Міністерство освіти і науки України
Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації

Комплексна бакалаврська дипломна робота на тему:

«Засіб шифрування на основі квазігрупи. Частина 1. Реалізація квазігрупи»

Виконав: студент 4 курсу групи 1БС-19 б
спеціальності 125 Кібербезпека
_____ Пилявець І. Ю.
Керівник: к. ф.-м. н., доцент каф. ЗІ
_____ Шелепало Г. В.
«17» червня 2022 р.
Рецензент: к. т. н., доц., доц. каф. ПЗ
_____ Майданюк В. П.
«19» червня 2023 р.

Допущено до захисту
Завідувач кафедри ЗІ
д. т. н., проф.
_____ Лужецький В. А.
«19» червня 2023 р.

Вінниця ВНТУ – 2023 року

Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації
Рівень вищої освіти І (бакалаврський)
Галузь знань – 12 Інформаційні технології
Спеціальність – 125 Кібербезпека
Освітньо-професійна програма – Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖУЮ
Зав. кафедри ЗІ, д. т. н., проф.
_____ В. А. Лужецький
_____ 2023 року

З А В Д А Н Н Я
НА КОМПЛЕКСНУ БАКАЛАВРСЬКУ ДИПЛОМНУ РОБОТУ СТУДЕНТУ

Пилявцю Ігорю Юрійовичу

1. Тема роботи: «Засіб шифрування на основі квазігрупи. Частина І: Реалізація квазігрупи»,
   керівник роботи: Шелепало Галина Василівна к.ф.-м.н., доцент, затверджені наказом ректора ВНТУ від 20 березня 2023 року №67.
2. Строк подання студентом роботи 17 червня 2023 р.
3. Вихідні дані до роботи:
   - приклади використання квазігруп у криптографії;
   - сучасні алгоритми шифрування на основі квазігруп;
   - вимоги до засобів LW-криптографії.
4. Зміст текстової частини: Вступ. 1 Аналіз літератури та вибір методів дослідження. 2 Програмний засіб для обчислення квазігруп. 3 Логічні схеми CIP-квазігруп. Висновки. Список використаних джерел. Додатки.
5. Перелік ілюстративного матеріалу: схема роботи програмного засобу, таблиці Келі CIP-квазігруп 4-го порядку, таблиця взаємно оборотних пар CIP-квазігруп, квазігрупа 16-го порядку, таблиця Келі групи Кляйна, таблиця істинності для всіх CIP-квазігруп 4-го порядку, діаграма Вейча.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Шелепало Г. В., к. ф.-м. н., доцент	20.03.2023	16.06.2023
2	Шелепало Г. В., к. ф.-м. н., доцент	20.03.2023	16.06.2023
3	Шелепало Г. В., к. ф.-м. н., доцент	20.03.2023	16.06.2023

7. Дата видачі завдання: 20 березня 2023 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської дипломної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз завдання. Вступ	20.03.23 – 26.03.23	
2	Аналіз інформаційних джерел за напрямком комплексної бакалаврської дипломної роботи	27.03.23 – 09.04.23	
3	Розробка моделей та алгоритмів	10.04.23 – 23.04.23	
4	Результати реалізації	24.04.23 – 21.05.23	
5	Висновки	22.05.23 – 24.05.23	
6	Оформлення пояснювальної записки	25.05.23 – 31.05.23	
7	Попередній захист БДР	01.06.23 – 15.06.23	
8	Виправлення зауважень, підготовка ілюстративного матеріалу	16.06.23 – 19.06.23	
9	Представлення БДР до захисту, рецензування	20.06.23 – 23.06.23	
10	Захист БДР	20.03.23 – 26.03.23	

Студент _____ Ігор ПИЛЯВЕ

Керівник роботи _____ Галина ШЕЛЕПА

АНОТАЦІЯ

Комплексна бакалаврська дипломна робота складається з 67 сторінок формату А4, на яких є 38 рисунків, 5 таблиці, список використаних джерел, що налічує 30 найменувань.

Комплексною бакалаврською дипломною роботою пропонується новий підхід до потокового шифрування на основі квазігруп. Зокрема, розглядається використання квазігруп 4-го порядку зі спеціальними властивостями схрещеної оборотності. Цей математичний інструмент відкриває нові можливості для поліпшення ефективності та безпеки шифрування, а також дозволяє збільшити обчислювальну стійкість криптографічних систем, що базуються на квазігрупах. Сформовано логічні функції CIP-квазігруп та обчислено апаратні витрати для їх реалізації.

Ключові слова: захист інформації, квазігрупи, LW-криптографія, безпека, крипто примітив.

ABSTRACT

The bachelor thesis consists of 67 pages of A4 format, on which there are 38 figures, 5 tables, the list of used sources contains 30 names.

A comprehensive bachelor's thesis proposes a completely new approach to stream encryption based on quasigroups. In particular, the use of fourth-order quasigroups with special properties of crossed reversibility is considered. This approach opens up new possibilities for improving the efficiency and security of encryption, and also allows to increase the computational stability of cryptographic systems based on quasigroups. The logical functions of CIP-quasigroups were formed and the hardware costs for their implementation were calculated.

Keywords: information protection, quasigroups, LW-cryptography, security, crypto primitive.

ЗМІСТ

ВСТУП 4
1 АНАЛІЗ ЛІТЕРАТУРИ ТА ВИБІР МЕТОДІВ ДОСЛІДЖЕННЯ 6
1.1 Поняття квазігрупи: застосування та обґрунтування 6
1.2 Огляд інформаційних джерел: розвиток дослідження 8
1.3 Означення та властивості квазігруп (латинських квадратів) 15
1.4 Використання квазігруп у криптографії 19
Висновки до розділу 23
2 ПРОГРАМНИЙ ЗАСІБ ДЛЯ ОБЧИСЛЕННЯ КВАЗІГРУП 25
2.1 Канонічний розклад CIP-квазігрупи (латинського квадрату) 25
2.2 Прямий добуток квазігруп (латинських квадратів) 28
2.3 Розробка засобу для побудови латинських квадратів різних порядків 31
2.3.1 Вибір мови програмування 31
2.3.2 Середовище розробки 35
2.3.3 Опис програмного засобу 36
2.3.4 Результат роботи та тестування програмного засобу 37
Висновки до розділу 40
3 ЛОГІЧНІ СХЕМИ CIP-КВАЗІГРУП 41
3.1 Логічні функції 41
3.2 Мінімізація на основі діаграм Вейча 42
3.3 Синтез логічних схем 43
3.4 Перетворення виразів з урахуванням базису 56
Висновки до розділу 60
ВИСНОВКИ 62
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 65
Додаток А ПЕРЕЛІК ПУБЛІКАЦІЙ ЗА ТЕМОЮ 69
Додаток Б АПРОБАЦІЯ РЕЗУЛЬТАТІВ ДОСЛІДЖЕНЬ 70
Додаток В КОД ПРОГРАМНОГО ЗАСТОСУНКУ 71
Додаток Г ПРОТОКОЛ ПЕРЕВІРКИ БАКАЛАВРСЬКОЇ ДИПЛОМНОЇ РОБОТИ НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ 74

ВСТУП

Сьогодні за допомогою мобільних пристроїв та інших різних ґаджетів можна легко в режимі реального часу, не виходячи із дому, здійснювати покупки чи продажі, сплачувати платежі, здійснювати банківські операції, керувати пристроями в системах розумних будинків віддалено. Це, в свою чергу, вимагає забезпечення захисту конфіденційності інформації, що передається. Тому, в теперішніх реаліях, стає все більш важливим завданням розробити такий захист інформації. Інструментами для забезпечення конфіденційності інформації є алгоритми шифрування, які займають центральне місце в безпеці даних. В найрізноманітніших пристроях з обмеженими обчислювальними можливостями використовується потокове шифрування.

