УДК 512.548.7

В.Д. САВЧУК

ШИФРУВАННЯ ІНФОРМАЦІЇ МЕТОДОМ ГІЛА ІЗ ВИКОРИСТАННЯМ СИСТЕМ БАГАТОМІСНИХ ОРТОГОНАЛЬНИХ КВАЗІГРУП НАД ПОЛЕМ ЛИШКІВ

Вінницький національний технічний університет, м. Вінниця, Україна

Анотація. У роботі досліджено можливості вдосконалення класичного шифру Гілла шляхом використання систем багатомісних ортогональних квазігрупових операцій, побудованих над скінченними полями лишків простого порядку. Запропонований підхід базується на встановленні зв'язку між ортогональними n-арними квазігрупами та оборотними матрицями, що дозволяє формувати нові криптографічні перетворення для захисту інформації. Розглянуто теоретичні засади побудови таких структур, їх властивості та умови ортогональності. У статті доведено критерії існування оборотних матриць, елементи яких належать полю лишків та є ненульовими. На основі отриманих математичних результатів розроблено алгоритм побудови систем ортогональних лінійних n-арних квазігруп довільної розмірності. Запропонований алгоритм забезпечує однозначність розв'язку відповідних систем рівнянь, що є необхідною умовою коректного процесу шифрування та дешифрування повідомлень. Наведено приклад побудови системи п'яти ортогональних квазігруп арності п'ять над скінченною множиною лишків, що підтверджує практичну реалізованість запропонованого підходу. Окрему увагу приділено оцінюванню криптографічної стійкості розробленого методу. Показано, що кількість можливих ключових матриць стрімко зростає зі збільшенням їх розмірності, що істотно ускладнює проведення атак методом повного перебору. Використання множини матриць різної розмірності та випадкового порядку їх застосування додатково підвищує рівень захищеності системи. Отримані результати можуть бути використані під час розроблення сучасних блочних криптографічних алгоритмів, систем захисту даних та інформаційно-комунікаційних мереж.

Ключові слова: Шифр Гіла, оборотна матриця, визначник, ортогональність, лінійна квазігрупа

Abstract. The paper explores the possibilities of improving the classical Gill cipher by using systems of multi-place orthogonal quasigroup operations built on finite residue fields of simple order. The proposed approach is based on establishing a connection between orthogonal n-ary quasigroups and invertible matrices, which allows the formation of new cryptographic transformations for information protection. The theoretical principles of constructing such structures, their properties and orthogonality conditions are considered. The article proves the criteria for the existence of invertible matrices whose elements belong to the residue field and are nonzero. Based on the obtained mathematical results, an algorithm for constructing systems of orthogonal linear n-ary quasigroups of arbitrary dimension is developed. The proposed algorithm ensures the uniqueness of the solution of the corresponding systems of equations, which is a necessary condition for the correct process of encrypting and decrypting messages. An example of constructing a system of five orthogonal quasigroups of arity five over a finite set of residues is given, which confirms the practical feasibility of the proposed approach. Special attention is paid to assessing the cryptographic stability of the developed method. It is shown that the number of possible key matrices increases rapidly with increasing their dimension, which significantly complicates the implementation of brute force attacks. The use of a set of matrices of different dimensions and a random order of their application additionally increases the level of system security. The results obtained can be used in the development of modern block cryptographic algorithms, data protection systems and information and communication networks.

Keywords: Gil cipher, invertible matrix, determinant, orthogonality, linear quasigroup

DOI: 10.31649/1681-7893-2026-51-366-373

ВОЛОКОННО-ОПТИЧНІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНИХ (INTERNET, INTRANET ТОЩО) ТА ЕНЕРГЕТИЧНИХ МЕРЕЖАХ

1. ВСТУП

Метод Гілла – це метод, який був запропонований Л. Гіллом ще у 1929 році [1]. Він полягає у множенні вектора (відкритого тексту) на (ключ) оборотну матрицю відповідної розмірності, отриманий результат є вектор (закритий текст). Дешифрування полягає у множенні вектора (закритого тексту) на матрицю обернену до матриці «ключ». Оскільки множення вектора (змінних) на оборотну матрицю та система лінійних рівняннь тієї ж розмірності є еквівалентними, тому задача створення оборотних матриць та систем лінійних рівняннь є рівносильними. В даній праці пропонується алгоритм побудови систем лінійних ортогональних квазігруп, як побудови оборотних матриць довільної розмірності на множині простого порядку. Оскільки у лінійних квазігруп усі коефіцієнти мають бути не нульовими елементами поля лишків, то і матриці не будуть містити нульових елементів.

