо-, алфавітно- цифрової та іншої інформації на суспільно-комунікаційну поведінку суб'єктів права. *Оптико-електронні інформаційно-енергетичні технології.* 2015. № 1 (29). С. 51–55.
5. Nykolaychuk L. Generelization of information models classes and communication interaction of he subjects of law of information society. The Experience of Designing and Application of CAD System in Microelectronics. *Proceedings of XIIIth International Conference.* CADSM'2015. Lviv-Poljana, Ukraine, 2015. P.143–146.
6. Касьянов В. О. Суб'єктивний аналіз : монографія. Київ : НАУ, 2007. 381 с.
7. Кононюк А. Ю. Нейронні мережі і генетичні алгоритми. Київ : Корнійчук, 2008. 446 с.
8. Николайчук Я. М., Заведюк Т. О. Патент № 82444 Модель нейрона. Бюл. № 15. 2013.
9. Николайчук Я. М., Заведюк Т.О.. Патент № 70662 Модель аксона нейрона. Бюл. № 12, 2012.
10. Джерард Р. Концепция информации и биологические системы. Москва, 1966. 336 с.
11. Николайчук Я. М., Заведюк Т. О. Патент на винахід № 100263, Україна, МПК H03K5/153. Пристрій формування імпульсів. Опубл. 10.12.2012. Бюл. № 23.
12. Николайчук Л. М. Патент № 117659 Інформаційна нейромодель суб'єкта права. Бюл. № 13. 2017.

## METHODS OF NEYROPROCESSOR SURVEY OF SIGNALS AND COMMUNICATION RELATIONS IN THE ENVIRONMENT OF SUBJECTS OF LAW

The concept of adequacy of models of neuroprocessor processing of signals and communication interactions in the information environment of subjects of law is substantiated. The relationship between the concepts of probabilistic and subjective entropy in the theory of information and jurisprudence is shown. Models of pulse-quadratic transformation of harmonic signals at the entrance of the formal neuron, neon axon model, recurrent correlation neuron and informative neuromodel of the subject are proposed.

**Key words:** *neuroprocessors, components of biological neurons, probabilistic and subjective entropy, models of components of the neuron and subjects of law.*

Одержано 14.02.2019

УДК 681.32
DOI: 10.32626/2308-5916.2019-19.101-107

**Я. М. Николайчук*,** д-р техн. наук,
**Н. Я. Возна*,** канд. техн. наук,
**В. М. Грига**,** канд. техн. наук,
**Б. Б. Круліковський***,** канд. техн. наук,
**А. Я. Давлетова*,** асистент

*Тернопільський національний
економічний університет м. Тернопіль,
**Прикарпатський національний університет
імені В. Стефаника м. Івано-Франківськ,
***Національний університет водного господарства
та природокористування м. Рівне

# ВИСОКОПРОДУКТИВНІ МАТРИЧНІ ТА ПОТОКОВІ ПЕРЕМНОЖУВАЧІ ЦИФРОВИХ ДАНИХ

Запропоновані алгоритми та структури високопродуктивних матрично-потокових перемножувачів багаторозрядних двійкових чисел, в яких застосовні компоненти з мінімаксними характеристиками часової, апаратної та структурної складності. Розроблений алгоритм матричного виконання операцій множення згідно структури перемножувача Брауна, який реалізує виконання операції додавання в однорозрядному повному двійковому суматорі та формування переносів за мінімально досяжний інтервал часу — один мікротакт. Розроблений алгоритм та структура потокового матричного перемножувача з високим рівнем розпаралелення обчислювальних операцій, в якому процеси завантаження кодів перемножуваних двійкових чисел відбуваються паралельно з процесами матричного перемноження та зчитування результатів множення у попередньому циклі. У порівнянні з відомими структурами потокові перемножувачі дозволяють суттєво зменшити число входів/виходів мікроелектронних кристалів, які реалізують операції перемноження багаторозрядних двійкових чисел.

**Ключові слова**: *матрично-потокові перемножувачі, парафазна структура Брауна, максимальна швидкодія, розпаралелення обчислювальних операцій.*

**Вступ.** Перемножувачі двійкових чисел є важливими компонентами арифметико-логічних пристроїв універсальних та спеціалізованих процесорів. При значній розрядності множників 32-512 біт такі перемножувачі застосовуються в універсальних комп'ютерах як швидкодіючі співпроцесори [1–4]. У сучасній обчислювальній техніці найширше

© Я. М. Николайчук, Н. Я. Возна, В. М. Грига,
Б. Б. Круліковський, А. Я. Давлетова, 2019

застосування отримали матричні перемножувачі з паралельним вводом та виводом даних, що суттєво знижує ефективність їх використання як потокові перемножувачі, які є базовими компонентами мультиядерних та систолічних процесорів [2]. Особливо негативно цей недолік проявляється при опрацюванні багаторозрядних двійкових кодів (1024÷4096 біт) процесорами шифрування даних [4]. Крім того є практично недоцільним реалізація чіпів перемножувачів з вказаним числом виводів. Перспективним напрямком вирішення цієї проблеми є створення потокових перемножувачів з високим рівнем розпаралелення обчислювальних операцій та біт-орієнтованою організацією вводу та виводу даних.

**Дослідження структури та системних характеристик матричних перемножувачів.** В матричних перемножувачах сумування здійснюється матрицею суматорів, які складаються із послідовних рядків однорозрядних суматорів із збереженням переносу. Найбільш відомими матричними перемножувачами є перемножувач Брауна з горизонтальним та вертикальним розповсюдженням переносу [1–3]. Перемножувачі, які побудовані за алгоритмами Бо-Вулі та Пезариса [1] для множення двійкових чисел в доповнюючих кодах та інші.

На рис. 1 показано матричний перемножувач для 4-ох розрядних двійкових чисел, в якому кожному стовпцю у матриці множення відповідає діагональ перемножувача. Схема відома, як перемножувач Брауна [1] або перемножувач з горизонтальним розповсюдженням переносу. Біти часткових добутків виду ( $a_i b_j$ ) формуються за допомогою елементів «І». Для сумування часткових добутків застосовуються два види однорозрядних суматорів із збереженням переносу: напівсуматори (НС) і повні суматори (СМ).

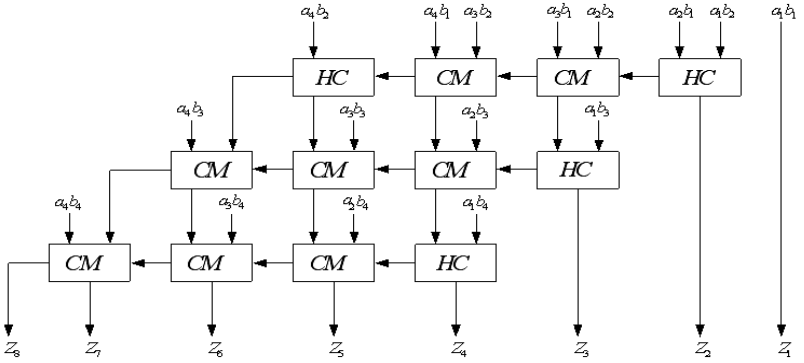



***Рис. 1.*** *Структура матричного перемножувача Брауна 4x4 з горизонтальним розповсюдженням переносу*

Матричний перемножувач Брауна ( $n \times n$ ) складається з $n^2$ операцій логічного добутку та ( $n^2 - n$ ) — операцій однорозрядного

двійкового сумування. Для повного двійкового сумування потрібно ($n^2 - 2n$) операцій, а для не повного сумування $n$ операцій, де $n$ — розрядність вхідних даних.

Для реалізації напівсуматора, який виконує операцію не повного двійкового сумування потрібно 5 логічних елементів (рис. 2, а) а для повного суматора, який виконує операцію повного двійкового сумування потрібно 11 логічних елементів (рис. 2, б).

Час розповсюдження вихідного переносу неповного суматора складає 1 мікротакт а повного 5 мікротактів, а час формування суми складає 3 мікротакти для неповного суматора і 6 мікротактів для повного суматора.

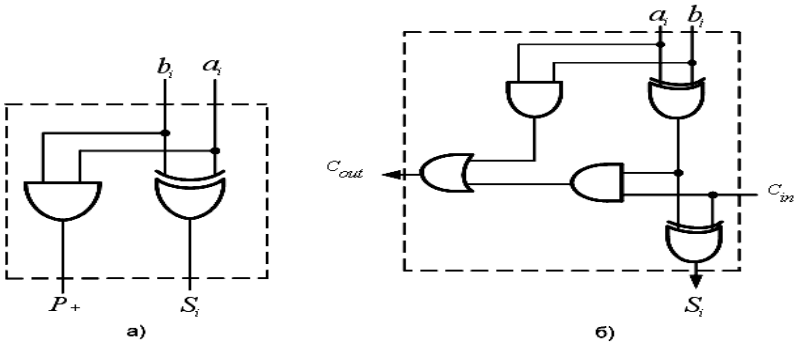



***Рис. 2.*** *Внутрішня структура однорозрядного суматора: а — неповного; б — повного на елементах виключне АБО*

Матричний перемножувач Брауна характеризується наступними системними характеристиками:

- швидкодія структури перемножувача визначається найбільш довгим маршрутом розповсюдження сигналу, що складає $(3n-4)$ однорозрядних суматора, і розраховується згідно виразу $\tau_{МП} = 2\tau_{НС} + (3n-6)\times\tau_{ПС}$, де $\tau_{НС}$, $\tau_{ПС}$ — відповідно часова складність (затримка сигналів) у структурі однофазного неповного та повного однорозрядного двійкового суматора;
- апаратна складність перемножувача визначається сумарною кількістю логічних елементів та вентилів у його структурі і розраховується згідно виразу: $A_{МП} = n\times A_{НС} + (n^2 - 2n)\times A_{ПС}$, де $A_{НС}$, $A_{ПС}$ — відповідно апаратна складність повного та неповного одорозрядного двійкового суматора;
- структурна складність перемножувача визначається зваженою сумою структурної складності його компонентів згідно виразу:

$S_{МП} = \sum_{i=1}^{m} \alpha_i S_i$, де $\alpha_i$ — онтологічна оцінка структурної складності $S_i$-го компонента, $m$ — кількість структурно-класифікованих компонентів [5].

Оцінка часової складності матричного перемножувача (рис. 1) розраховується з урахуванням горизонтальних затримок сигналів наскрізних переносів та вертикальних затримок сигналів при формуванні бітів суми. Тобто системні характеристики часової складності відомих однорозрядних двійкових суматорів (рис. 2) з горизонтальними (+) і вертикальними ( $s$ ) інформаційними зв'язками відповідно складають:

$$\tau_{МП} = 2\tau_{НС} + (3n-6)\times\tau_{ПС} =$$
$$= 2\times 3 + (3\times 4 - 6)\times 6 = 6 + (12-6)\times 6 = 42\nu.$$

Оцінка апаратної складності матричного перемножувача (рис. 1) розраховується з урахуванням кількості логічних елементів, які містять однорозрядні двійкові суматори (рис. 2) і становить:

$$A_{МП} = n\times A_{НС} + (n^2 - 2n)\times A_{ПС} = 4\times 5 + (4^2 - 2\times 4)\times 11 =$$
$$= 20 + (16-8)\times 11 = 108\,(\textit{вентилів}).$$

Оцінка структурної складності матричного перемножувача (рис. 1) становить $S_{МП} = 1026$ одиниць.

Недоліком матричного перемножувача Брауна є обмежені функціональні можливості та низька швидкодія, яка обумовлена тим, що базовий компонент матриці однорозрядних суматорів не містить парафазних входів та виходів, що потребує не менше $2 \div 3$ мікротакти часової затримки сигналів переносів і не дозволяє, у принципі, реалізувати відповідні вертикальні та горизонтальні переноси між виходами та входами однорозрядних суматорів з часовою затримкою 1 мікротакт.

Запропонована структура потокового матричного перемножувача багаторозрядних двійкових чисел на основі парафазних однорозрядних суматорів, яка показана на рис. 3.

В даній структурі потокового матричного перемножувача додатково введено матрицю однорозрядних повних суматорів з парафазними входами та виходами, що дозволило реалізувати інформаційні переноси між суматорами з гранично мінімальною затримкою сигналів на 1 мікротакт, а крім того підвищити регулярність структури матриці суматорів, що спрощує проектування та нарощення розрядності утилітів таких багаторозрядних пристроїв на реконфігурованих програмних кристалах ПЛІС.

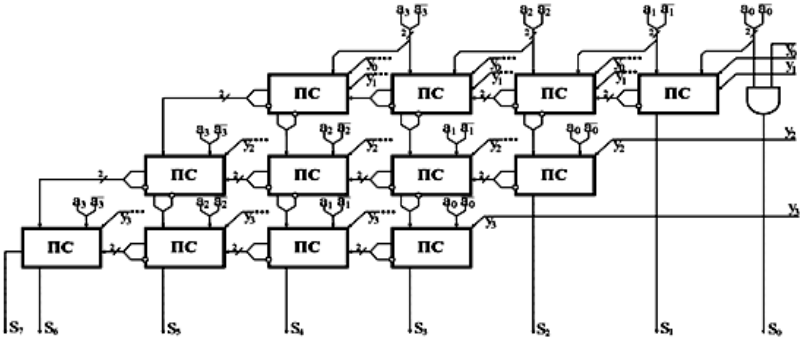



***Рис. 3.*** *Структура потокового матричного перемножувача на основі однорозрядних суматорів з парафазними входами і виходами*

**Розробка структури та компонентів потокового перемножувача багаторозрядних двійкових чисел.** На рис. 4 подано структуру потокового перемножувача двійкових чисел. Перемножувач містить: вхідний регістр зсуву (R1), регістри пам'яті (R2, R3), матрицю одно розрядних двійкових суматорів (МС), вихідний регістр пам'яті та зсуву (R4), та логічний елемент "Виключаюче АБО" (ЛЕ).

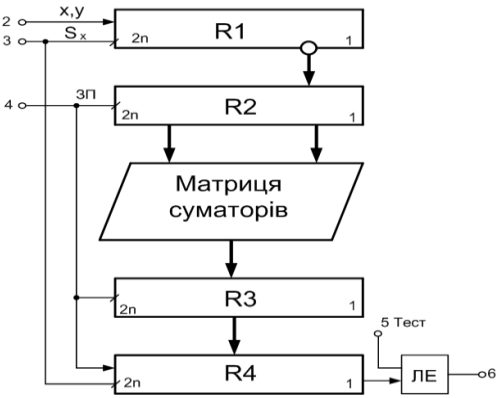



***Рис. 4.*** *Структура потокового перемножувача двійкових чисел*

На даному рисунку: вхід 2 — біт-орієнтований ввід кодів множників *x, y*; вхід 3 — тактова синхронізація зсувів R1 та R4; вхід 4 — запис даних у регістри R2-R4; вхід 5 — біт-орієнтований вхід тестового коду; вихід 6 — вихід біт-орієнтованого двійкового коду добутку x на *y*.

В потоковому перемножувачі регістр R1 виконує операцію перетворення *n*-розрядних біт-орієнтованих кодів множників *x* та y у паралельний пара фазний 2*n*-розрядний двійковий код. Часова складність Ттгр = 2 мікротакти, тобто занесення кодів (*x, y*) в регістр R1 здійсню-

ється за 4*n* мікротактів. Регістр R2 призначений для зберігання кодів множників на часовий інтервал занесення вхідних кодів (*x*, *y*) у регістр зсуву R1. Матриця однорозрядних повних парафазних суматорів МС виконує операцію перемноження кодів (*x*, *y*) на виході якої формується 2*n*-розрядний вихідний код добутку на інтервалі часу *k x* 2*n*, де *k* — затримка сигналів формування наскрізних переносів та суми на виходах суматорів. Регістр R3 зберігає код добутку до кінця інтервалу зчитування прямих кодів добутків до завершення біт-орієнтованого зчитування добутків на виході перемножувача. Логічний елемент виключаюче АБО призначений для реалізації операції тестування безпомилковості роботи перемножувача. З метою контролю надійності роботи перемножувача на початку певного числа циклів здійснюється тестування правильності його роботи шляхом порівняння добутку заданих перемножувачів (*x*, *y*) з тестовим кодом добутку, який поступає на вхід 5 перемножувача. При цьому на виході 6 логічного елемента виключаюче АБО формується 2*n* — розрядний потік нулів, яка свідчить про безпомилковість виконання операції множення. На початку кожного циклу перемноження сигналом входу 4 здійснюється запис пара фазних кодів регістра R1 у регістр R2 та прямих кодів добутків регістра R3 у регістр R4. У наступному циклі роботи перемножувача сигналами синхронізації S*x* входу 3 тактується занесення біт-орієнтованих кодів множників *x* та *y* в регістр R1. Одночасно цими сигналами тактується зчитування біт-орієнтованих кодів добутків на виході 6 пристрою. Одночасно з виконанням операцій вводу та виводу даних у матричній структурі суматорів МС здійснюється перемноження двійкових кодів *x* та *y* за 1 мікротакт. Регістри зсуву побудовані на основі D-тригерів.

**Висновки.** Виконано аналіз структурних схем матричних перемножувачів Брауна, потоково матричних та потокових перемножувачів, досліджені системні характеристики часової, апаратної та структурної складності матричного перемножувача Брауна з горизонтальним розповсюдженням переносів на основі однорозрядних неповних та повних суматорів з однофазними входами та виходами. Відмічена принципова неможливість підвищення граничної швидкодії такого класу перемножувачів при застосуванні в матриці перемножувача однофазних суматорів. Відомі перемножувачі характеризуються також низькою потоковою швидкодією оскільки введення поточних кодів перемножувачів здійснюється тільки після завершення попереднього циклу перемноження. Запропонована нова структура потокового перемножувача з високим рівнем розпаралелення операцій шляхом паралельного вводу, зчитування та перемноження цифрових даних. При цьому суттєво зростає інформаційна активність компонентів перемножувача на 1–2 порядки у порівнянні з відомими структурами.