На сьогоднішній день алгоритми шифрування на основі квазігруп успішно використовуються, але дослідження в цій галузі ще не вичерпали свій потенціал. Існує потреба у подальшому вивченні та розвитку квазігрупових алгоритмів шифрування з метою покращення їх ефективності та організації безпеки на їх основі.

Розвиток технологій в напрямку зменшення розмірів апаратури, який створює попит на пристрої, що можуть бути реалізовані в малоресурсних системах, обґрунтовує розробку нових алгоритмів потокового шифрування для LW-криптографії на основі квазігруп, що і є актуальністю бакалаврської дипломної роботи.

Об'єктом дослідження є процес потокового шифрування на основі квазігруп (латинських квадратів).

Предметом дослідження є методи побудови квазігруп різних порядків та засоби, що їх реалізують.

Метою бакалаврської роботи є зменшення апаратних витрат засобу потокового шифрування шляхом використання середніх CIP-квазігруп 4-го порядку з функцією оборотності x^2 серед ізотопів групи Кляйна. Для досягнення поставленої мети сформовано такі задачі:

- здійснити аналіз квазігруп як криптографічного примітиву ;
- побудувати квазігрупи вищих порядків;
- синтезувати логічні схеми, що реалізують квазігрупи та мінімізувати формули для апаратної частини шифрування.

Проміжні результати дослідження знайшли своє втілення у таких роботах:

1) CIP-квазігрупи 4-го порядку з оборотним елементом X2 серед ізотопів групи Клейна [1].

2) Алгоритм шифрування на основі CIP-квазігруп [2].

3) Концепція шифру на основі CIP-квазігруп [3].

4) Огляд методів шифрування за допомогою квазігрупових операцій [4].

5) Комп'ютерна програма "Тестування множини непарних складених чисел на приналежність до Кармайклових чисел" [5].

1 АНАЛІЗ ЛІТЕРАТУРИ ТА ВИБІР МЕТОДІВ ДОСЛІДЖЕННЯ

Даний розділ присвячений аналізу літературних джерел, розвитку досліджень квазігруп, їх властивостям та використанню у криптографії.

1.1 Поняття квазігрупи: застосування та обґрунтування

Математичний інструмент «квазігрупа» використовується для описання різних алгебричних структур з огляду на застосування в різних галузях науки. Здебільшого, квазігрупи почали вивчатися, як об’єкти, що мають схожі властивості до груп, але не групи і не напівгрупи. Квазігрупа є загальним поняттям, що допускає більш широкий спектр можливих операцій та відповідних оборотних властивостей.

Поняття «групи» було введено раніше, ніж поняття «квазігрупи». Група в математиці відіграє центральну роль і є одним з фундаментальних об'єктів в алгебрі. Вона була вивчена та формалізована ще в XIX столітті. Концепція «групи» розроблялася протягом довгого періоду часу і включала роботу багатьох математиків. Її поява пов'язана з дослідженням властивостей симетрії, переставних законів та операцій над різними об'єктами. Ранні форми дослідження групи можна прослідкувати ще у роботах Карла Фрідріха Гаусса, Леонарда Ейлера та Жозефа-Луї Лагранжа.

Поняття «квазігрупи», як самостійної алгебраїчної структури, з'явилося пізніше. Воно було вперше введено українськи алгебрист Антон Казимирович Сушкевич з Харкова і започаткував вивчення квазігруп в своїй праці [6]. Батьком розвитку квазігрупової теорії вважають Валентина Даниловича Білоусова, який жив і працював у Кишиневі, республіка Молдова [7].

Основна відмінність квазігрупи від групи полягає в тому, що в квазігрупі не всі елементи мають обернений елемент. Тобто, для деяких елементів може бути неможливо знайти такий елемент, що комбінується з даним так, щоб отримати одиничний елемент. В інших випадках можуть існувати кілька можливих комбінацій для отримання одного й того ж результату.

Квазігрупи виникли як спеціальний клас алгебричних структур, що були досліджені та використовувалися у різних галузях математики, комбінаторики, статистики, фізики та інших прикладних наукових дисциплінах. Вони виявилися корисними для моделювання різних процесів та аналізу систем, де операції можуть мати обмежені або часткові властивості групи.

Вивчення квазігруп продовжується і сьогодні. Вона залишається об'єктом активних досліджень не лише в математиці, але й інших наукових дисциплінах. Квазігрупи знайшли застосування у таких галузях, як алгебра (групова операція, рівняння і тотожності), математичний аналіз (оборотна функція, функційні рівняння), геометрія (номограма, сітка, гратка), криптографія (код, шифр, геш-функція тощо), фізика (симетрія фізичних частинок та полів), комбінаторика (латинські квадрати), статистика (модель розподілу взаємодії процесу та явищ), теорія автоматів (графи та мультиграфи), економіка, сільське господарство та багато інших.

У криптографії, наприклад, квазігрупи використовуються для побудови криптографічних протоколів, систем та алгоритмів шифрування, теорії кодів та побудови геш-функцій. Вони дозволяють реалізувати різні операції шифрування та дешифрування з певними комбінаторними властивостями, що забезпечують безпеку та надійність системи.

У фізиці квазігрупи використовуються для вивчення симетрій та взаємодій між фізичними частинками та полів. Вони допомагають аналізувати та описувати різні фізичні системи з точки зору їх симетрій та властивостей.

У загальній математиці та комбінаториці квазігрупи використовуються для моделювання та вивчення різних комбінаторних структур, таких як множини з операціями, що мають обмежені або часткові властивості групи. Вони дозволяють аналізувати та класифікувати різні комбінаторні об'єкти та вирішувати складні комбінаторні задачі. Наприклад, в комбінаториці, квазігрупа – це операція, яка зображена у вигляді таблиці Келі, результатом множення елементів якої є латинський квадрат, тобто квадратна таблиця, що задана

символами скінченної множини так, щоб кожний елемент цієї множини зустрічався точно один раз в кожному рядку і точно один раз в кожному стовпці.

Таким чином, поняття квазігрупи є важливим та актуальним у математиці, алгебрі та комбінаториці. Воно виникло з потреби описувати алгебричні структури з певними комбінаторними властивостями, що можуть відрізнятися від властивостей групи. Квазігрупи знаходять застосування в різних галузях науки та дозволяють аналізувати та моделювати різноманітні процеси та системи.

1.2 Огляд інформаційних джерел: розвиток дослідження

Одним із основних авторитетних інформаційних джерел, де описано застосування теорії квазігруп, луп та пов’язаних з ними алгебричних структур є книга «Квазігрупи і лупи: теорія і застосування», видана у 1990 році Галиною Орлик-Пфлугфельдер, Джонатаном Д. Х. Смітом і Оріном Чейном, в якій описано історичний розвиток застосування квазігруп та луп, починаючи з 1943 по 1990 роки [8].

Книга розпочинається з опису основних понять, властивостей та допоміжних тверджень для розуміння теорії квазігруп, луп, кубів, гіперкубів та їх комбінаторних аналогів. Автори досліджують основні алгебричні властивості квазігруп, зокрема, важливу увагу приділено асоціативності, медіальності (бісиметрії), дистрибутивності, симетричності та лупам Муфанг. Вони розглядають різні класи квазігруп та вивчають властивості кожного окремого класу для застосування.