Сучасні дослідження показують, що даний підхід далеко не вичерпаний і має досить великий інтерес у науковців. Удосконалення методу Гілла висвітлено у працях О. Гутік, О. Попадюк [2]

Ортогональність операцій має важливе прикладне значення. Цьому питанню присвячено багато праць. Зокрема Г. Манном у праці [3] описано побудову бінарних ортогональних операій. Л. Пейджем [4] і М. Холлом [5] було знайдено необхідні і достатні умови існування ортогональной пари для груп. Результати дослідження ортогональних багатомісних квазігруп викладено у праці Білявської Г. та Муллена Г. у праці [6], а також Сохацький Ф. та Фриз І. у праці [8] досліджували властивості ортогональних багатомісних операцій та дано алгоритми їх побудови. У працях [9] та [10] продовжує дослідження ортогоналтних операцій. Алгоритми побудови багатомісних операцій досліджували Смайл Марковскі та Александра Мілева у праці [11]. Алгоритми побудови пари латинських ортогональних квадратів, як еквівалента квазігруп, описано Д. Кідвелом у праці [7]. В даній праці викладені алгоритми побудови систем ортогональних квазігрупових операцій при $n > 2$.

2. ТЕОРЕТИЧНІ ВІДОМОСТІ, ОПИС МЕТОДУ

Нагадаємо, що операція f, яка визначена на множині Q, називається i-оборотною, якщо для довільних елементів $a_1,...,a_{i-1},b,a_{i+1},...,a_n$ із Q існує єдиний елемент $x \in \mathrm{Q}$ такий, що $f(a_1,...,a_{i-1},x,a_{i+1},...,a_n)=b$.

Операція f називається *оборотною* або *квазігруповою*, якщо вона i-оборотна для всіх $i \in \overline{1,n}$. Тоді пару $(\mathrm{Q};f)$ називають *квазігрупою*, точніше n*-арною квазігрупою*.

Групові ізотопи. [8] n-арний групоїд $(\mathrm{Q};f)$ називається *груповим ізотопом*, якщо існує група $(G;+)$ та бієкції $\alpha_1,...,\alpha_n,\alpha_{n+1}$ із Q на G такі, що виконується рівність $f(x_1,...,x_n)=\alpha_{n-1}^{-1}(\alpha_1 x_1+...+\alpha_n x_n)$, для всіх $x_1,...,x_n \in \mathrm{Q}$.

Отже, n-арний групоїд $(\mathrm{Q};f)$ є *квазігрупою*, якщо операція f оборотна.

Означення 1. [8] Нехай $(\mathrm{Q};f)$ n-арний груповий ізотоп і нехай $(\mathrm{Q};+,0)$ - група, $\alpha_1,...,\alpha_n$ - унітарні підстановки, тобто $\alpha_1 0=...=\alpha_n 0=0$, та $a \in \mathrm{Q}$. Якщо $f(x_1,...,x_n)=\alpha_1 x_1+...+\alpha_n x_n+a$, то послідовність $(+,\alpha_1,...,\alpha_n,a)$ називається 0-канонічним розкладом $(\mathrm{Q};f)$, $(\mathrm{Q};+)$ - група розкладу, $\alpha_1,...,\alpha_n$ її коефіцієнти, a називається вільним членом.

Теорема 1. [8] Довільний елемент n-арного груповогу ізотопу однозначно визначає його канонічний розклад.

Отже, n-арний групоїд $(\mathrm{Q};f)$ є *квазігрупою*, якщо операція f оборотна. Зауважимо, що унарні квазігрупові операції - це підстановки носія.