**Список використаних джерел:**

1. Цилькер Б. Я., Орлов С. А. Организация ЭВМ и систем : учебник для вузов. Питер, 2006. 668 с.
2. Мельник А. О. Архітектура комп'ютера. Луцьк : Волинська обласна друкарня, 2008. 470 с.
3. Самофалов К. Г., Романкевич А. М., Валуйский В. Н., Каневский Ю. С., Пиневич М. М. Прикладная теория цифровых автоматов. Киев : Вища шк. Головное изд-во, 1987. 375 с.
4. Valeriy Zadiraka, Yaroslav Nykolaichuk. Methods of effective protection of information flows. Ternopil : Terno-graf, 2014. 308 p.
5. Николайчук Я. М., Возна Н. Я., Пітух І. Р. Проектування спеціалізованих комп'ютерних систем : навчальний посібник. Тернопіль : ТзОВ «Терно-граф», 2010. 302 с.

## HIGH-PERFORMANCE MATRIX AND STREAM MULTIPLIERS OF DIGITAL DATA

The algorithms and structures of high-performance matrix-stream multipliers of multi-bit binary numbers are proposed, in which components are used with minimal characteristics of time, hardware and structural complexity. The algorithm of matrix execution of multiplication operations according to the structure of the Brown multiplier is developed, which implements the addition operation in a one-bit full binary adder and the formation of transfers at a minimum reachable time interval — one micro-cycle. The algorithm and structure of the current matrix switch with a high level of deployment of computational operations are developed, in the process of loading codes of transitive binary numbers occurs in parallel with procedural matrix recount and coincidence of results. Compared to known structures, stream multipliers can significantly reduce the number of in/out of microelectronic crystals that implement operations for multiplying multi-bit binary numbers.

**Key words:** *matrix-flow multipliers, paraphase structure of Brown, maximum performance, parallelization of computational operations.*

Одержано 31.01.2019

УДК 004.71:621.39.002.5
DOI: 10.32626/2308-5916.2019-19.108-113

**М. І. Огурцов,** науковий співробітник
Інститут кібернетики імені В. М. Глушкова НАН України, м. Київ

# РОЗРОБКА ПРОТОКОЛУ ЗАХИЩЕНОГО ОБМІНУ ДАНИМИ ДЛЯ СПЕЦІАЛЬНИХ МЕРЕЖ

Через стрімке зростання масштабу, складності задач і розширення сфер практичних застосувань мереж спеціального призначення необхідна розробка нових протоколів роботи таких мереж, які б мали високу адаптивність до умов застосування, а також включали надійні засоби захисту інформації. Метою досліджень стала розробка протоколу, алгоритму, математичного апарату і відповідного програмного забезпечення для спеціальних мереж з використанням синхронної і асинхронної передачі зашифрованих пакетів даних. Для шифрування після проведеного аналізу існуючих алгоритмів обраний для використання симетричний алгоритм AES. На основі отриманих результатів проведеного аналізу розроблено алгоритми криптографічного захисту інформації, яка циркулює у таких мережах. Розроблений і апробований новий протокол захищеного обміну даними для мереж спеціального призначення з урахуванням особливостей спеціальних мереж, що відповідають міжнародним стандартам, зокрема, у складних ситуаціях. Розроблені протокол та алгоритми дозволяють виконувати захист інформаційних потоків для децентралізованих чарункових та ad hoc мереж у польових умовах. Розроблене програмно-алгоритмічне забезпечення апробоване шляхом створення модельних зразків мереж спеціального призначення та проведення тестування мережевої взаємодії їх вузлів. Проведені натурні експерименти з апробації розробленого програмно-алгоритмічного забезпечення в лабораторних умовах підтвердили його застосовність і працездатність та довели потенційну можливість його впровадження. Проведене тестування на практиці показало, що затримки шифрування для реалізації розробленого протоколу склали декілька десятків мс, що дозволяє без проблем передавати сигнали, текст, службові команди, відео, зображення та звук. Застосування розробленого протоколу дозволить підвищити надійність, захищеність та керованість спеціальних мереж у польових умовах.

**Ключові слова**: *спеціальні мережі, захист інформації, безпровідні мережі, криптографія, AES.*

**Вступ.** Завдяки швидкому зростанню масштабу та рівня складності задач і розширення сфер практичних застосувань мереж спеціального призначення підвищується актуальність питання захищеної передачі


© М. І. Огурцов, 2019

даних у таких мережах. Зокрема, велику актуальність набувають питання створення і практичної реалізації алгоритмів захищеної передачі даних та їх маршрутизації для спеціальних мереж, призначених для функціонування, наприклад, систем керування рухомими технічними об'єктами з мультимедійною інформацією і передачею кодованих команд у зашифрованому виді. Існуючі стандарти для безпровідних мереж, що функціонують за вимогою, і мобільні пристрої, доступні на ринку, не передбачають роботу в умовах використання засобів радіоелектронної боротьби, високого рівня активних завад та хакерських атак [1–3]. Крім того, вони не відповідають міжнародним стандартам.

Якщо при побудові спеціальної мережі не використовувати засоби захисту інформації, то потік даних, що циркулює у мережі, буде доступний будь-кому, хто має відповідні технічні засоби [4]. Зважаючи на можливі обмеження обчислювальних потужностей, необхідно дослідити варіанти застосування стандартних симетричних та/або асиметричних схем шифрування для та схем розповсюдження ключів [5–8]. Але на даний момент у більшості випадків засоби захисту інформації у спеціальних мережах не застосовуються [9]. А в тій незначній частині, де вони використовуються, звичайно застосовують лише стандартні засоби захисту інформації від виробника обладнання, що було використане для побудови спеціальних мереж. В поточних умовах такий підхід є неприйнятим, тому розробка загального протоколу захищеного обміну даними для спеціальних мереж є актуальною науковою задачею.

**Мета досліджень** це розробка протоколу, математичного апарату і відповідного програмного забезпечення захищеного безпровідного зв'язку у спеціальній мережі з використанням синхронної і асинхронної передачі зашифрованих пакетів даних та кодованих команд. Актуальність цих досліджень обумовлюється розширенням спектру завдань при застосуванні спеціальних мереж, зокрема роботизованих систем спеціального призначення, що керуються через безпровідні мережі, та важливістю інформації, яка циркулює всередині таких мереж.

**Передача зашифрованих повідомлень.** Практична реалізація розроблених протоколу та алгоритмів для їх апробації виконувалась на базі платформи Arduino з використанням радіоканалу на xBee пристроях зв'язку для підтвердження правильних результатів шифрування/розшифрування. Для шифрування після проведеного аналізу існуючих алгоритмів обраний для використання симетричний алгоритм AES [3, 7, 8, 10] — на основі бібліотек AESLib та Mark Tillotson's AES Library [11, 12] як таких, що успішно пройшли дослідження тестування правильності їх реалізації, проведене на основі [13].

Першим кроком для виконання поставленої задачі стала розробка алгоритму та практичної реалізації для двобічної передачі зашифрованих повідомлень.

**Алгоритм та програмна реалізація шифрування в chain-mode.** Наступним кроком стало застосування шифрування в режимі chain-mode. При застосуванні цього режиму однакові пакети, що шифруються послідовно один за одним, будуть на виході видавати різний шифртекст. Використання цього режиму дозволить значно підвищити рівень захисту даних, що передаватимуться в мережах спеціального призначення.

Для надійного захисту інформації, що шифрується алгоритмом AES в режимі chain-mode, слід використовувати випадковим чином згенерований вектор ініціалізації IV. Найбільш ефективним є використання апаратно згенерованого випадкового вектора ініціалізації [3, 8].

Проведений аналіз показав, що найнадійнішим буде використання такого **розробленого алгоритму**:

- генерація частково-випадкового вектора IV на першому вузлі мережі;
- шифрування вектора IV довготерміновим ключем;
- передача зашифрованого вектора IV іншим вузлам мережі;
- розшифрування вектора IV та використання AES на його основі в режимі chain-mode.

У випадку слідування цьому алгоритму навіть якщо ключ шифрування буде скомпрометовано, без знання початкового вектора зловмиснику неможливо буде розшифрувати отримані повідомлення.

Розроблена програма генерації випадкового вектора зчитує шумові сигнали з непідключених контактів Arduino плати та використовує ці випадкові значення для ініціалізації вектора IV.

**Протокол захищеного обміну даними в спеціальній мережі.** На основі отриманих результатів розроблений новий протокол захищеного обміну даними в спеціальних мережах [4, 5].

На першому етапі роботи виконується ініціалізація мережі. Кожен вузол мережі зберігає однаковий довготерміновий ключ, що використовується лише на етапі ініціалізації. При цьому на кожному вузлі таблиця маршрутизації будується незалежно. Пакет даних містить:

- 128 біт зашифрованих даних;
- 8 бітів адреса;
- додаткові службові дані (за необхідності).

Розглянемо послідовність роботи розробленого протоколу.

1. Для кожного іншого вузла окремо, на основі фізичних випадкових даних генерується початковий вектор IV.
2. Вектор IV шифрується довготерміновим ключем, послідовно передається відповідному вузлу (з підтвердженням отримання), з яким встановлюється інформаційний зв'язок.
3. Після успішної передачі вектор IV зберігається обома вузлами у таблиці маршрутизації для відповідного вузла.

4. В подальшому цей вектор починає використовуватись для передачі даних між ними з підтвердженням отримання кожного пакету. Тобто для кожної пари вузлів використовується індивідуальний вектор IV.
5. Кроки 1–4 повторюються, поки не визначено, з якими вузлами з множини усіх вузлів мережі є прямий зв'язок.
6. За необхідності передати дані визначається, чи є прямий зв'язок з отримувачем, чи потрібна ретрансляція.
7. Якщо прямого зв'язку немає — відбувається спроба встановити зв'язок через ретрансляцію, використовуючи вузли, що перебувають на прямому зв'язку.
8. Якщо вузол отримав пакет, призначений не для нього — він розшифровує пакет, визначає по власній таблиці маршрутизації, як і відправник, куди слати цей пакет — і повторює процедуру, починаючи з кроку 6.
9. Якщо в мережі з'явився новий вузол, інформаційний обмін з яким попередньо не виконувався, слід повторити такі ж дії, що і в пункті 1.

**Висновки.** В результаті проведених наукових досліджень розроблено алгоритми криптографічного захисту інформації, яка циркулює у спеціальних мережах. Створено і апробовано протокол захисту даних при їх передачі для мереж спеціального призначення з урахуванням особливостей таких мереж, зокрема, в ускладнених ситуаціях, що відповідає міжнародним стандартам (ДСТУ ISO/IEC 15946-3, ДСТУ ISO/IEC 11770-3, ДСТУ ISO/IEC 18033-3:2015 та ін.). В результаті проведених натурних експериментів визначено, що при його застосуванні жодні дані не циркулюють у мережі у незашифрованому вигляді.

Розроблені протокол та алгоритми дозволяють виконувати захист інформаційних потоків для децентралізованих чарункових та ad hoc мереж у польових умовах. Виконано всебічну верифікацію імплементації розроблених алгоритмів, що підтвердила їх відповідність відповідним стандартам.

Створене програмно-алгоритмічне забезпечення апробовано шляхом створення модельних зразків мереж спеціального призначення та проведення тестування мережевої взаємодії їх вузлів. Проведені натурні експерименти з апробації розробленого програмно-алгоритмічного забезпечення у лабораторних умовах підтвердили його застосовність і працездатність та довели потенційну можливість його впровадження. Проведене тестування на практиці показало, що затримки шифрування для реалізації розробленого протоколу склали декілька десятків мс, що дозволяє без проблем передавати сигнали, текст, службові команди, відео, зображення та звук.

Досягнуті результати дозволяють, при збільшенні розмірів, потужності, вологозахищеності та інших параметрів розроблених до-

слідних зразків вузлів спеціальної мережі, необхідних для ефективного їх використання, застосовувати їх (та відповідне розроблене програмне забезпечення) у незмінному вигляду у спеціальних застосуваннях. Це надасть можливість підвищити надійність, захищеність та керованість спеціальних мереж у польових умовах.

**Перспективами подальших досліджень** в напрямі створення засобів захищеної передачі даних у мережах спеціального призначення є створення прототипу захищеної системи дистанційного спеціального зв'язку з резервними каналами: Wi-Max базова станція і бортовий Wi-Max/WiFi модем та резервні захищені мережі GPRS/GSM.

**Список використаних джерел:**


1. Домарев В. В., Хорошко В. А., Чекатков А. А. Методы и средства защиты информации. Киев : Юниор, 2003. 504 с.
2. Безопасность информационных технологий. Методология создания систем защиты. Киев : ООО «ТИД ДС», 2001. 688 с.
3. Фергюсон Н., Шнайер Б. Практическая криптография ; пер. с англ. М. : Издательский дом «Вильямс», 2005. 424 с.
4. Огурцов М. И. Разработка протокола защищенного обмена данными для сетей специального назначения. *Міжнародна науково-практична конференція «Проблеми кібербезпеки інформаційно-телекомунікаційних систем»* (PCSITS), 5–6 квітня 2018, м. Київ, С. 166–169.
5. Огурцов М. І. Розробка протоколу захищеного обміну даними для спеціальних мереж. *Системний аналіз та інформаційні технології: матеріали 20-ї Міжнародної науково-технічної конференції SAIT 2018*, Київ, 21–24 травня 2018 р. Київ : ННК «ІПСА», НТУУ «КПІ», 2018. С. 249–251.
6. Kahn D. The Codebreakers. The Story of Secret Writing. New York : Charles Scribner's Sons, 1967. 473 p.
7. Schneier B. Applied cryptography: protocols, algorithms, and source code in C. John Wiley&Sons, 2007. 816 p.
8. Венбо Мао. Современная криптография. Теория и практика. М. : Вильямс, 2005. 768 с.
9. Корольов В. Ю, Поліновський В. В., Огурцов М. І. Моделювання мереж зв'язку рухомих дистанційно керованих систем на базі HLA. *Вісник Хмельницького національного університету.* Технічні науки. 2017. № 1 (245). С. 160–165.
10. FIPS, PUB. «197, Advanced Encryption Standard (AES), National Institute of Standards and Technology, US Department of Commerce, November 2001». URL: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.
11. Arduino Library for AES Encryption (source based on avr-crypto-lib) URL: https://github.com/ DavyLandman/AESLib.
12. Mark Tillotson's AES Library. URL: http://utter.chaos.org.uk:/~markt/AES-library.zip.
13. Lawrence E. Bassham III The Advanced Encryption Standard Algorithm Validation Suite (AESAVS). URL: http://csrc.nist.gov/groups/STM/cavp/-documents/ aes/AESAVS.pdf.

## SECURE DATA EXCHANGE PROTOCOL DEVELOPMENT FOR SPECIAL NETWORKS

Due to the rapid growth of special purpose networks scale, tasks complexity and the practical applications areas expansion, it is necessary to develop new protocols for such networks. Their operation should have high adaptability to the usage conditions and also should include reliable information security means and algorithms. The research purpose was to develop a protocol, algorithm, mathematical apparatus and related software for special networks using synchronous and asynchronous encrypted data packets transmission and coded commands. For encryption, after existing algorithms analysis completion, the AES symmetric algorithm was chosen. On the basis of the conducted analysis results, a new protocol for secure data exchange in special purpose networks was developed and tested taking into account special networks features, including operations in difficult situations that meet Ukrainian and international standards. Cryptographic protection algorithms for information, circulating in such networks, were developed. The developed algorithms allow to protect the information flows for decentralized cellular and ad hoc networks in the field conditions. The developed software and algorithmic support were tested by creating physical special purpose networks models and conducting network interaction testing of their nodes. Conducted practical experiments for the developed software-algorithmic approbation in laboratory conditions confirmed its applicability and efficiency and proved the potential possibility of its implementation. The conducted testing showed that the encryption adds delays due to the developed protocol implementation is up to several tens of ms, which allows comfortable transmission of signals, text, commands, video, images and sound. The developed protocol application will increase the special networks reliability, security and control in the field.

**Key words**: *specialized networks, information security, wireless networks, cryptography, AES.*

Одержано 22.01.2019

УДК 621.391:519.2
DOI: 10.32626/2308-5916.2019-19.114-119

**А. М. Олексійчук,** д-р техн. наук,
**С. М. Конюшок,** канд. техн. наук,
**М. В. Поремський,** аспірант

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського», м. Київ

# ОБҐРУНТУВАННЯ СТІЙКОСТІ ПОТОКОВОГО ШИФРУ «СТРУМОК» ВІДНОСНО КОРЕЛЯЦІЙНИХ АТАК НАД СКІНЧЕННИМИ ПОЛЯМИ ХАРАКТЕРИСТИКИ 2

Потоковий шифр SNOW 2.0 запропонований у 2002 р. як альтернатива попередньої (більш слабкої) версії — SNOW. На сьогодні цей шифр є стандартизованим та являє собою один з найбільш швидких програмно орієнтованих потокових шифрів.

Найбільш потужними з відомих атак на SNOW 2.0 є кореляційні атаки, сутність яких полягає у складанні та розв'язанні систем лінійних рівнянь із спотвореними правими частинами, зокрема, систем рівнянь над полями порядку більшого ніж 2. Не дивлячись на певний прогрес у цьому напрямі, залишаються не вирішеними задачі, пов'язані з розробкою методів оцінювання та обґрунтування стійкості SNOW 2.0-подібних потокових шифрів відносно кореляційних атак. На сьогодні відсутні методи, які дозволяють обґрунтовувати стійкість зазначених шифрів відносно відомих кореляційних атак безпосередньо за параметрами їх компонент. Крім того, спроба застосувати відомі методи оцінювання стійкості SNOW 2.0 відносно кореляційних атак до інших потокових шифрів (наприклад, шифру «Струмок», який запропоновано в ролі кандидата на національний стандарт шифрування України) наштовхується на труднощі, пов'язані з розміром задач, які треба розв'язувати для отримання оцінок. На відміну від SNOW 2.0, побудованого над полем порядку $2^{32}$, шифр «Струмок» задається над полем порядку $2^{64}$, що призводить до неможливості практичного застосування відомих певних алгоритмів, часова складність яких збільшується від $2^{32} \div 2^{37}$ до $2^{64}$ двійкових операцій.

Мета даної роботи — обґрунтування стійкості шифру «Струмок» відносно широкого класу кореляційних атак, який охоплює, зокрема, відомі атаки на SNOW 2.0. Основним результатом є теорема, яка встановлює аналітичну оцінку параметра, що характеризує ефективність кореляційних атак на SNOW 2.0-подібні шифри у термінах їх компонент. Це дозволяє на практи-


© А. М. Олексійчук, С. М. Конюшок, М. В. Поремський, 2019

ці оцінювати та обґрунтовувати стійкість таких шифрів відносно кореляційних атак над полями характеристики 2.