Детально описані дослідження різних аспектів застосування квазігруп та луп у деяких галузях науки. Зокрема, наведено приклади застосування квазігруп у криптографії, комбінаториці, теорії кодування та математичній фізиці. Наприклад, автори розглядають використання квазігруп для побудови ефективних, на той час, криптографічних протоколів, а також для кодування та декодування інформації. Вони вивчають роль квазігруп у структурах, що

виникають у фізичних теоріях, в механіці, в апаратурі та досліджують квазігрупові зв'язки з іншими алгебричними конструкціями для застосування.

Вклад Галини Орлик-Пфлугфельдер у науку полягає в тому, що зроблений історичний огляд використання теорії квазігруп розширює розуміння про квазігрупи та лупи, їх властивості та практичне застосування. Дані дослідження сприяють розвитку алгебричних структур та відкривають нові можливості для використання квазігруп у різних галузях науки та технологій. Вони не тільки вивчають основні концепції та теоретичні аспекти, але й наводять конкретні практичні приклади та описують застосування, що допомагають краще зрозуміти поданий матеріал.

Книга Джонатана Д. Х. Сміта «Вступ до квазігруп та їх представлення» [9] є важливим джерелом інформації для студентів, науковців і фахівців, які цікавляться алгеброю, теорією кодування, криптографією та галузями математики. Вона сформована так, що стимулює до нових досліджень і відкриттів у цих важливих галузях математики. Книга допомагає отримати детальні знання про різноманітні алгебричні структури: квазігрупи, лупи, оборотні функції, мультиплікативні таблиці та обернені операції. У вступних розділах книги подано структуровані основні поняття та виведено властивості квазігруп, парастрофні перетворення, симетричність, інвертованість, асоціативність та бісиметрія (медіальність). Автор глибоко досліджує різні аспекти квазігруп та їх представлення, подає їх у різних формах, зображеннях: формулами, таблицями, словесно. Описує різні методи та конструкції для представлення квазігруп, включаючи канонічні форми, групові розширення та інші. Вивчаються властивості та особливості різних класів квазігруп, зокрема розподільні квазігрупи, лупи та інверсні квазігрупи.

Основний вклад Д. Сміта у науку – це дослідження з теорії квазігруп та їх застосування в криптографії, що розширює розуміння про цю важливу математичну структуру для використання шифрів. Автор вивчає властивості та структури квазігруп, їх відношення з іншими алгебричними конструкціями, досліджує роль квазігруп та луп у різних областях, зокрема в криптографії.

Квазігрупи мають потенціал для застосування у криптографічних примітивах, а автор книги надає базові поняття та методи, що можуть бути корисними для подальших досліджень та розробок у цій галузі.

Найновішою книгою із застосування квазігруп та латинських квадратів є книга «Латинські квадрати та їх застосування» Дональда Кідвела та Джозефа Денеша за 2015 рік [10]. Це друге видання, доповнене та уточнене відповідно до нових досліджень та отриманих результатів щодо застосування латинських квадратів у різних галузях.

У книзі автори починають з визначення латинських квадратів та їх основних властивостей. Латинський квадрат – це квадратна матриця розмірністю n × n, де кожен рядок і кожний стовпець містять різні елементи зі множини 1 до n. Основна властивість латинських квадратів – відсутність повторень в рядках і стовпцях.

Книга розглядає різні методи побудови латинських квадратів, такі як методи методів Боуэрса, Латушека, Ітані, а також методи на основі блочного проектування та комбінаторних структур. Автори досліджують властивості цих методів та їх застосування в різних областях, включаючи дизайн експериментів, кодування і комбінаторику.

У книзі також розглядаються розширення латинських квадратів, такі як мультиплікативні латинські квадрати, латинські квадрати з обмеженнями, латинські квадрати з додатковими властивостями тощо. Автори досліджують структуру цих розширень і їх використання в різних дисциплінах.

Книга також пропонує приклади реальних застосувань латинських квадратів, таких як планування експериментів у статистиці, розкладання розкладок, розкладання матриць, розподіл графів, графічні дизайни, кодування і декодування, ігри та криптографія.

"Latin Squares and Their Applications" є комплексним джерелом інформації про латинські квадрати, їх властивості та застосування. Книга призначена для студентів, вчених і дослідників, які цікавляться комбінаторикою, дизайном

експериментів, математикою та іншими галузями, де латинські квадрати використовуються.

Наступним евристичним виданням із застосування даного напрямку є зібрання статей у монографії Віктора Щербакова за 2017 рік [11]. Ця книга присвячена вивченню та дослідженню квазігруп, їх структури, властивостей та застосувань у різних галузях математики та інших наук.

У книзі автор розпочинає з визначення квазігруп та їх основних властивостей. Квазігрупа – це множина з операцією, яка задовольняє умову лівої та правої дистрибутивності. Автор досліджує різні типи квазігруп, включаючи латинські квазігрупи, групоподібні квазігрупи, неперетинні квазігрупи та багато інших.

У книзі детально розглядаються властивості квазігруп, такі як асоціативність, обернені елементи, ліва та права ідентичність, квазіінверсність та інші. Автор також досліджує питання існування та конструкції квазігруп з певними властивостями.

Книга присвячена не лише теоретичним аспектам квазігруп, але також розглядає їх застосування в різних галузях, таких як комбінаторика, криптографія, кодування, стеганографія, теорія графів та дизайн експериментів. Автор надає приклади та застосування квазігруп у цих галузях, досліджує їх властивості та пропонує нові підходи до вирішення задач за допомогою квазігруп.

"Inverse Properties in Neutrosophic Triplet Loop and Their Application to Cryptography" є дослідженням, що розглядає взаємозв'язок між нейтрософічними тріплетними петлями, оберненими елементами та їх застосуванням у криптографії. Нейтрософічні тріплетні петлі є спеціальним класом квазігруп, які використовуються в алгебрі та криптографії для моделювання та розробки криптографічних протоколів та систем [12].

В рамках цього дослідження, автори глибоко вивчають поняття та властивості нейтрософічних тріплетних петель. Вони аналізують основні операції, такі як множення, додавання та віднімання, та їх властивості, зокрема

асоціативність, однозначність та інверсійність. Особлива увага приділяється вивченню обернених елементів у нейтрософічних тріплетних петлях, включаючи їхню унікальну поведінку та взаємозв'язок з іншими елементами.

Далі автори досліджують можливості застосування нейтрософічних тріплетних петель у криптографії. Вони розглядають використання цих петель для розробки криптографічних протоколів та систем шифрування, аутентифікації та цифрового підпису. Вони вивчають стійкість та безпеку таких систем, зосереджуючись на особливостях нейтрософічних тріплетних петель та їх впливі на криптографічні алгоритми та протоколи.

Автори вносять значний вклад у дослідження квазігруп та криптографії, розширюючи наше розуміння про застосування нейтрософічних тріплетних петель у криптографічних системах. Вони проводять теоретичний аналіз властивостей цих петель та їхній взаємозв'язок з криптографічними конструкціями, а також пропонують нові підходи до розробки криптографічних протоколів, які базуються на нейтрософічних тріплетних петлях. Їхні дослідження мають потенціал для вдосконалення безпеки та ефективності криптографічних систем у реальних застосуваннях.

"International Journal of Mathematical Combinatorics, Volume 2, 2011" є науковим журналом, який публікує статті та дослідження з математичної комбінаторики, включаючи теми, пов'язані з квазігрупами та криптографією. В даному журналі автори вносять свій внесок у розвиток цих областей шляхом публікації оригінальних досліджень, нових підходів та результатів своїх досліджень [13].

У даному томі журналу автори можуть досліджувати різні аспекти квазігруп та їх застосування в криптографії. Вони можуть досліджувати алгебраїчні та комбінаторні властивості квазігруп, розвивати нові методи для аналізу та класифікації цих структур, а також досліджувати їх застосування у криптографічних протоколах та системах.