Групоїд $(\mathrm{Q};\mathrm{g})$ називається:

- n-арним похідним бінарної групи $(\mathrm{Q};+)$, якщо $\mathrm{g}(x_1,...,x_n)=x_1+...+x_n$;
- груповим ізотопом, якщо він ізотопний n-арній похідній деякої бінарної групи;
- лінійним над групою, якщо він є груповим ізотопом цієї групи, причому компоненти ізотопізму є її лінійними перетвореннями.

- цетральною квазігрупою або Т-квазігрупою, якщо він лінійний над деякою комутативною групою.

3. ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ

Ортогональність n-арних лінійних квазігруп

Нехай $\mathrm{Q} = Z_m$, де $m = pq$, та p і q прості числа більше 2. $Z_m^* = \{b_k\}$ таких $(b_k; m) = 1$, для всіх $k = 1,...,\varphi(m)$.

n-вибірка n-арних лінійних операцій, визначених на множині Q та заданих системою:

$$\begin{cases} f_1(x_1,...,x_n) = a_{11}x_1 + a_{12}x_2 + ... + a_{1n}x_n = b_1, \\ f_2(x_1,...,x_n) = a_{21}x_1 + a_{22}x_2 + ... + a_{2n}x_n = b_2, \\ ....., \\ f_n(x_1,...,x_n) = a_{n1}x_1 + a_{n2}x_2 + ... + a_{nn}x_n = b_n. \end{cases} \quad (1)$$

ортогональні, коли для кожної вибірки $b_1,...,b_n \in \mathrm{Q}$ система (1) має єдиний розв'язок.

З іншого боку система (1) має єдиний розв'язок (система ортогональна), якщо матриця

$$\begin{pmatrix} a_{11} & ... & a_{1n} \\ ... & ... & ... \\ a_{n1} & ... & a_{nn} \end{pmatrix} \quad (1)$$

оборотна, або іншими словами, коли визначник матриці A взаємно простий з модулем. Тобто $(\det A; m) = 1$.

Оскільки система (1) та матриця (1) еквівалентні, то задачу про побудову n-вибірку n-арних ортогональних квазігрупових операцій зводиться до побудови відповідної оборотної матриці.

Постає питання, за яких умов в Z_m можна побудувати оборотну матрицю, яка складається з елементів Z_m^*.

Твердження 1. *Нехай*

$$A = \begin{pmatrix} a_{11} & ... & a_{1n} \\ ... & ... & ... \\ a_{n1} & ... & a_{nn} \end{pmatrix} \quad (2)$$

$n \times n$ *матриця, де* $a_{ij} \in Z_m^*$, *та* $\det A \in Z_m^*$. *Матриця* A *оборотна тоді і тільки тоді, коли для довільних* $a_{ij} \in Z_m^*$, *для всіх* $i = 1,...,\mathrm{n}$, $j = 1,...n$ *та для* $i = 2,...,n$ *кожне*

$$a_{ii} = \left(\det A - \left(a_{i1}A_{i1} + ... + a_{\mathrm{i}(\mathrm{i}-1)}A_{\mathrm{i}(\mathrm{i}-1)}\right)\right)A_{ii}^{-1} \quad (3)$$

При умові, що $\left(\det A - \left(a_{i1}A_{i1} + ... + a_{\mathrm{i}(\mathrm{i}-1)}A_{\mathrm{i}(\mathrm{i}-1)}\right)\right) \in Z_m^*$. *Де* A_{ij} - *відповідні алгебричні доповнення, та* $A_{ii} \in Z_m^*$, *для всіх* $i = 2,...,n$.

Доведення 1) Покажемо, що (3) виконується при $n = 2$.

Нехай

$$B_2 = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

матриця розмірності 2×2 , де $a_{ij} \in Z_m^*$, та $\det B_2 \in Z_m^*$. Тоді B_2 є оборотною матрицею в Z_m, тоді і тільки тоді, коли для довільних елементів $a_{11}, a_{12}, a_{21} \in Z_m^*$, $a_{22} = \left(\det B + a_{12}a_{21}\right)a_{11}^{-1}$, при умові, що $\det B + a_{12}a_{21} \in Z_m^*$. Припустимо, що $\det B + a_{12}a_{21} \notin Z_m^*$, тоді $\left(\det B + a_{12}a_{21}\right)a_{11}^{-1} \notin Z_m^*$ та $a_{22} \notin Z_m^*$, а це суперечить вибору елемента a_{22}.