**Ключові слова:** *потоковий шифр, кореляційний криптоаналіз, система лінійних рівнянь зі спотвореними правими частинами, обґрунтування стійкості, «Струмок».*

**Вступ.** Нагадаємо означення класу SNOW 2.0-подібних потокових шифрів [1, 2], до яких відноситься шифр «Струмок» [3].

Позначимо $V_r$ множину двійкових векторів довжини $r \geq 2$. Задамо на цій множині структуру поля порядку $2^r$, узгоджену з операцією $\oplus$ покоординатного булевого додавання двійкових векторів. Ототожнимо також звичайним чином елементи множини $V_r$ з $r$-розрядними цілими числами та позначимо символом $+$ операцію додавання цих чисел за модулем $2^r$.

За означенням [2] вхідними даними для побудови генератора гами $r$-розрядного SNOW 2.0-подібного потокового шифру є примітивний многочлен $g(z) = z^n \oplus c_{n-1}z^{n-1} \oplus \ldots \oplus c_0$ над полем $F_{2^r}$, підстановка $\sigma : V_r \to V_r$ та натуральне число $\mu \in \overline{1, n-2}$. Генератор гами являє собою скінченний автономний автомат з множиною станів $V_r{}^n \times V_r{}^2$, функцією переходів

$$h((x_{n-1}, x_{n-2}, \ldots, x_0), u, v) = ((x_n, x_{n-1}, \ldots, x_1), x_\mu + v, \sigma(u)),$$

та функцією виходів

$$f((x_{n-1}, x_{n-2}, \ldots, x_0), u, v) = x_0 \oplus (x_{n-1} + u) \oplus v,$$

де $x_0, \ldots, x_{n-1}, u, v \in V_r$, $x_n = c_{n-1}x_{n-1} \oplus \ldots \oplus c_0 x_0$. Отже, знак гами в $i$-му такті визначається за початковим станом $((x_{n-1}, x_{n-2}, \ldots, x_0), u_0, v_0)$ генератора за допомогою рекурентних співвідношень $\gamma_i = x_i \oplus (x_{i+n-1} + u_i) \oplus v_i$, $u_{i+1} = x_{i+\mu} + v_i$, $v_{i+1} = \sigma(u_i)$, справедливих для усіх $i = 0, 1, \ldots$.

Надалі вважатимемо, що $r = pt$, де $p, t \in \mathbf{N}$, $p, t \geq 2$, і підстановка $\sigma$ має такий вигляд:

$$\sigma(z_1, \ldots, z_p) = (s_1(z_1), \ldots, s_p(z_p))D, \ (z_1, \ldots, z_p) \in F_{2^t}^p, \qquad (1)$$

де $s_i$ — підстановка (вузол заміни) на множині $V_t$, яка ототожнюється з адитивною групою поля $F_{2^t}$, $i \in \overline{1, p}$, $D$ — оборотна матриця порядку $p$ над полем $F_{2^t}$.

Зауважимо, що у шифрі «Струмок» використовуються такі параметри [3]: $t = 8$, $p = 8$ ($r = 64$), $n = 16$, $\mu = 13$. Підстановка $\sigma$

має вигляд (1), де вузли заміни та матриця $D$ задаються так само, як у блоковому шифрі «Калина» [4].

**Постановка задачі й отримані результати.** Найбільш потужними з відомих сьогодні атак на SNOW 2.0 є кореляційні атаки [5–8], спрямовані на відновлення початкового стану лінійного регістру зсуву (ЛРЗ), що входить до складу генератора, за шифрувальною гамою. В роботі [9] описано загальну схему побудови таких атак на довільні SNOW 2.0-подібні шифри і показано, що усі вони базуються на складанні та розв'язанні певних наслідків системи лінійних рівнянь із спотвореними правими частинами

$$\gamma_i \oplus \gamma_{i+1} = x_i \oplus x_{i+1} \oplus x_{i+\mu} \oplus x_{i+n-1} \oplus x_{i+n} \oplus \xi_i, \; i = 0, 1, \ldots, \qquad (2)$$

де

$$\xi_i = ((x_{i+n-1} + u_i) \oplus x_{i+n-1} \oplus \sigma(u_i)) \oplus ((x_{i+n} + x_{i+\mu} + v_i) \oplus \\ \oplus (x_{i+n} \oplus x_{i+\mu} \oplus v_i)), \; i = 0, 1, \ldots, \qquad (3)$$

причому знаки $x_i$, $x_{i+1}$, $x_{i+\mu}$, $x_{i+n-1}$, $x_{i+n}$ лінійної рекуренти у формулі (2) є відомими лінійними функціями початкового стану ЛРЗ, а змінні $x_{i+\mu}$, $x_{i+n-1}$, $x_{i+n}$, $u_i$, $v_i$ у формулі (3) є незалежними випадковими величинами з рівномірним розподілом на множині $V_r$.

Відповідно до [9] будь-яка кореляційна атака на шифр визначається додатним дільником $r'$ числа $r$ та ненульовим елементом $c$ поля $F_{2^r}$ і полягає у складанні та розв'язанні певної системи рівнянь від $l = nr''$ невідомих, де $r'r'' = r$, із спотвореними правими частинами над полем $F_{2^{r'}}$, причому закон розподілу спотворень $\eta_i$ у правих частинах рівнянь має такий вигляд:

$$\mathbf{P}\{\eta_i = z\} \;\; = \sum_{x \in F_{2^r}:\; \mathrm{Tr}_{2^{r'}}^{2^r}(cx) = z} \mathbf{P}\{\xi_i = x\}, \; z \in F_{2^{r'}}, \qquad (4)$$

$i = 0, 1, \ldots$, де $\mathrm{Tr}_{2^{r'}}^{2^r}(\cdot)$ позначає функцію сліду поля $F_{2^r}$ в полі $F_{2^{r'}}$.

Для оцінювання середньої трудомісткості атаки і обсягу матеріалу (кількості знаків гами), потрібного для її успішної реалізації, можна використовувати наступний алгоритм [8].

**Алгоритм 1.**

**Вхідні дані:**

- натуральні числа $n$, $p$, $t$;
- число $k \geq 2$, що є степенем двійки;
- верхня оцінка $\Delta_{r'}(k)$ параметра

$$\Delta_{c,r'}(k) = 2^{-r'} \sum_{z \in F_{2^{r'}}} (2^{r'} \mathbf{P}\{\eta_1 \oplus \cdots \oplus \eta_k = z\} - 1)^2, \qquad (5)$$

де $\eta_1,...,\eta_k$ є незалежними випадковими величинами, розподіленими за законом (4).

1. Покласти $r'' = pt(r')^{-1}$, $l = nr''$, $\theta = 1 + \log k$.
2. Для кожного $l' \in \overline{1, l-1}$ обчислити

$$m_{r'}(k) = 2(\Delta_{r'}(k))^{-1} l' r' \ln 2,$$

$$T_{r'}(k,l') = (m_{r'}(k))^{\frac{1}{\theta}} k 2^{\frac{r'(l-l')}{\theta}} + r'(m_{r'}(k) + r' l' 2^{r' l'}) + 2^{r'(l'+1)}.$$

3. Обрати $l^* \in \overline{1, l-1}$ таке, що $T_{r'}(k,l^*) = \min\{T_{r'}(k,l') : l' \in \overline{1, l-1}\}$.

**Результат:**

- число $l^*$ фрагментів (довжини $r'$ бітів кожний) початкового стану ЛРЗ, які відновлюються за допомогою атаки;
- нижня оцінка середньої часової складності атаки $T_{r'}(k,l^*)$;
- нижня оцінка обсягу матеріалу

$$N_{r'}(k,l^*) = k 2^{\frac{r'(l-l^*)}{\theta}} (2 l^* r' \ln 2)^{\frac{1}{\theta}} (\Delta_{r'}(k))^{-\frac{1}{\theta}},$$

- потрібного для успішної реалізації атаки.

Для того, щоб алгоритм 1 можна було використовувати на практиці, треба вміти оцінювати значення параметра (5) за числом $r'$, елементом $c \in F_{2^{r'}} \setminus \{0\}$ та компонентами шифру (матрицею $D$ і вузлами заміни $s_i$, $i \in \overline{1, p}$; див. формулу (1)). Отже, постає задача отримання аналітичних верхніх оцінок параметра (5) безпосередньо за компонентами алгоритму шифрування та параметрами кореляційної атаки.

Розв'язок цієї задачі містить наступна теорема (доведення якої виходить за межі статті).

**Теорема.** За умов, зазначених вище, справедлива нерівність

$$\Delta_{c,r'}(k) \le (2^{r'} - 1)\left(n_{\max}\right)^{2k\left\lceil \frac{B(D^T)}{2} \right\rceil}, \qquad (6)$$

де

$$n_{\max} = \max\{n_{a,b}(s_i) : (a,b) \in V_t \times V_t \setminus \{(0,0)\}, i \in \overline{0, p-1}\}, \qquad (7)$$

$$B(D^T) = \min\{wt(z) + wt(zD^T) : z \in F_{2^t}{}^p \setminus \{0\}\}, \qquad (8)$$

і для будь-яких $a, b \in V_t$, $i \in \overline{0, p-1}$:

$$n_{a,b}(s_i) = \max\{|A^{(i)}_{a,b}(0,0)| + |A^{(i)}_{a,b}(0,1)|, |A^{(i)}_{a,b}(1,0)| + |A^{(i)}_{a,b}(1,1)|\},$$

$$A^{(i)}_{a,b}(u,u') = 2^{-2t} \sum_{\substack{x_i, y_i \in V_t: \\ \mathrm{msb}(x_i + y_i + u) = u'}} (-1)^{(x_i^t + y_i^t + u)a \oplus x_i a \oplus s_i(y_i) b}, \; u, u' \in \{0,1\},$$

де $msb(x_i + y_i + u)$ є найстарший розряд суми цілих чисел, що відповідають зазначеним двійковим векторам довжини $t$, $\overset{t}{x_i} + \overset{t}{y_i} + u$ позначає суму цих чисел за модулем $2^t$.

Використовуючи теорему і алгоритм 1, отримаємо оцінки ефективності кореляційних атак над полем $F_{256}$ на шифр «Струмок» (таблиця). Відзначимо, що в цьому випадку $t = 8$, $p = 8$, $n = 16$, $B(D^T) = p + 1 = 9$, і як показує пряме обчислення, значення параметра (7) дорівнює $n_{\max} = 3 \cdot 2^{-4}$.

Таблиця

*Результати виконання алгоритму 1 для шифру «Струмок»* ($r' = 8$)

| $k$ | $l^*$ | $\log_2 T_{r'}(k, l^*)$ | $\log_2 N_{r'}(k, l^*)$ |
|---|---|---|---|
| 2 | 44 | 363,91 | 361,62 |
| 4 | 34 | 285,42 | 285,06 |
| 8 | 29 | 249,40 | 249,38 |
| 16 | 1 | 384,88 | 283,58 |

**Висновки.** Результати обчислень, наведені в таблиці свідчать про те, що будь-яка із зазначених кореляційних атак на «Струмок» має середню часову складність не менше ніж $2^{249,40}$ та потребує не менше ніж $2^{249,38}$ знаків гами. Це свідчить про практичну стійкість зазначеного шифру за умови, що довжина відрізку гами, яка виробляється при будь-якому фіксованому ключі, не перевищує (наприклад) $2^{80}$.

**Список використаних джерел:**


1. Ekdahl P., Johansson T. A new version of the stream cipher SNOW. *Selected Areas in Cryptography — SAC*. 2002. LNCS 2295. Springer-Verlag. P. 47–61.
2. Олексійчук А. М. Достатня умова стійкості SNOW 2.0-подібних потокових шифрів відносно певних атак зі зв'язаними ключами. *Захист інформації*. 2016. Т. 18. № 3. С. 261–268.
3. Gorbenko I., Kuznetsov A., Gorbenko Yu., Alekseychuk A., Timchenko V. Strumok Keystream Generator. *The 9th IEEE International Conference on Dependable Systems, Services and Technologies*, DESSERT'2018, 24–27 May, 2018. Kyiv, Ukraine. P. 292–299.
4. Oliynykov R. V., Gorbenko I. D., Kazymyrov O. V. [et. al]. A New Encryption Standard of Ukraine: The Kalyna Block Cipher. *Cryptology ePrint Archive*. URL: http://eprint.iacr.org/ 2015/650.
5. Nyberg K., Wallen J. Improved linear distinguishers for SNOW 2.0. *Fast Software Encryption* — FSE 2006. LNCS 4047. Springer-Verlag. P. 144–162.
6. Maximov A., Johansson Th. Fast computation for large distribution and and its cryptographic application. *Advanced in Cryptology*. ASIACRYPT 2005. — LNCS 3788. Springer-Verlag. P. 313–332.

7. Lee J.-K., Lee D. H., Park S. Cryptanalysis of SOSEMANUC and SNOW 2.0 using linear masks. *Advanced in Cryptology.* ASIACRYPT 2008. LNCS 5350. Springer-Verlag. P. 524–538.
8. Zhang B., Xu C., Meier W. Fast correlation attacks over extension fields, large-unit linear approximation and cryptanalysis of SNOW 2.0. *Cryptology ePrint Archive*. URL: http://eprint.iacr.org/2016/311.
9. Олексійчук А. М., Поремський М. В. Загальна схема побудови кореляційних атак на SNOW 2.0-подібні потокові шифри. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. Вип. 1 (35). 2018. С. 70–79.

## SECURITY JUSTIFICATION FOR STRUMOK STREAM CIPHER AGAINST CORRELATION ATTACKS OVER FINITE FIELDS OF CHARACTERISTIC 2

The stream cipher SNOW 2.0 was proposed in 2002 as an alternative to the previous (weaker) version — SNOW. This cipher is standardized today and is one of the fastest program-oriented stream ciphers.

The most powerful known attacks on SNOW 2.0 are correlation attacks, the essence of which is to form and solve systems of noised linear equations, in particular, over finite fields of order greater than 2. Despite some progress in this direction, remain unresolved problems related to the development of methods for evaluation and justification the security of SNOW 2.0-like stream ciphers against correlation attacks. To date, there are no methods that can justify the security of these ciphers against known correlation attacks directly from the parameters of their components. In addition, an attempt to apply known methods for evaluating the security of SNOW 2.0 against correlation attacks to some other stream ciphers (for example, Strumok, which is a candidate for National encryption standard of Ukraine) faces the difficulties associated with the size of tasks that have been solved. Unlike SNOW 2.0, constructed above the field of order $2^{32}$, the Strumok cipher is set over a field of order $2^{64}$, which leads to the impossibility of practical implementation of some known algorithms, the time complexity of which increases from $2^{32} \div 2^{37}$ to $2^{64}$ bit operations.

The purpose of this article is to justify the security of Strumok against a wide class of correlation attacks, including known attacks on SNOW 2.0. The main result is a theorem that establishes an analytical bound for parameter characterizing the effectiveness of correlation attacks on SNOW 2.0-like ciphers in terms of their components. This allows in practice to evaluate and justify the security of such ciphers against correlation attacks over finite fields of characteristic 2.

**Key words:** *stream cipher, correlation cryptanalysis, system of noised linear equations, security justification, Strumok.*

Одержано 15.01.2019

УДК 004.056.55
DOI: 10.32626/2308-5916.2019-19.120-125

**В. В. Онопрієнко*,** канд. техн. наук, доцент,
**В. А. Пономар**,** канд. техн. наук

* ПАТ «Інститут інформаційних технологій», м Харків,
**Харківський національний університет імені В. Н. Каразіна, м. Харків

# ПОРІВНЯЛЬНИЙ АНАЛІЗ ПОСТКВАНТОВИХ АСИМЕТРИЧНИХ АЛГОРИТМІВ ШИФРУВАННЯ

Робота присвячена аналізу кандидатів на постквантовий стандарт асиметричного шифрування. З розвитком технологій квантових обчислень і появою квантового комп'ютера виникає загроза поточному стану захищеності криптографічних систем з відкритим ключем. З появою квантового комп'ютера, який буде мати необхідний для методів квантового криптоаналізу об'єм регістру розподілених квантів, стійкість існуючих криптоалгоритмів значно знизиться. З цього випливає необхідність створення алгоритмів стійких до методів квантового криптоаналізу. Європейський проект «Нові європейські алгоритми для електронного підпису, цілісності та шифрування» (NESSIE) та Національний інститут стандартів і технологій (NIST) США об'явили про початок набору претендентів на конкурс постквантових алгоритмів, стандарти щодо яких планується прийняти в 2020–2022 рр. Для порівняння обрано методику оцінювання на основі інтегральних оцінок безумовних і умовних критеріїв. Аналіз проводився серед алгоритмів, що пройшли загальні безумовні критерії. Як умовні критерії обрано чисельні характеристики алгоритмів. Крім того висувалися додаткові безумовні критерії.

Актуальна задача — це порівняльний аналіз та оцінка можливості використання постквантових механізмів, які представлені існуючими на даний момент алгоритмами, в залежності від умов застосування. На даний момент проводиться лише дослідження можливості використання відповідних криптоперетворень у постквантовий період, але що не проводився аналіз переваг одних над іншими. Крім того необхідно оцінити саму можливість використання таких алгоритмів з урахуванням обмежень, що накладаються існуючими інформаційними системами.

Результати досліджень дозволяють зрозуміти поточний стан розвитку постквантових криптоалгоритмів і спрогнозувати можливий їх подальший розвиток. Цей прогноз важливий тим, що постквантові криптографічні механізми являють собою новий етап розвитку та застосування криптографії. Крім того практичне значення дослідження полягає в отриманні оцінки постквантових алгоритмів.

**Ключові слова:** *постквантові криптографічні алгоритми, порівняльна оцінка криптоалгоритмів, критерії порівняння криптоалгоритмів.*


© В. В. Онопрієнко, В. А. Пономар, 2019

**Вступ.** Останнім часом все більшої актуальності набуває питання захисту інформації від атак з використанням квантового комп'ютера. Це питання постає через те, що за останніми дослідженнями, захист класичних криптографічних алгоритмів електронного підпису від методів квантового криптоаналізу буде значно меншим. Тому постає необхідність створення нових алгоритмів підпису та шифрування, що буде використовувати криптографічні перетворення, що є стійкими до методів квантового криптоаналізу. Але додатково висувається вимога до механізмів захисту ключів за допомогою алгоритмів інкапсуляції ключів.