Внесок авторів полягає у тому, що вони представляють нові ідеї, теоретичні концепції та експериментальні докази, які сприяють розвитку квазігруп та

криптографії. Вони можуть пропонувати нові алгоритми шифрування, методи аутентифікації або протоколи для обміну ключами, які ґрунтуються на властивостях квазігруп та використовуються для забезпечення безпеки в інформаційних системах.

Крім того, автори можуть внести свій внесок у теоретичну аспект квазігруп та криптографії шляхом розробки нових математичних моделей, алгоритмів або підходів, які покращують ефективність та безпеку криптографічних систем. Їхні дослідження можуть стати основою для подальших досліджень та розробки нових методів захисту інформації.

Загалом, "International Journal of Mathematical Combinatorics, Volume 2, 2011" відіграє важливу роль у сприянні обміну ідеями та публікації нових результатів у сфері квазігруп та криптографії. Внесок авторів у цей журнал допомагає просувати ці області досліджень вперед, сприяючи розвитку нових методів та забезпеченню безпеки інформаційних систем.

Стаття "A Public Key Block Cipher Based on Multivariate Quadratic Quasigroups" описує новий алгоритм блочного шифрування з використанням квазігруп мультиваріативних квадратних типу. Автори статті пропонують новий підхід до розробки криптографічних алгоритмів, який базується на властивостях квазігруп [14].

Квазігрупи є алгебраїчними структурами, які використовуються в криптографії для побудови стійких криптографічних примітивів, таких як шифри, підписи та інші. Квазігрупи мають особливі властивості, що робить їх цікавими для застосування у криптографії.

У статті автори описують побудову алгоритму блочного шифрування з використанням квазігруп мультиваріативних квадратних типу. Вони представляють математичні основи алгоритму, включаючи використання квазігруп для забезпечення безпеки шифрування та розшифрування.

Внесок у дослідження квазігруп полягає в розробці нового криптографічного алгоритму, який базується на використанні квазігруп мультиваріативних квадратних типу. Цей алгоритм може мати важливе значення

для розвитку криптографії після квантового комп'ютера, оскільки квазігрупи можуть виконувати ключову роль у стійких криптографічних протоколах, що залишаються стійкими навіть у випадку появи квантових комп'ютерів.

Ця стаття може бути корисним джерелом інформації для дослідників та професіоналів, які працюють у галузі криптографії, особливо тих, хто зацікавлений у використанні квазігруп у криптографічних системах та протоколах.

Стаття "Large quasigroups in cryptography and their properties testing" авторства J. Dvorsky tas співавторів є важливим дослідженням, яке представлене на конференції "2009 World Congress on Nature & Biologically Inspired Computing (NaBIC 2009)". Ця стаття зосереджена на використанні великих квазігруп у криптографії та проведенні тестування їхніх властивостей [15].

У сфері криптографії квазігрупи використовуються для побудови безпечних криптографічних систем. Автори статті досліджують потенційні можливості використання великих квазігруп у таких примітивах, як шифрування та підписи. Вони аналізують різні аспекти використання квазігруп, включаючи їх стійкість до атак, ефективність алгоритмів на основі квазігруп та відповідність до криптографічних вимог.

Окрім цього, стаття також зосереджена на тестуванні властивостей квазігруп, що має важливе значення для їхнього використання в криптографічних системах. Автори пропонують методи тестування, що дозволяють перевірити властивості квазігруп, такі як асоціативність та комутативність. Це допомагає забезпечити коректність та безпеку криптографічних примітивів на основі квазігруп.

Внесок даної статті в дослідження квазігруп в криптографії полягає у розширенні наших знань про потенційні можливості використання великих квазігруп у криптографічних системах. Аналізуючи їхні властивості та тестуючи їх, ми отримуємо глибше розуміння про придатність квазігруп для застосування в криптографії. Це може призвести до розробки нових методів і алгоритмів, а також до покращення безпеки криптографічних систем в пост-квантовій епохи.

1.3 Означення та властивості квазігруп (латинських квадратів)

В бакалаврській дипломній роботі розглядаються операції, що визначені на одній і тій же множині. Таку множину називають базовою (носій) і позначають через Q. Операції досліджуються на множині бінарних операцій (функцій). Бінарні операції – це ті, в яких дві невідомих змінних визначаються третьою змінною.

Бінарною операцією (двомісною функцією), яка визначена на деякій множині, є відображенням квадрату цієї множини в себе.

Функція, що визначена на скінченій чи нескінченній множині називається квазігруповою (оборотною), якщо вона оборотна по кожній своїй змінній.

Функції (операції) позначаються префіксними символами

$$f(x; y) = z$$

та інфіксними символами

$$x \cdot y = z$$

Тотожне інфіксне позначення між двома символами змінних x та y будемо опускати, тобто запис матиме вигляд xy, розуміючи при цьому, що між цими двома змінними x та y знаходиться операція $(\cdot)$.

Операцію f називають лівооборотною, якщо довільний її правий зсув є підстановкою базової множини. Інакше кажучи, якщо рівняння

$$f(x; a) = b$$

має єдиний розв'язок для всіх a, b із Q. Тоді розв'язок цього рівняння позначається через

$$^{\ell}f(b; a) = x$$

Очевидно, що $^{\ell}f$ є бінарною операцією, яку називають лівим діленням (спряженням) операції f і виконуються перша та друга тотожності з

$$f(^{\ell}f(x; y); y) = x, \qquad ^{\ell}f(f(x; y); y) = x, \tag{1.1}$$
$$f(x; {}^{r}f(x; y)) = y, \qquad {}^{r}f(x; f(x; y)) = y.$$

Аналогічно визначається правооборотна операція і праве ділення (спряження) ^{r}f, для якого виконуються третя і четверта рівності із (1.1).

Функція f називається оборотною або квазігруповою, якщо вона є правооборотною і лівооборотною. При цьому тотожності називаються визначальними або первинними, а групоїд $(Q;\ f)$ називається квазігрупою. В літературі відоме інше простіше означення квазігрупи, де позначення операцій подане в інфіксному вигляді. Квазігрупа – це групоїд $(Q;\cdot)$ такий, що для довільних елементів $a,\ b$ елементів з базової множини Q система рівнянь

$$a\cdot x=b$$

$$y\cdot a=b$$

має єдиний розв'язок.

Квазігрупа називається лупою, якщо вона має нейтральний елемент, тобто такий елемент e таке, що

$$\mathrm{e}\cdot x=x\cdot \mathrm{e}=\mathrm{e}$$

для всіх x з множини Q. Перетворення α носія Q називається унітарним у лупі $(Q;\ \cdot,\ e)$, якщо α(e) = e.

Квазігрупа є групою, якщо вона асоціативна, тобто виконується закон асоціативності відносно операції носія.

Дві квазігрупи $(A;*)$ та $(B;\diamond)$ називаються ізотопними між собою, якщо існує три бієктивних відображення α,β,γ з множини A в множину B такі, що виконується рівність:

$$\alpha(x)\diamond\beta(y)=\gamma(x*y).$$

У дослідженнях бакалаврської дипломної роботи вивчаються не всі квазігрупи, а лише бінарні квазігрупові операції четвертого порядку. Всього таких квазігруп (латинських квадратів) четвертого порядку є 576 [16]. Використано той факт, що четвертого порядку квазігруп існує лише дві неізоморфні лупи: четвертна группа Кляйна $Z_2^2=Z_2\times Z_2$ (де операція $(\times)$ позначає прямий добуток циклічних груп Z_2 на Z_2) та циклічна група Z_4. Кожна квазігрупа четвертого порядку точно ізотопна одній із цих груп. Для реалізації квазігруп 4-го порядкув роботі розглянуто лише квазігрупи над ізотопами групи Кляйна.