Нехай $\det B + a_{12}a_{21} \in Z_m^*$, тоді $a_{22} = \left(\det B + a_{12}a_{21}\right)a_{11}^{-1} \in Z_m^*$.

2) Покажемо істинність (3) для матриць розмірності 3×3.Нехай

$$B_3 = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & {}_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix},$$

матриця, де $a_{ij} \in Z_m^*$. З наслідку до теореми Лапласа, про розклад визначника за рядком чи стовпцем, випливає, якщо матриця B_3 оборотна, то існує принаймні один мінор розмірності 2×2 , який взаємно простий з модулем m. Тому, не втрачаючи загальності, нехай таким мінором буде

$$M_{33} = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}$$

Оскільки $M_{33} \neq 0$, то існує M_{33}^{-1}. Очевидно, що $A_{33} = M_{33}$, де A_{33} - алгебричне доповнення елемента a_{33}.

Розкладемо визначник матриці B_3 за третім рядком, отримаємо:

$$\det B_3 = a_{31}\begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix} - a_{32}\begin{vmatrix} a_{11} & a_{13} \\ a_{21} & a_{23} \end{vmatrix} + a_{33}\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}.$$

Нас цікавить випадок, коли матриця B_3 - оборотна, тобто $\det B_3 \neq 0$. Звідси отримаємо:

$$a_{33} \neq \left(a_{32}\begin{vmatrix} a_{11} & a_{13} \\ a_{21} & a_{23} \end{vmatrix} - a_{31}\begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix}\right) A_{33}^{-1}.$$

Нехай

$$a_{33} = \left(a_{32}\begin{vmatrix} a_{11} & a_{13} \\ a_{21} & a_{23} \end{vmatrix} - a_{31}\begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix}\right) A_{33}^{-1},$$

тоді

$$\det B_3 = a_{31}\begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix} - a_{32}\begin{vmatrix} a_{11} & a_{13} \\ a_{21} & a_{23} \end{vmatrix} + a_{33}\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} =$$

$$= a_{31}\begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix} - a_{32}\begin{vmatrix} a_{11} & a_{13} \\ a_{21} & a_{23} \end{vmatrix} + \left(a_{32}\begin{vmatrix} a_{11} & a_{13} \\ a_{21} & a_{23} \end{vmatrix} - a_{31}\begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix}\right) A_{33}^{-1}A_{33} = 0,$$

а це суперечить тому, що матриця B_3 - оборотна. І навпаки, нехай $\det B_3 = 0$, тоді

$$a_{31}\begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix} - a_{32}\begin{vmatrix} a_{11} & a_{13} \\ a_{21} & a_{23} \end{vmatrix} + a_{33}\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = 0,$$

а звідси маємо

$$a_{33} = \left(a_{32} \begin{vmatrix} a_{11} & a_{13} \\ a_{21} & a_{23} \end{vmatrix} - a_{31} \begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix} \right) A_{33}^{-1},$$

А це суперечить вибору елемента a_{33}.

Оскільки (3) виконується для матриць розмірності 2×2 та 3×3, тому припустимо, що (3) виконується для всіх $i = n-1$ та доведемо істинність для $i = n$. Розглянемо матрицю A (2). Якщо матриця A оборотна, то $\det A \neq 0$ та згідно наслідку до теореми Лапласа, випливає існування принаймні одного оборотного мінора розмірності $(n-1)\times(\mathrm{n}-1)$. Тому, не втрачаючи загальності, нехай таким мінором буде

$$M_{nn} = \begin{vmatrix} a_{11} & \dots & a_{1(\mathrm{n}-1)} \\ \dots & \dots & \dots \\ a_{(n-1)1} & \dots & a_{(\mathrm{n}-1)(\mathrm{n}-1)} \end{vmatrix},$$

Тоді, $A_{nn} = M_{nn}$, де A_{nn} - алгебричне доповнення елемента a_{nn}.