Як підтвердження необхідності розробки постквантових алгоритмів необхідно привести роботу [1]. В ній відмічається, що в серпні 2015 року агентство національної безпеки (АНБ) уряду США виступило з великою заявою про необхідність розробки стандартів пост квантової криптографії. В цій статті проаналізована небезпека застосування квантових комп'ютерів для сучасних криптоалгоритмів, та запропоновано механізми криптоперетворень, що є стійкими до квантового криптоаналізу різних типів.

Аналіз літературних джерел [1–3] показав, що нині ще відсутні порівняння між потенційно можливими постквантовими механізмами, а також дані про можливості їх застосування в залежності від умов та середовища. Водночас саме вибір найбільш перспективних криптографічних перетворень для пост квантового застосування є надзвичайно важливим, так як він визначить подальший напрямок розвитку криптографії асиметричної криптографії.

**Метою досліджень** є оцінка та порівняльний аналіз існуючих методів постквантових криптоперетворень алгоритмів у залежності від висунутих вимог та умов їх застосування. Це надасть можливість, по-перше, виділити алгоритми, які скоріше за все стануть майбутніми постквантовими стандартами, а по-друге — спрогнозувати подальший напрямок розвитку асиметричної криптографії.

**Матеріали та методи дослідження.** При порівняльному аналізі використовувалася сукупність безумовних і умовних оцінок. Умовними оцінками виступали наступні характеристики алгоритмів:

1) $I_{ст.}$ — рівень криптографічної стійкості;
2) $l_{в.к}$ — довжина відкритого ключа;
3) $l_{о.к}$ — довжина особистого ключа;
4) $l_{рез.}$ — довжина результату криптоперетворення;
5) $T_{пр.}$ — швидкість прямого криптоперетворення;
6) $T_{зв.}$ — швидкість зворотнього криптоперетворення;
7) $T_{гкп.}$ — швидкість генерації ключової пари.

При оцінюванні використовувався метод попарних порівнянь. Експертні оцінки використовувалися для оцінки важливості кожної з наведених характеристик, а безпосередньо при порівнянні алгоритмів

використовувалися об'єктивні числові значення, шкала оцінки (яка при оцінювані об'єктивних показників характеристик враховує порядок переваги одного алгоритма над іншим за цією характеристикою), та вагові коефіцієнти важливості характеристик, що були отримані при експертному оцінюванні (табл. 1).

Таблиця 1

*Експертні оцінки характеристик криптоалгоритмів*

| Показники / Експерти | $I_{ст.}$ | $l_{в.к}$ | $l_{о.к}$ | $l_{рез.}$ | $T_{пр.}$ | $T_{зв.}$ | $T_{гкп.}$ |
|---|---|---|---|---|---|---|---|
| 1 | 0,073 | 0,045 | 0,033 | 0,262 | 0,275 | 0,275 | 0,038 |
| 2 | 0,067 | 0,067 | 0,029 | 0,198 | 0,298 | 0,298 | 0,043 |
| 3 | 0,080 | 0,035 | 0,035 | 0,341 | 0,229 | 0,229 | 0,053 |
| 4 | 0,098 | 0,051 | 0,029 | 0,390 | 0,205 | 0,205 | 0,023 |
| 5 | 0,083 | 0,083 | 0,039 | 0,386 | 0,191 | 0,191 | 0,027 |
| W | 0,080 | 0,056 | 0,033 | 0,315 | 0,239 | 0,239 | 0,037 |

В даному дослідженні при виборі алгоритмів висувалися додаткові безумовні вимоги:

1) алгоритм має гарантувати, що найменше 3 рівень безпеки за класифікацією NIST [3];
2) якщо існує декілька варіантів наборів параметрів для одного алгоритму, то в порівнянні бере участь варіант, що гарантує найбільшу безпеку.

В табл. 2 наведені характеристики обраних для порівняння алгоритмів, швидкодія задана в мільйонах ($10^6$) тактів.

На рис. 1 показано гіксограму відносної переваги алгоритмів. Як видно найбільшу перевагу має алгоритм NTRU Prime IIT Ukraine, на другому місці — LAC, на третьому — OKCN/AKCN/CNKE.

Для уточнення результатів проведено порівняння з використанням методу ранжування. Відмінність цього методу в тому, що він враховує лише кількість характеристик за якими у алгоритма є перевага та кількість алгоритмів над якими за цією характеристикою він кращий, але не враховує розмір цієї переваги.

Таблиця 2

*Характеристики алгоритмів шифрування*

| Алгоритми | Тип | $I_{ст.}$ | $l_{в.к}$ | $l_{о.к}$ | $l_{рез.}$ | $T_{пр.}$ | $T_{зв.}$ | $T_{гкп.}$ |
|---|---|---|---|---|---|---|---|---|
| Giophantus | Lattices | 5 | 27204 | 1134 | 54408 | 420,543 | 792,577 | 0,213 |
| KINDI | Lattices | 5 | 2368 | 2752 | 3328 | 0,705 | 0,919 | 0,489 |
| LAC | Lattices | 5 | 1056 | 2080 | 2048 | 0,137 | 0,133 | 0,573 |
| LEDApkc | Codes | 5 | 12384 | 40 | 24768 | 92,84 | 264,938 | 0,810 |
| LIMA | Lattices | 5 | 12289 | 18433 | 12291 | 0,909 | 1,126 | 1,084 |
| Lizard | Lattices | 5 | 8192 | 998266 | 8512 | 0,805 | 0,568 | 1,307 |
| LOTUS | Lattices | 5 | 1470976 | 1630720 | 1768 | 0,901 | 1,087 | 3,057 |

Продовження таблиці 2

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| McNie | Codes | 5 | 630 | 584 | 729 | 3,504 | 7,707 | 4,239 |
| NTRUEncrypt | Lattices | 5 | 64232 | 63912 | 127696 | 174,2 | 0,299 | 47,297 |
| Odd Manhattan | Lattices | 5 | 4454241 | 4456650 | 616704 | 141,625 | 155,302 | 127,488 |
| OKCN/ AKCN/ CNKE | Lattices | 5 | 1312 | 992 | 1200 | 0,568 | 0,631 | 366,432 |
| Round2 | Lattices | 5 | 830 | 1039 | 953 | 0,905 | 1,135 | 1599,640 |
| RQC | Codes | 5 | 40 | 1795 | 3574 | 6,46 | 18 | 1899,306 |
| Titanium | Lattices | 5 | 23552 | 32 | 8320 | 2,974 | 0,561 | 2147,483 |
| NTRU Prime IIT Ukraine | Lattices | 5 | 1578 | 243 | 1578 | 0,074 | 0,138 | 3248,122 |

В табл. 3 наведені експертні оцінки та вагові коефіцієнти важливості характеристик криптографічних алгоритмів асиметричного шифрування.

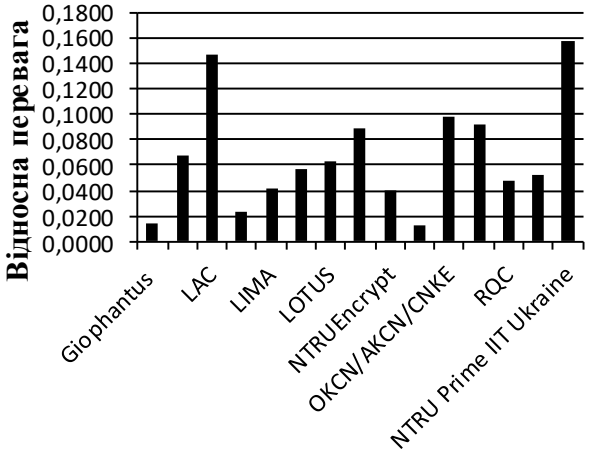



***Рис. 1.*** *Відносна перевага алгоритмів асиметричного шифрування*

Таблиця 3

*Експертні оцінки характеристик криптоалгоритмів за методом ранжування*

| Показники / Експерти | $I_{ст.}$ | $l_{в.к}$ | $l_{о.к}$ | $l_{рез.}$ | $T_{пр.}$ | $T_{зв.}$ | $T_{гкп.}$ |
|---|---|---|---|---|---|---|---|
| 1 | 4 | 3 | 1 | 5 | 6 | 7 | 2 |
| 2 | 3 | 4 | 1 | 5 | 6 | 7 | 2 |
| 3 | 4 | 2 | 1 | 7 | 5 | 6 | 3 |

Продовження таблиці 3

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 4 | 4 | 3 | 2 | 7 | 6 | 5 | 1 |
| 5 | 4 | 3 | 2 | 7 | 6 | 5 | 1 |
| W | 0,136 | 0,107 | 0,050 | 0,221 | 0,207 | 0,214 | 0,064 |

На рис. 2 показано гіксограму відносної переваги алгоритмів, що отримано методом ранжування. Як видно найбільшу перевагу мають алгоритми NTRU Prime IIT Ukraine та LAC (в них однакове значення переваги), на третьому — OKCN/AKCN/CNKE.

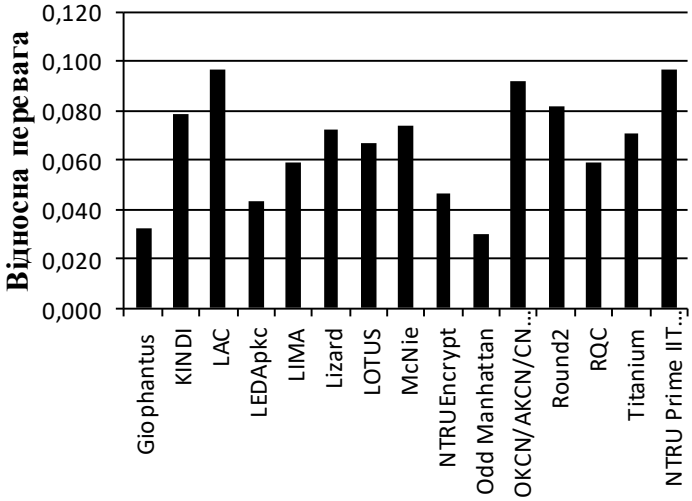



***Рис. 2.*** *Відносна перевага алгоритмів асиметричного шифрування за методом ранжування*

**Висновки.** З результатів порівняння постквантових алгоритмів шифрування максимального рівня захисту можна зробити висновок, що алгоритми, що базуються на криптоперетвореннях у решітках числового поля мають перевагу над алгоритмами з іншими математичними апаратами, що дозволяє зосередити увагу над дослідженням саме цих алгоритмів.

**Список використаних джерел:**

1. Koblitz N., Menezes A. J. A riddle wrapped in an enigma. URL: https://eprint.iacr.org/2015/1018.pdf.
2. Moody D. Post-Quntum Cryptography: NIST's Plan for the Future. *The Seventh International Conference on Post-Quntum Cryptography*, Japan, 2016. URL: https://pqcrypto2016.jp/data/pqc2016_nist_announcement.pdf.
3. Mosca M. Setting the Scene for the ETSI Quantum-safe Cryptography Workshop. *E-proceedings of «1st Quantum-Safe-Crypto Workshop»*, Sophia Antipolis, Sep 26–27, 2013. URL: http://docbox.etsi.org/Workshop/2013/-201309_CRYPTO/eproceedings_Crypto_2013.pdf.

## COMPARATIVE ANALYSIS OF POST-QUANTUM ASYMMETRIC ENCRYPT ALGORITHMS

Due to the development of technologies for quantum computing and the introduction of quantum computer, there is a threat to the current state of protection of cryptographic systems with a public key. With an advent of quantum computer that would have the volume of register required for the methods of quantum cryptanalysis, the stability of existing crypto algorithms will significantly degrade. This necessitates the creation of algorithms resistant to the methods of quantum cryptanalysis. The European project «New European Schemes for Signatures, Integrity, and Encryptions» (NESSIE) and the National Institute of Standards and Technologies (NIST) of the USA announced a start of recruiting the applicants for the contest of post-quantum algorithms whose standards are planned to be adopted over 2020–2022. In order to compare, a procedure for evaluation was selected based on integral assessments of unconditional and conditional criteria. An analysis was conducted among the algorithms that fulfilled general unconditional criteria. As conditional criteria, we chose numerical characteristics of algorithms. In addition, additional unconditional criteria were put forward.

A relevant task is the comparative analysis and evaluation of a possibility to use the post-quantum mechanisms, which are represented by the algorithms that already exist, depending on the conditions of applying them. At present, only the possibility of using the appropriate crypto transformations over a post-quantum period is being examined, but the analysis of advantages of one over another has not been run yet. In addition, it is necessary to evaluate the very possibility to use such algorithms taking into account those constraints that are imposed by the existing information systems.

Results of present research allow us to understand current state in the development of post-quantum crypto algorithms and to predict their possible further development.

This forecast is important in that the post-quantum cryptographic mechanisms represent a new stage in the development and use of cryptography. In addition, the practical value of the research consists in obtaining the evaluation for post-quantum algorithms.

**Key words:** *post-quantum cryptographic algorithms, comparative assessment of crypto algorithms, comparison criteria of crypto algorithms.*

Одержано 12.02.2019

UDC 519.859
DOI: 10.32626/2308-5916.2019-19.126-131

**A. Pankratov,** Dr. Sci.,
**T. Romanova,** Dr. Sci.

Institute for Mechanical Engineering Problems
National Academy of Sciences of Ukraine, Kharkiv

# DECOMPOSITION ALGORITHM FOR OPTIMIZATION PLACEMENT PROBLEMS

The paper considers a placement problem of 2D convex objects in a rectangular domain of minimum area, that related to the field of Packing and Cutting problems. Our objects may be continuously translated and rotated. A nonlinear programming model of the problem is derived using the phi-function technique. We develop an efficient decomposition algorithm to search for local optimal solutions for the placement problem. The algorithm reduces our problem to a sequence of nonlinear programming subproblems of considerably smaller dimension and a smaller number of nonlinear inequalities. The benefit of this approach is borne out by the computational results.

**Key words:** *placement problem, mathematical model, nonlinear optimization, decomposition algorithm.*

**Introduction.** Optimal placement problem is a part of operational research and computational geometry. It is also known as Packing and Cutting problem [1, p. 1109–1130, 2, p. 397–415]. It has multiple applications in modern biology, mineralogy, medicine, materials science, nanotechnology, robotics, coding, pattern recognition systems, control systems, space apparatus control systems, as well as in the chemical industry, power engineering, mechanical engineering, shipbuilding, aircraft construction, civil engineering, etc. The problems are NP-hard [3, p. 139–183] and, as a result, solution methodologies generally employ heuristics. Some researchers develop approaches based on mathematical modeling and general optimization procedures.

Our approach is based on mathematical modeling of relations between geometric objects, using the phi-function technique (see e. g. [4, p. 539–544, 5, p. 283–294]) and thus reducing the Packing and Cutting problem to a nonlinear programming problem. It contains all globally optimal solutions. It is possible, at least in theory, to use a global solver for the nonlinear programming problem and obtain a solution, which is an optimal packing. However in practice, the model contains a large number of variables and a huge number of inequalities. Specifically, the model involves $O(n^2)$ nonlinear inequalities and $O(n^2)$ variables due to additional variables in quasi-phi-functions, where $n$ is the number of convex objects.


© A. Pankratov, T. Romanova, 2019

As a result, even finding a locally optimal solution becomes an unrealistic task for the available state of the art NLP-solvers. In order to search for a «good» locally optimal object placement within a reasonable computational time we propose here a decomposition algorithm.

**Problem formulation.** We consider here a placement problem in the following setting. Let $\Omega$ denote a rectangular domain of length $l$ and width $w$. Both of these dimensions may be variable, or one may be fixed and the other variable. Suppose a set of convex objects $E_i$, $i \in \{1,2,...,n\} = I_n$, is given to be placed in $\Omega$ without overlaps. The position of object $E_i$ in the fixed coordinates is specified by the coordinates $(x_i, y_i)$ of its center and the rotation angle $\theta_i$. We call $(x_i, y_i, \theta_i)$ the vector of placement parameters of $E_i$. Minimum allowable distances between objects $E_i$ and $E_j$, $j > i \in I_n$, as well as, between each object $E_i$, $i \in I_n$, and the frontier (border) of $\Omega$ may be given.

*Object placement optimization problem*. Place the set of objects $E_i$, $i \in I_n$, within a domain $\Omega = \{(x, y) \in R^2 : 0 \le x \le l, 0 \le y \le w\}$ of minimum area taking into account distance constraints. If one of the two dimensions ($l$ or $w$) is fixed, we need to minimize the other one. If both are variable, it is natural to minimize the area $F = l \cdot w$ of the container.

**Mathematical model.** The vector $u \in R^\sigma$ of all our variables can be described as follows: $u = (l, w, u_1, u_2, ..., u_n, \tau)$, $u_i = (x_i, y_i, \theta_i)$ is the vector of placement parameters for the object $E_i$, $i \in I_n$, $\tau$ denotes the vector of additional variables, that includes two auxiliary variables $(\tau_{ij}^1, \tau_{ij}^2)$ for each quasi phi-functions of objects $E_i$ and $E_j$, $R^\sigma$ denotes the σ-dimensional Euclidean space, where $\sigma = 2n^2 + n + 2$.

A mathematical model of the object placement optimization problem may now be stated in the form:

$$\min_{u \in W \subset R^\sigma} F(u), \tag{1}$$

$$W = \{u \in R^\sigma : \widehat{\Phi}'_{ij} \ge 0, \widehat{\Phi}_i \ge 0, i = 1,2,...,n, j = 1,2,...,n, j > i\}, \tag{2}$$

where $F(u) = l \cdot w$, $\widehat{\Phi}'_{ij}$ is an adjusted quasi phi-function [5, p. 283–294] defined for the pair of objects $E_i$ and $E_j$, $\widehat{\Phi}_i$ is an adjusted phi-function [4, p. 539–544] defined for the object $E_i$ and the object $\Omega^*$ (to hold the *containment* constraint), taking into account minimum allowable distance $\rho$.