Якщо квазігрупа скінченна, то внутрішня частина таблиці Келі є латинським квадратом, тобто таблиця множення скінченної квазігрупи утворює латинський квадрат. І навпаки, довільний латинський квадрат може бути вибраний за таблицю множення, щоб утворити квазігрупу. Нагадаємо, що латинський квадрат – це таблиця розміру $n \times n$, де кожний елемент зустрічається в кожному рядку та стовпчику всього раз. Розмір квазігрупи називається «порядком», наприклад, квазігрупа 4-го порядку – це латинський квадрат розміром 2×2 [17].

Оскільки квазігрупу можна подати у вигляді таблиці Келі, тобто таблиці відповідного множення, що вказує визначена операція вибраного носія, то таблиця Келі групи Кляйна 4-го порядку зображена на рисунку 1.1, для якої виконується рівність

$$x \oplus x = 0,$$

де операція $\oplus$ – це додавання за модулем 4.

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

Рисунок 1.1 – Таблиця Келі групи Кляйна

Для реалізації квазігрупи в апаратному забезпеченні потрібні цікаві специфічні властивості як самих квазігруп так і їх відповідних комбінаторних аналогів – латинських квадратів, такі, щоб використання їх у шифруванні було простим в реалізації. Такими специфічними властивостями для апаратної реалізації квазігрупи виявилися властивості схрещеної оборотності, так звані CIP-квазігрупи (cross inverse properties, що в перекладі означає «властивість схрещеної оборотності»).

Квазігрупа $(Q;\cdot)$ є середньою, лівою та правою CIP-квазігрупою [18] якщо відповідно існують відображення h, t, b такі, що для всіх змінних x та y виконуються такі рівності:

$$h(x)\cdot xy=y$$

$$yx\cdot y=t(x)$$

$$y\cdot xy=b(x)$$

де h, t, b називають лівою, правою та середньою функцією оборотності.

Враховуючи дане загальне означення для CIP-квазігруп, де функції оборотності рівні між собою та з досліджень класифікації мінімальних тотожностей отриманих в [19], середні CIP-квазігрупи 4-го порядку з функцією оборотності x^2 визначаються тотожностями, які мають вигляд:

$$x\cdot yx^2=y, \qquad xy\cdot x^2=y, \qquad (1.2.)$$

$$x^2y\cdot x=y, \qquad x^2\cdot yx=y.$$

Останні тотожності визначають многовид середніх CIP-квазігруп з оборотним елементом x^2.

Функція ${}^{\sigma}f$ називається σ-парастрофом функції f, якщо вона визначається таким співвідношенням:

$${}^{\sigma}f(x_{1\sigma};x_{2\sigma})=x_{3\sigma} \Leftrightarrow f(x_1;x_2)=x_3$$

для будь-якого $\sigma \in S_3 := \{\iota, s, \ell, r, s\ell, sr\}$, де S_3 позначає симетричну групу третього порядку, а основні парастрофи $s := (12)$, $\ell := (13)$, $r := (23)$ – це цикли довжини два. Кожна бінарна квазігрупова операція має перетворення елементів множини, які називаються парастрофами головної квазігрупової операції. Їх в бінарному випадку всього є шість $\{\iota, s, \ell, r, s\ell, sr\}$,: головна операція $\{\iota\}$, ліве ділення $\{\ell\}$, праве ділення $\{r\}$, комутування $\{s\}$, комутування правого ділення $\{sr\}$ та комутування лівого ділення $\{s\ell\}$.

Алгебричним означенням квазігрупи [20] є таке формулювання. Квазігрупа – це універсальна алгебра з трьома бінарними операціями $(Q;\cdot;\cdot;\cdot)$

сигнатури (2,2,2), такими, що виконуються шість таких тотожностей: тотожності (1.1) для всіх елементів x, y з множини Q, які записані в інфіксному позначенні:

$$(x \overset{\ell}{\cdot} y)y = x, \qquad xy \overset{\ell}{\cdot} y = x,$$

$$x \cdot (x \overset{r}{\cdot} y) = y, \qquad x \cdot xy \overset{r}{=} y.$$

та тотожності виду

$$x \cdot (y \overset{r}{\cdot} x) \overset{\ell}{=} y, \qquad (x \overset{r}{\cdot} y) \cdot x \overset{\ell}{=} y.$$

В [21] доведено, що будь які трійки тотожностей, які можна вибрати із шести поданих, є аксіомами многовида квазігруп. Якщо $(Q, \cdot)$ є квазігрупою як групоїд, то $(Q; \overset{\ell}{\cdot}; \overset{r}{\cdot}; \cdot)$ є еквівалентною квазігрупою в розумінні універсальної алгебри.

1.4 Використання квазігруп у криптографії

Застосування квазігруп в криптографії є широким і різноманітним, вони займають важливе місце в розробці безпечних криптографічних протоколів, алгоритмів та систем.

Перш за все, квазігрупи використовуються для побудови криптографічних алгоритмів з властивістю нелінійності. Лінійність означає, що операція не впливає на криптографічні властивості даних, що обробляються. І саме нелінійні операції ускладнюють атаки та аналіз криптографічних алгоритмів. Квазігрупи дозволяють використовувати різноманітні операції, такі як композиція, обернення та асоціативність, для побудови ефективних та безпечних криптографічних систем.

По-друге, застосування квазігруп в асиметричній криптографії. В асиметричних криптосистемах використовується пара ключів – приватний ключ для розшифрування та цифрового підпису, і публічний ключ для шифрування та перевірки підпису. Квазігрупи можуть забезпечити властивості безпеки та невідомості приватного ключа, а також ефективність операцій шифрування та

підписування. Вони дозволяють реалізувати різноманітні алгоритми, такі як, до прикладу, RSA (Rivest-Shamir-Adleman), що є одними з найпоширеніших асиметричних криптосистем [22].

По-третє, використання квазігруп пов'язане з розподіленими протоколами та безпекою. Розподілені протоколи дозволяють забезпечити безпеку та надійність обміну даними між різними сторонами, навіть якщо деякі з них можуть бути ненадійними або недоступними. Квазігрупи допомагають вирішувати проблеми довіри та цілісності у розподілених середовищах, де можуть виникати атаки та зловживання. Вони використовуються для забезпечення конфіденційності та цілісності даних під час їх передачі по мережі.

По-четверте, використання квазігруп для захисту від зламу в криптоаналізі. Квазігрупи можуть бути використані для побудови криптографічних систем, що важко піддаються криптоаналізу. Властивості квазігруп, такі як нелінійність, складність симетричних перетворень та стійкість до різних атак, роблять їх привабливими для застосування в криптографії. Вони забезпечують високий рівень безпеки для шифрування повідомлень, цифрового підпису, аутентифікації та інших криптографічних операцій.

По-п’яте, криптографічні хеш-функції, які використовуються в LW-криптографії, можуть використовувати перетворення, що базуються на алгебраїчних структурах, подібних до квазігруп. Такі хеш-функції забезпечують контроль цілісності даних і захист від підроблення.

Було проаналізовано використання квазігруп у Edon80 – це хеш-функція, яка використовує квазігрупи для забезпечення криптографічної стійкості. Квазігрупи використовуються в Edon80 для здійснення операцій змішування та перестановки даних з метою створення надійного хеш-коду [23].