Розкладемо визначник матриці A за n-тим рядком, отримаємо:

$$\det A = a_{n1}A_{n1} + \dots + a_{n(\mathrm{n}-1)}A_{n(\mathrm{n}-1)} + a_{nn}A_{nn}$$

Оскільки матриця A - оборотна, то

$$a_{n1}A_{n1} + \dots + a_{n(\mathrm{n}-1)}A_{n(\mathrm{n}-1)} + a_{nn}A_{nn} \neq 0,$$

Звідси отримаємо:

$$a_{nn} \neq -\left(a_{n1}A_{n1} + \dots + a_{\mathrm{n}(\mathrm{n}-1)}A_{\mathrm{n}(\mathrm{n}-1)} \right) A_{nn}^{-1}.$$

3. АЛГОРИТМ ПОБУДОВИ n-ВИБІРКИ ОРТОГОНАЛЬНИХ ЛІНІЙНИХ n-АРНИХ КВАЗІГРУП

Як зазначалося у Розділі 2: задача про побудову n-вибірки ортогональних n-арних квазігруп, які визначені в $GF_{(p)}$, зводиться до побудови оборотних матриць розмірності $n\times n$, які складаються із ненульових елементів поля.

Розглянемо $GF_{(p)}$, де p - просте число, $a_{ij} \in GF_{(p)}^{*}$. Тоді оборотна матриця розмірності $n\times n$, яка складається із ненульових елементів поля, будується за такими кроками:

Алгоритм 1.

Крок 1. Елементи a_{ij} - обираються довільним чином із $GF_{(p)}^{*}$, крім a_{ii}, де $i \in \{2,\dots,n\}$;

Крок 2. Кожен елемент a_{ii}, де $i \in \{2,\dots,n\}$ - обирається довільним чином із $GF_{(p)}^{*}$, при умові, що $a_{ii} \neq -\left(a_{i1}A_{i1} + \dots + a_{i(i-1)}A_{i(i-1)} \right) A_{ii}^{-1}$.

Приклад . Побудуємо п’ятірку ортогональних лінійних квазігруп арності п’ять, які визначені над Z_{11}.

Будуємо оборотну матрицю розмірності 5×5, яка складається із ненульових елементів Z_{11} за алгоритмом 1.

1. $a_{ij} \in Z_{11}^{*}$, обираємо довільним чином, крім a_{ii}, де $i = 2,\dots,5$. Нехай матриця A має вигляд:

$$A=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 6 & a_{22} & 7 & 8 & 9 \\ 10 & 1 & a_{33} & 2 & 3 \\ 4 & 5 & 6 & a_{44} & 7 \\ 8 & 9 & 10 & 1 & a_{55} \end{pmatrix};$$

2. Обираємо a_{22} таке, що $a_{22} \neq 6\cdot 2\cdot 1^{-1}$, $a_{22} \neq 1$. Нехай $a_{22}=2$;

3. Обираємо a_{33} таке, що $a_{33} \neq \left(1\begin{vmatrix} 1 & 3 \\ 6 & 7 \end{vmatrix} - 10\begin{vmatrix} 2 & 3 \\ 2 & 7 \end{vmatrix}\right)\cdot 1^{-1}$. $a_{33} \neq 3$. Нехай $a_{33}=1$.

4. Обираємо a_{44} таке, що

$$a_{44} \neq \left(4\begin{vmatrix} 2 & 3 & 4 \\ 2 & 7 & 8 \\ 1 & 1 & 2 \end{vmatrix} - 5\begin{vmatrix} 1 & 3 & 4 \\ 6 & 7 & 8 \\ 10 & 1 & 2 \end{vmatrix} + 6\begin{vmatrix} 1 & 2 & 4 \\ 6 & 2 & 8 \\ 10 & 1 & 2 \end{vmatrix}\right)\cdot 4^{-1}\cdot$$

$a_{44} \neq 5$. Нехай $a_{44}=1$.