Our constrained optimization problem (1), (2) is a continuous nonlinear programming problem. The frontier of $W$ is usually made of nonlinear surfaces containing valleys, ravines. A matrix of the inequality system which specifies $W$ is strongly sparse and has a block structure.

Problem (1), (2) is an exact formulation for the object placement optimization problem. Our objective function is a quadratic; each quasi-phi-function inequality in (2) is described by a system of inequalities with differentiable functions.

**A solution strategy.** Our solution strategy consists of three major stages. First we generate a number of starting points from the feasible set of the problem (1), (2). Then starting from each point obtained at Stage 1 we search for a local minimum of the objective function $F(u)$ of problem (1), (2). Lastly, we choose the best local minimum from those found at Stage 2. This is our best approximation to the global solution of the problem (1), (2).

An essential part of our local optimization scheme (Stage 2) is the decomposition algorithm that reduces the dimension of the problem and computational time. It is due to this reduction that our strategy can process large sets of non-identical convex objects (100 and more). The reduction scheme used by our algorithm is described below. The actual search for a local minimum is performed by IPOPT [6, p. 25–57], which is available at an open access non-commercial software depository (https://projects.coin-or.org/Ipopt).

**Description of the Decomposition Algorithm**. Let $u^{(0)} \in W$ be one of the starting points found by the previous method. The main idea of the algorithm is as follows.

First we circumscribe a circle $C_i$ of radius $a_i$ around each object $E_i$, $i = 1, 2, ..., n$. Then for each circle $C_i$ we construct an «individual» rectangular container $\Omega_i \supset C_i \supset E_i$ with equal half-sides of length $a_i + \varepsilon$, $i = 1, 2, ..., n$, so that $C_i$, $E_i$ and $\Omega_i$ have the same center $(x_i^0, y_i^0)$ subject to the sides of $\Omega_i$ being parallel to those of $\Omega$, $a_i$ is a diameter of $E_i$. We take the fixed value of $\varepsilon$ of the procedure as $\varepsilon = \sum_{i=1}^{n} a_i / n$. Further we fix the position of each individual container $\Omega_i$ and let the local optimization algorithm move the corresponding object $E_i$ only within the container $\Omega_i$. It is clear that if two individual containers $\Omega_i$ and $\Omega_j$ do not have common interior points for $\rho = 0$, i. e. $\Phi^{\Omega_i,\Omega_j} \geq 0$, (or $\text{dist}(\Omega_i, \Omega_j) \geq \rho$ for $\rho > 0$, i. e. $\widehat{\Phi}^{\Omega_i,\Omega_j} \geq 0$), then we do not need to check the non-overlapping (or distance) constraint for the corresponding pair of objects $E_i$ and $E_j$.

The above key idea allows us to extract subsets of our feasible set $W$ of the problem (1), (2) at each step of our optimization algorithm as follows.

We create an inequality system of additional constraints on the translation vector $v_i$ of each object $E_i$ in the form: $\Phi^{C_i\Omega^*_{1i}} \geq 0$, $i \in I_n$, where $\Phi^{C_i\Omega^*_{1i}} = \min\{-x_i + x_i^0 + \varepsilon, -y_i + y_i^0 + \varepsilon, x_i - x_i^0 + \varepsilon, y_i - y_i^0 + \varepsilon\}$, is the phi-function for the circle $C_i$ and object $\Omega^*_{1i} = R^2 \setminus \operatorname{int}\Omega_{1i}$.

The inequality $\Phi^{C_i\Omega^*_i} \geq 0$ is equivalent to the system of four linear inequalities $-x_i + x_i^0 + \varepsilon \geq 0$, $-y_i + y_i^0 + \varepsilon \geq 0$, $x_i - x_i^0 + \varepsilon \geq 0$, $y_i - y_i^0 + \varepsilon \geq 0$.

Then we form a new subregion defined by

$$W_1 = \{u \in R^{\sigma-\sigma_1} : \widehat{\Phi}'_{ij} \geq 0, (i,j) \in \Xi_1, \widehat{\Phi}_i \geq 0, \Phi^{C_i\Omega^*_{1i}} \geq 0, i \in I_n\},$$

where $\Xi_1 = \{(i,j) : \widehat{\Phi}^{\Omega_{1i}\Omega_{1j}} < 0, i > j = 1,2,...,n\}$.

In other words, we delete from the system, which describes feasible region $W$, quasi phi-function inequalities for all pairs of objects whose individual containers do not overlap and we add additional inequalities $\Phi^{C_i\Omega^*_{1i}} \geq 0$, which describe the containment of the circles $C_i$ in their individual containers $\Omega_{1i}$, $i = 1,2,...,n$. Eo ipso we reduce the number of additional variables by $\sigma_1$. Then our algorithm searches for a point of local minimum $u^*_{w_1}$ of the subproblem

$$\min_{u_{w_1} \in W_1 \subset R^{\sigma-\sigma_1}} F(u_{w_1}).$$

When the point $u^*_{w_1}$ is found, it is used to construct a starting point $u^{(1)}$ for the second iteration of our optimization procedure.

At that iteration we again identify all the pairs of objects with non-overlapping individual containers, form the corresponding subregion $W_2$ (analogously to $W_1$) and let our algorithm search for a local minimum $u^*_{w_2} \in W_2$. The resulting local minimum $u^*_{w_2}$ is used to construct a starting point $u^{(2)}$ for the third iteration, etc.

Then we solve the $k$-th subproblem with starting point $u^{(k-1)}$ on a subregion $W_k$:

$$\min_{u_{w_k} \in W_k \subset R^{\sigma-\sigma_k}} F(u_{w_k}), \qquad (3)$$

$$W_k = \{u \in R^{\sigma-\sigma_k} : \widehat{\Phi}'_{ij} \geq 0, (i,j) \in \Xi_k, \widehat{\Phi}_i \geq 0, \Phi^{C_i\Omega^*_{ki}} \geq 0, i \in I_n\}, \quad (4)$$

where $\Xi_k = \{(i,j) : \widehat{\Phi}^{\Omega_{ki}\Omega_{kj}} < 0, i > j = 1,2,...,n\}$.

If the point $u^*_{w_k}$ of local minimum of the *k*-th subproblem belongs to the frontier of an «artificial» subset

$$\Pi^{\varepsilon}_k = \{u \in R^{\sigma-\sigma_k} : -x_i + x_i^{(k-1)} + \varepsilon \geq 0, -y_i + y_i^{(k-1)} + \varepsilon \geq 0,$$
$$x_i - x_i^{(k-1)} + \varepsilon \geq 0, \;\; y_i - y_i^{(k-1)} + \varepsilon \geq 0, \;\; i = 1,...,n\},$$

(i. e. $u^*_{w_k} \in fr\Pi^{\varepsilon}_k$), we take the point $u^*_{w_k} = u^{(k)}$ as a center point for a new subset $\Pi^{\varepsilon}_{k+1}$ and continue our optimization procedure, otherwise (i. e. $u^*_{w_k} \in \operatorname{int}\Pi^k_{\varepsilon}$) we stop our iterative procedure.

We note that dist($u^*_{w_k}$, $u^*_{w_{k+1}}$) $\geq \varepsilon$, if $u^*_{w_{k+1}} \in fr\Pi^k_{\varepsilon}$, and the value of $\varepsilon$ is considerably greater than the accuracy of IPOPT ($10^{-8}$). Thus, we may conclude that the stopping condition of the decomposition algorithm is always reached in a finite number of iterations.

We claim that the point $u^* = u^{(k)*} = (u^*_{w_k}, \tau^*_k) \in R^{\sigma}$ is a point of local minimum of the problem (1), (2), where $u^*_{w_k} \in R^{\sigma-\sigma_k}$ is the last point of our iterative procedure and $\tau^*_k$ is a vector of redefined values of the previously deleted additional variables $\tau_k \in R^{\sigma_k}$. The assertion comes from the fact that any arrangement of each pair of objects $E_i$ and $E_j$ subject to $(i,j) \in \Xi \setminus \Xi_k$ guarantees that there always exists a vector $\tau_k$ of additional variables such that $\widehat{\Phi}'_{ij} \geq 0, (i,j) \in \Xi \setminus \Xi_k$ at the point $u^{(k)*}$. Here $\Xi = \{(i,j), i > j = 1,2,...,n\}$. Therefore the values of additional variables of the vector $\tau_k$ have no effect on the value of our objective function, i. e $F(u^*_{w_k}) = F(u^{(k)*})$. That is why, indeed, we do not need to redefine the deleted additional variables of the vector $\tau_k$ at the last step of our algorithm.

So, while there are O($n^2$) pairs of objects in the container, our algorithm may in most cases only actively controls O(*n*) pairs of objects (this depends on the sizes of objects and the value of $\varepsilon$), because for each object only its «$\varepsilon$-neighbors» have to be monitored.

The parameter $\varepsilon$ provides a balance between the number of inequalities in each nonlinear programming subproblem and the number of the subproblems which we need to generate and solve in order to get a local optimal solution of problem (1), (2).

**Concluding remarks.** The proposed decomposition algorithm allows us to reduce the problem (1), (2) with $O(n^2)$ inequalities and a $O(n^2)$-dimensional feasible set $W$ to a sequence of subproblems (3), (4), each with $O(n)$ inequalities and a $O(n)$-dimensional solution subset $W_k$. This reduction is of a paramount importance, since we deal with nonlinear optimization problems. We are going to apply our algorithm to optimization placement problems for composed 2D and 3D objects in the near future.

## Reference:


1. Wascher G., Hauner H. and Schumann H. An improved typology of cutting and packing problems. *European Journal of Operational Research.* 2007. Vol. 183 (3), № 16. P. 1109–1130.
2. Bennell J., Oliveira J. The geometry of nesting problems. A tutorial. *European J. Operational Research.* 2008. Vol. 184. P. 397–415.
3. Chazelle B., Edelsbrunner H., Guibas L. The complexity of cutting complexes. Discrete & Computational Geometry. 1989. Vol. 4 (2). P. 139–181.
4. Chernov N., Stoyan Yu., Romanova T. Mathematical model and efficient algorithms for object packing problem. *Computational Geometry: Theory and Applications*. 2010. Vol. 43 (5). P. 535–553.
5. Stoyan Yu., Pankratov A., Romanova T. Quasi-phi-functions and optimal packing of ellipses. *Journal of Global Optimzation.* 2016. Vol. 65 (2). P. 283–307.
6. Wachter A., Biegler L. T. On the implementation of an interior-point filter line-search algorithm for large-scale nonlinear programming. *Mathematical Programming.* 2006. Vol. 106 (1). P. 25–57.


## АЛГОРИТМ ДЕКОМПОЗИЦІЇ ДЛЯ РОЗВ'ЯЗАННЯ ОПТИМІЗАЦІЙНИХ ЗАДАЧ РОЗМІЩЕННЯ


У статті розглядається задача розміщення двовимірних опуклих об'єктів у прямокутній області мінімальної площі, яка відноситься до класу задач упаковки і розкрою. Об'єкти, що розміщуються, можуть неперервно транслюватися і обертатися. Будується математична модель задачі розміщення у вигляді задачі нелінійного програмування з використанням методу phi-функцій. Для пошуку локально-оптимальних розв'язків пропонується ефективний алгоритм декомпозиції, який зводить вихідну задачу до послідовності підзадач нелінійного програмування значно меншою розмірності з меншим числом нелінійних нерівностей. Перевага цього підходу підтверджується результатами численних експериментів.



**Ключові слова**: *задача розміщення, математична модель, нелінійна оптимізація, алгоритм декомпозиції.*

Date received 31.01.2019

УДК 681.514:621.029
DOI: 10.32626/2308-5916.2019-19.132-138

**І. Р. Пітух*,** канд. техн. наук,
**Г. Я. Процюк**,** асистент,
**В. Р. Процюк**,** канд. техн. наук

*****Тернопільський національний економічний університет, м. Тернопіль,
******Івано-Франківський національний технічний університет,
м. Івано-Франківськ

# АЛГОРИТМИ ОПРАЦЮВАННЯ МОНІТОРИНГОВИХ ДАНИХ У ДІАЛОГОВИХ СИСТЕМАХ

Систематизовані умови формування моніторингових даних, які є компонентами інтерактивних (діалогових) комп'ютеризованих систем контролю та управління складними промисловими об'єктами та технологічними установками. Наведені приклади формування діалогових даних (ДД) на різних рівнях дистрибутивних комп'ютерних систем. Показано, що на низовому рівні дистрибутивної системи моніторингу промислового об'єкта розміщені сенсори, виконавчі механізми, абонентська станція оператора-технолога та спецпроцесори. Головною функцією оператора абонентської станції є діагностування стану об'єкта керування на основі образно-кластерної моделі. Базовими функціями спецпроцесорів на низовому рівні дистрибутивної комп'ютеризованої системи є реалізація алгоритмів обчислення інформаційних моделей, на основі яких будується образно-кластерна модель станів об'єкта. Основними функціями ентропійного аналізу є розрахунок станів об'єкта управління на основі оцінок мір ентропії Р. Хартлі, К. Шеннона та Я. Николайчука. Такі моделі дозволяють запобігти появі станів об'єкту типу «розвиток аварії». Тому до швидкодії відповідних спецпроцесорів висуваються жорсткі вимоги. Сформульовані вимоги до алгоритмів опрацювання моніторингових даних у структурах інтерактивного обміну даними, які містять різну кількість діалогових вузлів, та структурну організацію їх підпорядкування та взаємодій.

Викладені теоретичні засади реалізації алгоритмів опрацювання ДД, які охоплюють статистичний, кореляційний, спектральний, кластерний та ентропійний аналіз. Наведена інформаційна технологія побудови системи логіко-статистичних інформаційних станів об'єктів управління та побудови образно-кластерних моделей.

**Ключові слова:** *інтерактивна комп'ютеризована система, образно-кластерна модель, алгоритм опрацювання моніторингових даних.*


© І. Р. Пітух, Г. Я. Процюк, В. Р. Процюк, 2019

**1. Умови формування моніторингових даних у структурі дистрибутивної комп'ютерної системи.** Класична архітектура дистрибутивної моніторингової комп'ютерної системи контролю промислового обладнання на підприємствах показана на рис. 1 [1].

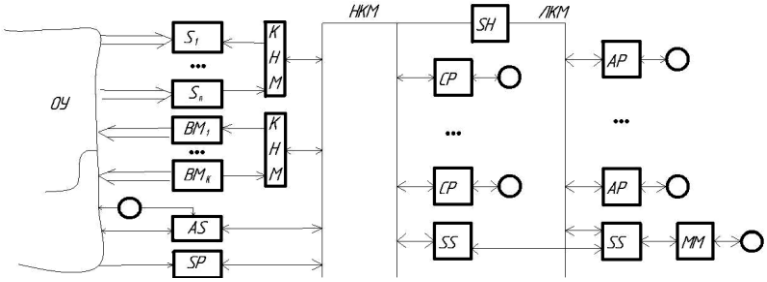



***Рис. 1.*** *Архітектура дистрибутивної системи моніторингу та керування промисловим об'єктом управління (ОУ — об'єкт управління;* $S_1 \div S_n$ *— сенсори; О — оператори;* $BM_1 \div BM_K$ *— виконавчі механізми; НКМ — низова; AS — абонентська станція; НКМ — контролер низової мережі (комп'ютерна мережа); СР — цехові процесори; SS — системний сервер; SH — сервер-шлюз; ЛКМ — локальна комп'ютерна мережа; АР — адміністративні процесори; ММ — модем)*

Аналіз цієї архітектури комп'ютеризованої системи дозволяє визначити топологію просторового розміщення ДД згідно з наступною систематизацією інтерактивних взаємодій:

1) оператор — об'єкт управління (О ↔ ОУ);
2) оператор — абонентська станція (ОС ↔AS);
3) контролер низової мережі — виконавчий механізм (КНМ — ВМ);
4) оператор абонентської станції — оператор цехового процесора (OAS↔OCP);
5) оператор AS — оператор адміністративного процесора (OAS↔OAP);
6) оператор СР — оператор AS (OCP↔OAP).

Розглянемо найбільш важливі діалогові взаємодії у структурі досліджуваної моніторингової системи [2, 3]. До класу важливих інформаційних взаємодій у комп'ютеризованих системах реального часу слід віднести наступні:

- параметри контролю технологічного процесу;
- інформаційні моделі етапів ОУ, які контролюють відхилення ОУ від норми і характеризуються пожежно-, вибухо-, екологічною небезпекою;
- моделі станів ОУ, які формуються спецпроцесорами (SP) на низовому рівні комп'ютерної системи;
- моделі станів ОУ у момент виникнення збурень у системі та проходженні перехідних процесів при зміні режимів роботи ОУ.

- для конкретних підприємств та технологічних процесів можуть бути побудовані відповідні проблемно-орієнтовані моделі моніторингу станів ОУ.

**2. Структура діалогових взаємодій з різною ієрархією повідомлень.** На рис. 2 показані структури діалогових інформаційних взаємодій у середовищі архітектури моніторингової системи промислового підприємства.

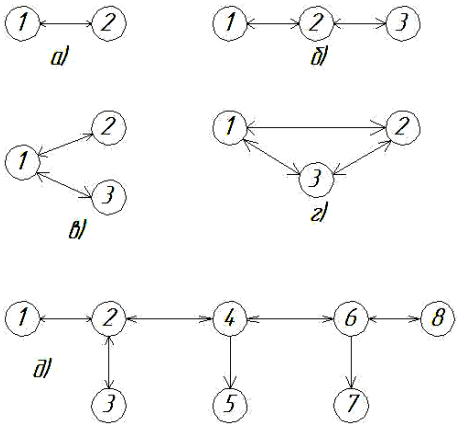



***Рис. 2.*** *Приклади інформаційних діалогових взаємодій у середовищі архітектури моніторингової комп'ютеризованої системи промислового підприємства*

Показані на рис. 2 діалогові взаємодії (ДВ) є типовими для мережно-ієрархічних архітектур комп'ютеризованих систем.

Виконаємо дослідження математичних алгоритмів при побудові важливої моделі станів ОУ, на основі побудови образно-кластерної моделі (ОКМ).

**3. Формалізація алгоритмів опрацювання моніторингових даних при побудові ОКМ.** ОКМ запропонована у [4–6] передбачає, у першу чергу, здійснення статистичного аналізу технологічних процесів згідно з наступними оцінками:

1) вибіркового математичного сподівання $(M_x)$;
2) ковзного математичного сподівання $(M_j)$;
3) вагового математичного сподівання $(M_v)$.