У процесі створення хеш-коду за допомогою Edon80, вхідні дані розбиваються на блоки фіксованого розміру. Кожен блок даних проходить через серію квазігрупових операцій, які перетворюють його в новий стан. Цей процес має на меті змішування та перестановку бітів у блоках, що робить його нелінійним та важким для обернення.

Квазігрупи використовуються для реалізації цих операцій змішування та перестановки. Вони надають необхідні алгебраїчні властивості для створення непередбачуваних перетворень даних, що ускладнює злам шифру та відновлення вхідних даних з хеш-коду.

Квазігрупи, які використовуються в Edon80, мають спеціальні алгебраїчні властивості, такі як асоціативність, замкненість, існування оберненої операції та ідемпотентність. Ці властивості гарантують коректне функціонування хеш-функції та забезпечують криптографічну стійкість.

Використання квазігруп у шифрі Edon80 має декілька переваг.

1) Криптографічна стійкість: Квазігрупи мають особливі алгебраїчні властивості, які роблять їх стійкими до криптоаналітичних атак. У шифрі Edon80 ці властивості використовуються для створення непередбачуваних та нелінійних перестановок даних, що ускладнює роботу зловмисників з відновленням початкових даних або впровадженням некоректних змін.

2) Ефективність обчислень: Операції з квазігрупами можуть бути ефективно реалізовані на сучасних обчислювальних пристроях. Це дозволяє забезпечити швидку обробку даних у хеш-функції Edon80, що є важливим для багатьох криптографічних застосувань, включаючи захист даних та аутентифікацію.

3) Математична основа: Використання квазігруп у шифрі Edon80 базується на математичних принципах та алгебраїчних властивостях. Це дозволяє проводити математичний аналіз безпеки та стійкості шифру, а також встановлювати теоретичні основи його роботи.

4) Гнучкість: Квазігрупи можуть бути використані для створення різних криптографічних примітивів, включаючи хеш-функції. Використання квазігруп у шифрі Edon80 дозволяє гнучко налаштовувати функцію хешування залежно від потреб конкретного застосування.

Загалом, використання квазігруп у шифрі Edon80 дозволяє забезпечити криптографічну стійкість, ефективність обчислень та математичну основу, що робить його важливим інструментом у сфері захисту даних та криптографії.

Окремо варто виділити використання CIP-квазігруп у LW-криптографії (Lightweight Cryptography). LW-криптографія спеціалізується на розробці криптографічних алгоритмів, які можуть працювати на пристроях з обмеженими обчислювальними ресурсами, такими як сенсори, розумні картки, мікроконтролери та інші embedded системи. Однією з ключових вимог до LW-криптографії є низький рівень споживання енергії та невеликий об'єм пам'яті, що потрібний для реалізації криптографічних алгоритмів.

Використання CIP-квазігруп у LW-криптографії дозволяє забезпечити стійкість та безпеку операцій шифрування та розшифрування. Основна ідея LW-криптографії полягає в тому, що блочний шифр на основі CIP-квазігруп застосовується двічі до вхідного повідомлення з різними ключами. Це називається подвійним шифруванням.

Один з ключів використовується для шифрування, а інший – для розшифрування. Такий підхід дозволяє досягти додаткового рівня безпеки та запобігти дешифруванню повідомлення при використанні тільки одного ключа.

Застосування CIP-квазігруп у LW-криптографії має кілька переваг:

1) Криптографічна стійкість: Використання CIP-квазігруп у LW-криптографії дозволяє забезпечити стійкість до криптоаналітичних атак та стійкість до обернених атак, таких як диференціальний та лінійний криптоаналіз.

2) Швидкодія: CIP-квазігрупи можуть бути ефективно обчислені на сучасних обчислювальних пристроях, що дозволяє реалізувати LW-криптографію з високою швидкодією.

3) Можливість паралельної обробки: Оскільки операції у CIP-квазігрупі є асоціативними, це відкриває можливість для паралельної обробки даних, що покращує ефективність обчислень у LW-криптографії.

Використання CIP-квазігруп у LW-криптографії дозволяє забезпечити стійкість та безпеку передачі та збереження даних в умовах обмежених ресурсів. Крім того, вони можуть бути оптимізовані для виконання на обмежених пристроях, забезпечуючи оптимальне співвідношення між безпекою та ефективністю.

В цілому, використання CIP-квазігруп у LW-криптографії дозволяє розробляти безпечні та ефективні криптографічні рішення для обмежених пристроїв з низькими обчислювальними та енергетичними ресурсами.

Застосування квазігруп в криптографії є дуже важливим для забезпечення безпеки в інформаційних системах. Вони дозволяють створювати ефективні та надійні криптографічні протоколи та алгоритми, які забезпечують конфіденційність, цілісність та автентичність даних. Дослідження та розвиток квазігруп у криптографії є активною галуззю, що дозволяє розробляти нові методи та алгоритми для захисту інформації у сучасному цифровому світі. Вивчення їх математичних властивостей і застосування в практичних криптографічних системах допомагає покращувати безпеку та забезпечувати захист від сучасних крипто аналітичних атак.

Висновки до розділу

CIP-квазігрупи (Cros Invers Properties) є важливим інструментом у сучасній криптографії з кількох причин, які детально розглянемо:

1) Криптографічна стійкість: CIP-квазігрупи мають специфічні властивості, які роблять їх стійкими до криптоаналітичних атак. Одна з таких властивостей – необоротність, що означає, що зі значень квазігрупи неможливо однозначно відновити початкові дані або ключ. Крім того, CIP-квазігрупи дуже чутливі до навіть малих змін вхідних даних або ключа, що робить атаки з використанням статистичного аналізу менш ефективними. Всі ці фактори сприяють забезпеченню високого рівня конфіденційності та безпеки при передачі та збереженні даних.

2) Ефективність обчислень: Операції, визначені на CIP-квазігрупах, можуть бути ефективно реалізовані на сучасних обчислювальних пристроях, включаючи комп'ютери, мобільні пристрої та мікроконтролери. Це означає, що обробка даних з використанням CIP-квазігруп може відбуватись швидко, що

дозволяє їх використання в реальному часі для шифрування, розшифрування та інших криптографічних операцій.

3) Гнучкість та розширюваність: CIP-квазігрупи можуть бути використані для побудови різних криптографічних примітивів, таких як блочні шифри, хеш-функції, генератори псевдовипадкових чисел та інше. Вони можуть бути поєднані з іншими криптографічними алгоритмами для створення складних систем шифрування та автентифікації. Це дає можливість гнучко налаштовувати криптографічні протоколи залежно від конкретних потреб і вимог застосування.

4) Математична основа: CIP-квазігрупи базуються на математичних структурах та алгебраїчних властивостях, що робить їх абстрактними та формальними. Це дозволяє проводити математичний аналіз їхніх властивостей, довести теоретичні твердження та забезпечити вивчення їх стійкості. Математична основа CIP-квазігруп сприяє розвитку криптографічних алгоритмів та дозволяє проводити формальну перевірку їхньої безпеки.

Враховуючи всі переваги, CIP-квазігрупи є важливим інструментом у сучасній криптографії та допомагають забезпечувати безпеку та конфіденційність в цифровому світі. Вивчення їх властивостей та використання в різних криптографічних системах допомагає розвивати цю науку та забезпечувати захист інформації у сучасному інформаційному суспільстві.

2 ПРОГРАМНИЙ ЗАСІБ ДЛЯ ОБЧИСЛЕННЯ КВАЗІГРУП

Даний розділ присвячений розробці програмного засобу для побудови квазігруп вищих порядків. Тут описано математичні методи для формування квазігруп 4-го порядку з властивостями схрещеної оборотності над ізотопами групи Кляйна. З отриманих формул канонічного розкладу квазігруп реалізовано практичний програмний засіб для побудови в реальному вигляді латинських квадратів за допомогою прямого добутку квазігруп.