5. Обираємо a_{55} таке, що

$$a_{55} \neq \left(9\begin{vmatrix} 1 & 3 & 4 & 5 \\ 6 & 7 & 8 & 9 \\ 10 & 1 & 2 & 3 \\ 4 & 6 & 1 & 7 \end{vmatrix} - 10\begin{vmatrix} 1 & 2 & 4 & 5 \\ 6 & 2 & 8 & 9 \\ 10 & 1 & 2 & 3 \\ 4 & 5 & 1 & 7 \end{vmatrix} + 1\begin{vmatrix} 1 & 2 & 3 & 5 \\ 6 & 2 & 7 & 9 \\ 10 & 1 & 1 & 3 \\ 4 & 5 & 6 & 7 \end{vmatrix} - 8\begin{vmatrix} 2 & 3 & 4 & 5 \\ 2 & 7 & 8 & 9 \\ 1 & 1 & 2 & 3 \\ 5 & 6 & 1 & 7 \end{vmatrix}\right)\cdot 6^{-1},\ a_{55} \neq 3.$$

Нехай $a_{55}=1$.

6. Як результат, матриця A матиме вигляд

$$A=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 6 & 2 & 7 & 8 & 9 \\ 10 & 1 & 1 & 2 & 3 \\ 4 & 5 & 6 & 1 & 7 \\ 8 & 9 & 10 & 1 & 1 \end{pmatrix};$$

7. Виписуємо систему лінійних квазігрупових операцій, які є ортогональними за побудовою:

$$\begin{cases} f_1(x_1,x_2,x_3,x_4,x_5)=1x_1+2x_2+3x_3+4x_4+5x_5=c_1; \\ f_2(x_1,x_2,x_3,x_4,x_5)=6x_1+2x_2+7x_3+8x_4+9x_5=c_2; \\ f_3(x_1,x_2,x_3,x_4,x_5)=10x_1+1x_2+1x_3+2x_4+3x_5=c_3; \\ f_4(x_1,x_2,x_3,x_4,x_5)=4x_1+5x_2+6x_3+1x_4+7x_5=c_4; \\ f_5(x_1,x_2,x_3,x_4,x_5)=8x_1+9x_2+10x_3+1x_4+1x_5=c_5. \end{cases}$$

де x_1,x_2,x_3,x_4,x_5 - відкритий текст, c_1,c_2,c_3,c_4,c_5 зашифрований текст.

4. ОЦІНЮВАННЯ КРИПТОГРАФІЧНОЇ СТІЙКОСТІ

Розглянемо довільну скінченну множину простого порядку p. Згідно алгоритму побудови матриці розмірності $n\times n$, n^2-n+1 елемент обираються довільним чином і на кожному місці може проймати $p-1$ значення, інші $n-1$ елементів матриці можуть набувати $p-2$ значень.

Звідси отримаємо таке співвідношення:

$$M_n=(p-1)^{n^2-n+1}(p-2)^{n-1}$$

де M_n - кількість оборотних матриць розмірності $n \times n$ на множині простого порядку p, які складаються із не нульових елементів.

Для прикладу візьмемо англійський алфавіт (великі та малі літери, 52 елемента), цифри від 0 до 9 (10 елементів), і для того щоб отримати множину простого порядку доповнимо 21-м спеціальними символами. Отримаємо $p = 83$. Нехай ми шифруємо послідовності по 8 бітів, тоді і розмірності матриць мають бути 8×8.

Звідси отримаємо $M_8 = (83-1)^{8^2-8+1}(83-2)^{8-1} = 82^{57} \times 81^7$, це досить велика кількість для взлому методом грубої сили.

Для підвищення стійкості алгоритму доцільно використовувати не одну матрицю, а множину матриць різної розмірності та застосовувати їх у довільному порядку, відповідно розбиваючи інформаційну послідовність, що значно підвищить стійкість алгоритму.

ВИСНОВКИ

У роботі розроблено математичні основи модифікації шифру Гілла на базі систем багатомісних ортогональних квазігруп, що дозволяє розширити функціональні можливості класичного матричного криптографічного підходу та підвищити його криптографічну ефективність. Запропонована модель забезпечує однозначність процесів шифрування та дешифрування завдяки використанню ортогональних *n* операцій.