Дані оцінки розраховуються згідно з виразами:

$$M_x = \frac{1}{n}\sum_{i=1}^{n} x_i \;;\; M_j = \frac{1}{n}\sum_{i=1+j}^{n+j} x_{i+j} \;;\; M_v = \frac{1}{n}\sum_{\substack{i=1\\ j=0}}^{n} V_{i-j}x_{i+j} \;, \qquad (1)$$

де $V_{i-j}$ — вагова функція.

Оцінки $M_x, M_j, M_v$ дозволяють контролювати роботу відповідних регуляторів технологічних процесів шляхом визначення модульної різниці між уставкою регулятора $M_*$ та дійсним обчисленим значенням $M_x$.

$$|M_x - M_*| \to \min; \quad |M_j - M_*| \to \min; \quad |M_v - M_*| \to \min. \qquad (2)$$

Недоліком оцінки $M_x$ є значний ефект старіння інформації, оскільки її значення відноситься до половини інтервалу вибірки n.

Тому оцінка $M_j$ дозволяє значно зменшити обсяг вибірки (на 1÷2 порядки), що суттєво зменшує ефект старіння інформації.

Оцінка $M_v$ за рахунок вагової функції $V_{i-j}$ надає поточним значенням цифрових даних $x_i$ абсолютної ваги. Тому така оцінка характеризується мінімальним ефектом старіння інформації і може ефективно застосовуватися для цифрової фільтрації даних та передбачення статистичних даних $x_i$.

Недоліком оцінок математичного сподівання є відсутність інформації про зміну динаміки станів ОУ.

Статистичні оцінки вибіркової та ковзної дисперсії дозволяють визначити середньоквадратичне відхилення стану ОУ від норми згідно з виразами:

$$D_x = \frac{1}{n}\sum_{i=1}^{n}(x_i - M_x)^2; \; D_{x_j} = \frac{1}{n}\sum_{\substack{i=1 \\ j=0}}^{n}(x_{i+j} - M_x)^2. \qquad (3)$$

Дана оцінка у лінійному просторі класифікується як середньоквадратичне відхилення і обчислюється згідно з виразами:

$$\sigma_x = \sqrt{D_x}; \; \sigma_{x_j} = \sqrt{D_{x_j}}. \qquad (4)$$

Важливими характеристиками станів ОУ є визначення автокореляційних та взаємокореляційних функцій відповідно до виразів:

$$H_{xx}(j) = \frac{1}{n}\sum_{i=1}^{n} sign\,\overset{\circ}{x}_i \cdot sign\,\overset{\circ}{x}_{i+j}, \; j \in \overline{o,m} \qquad (5)$$

$$P_{xx}(j) = \frac{1}{n}\sum_{i=1}^{n} \overset{\circ}{x}_i \cdot sign\,\overset{\circ}{x}_{i+1}; \; j \in \overline{o,m} \qquad (6)$$

$$K_{xx}(j) = \frac{1}{n}\sum_{i=1}^{n} x_i \cdot x_{i+j}; \; j \in \overline{o,m} \qquad (7)$$

$$R_{xx}(j) = \frac{1}{n}\sum_{i=1}^{n} \overset{\circ}{x}_i \cdot \overset{\circ}{x}_{i+j}; \; j \in \overline{o,m} \qquad (8)$$

$$C_{xx}(j)=\frac{1}{n}\sum_{i=1}^{n}(x_i-x_{i+j})^2\ ;\ \ j\in\overline{o,m}\ ; \tag{9}$$

$$G_{xx}(j)=\frac{1}{n}\sum_{i=1}^{n}\left|x_i-x_{i+j}\right|\ ;\ \ j\in\overline{o,m}\ ; \tag{10}$$

$$F_{xx}(j)=\frac{1}{n}\sum_{i=1}^{n}\breve{Z}_{i,i+j}\ \ ;\ \ \breve{Z}_{i,i+j}=\begin{cases}\dot{x}_i, & \dot{x}_i<x_{i+j}\\ \dot{x}_{i+j}, & \dot{x}_i>x_{i+j}\end{cases}. \tag{11}$$

Найвищу швидкодію обчислень функції автокореляції забезпечують знакова $H_{xx}(j)$ та релейна $P_{xx}(j)$, але потребують великого обсягу вибірки $n\geq 1024$. Найвищу точність обчислень забезпечують: коваріаційна $K_{xx}(j)$, структурна $C_{xx}(j)$, модульна $G_{xx}(j)$ та еквівалентності $F_{xx}(j)$, які потребують обсягів вибірки у границях $n\geq 512\div 128$.

Оцінка спектру технологічного процесу на основі дискретного косинусного перетворення Фур'є розраховується шляхом згортки нормованої центрованої знакової функції автокореляції згідно з виразом:

$$S(\omega_i)=\frac{1}{m}\sum_{i=1}^{m}H_{xx}(j)\cdot\cos(\omega_i)\cdot e^{-c\cdot j}\ , \tag{12}$$

де $e^{-c\cdot j}$ — коефіцієнт затухання енергії функції автокореляції $H_{xx}(j)$.

Застосування знакової функції $H_{xx}(j)$ при спектральному опрацюванні технологічного процесу дозволяє суттєво підвищити швидкодію алгоритму за рахунок заміни операції множення додаванням з константою $\pm 1$.

Оцінка ентропії станів ОУ може обчислюватися на основі виразів інформаційної, ймовірнісної та кореляційної мір ентропії запропонованих Р. Хартлі, К. Шенноном та Я. Николайчуком [1].

$$I_N=\log_2 N\ ;\ I_N=-\sum_{i=1}^{n}P_i\cdot\log_2 P_i\ ;$$

$$I_N=\hat{E}[\frac{1}{2}\log_2\frac{1}{m}\sum_{j=1}^{m}(D_x^2-R_{xx}^2(j))]. \tag{13}$$

При розрахунку наведених моделей станів ОУ необхідно враховувати ергономічні характеристики відображення образно-кластерної моделі на моніторі оператора у діапазоні $\Delta t=0,8\div 1,2$ с.

Таким чином, до швидкодії алгоритмів та процесорів обчислення моделей моніторингу станів ОУ ставляться жорсткі вимоги. Тому на рівні НКМ найефективнішим є застосування відповідних спецпроцесорів спектрального аналізу та визначення ентропії [7]. Швидкодія обчислень параметрів ОКМ на практиці повинна відповідати 36-ти кадрам за 1 хв.

Перспективним напрямком підвищення швидкодії алгоритмів цифрового опрацювання даних є застосування модульної арифметики залишкових класів [8].

**Висновки.** Викладені результати досліджень умов формування моніторингових даних у дистрибутивних діалогових комп'ютеризованих системах реального часу та теоретичні засади алгоритмів цифрового опрацювання параметрів технологічного процесу складають базову основу побудови образно-кластерної моделі (ОКМ) станів промислових об'єктів управління. Систематизовані структури діалогових інформаційних взаємодій між компонентами комп'ютерної моніторингової системи.

**Список використаних джерел:**


1. Николайчук Я. М. Спеціалізовані комп'ютерні технології в інформатиці : монографія / за заг. наук. ред. Я. М. Николайчука. Тернопіль : Бескиди. 2017. 919 с.
2. Пітух І. Р., Процюк Г. Я., Ширмовська Н. Г. Моделі інтегрованого моніторингу багатопараметричних промислових об'єктів в інтерактивних комп'ютеризованих системах. *Питання оптимізації обчислень (ПОО-XLII).* Чинадієво, 2015. С. 51–58.
3. Возна Н. Я. Процюк Г. Я., Пітух І. Р., Николайчук Я. М. Структуризація, методи та моделі інтерактивної взаємодії оператор — інформаційна система моніторингу об'єктів нафтогазової галузі. *Розвідка та розробка нафтових і газових родовищ.* Івано-Франківськ, 2015. № 2(55). С. 111–118.
4. Спосіб контролю параметрів технологічного процесу: Пат. 107039 Україна: МПК G05B 23/00 (2016.01), G06F 11/277 (2006.01). №u 2015 07 057; Пітух І. Р., Возна Н. Я., Процюк Г. Я., Николайчук Я. М. ; заявл. 17.04.2015; опубл. 25.11.2015, Бюл. № 22/2015. 5 с.
5. Николайчук Л. М., Процюк Г. Я., Пітух І. Р. Організація інтерактивної взаємодії оператора з комп'ютеризованою системою управління. *Сучасні комп'ютерні інформаційні технології:* Матеріали Всеукраїнської конференції з міжнародною участю. Тернопіль, 2017. С. 76–79.
6. Igor Pitukh et al., Information and Legal Aspects of the Communication Functions of the Computerized System Operator. *Modern Problem of Radio Engineering, Telecommunications and Computer Science: proceedings of the XIII th International Conference TSET'2016*, Slavske, February 23–26. 2016. P. 885–888.
7. Пристрій визначення ентропії: Пат. на корисну модель 121046 Україна: МПК g06F 17/00 (2017.019); №u 2017 05 669; Николайчук Л.М., Возна Н. Я, Пастух Т. У., заявл. 08.06.2017; опубл. 27.11.2017, Бюл. № 22/2017. 5 с.
8. Николайчук Я. М. Коди поля Галуа: теорія та застосування : монографія / за заг. наук. ред. Я. М. Николайчука. Тернопіль : ТзОВ «Терно граф», 2012. 392 с.


## ALGORITHMS OF MONITORING DATA PROCESSING IN DIALOG SYSTEMS

The article classifies conditions of formation of monitoring data, which is the component of interactive (dialog) computer systems of control and management over complex industrial objects and technological apparatus.

It shows examples of formation of dialog data (DD), which occur on different levels of distributive computer systems. The article phrases requirements for algorithms of monitoring data processing in structures of interactive data exchange, which consists of different dialog nodes, and it phrases structural order of interaction and subordination of the algorithms. It deals with an informational technology of creation of the system of logicaly-statistical informational states of management objects and building of image-cluster models.

**Key words:** *interactive computer system, image-cluster model, algorithm of monitoring data processing.*

Одержано 04.03.2019

УДК 551.568.85;621.391
DOI: 10.32626/2308-5916.2019-19.138-144

**Б. М. Шевчук**, д-р техн. наук

Інститут кібернетики імені В. М. Глушкова НАН України, м. Київ

# ПІДВИЩЕННЯ ІНФОРМАЦІЙНОЇ ЕФЕКТИВНОСТІ МЕРЕЖ ТА ЗАСОБІВ ІНТЕРНЕТУ РЕЧЕЙ

Основою підвищення інформаційної ефективності мереж та засобів Інтернету речей є реалізація процесорними засобами об'єктних систем безпровідних мереж комплексу алгоритмів оброблення, компактного кодування та захисту вибірок сигналів, кадрів відеоданих і вимірювальних величин, криптостійкого та завадостійкого передавання пакетів моніторингової інформації безпосередньо в місцях виникнення мережевих потоків. Алгоритми стиску та захисту моніторингових даних повинні бути оптимізовані за швидкодією і точністю кодування даних з урахуванням мінімізації обчислювальних операцій мікропотужними процесорами та мікроконтролерами об'єктних систем мереж Інтернету речей. Зменшення інформаційних потоків у місцях встановлення об'єктних систем мереж Інтернету речей досягається на основі адаптації алгоритмів кодування даних в залежності від умов введення і точності представлення моніторингових даних та формуванням кодово-сигнальних послідовностей пакетів моніторингової інформації з підвищеною інформаційною ємністю. Параметри завадостійкого передавання криптозахищених пакетів інформації вибираються в залежності від поточного рівня шумів у радіоканалі. Ключова характеристика ефективності функціонування об'єктних систем мереж Інтернету речей — поточна швидкість передачі стислої та захищеної моніторингової інформації. При наявних обчислювальних і канальних ресурсах об'єктних систем з урахуванням поточних умов введення і передавання моніторин-



© Б. М. Шевчук, 2019

гових даних, які є змінними, реалізація надійної та захищеної передачі даних у мережах Інтернету речей здійснюється постійною підтримкою процесорними засобами об'єктних систем максимальної швидкості передачі пакетів стислих та зашифрованих моніторингових даних. На практиці передача таких пакетів — це передача по радіоканалу псевдохаотичної беззбиткової інформації.

**Ключові слова**: *мережі Інтернету речей, об'єктні системи, алгоритми оброблення, стиску та захисту сигналів і кадрів відеоданих.*

**Вступ.** Мережі Інтернету речей (Internet of Things, скорочено IoT) — основа для прискореного впровадження новітніх інформаційно-комунікаційних технологій і засобів штучного інтелекту в різноманітні галузі людської діяльності. В результаті широкого проникнення та застосування засобів і мереж IoT у різноманітні галузі людської діяльності забезпечуються умови для ефективної перебудови економічних та суспільних процесів, звільнення працюючих людей від рутинних операцій, мінімізації впливу людського фактора в технологічних, економічних, політичних та суспільних процесах. Важливими пристроями безпровідних мереж IoT є об'єктні системи (ОС), які разом із сенсорами і відеосенсорами встановлюються на об'єктах моніторингу і керування (ОМіК) та перетворюють вихідні потоки даних від сенсорів на вихідні потоки пакетів даних. Невирішеними завданнями при побудові пристроїв і мереж IoT є мінімізація та формування захищених потоків пакетів моніторингових даних у місцях встановлення ОС мереж IoT.

**Мета роботи** — підвищення ефективності функціонування процесорів ОС мереж IoT на основі адаптації алгоритмів оброблення, кодування сигналів і відеоданих до рівня шумів введених моніторингових даних, стиску-захисту визначених достовірних масивів даних, формування та передавання захищених пакетів даних з підвищеною інформативністю.

**Підвищення ефективності функціонування мереж IoT.** Технологія IoT стартувала на початку 2000-х років як технологія міжмашинної взаємодії (machine-to-machine, M2M) для вирішення завдань дистанційного моніторингу об'єктів з використанням різноманітних радіотрактів сенсорних, локально-регіональних та мобільних мереж [1]. На даному етапі розвитку пристроїв і мереж IoT для обміну інформацією між абонентськими системами мереж IoT (ОС, центральною станцією (ЦС), роутерами (стаціонарними і мобільними ретрансляторами, безпілотними апаратами, високо піднятими платформами, дирижаблями, мікро- та нано-супутниками) широкого розповсюдження отримали різноманітні технології безпровідної передачі даних [2]. Враховуючи, що інтеграція різноманітних пристроїв, об'єктів та речей з Інтернетом

вимагає присвоєння їм IP-адрес (унікальних ідентифікаторів), найбільш ефективним є використання засобів мобільних мереж 3G, 4G, 5G, сенсорних мереж (ZigBee, 6LoWPAN, Bluetooth і ін.), локальних мереж Wi-Fi, а також діючих мереж передачі даних. Перспективним є застосування в пристроях IoT сучасних радіомодулів LTE NB-IoT, наприклад, SIM7020E компанії SIMCom Wireless Solutions, для побудови мереж IoT з використанням розповсюдженої в Європі технології LoRaWAN [3]. Підвищення ефективності функціонування діючих та перспективних пристроїв та мереж IoT досягається за рахунок зменшення вихідних інформаційних потоків на об'єктах контролю і управління з використання енергоефективних мікроконтролерів широкого застосування без залучення спеціалізованих кодеків, відеокодеків та енерговитратних процесорів. В результаті при мінімальних енергетичних та апаратурних витратах в процесі виконання завдань тривалого моніторингу станів ОМіК кожною ОС мережі IoT зменшується кількість інформаційних пакетів (ІП), які передаються і ретранслюються в загальному радіоканалі. Ефективність передачі ІП досягається зменшенням інформаційних потоків у місцях встановлення ОС шляхом адаптації алгоритмів кодування даних у залежності від умов введення і точності представлення моніторингових даних засобами ОС та формуванням кодово-сигнальних послідовностей послідовностей (КСП) пакетів з підвищеною інформаційною ємністю, параметри завадостійкого передавання яких вибираються в залежності від поточного рівня шумів у радіоканалі [4, 5].

Первинними даними для ефективної реалізації передачі моніторингової інформації в мережах IoT є величина робочої смуги частот $F$ радіоканалу, максимальна та мінімальна кількість біт АЦП $q_{\max}$ і $q_{\min}$ для точного та менш точного кодування амплітудних значень відліків сигналів та яскравості пікселів відеоданих, максимальне значення кількості елементів шумоподібних сигналів (ШПС) $N_B$, від яких залежить максимальна тривалість КСП-ШПС та значення бази ШПС $B$. ОС є перетворювачами вхідних моніторингових даних у вихідні дані ІП, при цьому процесор (процесори) ОС виконує узагальнений алгоритм оброблення, кодування та передавання моніторингових даних $P_{pct}(F,\ f_{\max},\ q,\ \delta_d^N, P_p,\ \gamma_n)$, який суттєво залежить від параметрів введення, оброблення та передавання даних, де $F$ — величина робочої смуги частот радіоканалу, Гц, $f_{\max}$ — максимальна частота спектру вхідних даних, $q$ — кількість біт для кодування даних, $\delta_d^N$ — оцінка величини рівня вхідних шумів в околиці найбільш інформативних (суттєвих) відліків обвідної сигналів, $P_p \geq 2^{2048}$ — ве-

личина ступеня захисту даних засобами ОС радіомережі, $\gamma_n = (E_{is} / J_0)_n$ — необхідне енергетичне співвідношення сигнал/шум в радіоканалі, яке забезпечує умови для передачі пактів даних у радіоканалах з шумами з високою величиною безпомилкової передачі даних $P_n$, наприклад, $P_n \le 10^{-6} - 10^{-12}$. В процесі виконання послідовності обчислювальних операцій зменшуються об'єми введених, відфільтрованих та стислих моніторингових даних, які, після криптозахисту та завадостійкого кодування, є основою для формування і передачі КСП пакетів відповідної тривалості, як правило, змінної.