2.1 Канонічний розклад CIP-квазігрупи (латинського квадрату)

У даному параграфі роботи досліджено квазігрупи 4-го порядку. Всього таких квазігруп (латинських квадратів) є 576. Для реалізації квазігруп 4-го порядку в роботі розглянуто лише квазігрупи, побудовані над ізотопами групи Кляйна $Z_2^2 = Z_2 \times Z_2$ (де операція $(\times)$ позначає прямий добуток циклічних груп Z_2 на Z_2). Всі квазігрупи подано у вигляді таблиць Келі. Таблиця Келі групи Кляйна 4-го порядку зображена на рисунку 1.1, для якої виконується рівність

$$\bar{x} \oplus \bar{x} = \bar{0},$$

де операція $\oplus$ – це додавання за модулем 2, $\bar{x}$ означає вектор, координатами якого є елементи множини $\{0;1\}$, а $\bar{0}$ – нульовий вектор.

Встановлено [1], що середня CIP-квазігрупа $(Q;\cdot)$ з функцією оборотності x^2, яка задовольняє тотожності (1.2), над ізотопами групи Кляйна $(Z_2^2;\oplus;\ \bar{0})$ вона має канонічний розклад

$$x \cdot y = \bar{x}A \oplus \bar{y}A^{-1} \oplus \bar{a},$$

де матриця $A \in \left\{ \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}$ та довільний векторний елемент $\bar{a} \in \{(0,0);(0,1);(1,0);(1,1)\}$.

Для прикладу отримання латинського квадрата 4-го порядку, розглянемо

квазігрупу, в якій канонічний розклад визначений умовами, де $A=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$, $A^{-1}=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ та векторний елемент $\bar{a}=(0,0)$.

При цих вхідних даних для елементів CIP-квазігрупи маємо такі обчислення, де операція $(\cdot)$ – звичайне множення вектора на матрицю, а операція $\oplus$ – додавання елементів за модулем 2:

$$0\cdot 0=(0,0)\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}\oplus(0,0)\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\oplus(0,0)=0$$

$$0\cdot 1=(0,0)\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}\oplus(0,1)\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\oplus(0,0)=2$$

$$0\cdot 2=(0,0)\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}\oplus(1,0)\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\oplus(0,0)=3$$

$$0\cdot 3=(0,0)\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}\oplus(1,1)\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\oplus(0,0)=1$$

$$1\cdot 0=(0,1)\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}\oplus(0,0)\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\oplus(0,0)=3$$

$$1\cdot 1=(0,1)\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}\oplus(0,1)\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\oplus(0,0)=1$$

$$1\cdot 2=(0,1)\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}\oplus(1,0)\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\oplus(0,0)=0$$

$$1\cdot 3=(0,1)\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}\oplus(1,1)\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\oplus(0,0)=2$$

$$2\cdot 0=(1,0)\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}\oplus(0,0)\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\oplus(0,0)=1$$

$$2\cdot 1=(1,0)\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}\oplus(0,1)\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\oplus(0,0)=3$$

$$2\cdot 2=(1,0)\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}\oplus(1,0)\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\oplus(0,0)=2$$

$$2\cdot 3=(1,0)\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}\oplus(1,1)\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\oplus(0,0)=0$$

$$3\cdot 0=(1,1)\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}\oplus(0,0)\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\oplus(0,0)=2$$

$$3\cdot 1=(1,1)\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}\oplus(0,1)\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\oplus(0,0)=0$$

$$3\cdot 2=(1,1)\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}\oplus(1,0)\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\oplus(0,0)=1$$

$$3\cdot 3=(1,1)\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}\oplus(1,3)\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\oplus(0,0)=3$$

Результатом обчислень є CIP-квазігрупа 4-го порядку, латинський квадрат якої сформований на рисунку 2.1.

0	2	3	1
3	1	0	2
1	3	2	0
2	0	1	3

Рисунок 2.1 – Латинський квадрат CIP-квазігрупи 4-го порядку

Аналогічні обчислення проводяться всі всіх значень вільного члена канонічного розкладу квазігрупи, який поданий у вигляді векторного елемента $\bar{a} \in \{(0,0);(0,1);(1,0);(1,1)\}$. Результатом обчислень є 8 квазігруп, які подані у вигляді латинських квадратів в таблиці 2.2:

Таблиця 2.1 – Таблиці Келі CIP-квазігруп 4-го порядку

0)	0	1	2	3
0	0	3	1	2
1	2	1	3	0
2	3	0	2	1
3	1	2	0	3

1)	0	1	2	3
0	1	2	0	3
1	3	0	2	1
2	2	1	3	0
3	0	3	1	2

3)	0	1	2	3
0	2	1	3	0
1	0	3	1	2
2	1	2	0	3
3	3	0	2	1

5)	0	1	2	3
0	3	0	2	1
1	1	2	0	3
2	0	3	1	2
3	2	1	3	0

7)	0	1	2	3
0	0	2	3	1
1	3	1	0	2
2	1	3	2	0
3	2	0	1	3

2)	0	1	2	3
0	1	3	2	0
1	2	0	1	3
2	0	2	3	1
3	3	1	0	2

4)	0	1	2	3
0	2	0	1	3
1	1	3	2	0
2	3	1	0	2
3	0	2	3	1

6)	0	1	2	3
0	3	1	0	2
1	0	2	3	1
2	2	0	1	3
3	1	3	2	0

Висновком даного параграфу є отримання 8-ми CIP-квазігруп, які будуть використовуватися в алгоритмі шифрування в другій частині комплексної бакалаврської дипломної роботи.

2.2 Прямий добуток квазігруп (латинських квадратів)

Завданням даного параграфа описати алгебричну конструкцію квазігруп, таку як прямий добуток. Ця конструкція аналогічна прямому добутку груп, але з деякими змінами, оскільки квазігрупи можуть мати менші або модифіковані властивості порівняно з групами.

Взагалі кажучи, прямий добуток множин (іншими словами декартів добуток) – це всеможливі впорядковані пари елементів, де перша компонента однієї пари належить першій множині, а друга компонента цієї ж самої пари належить другій множині.

Легко переконатися, що прямий добуток квазігруп буде квазігрупою тоді і тільки тоді, коли кожна множина прямого добутку буде квазігрупою.

Нехай маємо дві квазігрупи $Q_1 = (G_1;*)$ та $Q_2 = (G_2;\triangle)$, де G_1 та G_2 – множини елементів, а операції $(*)$ та $(\triangle)$ – бінарні операції на цих множинах. Прямий добуток квазігруп Q_1 та Q_2 позначається:

$$Q_1 \times Q_2 := (G_1 \times G_2, \cdot) = (Q; \cdot),$$

де $G_1 \times G_2$ – декартовий добуток множин G_1 та G_2, а $(\cdot)$ – бінарна операція, яка визначена на $Q_1 \times Q_2$.

Бінарна операція $(\cdot)$ в прямому добутку квазігруп обчислюється для довільних елементів (a_1, b_1) та (a_2, b_2) з $G_1 \times G_2$ так:

$$((a_1, b_1) \cdot (a_2, b_2)) = (a_1 * a_2; b_1 \triangle b_2),$$

де $(*)$ та $(\triangle)$ – бінарні операції відповідних квазігруп Q_1 та Q_2.

Розглянемо для прикладу, прямий добуток двох квазігруп 4-го порядку, результатом якого маємо отримати квазігрупу 16-го порядку (див. Таблиця Келі квазігрупи 16-го порядку на рис. 2.3).