Отримано такі теоретичні та практичні результати:

1. Встановлено необхідні та достатні умови побудови оборотних матриць над скінченними полями лишків, елементи яких не містять нульових значень. Отримані теоретичні результати створюють математичне підґрунтя для формування широкого класу криптографічних ключів довільної розмірності та забезпечують можливість побудови систем ортогональних квазігруп із заданими властивостями.
2. Запропоновано універсальний алгоритм синтезу n-вибірок ортогональних лінійних *n* квазігруп, який дозволяє ефективно генерувати ключові матриці для криптографічних застосувань. Перевагою алгоритму є його масштабованість, можливість використання для різних розмірностей матриць та адаптація до множин як простого, так і складеного порядку за відповідних обмежень.
3. Проведена оцінка криптографічної стійкості показала, що зі збільшенням розмірності матриць кількість можливих ключів зростає експоненціально, що значно ускладнює реалізацію атак методом грубої сили. Додаткове використання декількох матриць різної розмірності та їх випадкове чергування дозволяє суттєво підвищити рівень захисту інформації.
4. Практична цінність дослідження полягає у можливості застосування отриманих результатів для розроблення перспективних блочних шифрів, засобів захисту даних у комп'ютерних мережах, телекомунікаційних системах, інформаційних ресурсах критичної інфраструктури та спеціалізованих програмно-апаратних комплексах криптографічного захисту інформації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ / REFERENCES

1. L.S. Hill, "Cryptography in an algebraic alphabet", American mathematical monthly, vol.36, NO.6, pp. 306-312, 1929. DOI: 10.1080/00029890.1929.11986963
2. O. Gutik, O. Popadiuk, Modified Hill cipher with noise and permutation, Bulletin of Lviv University. Applied Mathematics and Computer Science Series, No. 35, 2025. DOI: 30970/vam.2025.35.13682
3. Mann H.B. The construction of orthogonal Latin squares. Ann. Math. Statist. – 1942. – 13, P – 418-423.
4. Paige L.J. A note on finite abelian groups. Bull. Amer. Math. Soc. – 1947. – 53. DOI: https://doi.org/10.1090/S0002-9904-1947-08856-X
5. Hall M. A combinatorial problem on Abelian groups. Proc. 34 Amer. Math. Soc. – 1952. – 3.
6. Belyavskaya G., Mullen G. L. Orthogonal hypercubes and n-ary operations. Qasigroup Related Systems 13(2005), no. 1, 73-86. Посилання на PDF (math.md)
7. Keedwell D., Denes J. Latin Squares and their Applications // Second Edition – 2015. – P. 440. DOI: 10.1016/C2014-0-03412-0

8. Fryz I.V., Sokhatsky F.M. Block composition algorithm for constructing orthogonal n-ary operations // Discrete Math – 2017. – № 340. – P. 1957--1966. http://dx.doi.org/10.1016/j.disc.2016.11.012
9. Fryz I.V. Orthogonality and retract orthogonality of operations // Bul. Acad. Stiinte Repub. Mold. Mat – 2018. – № 1(86). – P. 24-33.
10. Fryz I.V. Algorithm for the complement of orthogonal operations // Comment. Math. Univ. Carolin – 2018. – № 59,2. – P. 135-151. http://dx.doi.org/10.14712/1213-7243.2015.241
11. Markovski S., Mileva A. On construction of orthogonal d-ary operations // De L'institute masemateque. Nouvelle serie – 2017–№ 101(115). – P. 109-119. Markovski S., Mileva A. On Construction of Orthogonal d-ary Operations (PDF)

Дата надходження: 5.02.2026
Дата прийняття до друку після рецензування: 1.04.2026
Дата публікації: 18.06.2026

САВЧУК ВІКТОР ДМИТРОВИЧ – асистент кафедри захисту інформації, Вінницький національний технічний університет, ***e-mail: savchukvd@ukr.net,***
https://orcid.org/0009-0003-5885-4455

Victor SAVCHUK

INFORMATION ENCRYPTION BY THE GIL METHOD USING THE SYMBOLS OF MULTIPLE ORTHOGONAL QUASIGROUPS OVER A FIELD OF REDUNDANCY

Vinnytsia National Technical University, Vinnytsia, Ukraine