Узагальнений алгоритм $P = P_{pct}(F,\ f_{\max},\ q,\ \delta_d^N,\ P_p,\ \gamma_n)$ виконує послідовність взаємодоповнених операцій оброблення, кодування і формування даних, що підлягають передаванню з використанням радіоканалу з шумами, тобто

$$P_{pct}(F, f_{\max}, q, \delta_d^N, P_p, \gamma_n) = P(p_F, p_{c1}, p_{c_2}, p_p, p_{ni}, p_{is}),$$

де $p_F$ — алгоритм фільтрації даних, $p_{c1}$ — алгоритм стиску даних з допустимими втратами інформації, $p_{c2}$ — алгоритм стиску даних без втрат, $p_p$ — алгоритм криптозахисту моніторингових даних з заданою величиною $P_p \ge 2^{2048}$ ступеня захисту даних засобами ОС радіомережі, $p_{ni}$ — алгоритм завадостійкого кодування даних з заданою величиною безпомилкової передачі даних $P_n$, $p_{is}$ — алгоритм формування КСП ІП з урахуванням оцінки енергетичного співвідношення сигнал/шум в радіоканалі. Відповідно КСП ІП часто є збитковими і характеризуються характеризується базою $B$ поточних канальних сигналів, що передаються в радіоканалі. З практичних міркувань базу канальних сигналів доцільно вибирати в таких діапазонах [4]: $B \le 1$, $B \ge 1$, $B > 10$.

Ключова характеристика ефективності функціонування ОС мереж IoT — поточна швидкість передачі стислої та захищеної інформації $R_i$. Для реалізації інформаційно-ефективної передачі моніторингових даних у радіомережах показник інформаційної ефективності системи передачі інформації $\eta = R_i / R_{\max}$ повинен максимально наближається до одиниці ($\eta \to 1$, $\eta < 1$), де $R_{i\max}$ — максимальна швидкість передачі даних. Відповідно, суть інформаційно-ефективної передачі даних у мережах IoT полягає у тому, що при наявних обчислювальних і канальних ресурсах ОС з урахуванням поточних умов введення і передавання моніторингових даних, які є змінними, досягнення надійної та захищеної передачі даних в мережах IoT здійснюється постійною підтримкою засобами ОС максимальної швидкості

передачі даних $R_{i\max}$. З урахуванням досягнення заданої ймовірності помилкового прийому даних інформаційних кадрів пакетів $P_n$, що відповідає ймовірності помилкового відновлення кодових послідовностей ІП абонентськими приймачами, поточна швидкість передачі інформації $R_i$ є змінною і залежить від вибору ключових параметрів процесів введення, кодування та передавання даних:

$$R_i = f(F, P_n, k_{1c}(\delta_d^N), k_2, k_3, B_{\min}(\gamma_n), L, t_{pc}(P_{CPU}, Ea_j), \log_2 M_{sc}),$$

де $k_{1c}(\delta_d^N)$ — коефіцієнт стиску сигналів і відеоданих з допустимими (контрольованими) втратами інформації, який суттєво залежить від оцінки допустимої величини рівня вхідних шумів $\delta_d^N$ в околиці найбільш інформативних (суттєвих) відліків обвідної сигналів, $k_2$ — коефіцієнт стиску даних без втрат, $B_{\min}(\gamma_n)$ — мінімально необхідна база КСП ІП для реалізації успішної та завадостійкої передачі даних у радіоканалі з шумами, яка вибирається в залежності від необхідного енергетичного співвідношення у радіоканалі $\gamma_n = (E_{is} / J_0)_n$, $L$ — кількість ортогональних моноканалів передачі інформації з кодовим розділенням каналів у робочій смузі частот $F$, $t_{pc}$ — тривалість часу обробки і кодування даних, який залежить від продуктивності абонентського процесора $P_{CPU}$ та ефективності $j$-х алгоритмів обробки і кодування даних $Ea_j$, $j = \overline{1, p}$, $p$ — кількість взаємодоповнюючих алгоритмів кодування даних засобами АС, $M_{sc}$ – кількість станів канальних сигналів (видів сигналів, рівнів та позицій маніпуляції або модуляції несучої).

При обмеженій величині робочої смуги частот $F$ максимальна канальна швидкість передачі інформації $v_{c\max} \le 2F / k_s = 1/k_s \cdot T_b$, де $F = 1/T$, $T = 2T_b$ — період повторення послідовностей бітових даних, $T_b$ — тривалість бітової послідовності, $k_s > 1.4$ — коефіцієнт, що враховує якість відновлення фронтів цифрових (імпульсних) сигналів. Враховуючи обмеження на мінімальну тривалість кодової послідовності $T_{is\min} = T_b$ суттєве підвищення інформаційної швидкості передачі даних $R_i >> r_{c\max}$ досягається за рахунок реалізації абонентськими процесорами стиску даних з втратами і без втрат, що враховується коефіцієнтом стиску даних $K_{ci}$ на інформаційному рівні засобів АС. Також $R_i$ збільшується шляхом використання радіотехнічних засобів багатоканальної передачі інформації з частотним, кодовим і просторо-

вим розділення каналів передачі, що для простоти аналізу можна враховувати коефіцієнтом стиску даних $K_{crt}$ на радіотехнічному рівні засобів АС. В результаті $R_i = K_c / k_s \cdot T_b$, де $K_c = K_{ci} \cdot K_{crt}$ — сумарний коефіцієнт стиску даних. При використанні спрощених радіотехнічних засобів (радіомодулів ISM діапазону частот, наприклад, з частотною модуляцією або маніпуляцією несучої), що характерно для розповсюджених засобів сенсорних мереж, $K_{crt} = 1$.

**Висновки.** Для підвищення інформаційної ефективності мереж та засобів Інтернету речей у місцях встановлення об'єктних систем безпровідних мереж необхідна реалізація процесорними засобами комплексу алгоритмів оброблення, компактного кодування та захисту вибірок сигналів і кадрів відеоданих, криптостійкого та завадостійкого передавання пакетів моніторингової інформації. Такі алгоритми повинні бути оптимізовані за швидкодією і точністю кодування даних з урахуванням мінімізації обчислювальних операцій процесорами об'єктних систем мереж Інтернету речей. Основою для зменшення інформаційних потоків у місцях встановлення об'єктних систем мереж є адаптація алгоритмів кодування даних у залежності від умов введення і точності представлення моніторингових даних та формуванням кодово-сигнальних послідовностей пакетів моніторингової інформації з підвищеною інформаційною ємністю. Важлива умова ефективної передачі захищених пакетів моніторингової інформації — підтримка об'єктними системами мереж Інтернету речей поточної максимальної швидкості передачі пакетів.

**Список використаних джерел:**


1. URL: http:// www. everest.ua/ai-platform/analystics.
2. Огірко І. В. Технології мереж для Інтернету речей. *Матеріали науково-практичної конференції «Інтернет речей: проблеми правового регулювання та впровадження»,* Україна, Київ, 24 жовтня 2017 року, Київ : Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», 2017. С. 44–52.
3. URL: http:// www.biz.liga.net/all/telecom.
4. Shevchuk B. M., Zadiraka V. K., Fraier S. V. Data Transfer Optimization in the Information Efficient Sensory, Local-Regional and Microsatellite Wireless Networks. *Optimization Methods and Applications.* In Honor of Ivan V. Sergienko's 80th Birthday. Editor: Butenko S., Pardalos P. M., Shylo V., Springer, 2017. P. 465–480.
5. Shevchuk B. M. Speed-Efficient Algorithms for Transmitting and Receiving High-Informative Packets in Radio Networks. *Cybernetics and Systems Analysis*. 2016, March, Vol. 52, Issue 2. P. 330–337.

## THE INFORMATION EFFICIENCY INCREASING OF THE MEANS AND NETWORKS

The basis of the information efficiency increasing of networks and means of Internet of Things is the implementation by processor means of object systems of wireless networks of complex algorithms of processing, compact coding and protection of signal samples, video data frames and measuring values, crypto- proof and noise-proof transmission of monitoring information packets directly in the places of origin of network streams. The algorithms of compression and monitoring data protection should be optimized for the speed and accuracy of data encoding, taking into account the minimization of computing operations by micro power microprocessors and microcontrollers of object systems of the Internet of Things. The reduction of information flows in places of installation of object systems of Internet networks of things is achieved on the basis of adaptation of data coding algorithms, depending on the conditions of input and the accuracy of the presentation of monitoring data and the formation of code-signal sequences of monitoring information packets with increased information capacity. Parameters of noise-proof transmission of crypto-proof information packets are selected depending on the current level of noise in the radio channel. The key characteristic of the operation efficiency of object systems of Internet of things networks is the current speed of the transmission of the compressed and protected monitoring information. With existing computing and channel resources of object systems taking into account the current conditions of input and transfer of monitoring data that are variables, the implementation of reliable and secure data transmission in networks of Internet of Things is carried out by constant support of processor means of object systems the maximum speed of packets of compressed and encrypted monitoring data. In practice, the transmission of such packets is the transmission of pseudo-chaotic break-even information.

**Key words:** *Internet things, object systems, algorithms for processing, compressing and protecting signals and video frames.*

Одержано 14.02.2019

УДК 519.6
DOI: 10.32626/2308-5916.2019-19.145-150

**І. З. Якименко**, канд. техн. наук,
**М. М. Касянчук**, канд. фіз.-мат. наук,
**С. В. Івасьєв**, канд. техн. наук
Тернопільський національний економічний університет, м. Тернопіль

# КРИПТОСИСТЕМА РАБІНА НА ОСНОВІ ОПЕРАЦІЇ ДОДАВАННЯ

У роботі наведено теоретичні основи криптосистеми Рабіна з використанням тільки операції додавання, завдяки чому досягається зменшення часової складності процесу шифрування / дешифрування інформаційних потоків. Запропонований підхід дозволяє збільшувати розмірності вхідних параметрів для підвищення стійкості без втрати швидкодії. Представлено приклад застосування запропонованої реалізації криптосистеми Рабіна.

**Ключові слова:** *криптосистема Рабіна, векторно-модульний метод модулярного множення, квадратичний лишок, операція додавання, часова складність.*

**Вступ.** На сьогоднішній день криптосистема Рабіна є однією з найбільш ефективних [1], оскільки для шифрування потрібна лише операція піднесення до квадрату за модулем, а не модулярне експоненціювання, як в асиметричних криптосистемах RSA та Ель-Гамаля [2]. Крім того, її стійкість ґрунтується на проблемі факторизації [3, 4] та пошуку квадратичного лишку [5]. Дана операція має субекспоненційну складність [6], тому для забезпечення достатньої стійкості при сьогоднішніх обчислювальних потужностях розрядність числових полів повинна бути більшою 1024 біт [7].

Поряд з перевагами, існує ряд недоліків, найголовніший з яких стосується процесу розшифрування з використанням китайської теореми про залишки, який характеризується значною часовою складністю при виконанні базових операцій [8, 9]. Інший недолік — це певні обмеження до вхідних параметрів, які повинні задовольняти рівність $p \bmod 4 = q \bmod 4 = 3$ для спрощення пошуку квадратичного лишку при дешифруванні. Крім того, в класичній криптосистемі Рабіна застосовується позиційна система числення, що у зв'язку із використанням багаторозрядних чисел призводить до зменшення швидкодії процесу шифрування/дешифрування та збільшення часової складності. Тому постає актуальна задача реалізації криптосистеми Рабіна на основі нових підходів, які дозволяють зменшити часову складність процесу шифрування/дешифрування шляхом заміни обчислювально складних арифметичних операцій операцією додавання.

**Класична криптосистема Рабіна.** Для генерування ключів у криптосистемі Рабіна вибираються два випадкових багаторозрядних

© І. З. Якименко, М. М. Касянчук, С. В. Івасьєв, 2019

простих числа $p$ і $q$. Шукається їх добуток $n = p \cdot q$, де число $n$ є відкритим ключем, числа $p$ і $q$ — закритим.

Процес шифрування повідомлення $M$ (текст) відбувається згідно такого виразу:

$$C = M^2 \bmod n. \tag{1}$$

При дешифруванні криптограми $C$ вводяться додаткові допоміжні величини $f$ і $s$:

$$f = C \bmod p;\ s = C \bmod q. \tag{2}$$

Для знаходження $M$ необхідно знайти квадратичні лишки за модулями $p$ і $q$:

$$x^2 \bmod p = f, \tag{3}$$

$$y^2 \bmod q = s. \tag{4}$$

В результаті отримуємо чотири системи порівнянь:

$$\begin{cases} M_1 \bmod p = x; \\ M_1 \bmod q = y; \end{cases} \quad \begin{cases} M_2 \bmod p = x; \\ M_2 \bmod q = -y; \end{cases}$$
$$\begin{cases} M_3 \bmod p = -x; \\ M_3 \bmod q = y; \end{cases} \quad \begin{cases} M_4 \bmod p = -x; \\ M_4 \bmod q = -y. \end{cases} \tag{5}$$

Одне з рішень (5) буде шуканим повідомленням $M$.

Слід зазначити, що для пошуку усіх розв'язків (5) достатньо знайти тільки два з них, наприклад $M_1$ та $M_2$. Тоді інші розв'язки шукаються з виразу $M_{3,4} = n - M_{1,2}$.

Однак використання класичних підходів при виконанні арифметичних операцій для шифрування/дешифрування на основі криптосистеми Рабіна характеризується великою часовою складністю. Тому у даній роботі пропонується реалізація криптосистеми Рабіна з використанням тільки операції додавання.

**Криптосистема Рабіна на основі операції додавання.** Для зменшення часової складності криптосистеми Рабіна при генерації ключів та шифруванні запропоновано використати векторно-модульний метод [10]. Одне з вибраних чисел $p$ і $q$ (наприклад, $p$) записується в двійковій формі: $p = \sum_{i=0}^{k-1} p_i \cdot 2^i$, де $k$ — його розрядність, $p_i = 0$ або1. Далі будується вектор-рядок $q_i = 2 \cdot q_{i-1} = 2^i q_0 = q$ (табл. 1).

Таблиця 1

*Представлення вектор-рядків для множення*

| $i$ | $k-1$ | … | 2 | 1 | 0 |
|---|---|---|---|---|---|
| $p_i$ | $p_{k-1}$ | … | $p_2$ | $p_1$ | $p_0$ |
| $q_i = 2 \cdot q_{i-1}$ | $q_{k-1}$ | … | $q_2$ | $q_1$ | $q_0 = q$ |

Результат множення $n = p \cdot q$ знаходиться згідно такої формули:

$$n = p \cdot q = \sum_{i=0}^{k-1} p_i \cdot q_i . \qquad (6)$$

Отже, операція множення замінюється операцією додавання тих $q_i$, для яких відповідні $p_i = 1$.

Аналогічно будується табл. 2 для шифрування. Число $M$ записується в двійковій формі $M = \sum_{i=0}^{k-1} d_i \cdot 2^i$ ($d_i = 0$ або 1) і формується вектор-рядок $m_i = 2 \cdot m_{i-1} \bmod n$, $m_0 = M$.

Таблиця 2

*Представлення вектор-рядків для множення за модулем*

| $i$ | $k-1$ | … | 2 | 1 | 0 |
|---|---|---|---|---|---|
| $d_i$ | $d_{k-1}$ | … | $d_2$ | $d_1$ | $d_0$ |
| $m_i = 2 \cdot m_{i-1} \bmod n$ | $m_{k-1}$ | … | $m_2$ | $m_1$ | $m_0 = M$ |

Результат шифрування знаходиться згідно формули:

$$C = M^2 \bmod n = \left( \sum_{i=0}^{k-1} d_i \cdot m_i \right) \bmod n. \qquad (7)$$

Відповідно, операція множення за модулем замінюється операцією модулярного додавання тих $m_i$, для яких відповідні $d_i$ дорівнюють 1.

В порівнянні з класичним підходом, даний метод характеризується меншою часовою складністю [11].

Для знаходження $x$ і $y$ в (3), (4) необхідно обчислити значення кореня квадратного за модулем. Класичні підходи з використання символів Якобі або Лежандра є трудомісткими [12]. Тому пропонується метод, який вимагає тільки операції додавання та перевірки, чи є число повним квадратом, що суттєво зменшує часову складову методу Рабіна. Отже, для того, щоб знайти значення $x \bmod p = \sqrt{f}$, необхідно виконати наступну послідовність дій: $f + p$, $f + 2p$, … , $f + i \cdot p$, де $i$ — значення, при якому число $f + i \cdot p$ буде повним квадратом. Аналогічним чином шукається $y^2 \bmod q = s$.

Для розв'язку систем (5) також пропонується використати метод додавання модуля. Для прикладу розглянемо першу систему порівнянь (5). Оскільки будь-яку конгруенцію $M_1 \bmod p = x$ можна представити у вигляді $M_1 = \lambda p + x$, де $\lambda = 0, 1, 2, \ldots$, то до залишку $x$ потрібно додавати модуль $p$ стільки разів, поки не буде виконуватись конгруенція $(x + \lambda p) \bmod q = M_1 \bmod q = y$.

Слід відмітити, що в класичних методах (китайській теоремі про залишки та алгоритмі Гарнера) необхідно шукати обернений елемент за модулем [13, 14], що супроводжується великою обчислювальною складністю і, відповідно, призводить до погіршення часових характеристик при реалізації криптоалгоритму Рабіна.

**Приклад використання запропонованих методів.** Нехай таємні ключі $p$ = 47, $q$ = 31, тоді згідно (6) і табл. 1 отримується: $n = p \cdot q = 31 \cdot 47 =$ 992 + 248 + 124 + 62 + 31 = 1457 (табл. 3).

Таблиця 3

*Пошук добутку $n = p \cdot q = 31 \cdot 47$*

| $i$ | 5 | 4 | 3 | 2 | 1 | 0 |
|---|---|---|---|---|---|---|
| $p_i$ | 1 | 0 | 1 | 1 | 1 | 1 |
| $q_i = 2 \cdot q_{i-1}$ | 992 | 496 | 248 | 124 | 62 | 31 |

Нехай відкритий текст $M$ = 118. На основі формул (1), (7) та таблиці 2 формується табл. 4.

Таблиця 4

*Процедура шифрування*

| $i$ | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
|---|---|---|---|---|---|---|---|
| $d_i$ | 1 | 1 | 1 | 0 | 1 | 1 | 0 |
| $m_i = 2 \cdot m_{i-1} \bmod n$ | 267 | 862 | 431 | 944 | 472 | 236 | 118 |

Звідси отримується значення шифртексту: $C \equiv 118^2 \bmod 1457 =$ = (267 + 862 + 431 + 472 + 236) mod 1457 = 811, тобто операція модулярного множення замінюється операцією додавання за модулем.

При дешифруванні криптограми $C$ використовуються вирази (2)–(4): $f$ = 811 mod 47 = 12, $s$ = 811 mod 31 = 5. Далі формуються послідовності, в яких шукається повний квадрат:

12, 12+47 = 59, 59+47 = 106, 106+47 = 153, 153+47 = 200,
200+47 = 247, 247+47 = 294, 294+47 = 341, 341+47 = 388,

388+47 = 435, 435+47 = 482, 482+47 = 529, $\sqrt{12} (\bmod 47) \equiv 23$ та 24;

5, 5+31=36, $\sqrt{5} (\bmod 31) \equiv 6$ та $31 - 6 = 25$.

Отже, потрібно розглянути чотири системи конгруенцій:

$$\begin{cases} M_1 \bmod 47 = 23; \\ M_1 \bmod 31 = 25; \end{cases} \quad \begin{cases} M_2 \bmod 47 = 24; \\ M_2 \bmod 31 = 25; \end{cases}$$

$$\begin{cases} M_3 \bmod 47 = 23; \\ M_3 \bmod 31 = 6; \end{cases} \quad \begin{cases} M_4 \bmod 47 = 24; \\ M_4 \bmod 31 = 6. \end{cases} \qquad (8)$$

Розв'язок перших двох з них зручно представити у вигляді табл. 5.

Таблиця 5

*Процедура дешифрування*

| $\lambda$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| Перша система | | | | | |
| $23+47\cdot\lambda$ | 23 | 70 | 117 | 164 | 211 |
| $(23+47\cdot\lambda)$ mod 31 | 23 | 8 | 24 | 9 | 25 |
| Друга система | | | | | |
| $24+47\cdot\lambda$ | 24 | 71 | 118 | | |
| $(24+47\cdot\lambda)$ mod 31 | 24 | 9 | 25 | | |

Отже, розв'язками (8) є значення $M_1 = 211$, $M_2 = 118$ (відкритий текст), $M_3 = 1457 - 211 = 1246$, $M_4 = 1457 - 118 = 1339$, які отримані без використання громіздких операцій та необхідності контролю переповнення розрядної сітки при виконанні проміжних обчислень.

**Висновки.** У роботі наведено теоретичні основи для реалізації криптоалгоритму Рабіна за допомогою використання тільки операції додавання. Це дозволяє збільшити швидкодію процесу шифрування/дешифрування інформаційних потоків шляхом уникнення виконання обчислювально громіздких операцій (множення, пошуку квадратного кореня за модулем, пошуку оберненого елемента тощо). Застосування такого підходу дозволяє будувати надійні та ефективні системи захисту за рахунок збільшення розмірності вхідних параметрів (розміру повідомлення, ключа), що призводить до підвищення стійкості та зменшення часової складності криптосистеми Рабіна.

**Список використаних джерел:**


1. Menezes A., van Oorschot P., Vanstone S. Handbook of Applied Cryptography. CRC Press, 2003. 780 p.
2. Arpit K., Mathur A. The Rabin cryptosystem and analysis in measure of chinese reminder theorem. *Int. J. Sci. Res. Public*. 2013. Vol. 3. P. 1–4.
3. Karpiński M., Ivasiev S., Yakymenko I., Kasianchuk M., Gancarczyk T. Advanced method of factorization of multi-bit numbers based on Fermat's theorem in the system of residual classes. *Proc. of 16th International Conference on Control, Automation and Systems* (ICCAS–2016). Gyeongju, Korea. Vol. 1. October, 2016. P. 1484–1486.
4. Kasianchuk M., Yakymenko I., Ivasiev S., Shevchuk R., Tymoshenko L. The Method of Factorizing Multi-Digit Numbers Based on the Operation of Adding Odd Numbers. *Proceedings of the conference «Advanced Computer Information Technology* (ACIT 2018)» (Ceske Budejovice, Czech Republic). P. 232–235.
5. Задірака В.К., Олексюк О.С. Комп'ютерна криптологія. Тернопіль ; Київ, 2002. 504 с.
6. Dasgupta S., Papadimitriou C., Vazirani U. Algorithms. McGraw-Hill Science, Engineering, 2006. 336 p.

7. Королев М. Е., Лапина Н. А. Сравнение производительности алгоритмов формирования электронной цифровой подписи. *Проблемы современной науки и образования.* 2017. С. 13—18.
8. Kasianchuk M., Yakymenko I., Pazdriy I., Melnyk A., Ivasiev S., Rabin's modified method of encryption using various forms of system of residual classes. *Proceedings of the XIV International Conference «The Experience of Designing and Application of CAD Systems in Microelectronics* (CADSM-2017)». Polyana-Svalyava (Zakarpattya), Ukraine. 2017. P. 222–224.
9. Касянчук М. М., Якименко І. З., Івасьєв С. В., Мандебура Н. М., Неміш В. М. Дослідження часових характеристик апаратної реалізації методів пошуку оберненого елемента за модулем. *Вісник Хмельницького національного університету.* Технічні науки. 2017. № 6 (255). С. 191–197.
10. Kozaczko D., Kasianchuk M., Yakymenko I., Ivasiev S. Vector Module Exponential in the Remaining Classes System. *Proceedings of the 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications* (IDAACS–2015). Warsaw, Poland. 2015. Vol. 1. P. 161–163.
11. Yakymenko I. Z., Kasianchuk M. M., Ivasiev S. V., Melnyk A. M., Nykolaichuk Y. M. Realization of RSA cryptographic algorithm based on vector-module method of modular exponention. *Proceedings of the 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering* (TCSET-2018). 2018. P. 550–554.
12. Івасьєв С.В., Якименко І.З. Касянчук М. М. Вдосконалений алгоритм пошуку символів Якобі. *Методи та системи оптико-електронної і цифрової обробки зображень та сигналів.* 2015. Том 29, № 1. С. 45–50.
13. *Rajba T., Klos-Witkowska A., Ivasiev S., Yakymenko I., Kasianchuk M.* Research of Time Characteris-tics of Search Methods of Inverse Element by the Module. *Proceedings of the 9th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications* (IDAACS–2017). 2017. Vol. 1. P. 82–85.
14. Касянчук М. М., Якименко І. З., Івасьєв С. В., Момотюк О. В. Експериментальне дослідження програмної реалізації методів пошуку оберненого елемента за модулем. *Інформатика та математичні методи в моделюванні.* 2017. Т. 7, № 3. С. 178–186.

## RABIN'S CRYPTO SYSTEM ON THE BASIS OF THE ADDITION OPERATION

The paper presents the theoretical backgrounds of the Rabin's cryptosystem using only on the addition operation in virtue of reducing the time complexity of the encryption / decryption process of information flows. The proposed approach allows to increase the dimension of the input parameters to improve stability without loss of performance. An example of application of the proposed implementation of Rabin's cryptosystem is presented.

**Key words:** *cryptosystem Rabin, vector-modular method of modular multiplication, quadratic residue, add-on operation, time complexity.*

Одержано 04.02.2019

## ВІДОМОСТІ ПРО АВТОРІВ

**Акользіна Ольга Сергіївна** — молодший науковий співробітник, Харківський національний університет імені В. Н. Каразіна, м. Харків, 4akolzinaolga@gmail.com

**Богаєнко Всеволод Олександрович** — кандидат технічних наук, старший науковий співробітник, Інститут кібернетики імені В. М. Глушкова НАН України, м. Київ, sevab@ukr.net

**Бойчура Михайло Володимирович** — науковий співробітник кафедри інформатики та прикладної математики, Рівненський державний гуманітарний університет, м. Рівне, mboichura@gmail.com

**Бомба Андрій Ярославович** — доктор технічних наук, професор, завідувач кафедри, Рівненський державний гуманітарний університет, м. Рівне, abomba@ukr.net

**Булавацький Володимир Михайлович** — доктор технічних наук, професор, провідний науковий співробітник, Інститут кібернетики імені В. М. Глушкова НАН України, м. Київ, v_bulav@ukr.net

**Вакал Євген Сергійович** — кандидат фізико-математичних наук, доцент, Київський національний університет імені Тараса Шевченка, м. Київ, jvakal@gmail.com

**Вакал Лариса Петрівна** — кандидат технічних наук, Інститут кібернетики імені В. М. Глушкова НАН України, м. Київ, lara.vakal@gmail.com

**Верлань Анатолій Федорович** — доктор технічних наук, професор, головний науковий співробітник, Інститут проблем моделювання в енергетиці імені Г. Є. Пухова НАН України, м. Київ, afverl@gmail.com

**Возна Наталія Ярославівна** — кандидат технічних наук, доцент, Тернопільський національний економічний університет, м. Тернопіль, nvozna@ukr.net

**Воронич Артур Романович** — кандидат технічних наук, доцент кафедри, Івано-Франківський національний технічний університет нафти і газу, м. Івано-Франківськ, a.voronych@it.nung.edu.ua

**Галата Лілія Павлівна** — асистент, Національний авіаційний університет, м. Київ, galataliliya@gmail.com

**Гладкий Анатолій Васильович** — доктор фізико-математичних наук, професор, завідувач лабораторією, Інститут кібернетики імені В. М. Глушкова НАН України, м. Київ, gladky@ukr.net

**Горбачук Василь Михайлович** — доктор фізико-математичних наук, старший науковий співробітник, Інститут кібернетики імені В. М. Глушкова НАН України, м. Київ, GorbachukVasyl@netscape.net

**Горбенко Іван Дмитрович** — доктор технічних наук професор, головний конструктор АТ «Інститут інформаційних технологій», професор, Харківський національний університет імені В. Н. Каразіна, м. Харків, gorbenkoi@iit.kharkov.ua

**Горбенко Юрій Іванович** — кандидат технічних наук, перший заступник головного конструктор, АТ «Інститут інформаційних технологій», м. Харків, iit@iit.kharkiv.ua

**Грига Володимир Михайлович** — кандидат технічних наук, доцент, Прикарпатський національний університет імені Василя Стефаника, м. Івано-Франківськ, v.dr_2000@ukr.net

**Давлетова Аліна Ярославівна** — аспірант, Тернопільський національний економічний університет, м. Тернопіль, a90f@meta.ua

**Дунаєвський Максим Сергійович** — аспірант, Інститут кібернетики імені В. М. Глушкова НАН України, м. Київ, MaxDunaievskyi@gmail.com

**Єсіна Марина Віталіївна** — кандидат технічних наук, науковий співробітник-консультант, АТ «Інститут інформаційних технологій», старший викладач, Харківський національний університет імені В. Н. Каразіна, м. Харків, m.v.yesina@karazin.ua

**Заведюк Тетяна Олексіївна** — кандидат технічних наук, викладач, Надвірнянський коледж Національного транспортного університету, м. Надвірна, paprikamail@gmail.com

**Замула Олександр Андрійович** — доктор технічних наук, доцент, науковий співробітник-консультант АТ «Інститут інформаційних технологій», професор кафедри, Харківський національний університет імені В. Н. Каразіна, м. Харків, zamylaaa@gmail.com

**Іванюк Віталій Анатолійович** — кандидат технічних наук, доцент, доцент кафедри, Кам'янець-Подільський національний університет імені Івана Огієнка, м. Кам'янець-Подільський, wivanyuk@gmail.com

**Івасьєв Степан Володимирович** — кандидат технічних наук, старший викладач, Тернопільський національний економічний університет, м. Тернопіль, stepan.ivasiev@gmail.com

**Касянчук Михайло Миколайович** — кандидат фізико-математичних наук, доцент, доцент кафедри, Тернопільський національний економічний університет, м. Тернопіль, kasianchuk@ukr.net

**Коваленко Богдан Анатолійович** — здобувач, Фізико-технічний інститут Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського, м. Київ, animantbk@gmail.com

**Ковальчук Людмила Василівна** — доктор технічних наук, професор, професор кафедри, Фізико-технічний інститут Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ, lusi.kovalchuk@gmail.com

**Конюшок Сергій Миколайович** — кандидат технічних наук, доцент, заступник начальника інституту (з наукової роботи), Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ, 3tooth@iszzi.kpi.com

**Корнієнко Богдан Ярославович** — доктор технічних наук, доцент, професор кафедри, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ, bogdanko@i.ua

**Круліковський Борис Борисович** — кандидат технічних наук, доцент, Національний університет водного господарства та природокористування, м. Рівне, kboris@ukr.net

**Кудін Антон Михайлович** — доктор технічних наук, старший науковий співробітник, професор кафедри, Фізико-технічний інститут Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», заступник директора департаменту безпеки, Національний банк України, м. Київ, pplayshner@gmail.com

**Кудряшов Іван Сергійович** — студент, Харківський національний університет імені В. Н. Каразіна, м. Харків, entick11@gmail.com

**Малачівський Петро Стефанович** — доктор технічних наук, професор, провідний науковий співробітник, Центр математичного моделювання Інституту прикладних проблем механіки і математики імені Я. С. Підстригача НАН України, м. Львів, petro.malachivskyy@gmail.com

**Малачівський Роман Петрович** — інженер, Національний університет «Львівська політехніка», м. Львів, roman.malachivsky@gmail.com

**Малєєва Ганна Андріївна** — аспірант, Харківський національний університет радіоелектроніки, АТ «Інститут інформаційних технологій», м. Харків, halina@iit.kharkov.ua

**Матійко Александра Андріївна** — викладач-стажист, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ, alexm1710@ukr.net

**Мітін Сергій Вячесчлавович** — старший викладач, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ, meetser@gmail.com

**Монцібович Борис Романович** — кандидат фізико-математичних наук, доцент, старший науковий співробітник, Центр математичного моделювання Інституту прикладних проблем механіки і математики імені Я. С. Підстригача НАН України, м. Львів, mon_ua@yahoo.com

**Морозов Олександр Олександрович** — молодший науковий співробітник, науково-виробниче приватне підприємство «Гіперон», м. Київ, Morozov4work@gmail.com

**Николайчук Любов Михайлівна** — кандидат юридичних наук, доцент кафедри, Івано-Франківський національний технічний університет нафти і газу, м. Івано-Франківськ, lmnykolaychuk@gmail.com

**Николайчук Ярослав Миколайович** — доктор технічних наук, професор, Тернопільський національний економічний університет, м. Тернопіль kafsks@gmail.com

**Огурцов Максим Ігорович** — науковий співробітник, Інститут кібернетики імені В.М. Глушкова НАН України, м. Київ, ogurtsov.maksym@incyb.kiev.ua

**Олексійчук Антон Миколайович** — доктор технічних наук, доцент, професор кафедри, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ, alex-dtn@ukr.net

**Онопрієнко Віктор Васильович** — кандидат технічних наук, доцент, генеральний директор АТ «Інститут інформаційних технологій», м. Харків, iit@iit.kharkov.ua

**Панкратов Олександр Вікторович** — доктор технічних наук, старший науковий співробітник, Інститут проблем машинобудування імені А. М. Підгорного НАН України, м. Харків, pankratov2001@yahoo.com

**Пізюр Ярополк Володимирович** — кандидат фізико-математичних наук, доцент, Національний університет «Львівська політехніка», м. Львів, pizyur@yahoo.com

**Пітух Ігор Романович** — кандидат технічних наук, доцент, доцент кафедри, Тернопільський національний економічний університет, м. Тернопіль, Pirom75@ukr.net

**Подгайко Владислав Олегович** — студент, Харківський національний університет імені В. Н. Каразіна, м. Харків, vladosla@ukr.net

**Пономар Володимир Андрійович** — кандидат технічних наук, науковий співробітник, Харківський національний університет імені В. Н. Каразіна, м. Харків, Laedaa@gmail.com

**Поремський Михайло Васильович** — аспірант, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ, undermyclouds@gmail.com

**Процюк Василь Романович** — кандидат технічних наук, доцент, доцент кафедри, Івано-Франківський національний технічний університет нафти і газу, м. Івано-Франківськ, aspvr@nung.edu.ua

**Процюк Галина Ярославівна** — асистент, Івано-Франківський національний технічний університет нафти і газу, м. Івано-Франківськ, aspvr@nung.edu.ua

**Романова Тетяна Євгенівна** — доктор технічних наук, професор, провідний науковий співробітник, Інститут проблем машинобудування імені А. М. Підгорного НАН України, м. Харків, tarom27@yahoo.com

**Федорчук Володимир Анатолійович** — доктор технічних наук, професор, завідувач кафедри, Кам'янець-Подільський національний університет імені Івана Огієнка, м. Кам'янець-Подільський, fedvolod@kpnu.edu.ua

**Хо Чі Лик** — магістрант, Харківський національний університет імені В. Н. Каразіна, м. Харків, hotriluc97@gmail.com

**Шевчук Богдан Михайлович** — доктор технічних наук, старший науковий співробітник, Інститут кібернетики імені В. М. Глушкова НАН України, м. Київ, incors@ukr.net

**Якименко Ігор Зіновійович** — кандидат технічних наук, доцент, доцент кафедри, Тернопільський національний економічний університет, м. Тернопіль, iyakymenko@ukr.net

## АЛФАВІТНИЙ ПОКАЖЧИК АВТОРІВ

## ЗМІСТ

Інститут кібернетики імені В. М. Глушкова
Національної академії наук України
Кам'янець-Подільський національний університет
імені Івана Огієнка

НАУКОВЕ ВИДАННЯ

# МАТЕМАТИЧНЕ ТА КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ

**Серія: Технічні науки**

Збірник наукових праць

**Випуск 19**

Редактор **В. П. Замула**
Комп'ютерна верстка **О. М. Коломис**

Підписано до друку 20.06.2018 р. Гарнітура «Таймс».
Папір офсетний. Друк різографічний.
Формат 60x84/16. Умовн. друк. арк. 9,3. Обл.-вид. арк. 10,1.
Тираж 100. Зам. № 862.

Кам'янець-Подільський національний університет імені Івана Огієнка,
вул. Огієнка, 61, м. Кам'янець-Подільський, 32300.
Свідоцтво серії ДК № 3382 від 05.02.2009 р.

Надруковано в Кам'янець-Подільському національному
університеті імені Івана Огієнка,
вул. Огієнка, 61, м. Кам'янець-Подільський, 32300.
Свідоцтво серії ДК № 3382 від 05.02.2009 р.