Нехай маємо два латинські квадрати (рис. 2.2).

0	3	1	2
2	1	3	0
3	0	2	1
1	2	0	3

а)

1	2	0	3
3	0	2	1
2	1	3	0
0	3	1	2

б)

Рисунок 2.2 – Латинський квадрат а) – квазігрупа №1, латинський квадрат б) – квазігрупа №2

Подальше обчислення виглядає так. Нехай маємо елементи множин з кожного латинського квадрата у вигляді першого рядка:

$$G_1 = \{0, 3, 1, 2\}$$

$$G_2 = \{1, 2, 0, 3\}$$

Згідно означення прямого добутку отримаємо пари значень:

$$G_1 \times G_2 = \{01, 02, 00, 03, 31, 32, 30, 33, 11, 12, 10, 13, 21, 22, 20, 23\}$$

В результаті отримано координати майбутніх елементів квазігрупи $Q_1 \times Q_2$. На прикладі одного елемента квазігрупи 16-го порядку розглянемо побудову прямого добутку квазігруп 4-го порядку. Замінивши отримані координати на їх вфідповідні значення маємо, що перший елемент квазігрупи буде з координатами. Взявши перші елементи координат ми отримаємо координати першого елемента в першій квазігрупі для побудови остаточного значення.За координатами (0;0) отримано значення 0.

Провівши аналогічні дії за координатами (1;1) у другій квазігрупі отримаємо 0. Об'єднавши значення у 00 та знайшовши його у порядку $G_1 \times G_2$ отримаємо 2 оскільки порядок координат в квазігрупі розпочинається з 0.

За таким алгоритмом пройшовши всі 256 елементів квазігрупи 16-го порядку отримаємо результат прямого добутку двох квазігруп 4-го порядку (рис. 2.3).

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	11	8	10	9	7	4	6	5	15	12	14	13	3	0	2	1
1	9	10	8	11	5	6	4	7	13	14	12	15	1	2	0	5
2	8	11	9	10	4	7	5	6	12	15	13	14	0	3	1	2
3	10	9	11	8	6	5	7	4	14	13	15	12	2	1	3	0
4	3	0	2	1	15	12	14	13	7	4	6	5	11	8	10	9
5	1	2	0	3	13	14	12	15	5	6	4	7	9	10	8	11
6	0	3	1	2	12	15	13	14	4	7	5	6	8	11	9	10
7	2	1	3	0	14	13	15	12	6	5	7	4	10	9	11	8
8	7	4	6	5	11	8	10	9	3	0	2	1	15	12	14	13
9	5	6	4	7	9	10	8	11	1	2	0	3	13	14	12	15
10	4	7	5	6	8	11	9	10	0	3	1	2	12	15	13	14
11	6	5	7	4	10	9	11	8	2	1	3	0	14	13	15	12
12	15	12	14	13	3	0	2	1	11	8	10	9	7	4	6	5
13	13	14	12	15	1	2	0	3	9	10	8	11	5	6	4	7
14	12	15	13	14	0	3	1	2	8	11	9	10	4	7	5	6
15	14	13	15	12	2	1	3	0	10	9	11	8	6	5	7	4

Рисунок 2.3 – Квазігрупа 16-го порядку

2.3 Розробка засобу для побудови латинських квадратів різних порядків

2.3.1 Вибір мови програмування

На сьогоднішній день є чимало мов програмування для створення різноманітних застосунків. Серед великої кількості є 3 основних які мають найбільший функціонал: Python, C++ та Java.

Python – це високорівнева мова програмування загального призначення, яка вирізняється своєю простотою, читабельністю та елегантністю синтаксису [24]. Ось кілька ключових характеристик та переваг Python:

1) Простота вивчення: Python має простий синтаксис, що дозволяє швидко вивчити основи мови. Читабельність коду є однією з основних принципів Python, що робить його добрим вибором для початківців у програмуванні.

2) Широкий спектр застосувань: Python використовується для розробки веб-додатків, наукових обчислень, штучного інтелекту, обробки даних, автоматизації завдань, ігор та багатьох інших. Його розширюваність та наявність великої кількості сторонніх бібліотек роблять його популярним в багатьох сферах розробки.

3) Велика спільнота та екосистема: Python має велику та активну спільноту розробників, яка підтримує мову та створює безліч сторонніх бібліотек та фреймворків. Це дозволяє програмістам швидко знаходити рішення для своїх завдань та отримувати підтримку.

4) Розширюваність: Python може бути розширений за допомогою модулів та пакетів, які додають додаткові функції та можливості. Наприклад, популярні бібліотеки, такі як NumPy, Pandas, TensorFlow та Django, дозволяють легко виконувати наукові обчислення, обробку даних, машинне навчання та веб-розробку.

5) Переносимість: Python доступний для різних операційних систем, включаючи Windows, macOS та Linux. Це дозволяє розробникам писати

програми, які працюють на різних платформах без необхідності відновлення коду.

6) Інтерактивна оболонка: Python надає інтерактивну оболонку, де користувач може відразу ж виконувати код та отримувати результати. Це зручно для експериментів та швидкої перевірки функціоналу.

Загалом, Python є потужним і гнучким інструментом для розробки програмних застосунків у різних сферах, завдяки своїй простоті, широкій підтримці спільноти та великій кількості бібліотек та фреймворків.

C++ – це мова програмування загального призначення, яка комбінує в собі високорівневі та низькорівневі можливості [25]. Ось кілька ключових характеристик та переваги мови програмування C++:

1) Продуктивність: C++ відомий своєю високою продуктивністю та швидкодією. Він надає прямий доступ до пам'яті, що дозволяє розробникам ефективно керувати ресурсами та оптимізувати роботу програм.

2) Низькорівневі можливості: C++ надає низькорівневі можливості, такі як маніпуляція з пам'яттю та використання вказівників, що дозволяє розробникам контролювати апаратне забезпечення та оптимізувати роботу програм на рівні, ближчому до машинного коду.

3) Об'єктно-орієнтоване програмування: C++ підтримує об'єктно-орієнтовану парадигму програмування, що дозволяє розробникам створювати класи, об'єкти та використовувати інкапсуляцію, наслідування та поліморфізм.

4) Розширюваність: C++ є розширюваною мовою програмування, що дозволяє розробникам використовувати сторонні бібліотеки та розширення. Це дозволяє швидко розробляти програми, використовуючи готові рішення та інструменти.

5) Кросплатформеність: C++ є кросплатформеною мовою програмування, що дозволяє розробляти програми для різних операційних систем, таких як Windows, macOS та Linux. Це забезпечує гнучкість та можливість запуску програм на різних платформах без необхідності відновлення коду.

6) Велика спільнота та ресурси: C++ має велику та активну спільноту розробників, яка надає підтримку, документацію та безліч ресурсів для вивчення мови. Це допомагає розробникам знайти відповіді на свої питання та ефективно використовувати C++ у своїх проектах.

Незважаючи на всі переваги, C++ також може бути складнішою мовою для вивчення порівняно з іншими, оскільки вона вимагає уваги до деталей та керування ресурсами. Однак, це зусилля варте для розробників, які шукають високою продуктивністю та низькорівневою контролем у своїх програмах.

Java – це високорівнева мова програмування, яка широко використовується у розробці програмного забезпечення та веб-додатків [26]. Ось кілька ключових характеристик та переваг мови програмування Java:

1) Платформа незалежна: Java є платформою незалежною мовою програмування, що означає, що програми, написані на Java, можуть запускатися на будь-якій операційній системі, яка підтримує віртуальну машину Java (JVM). Це забезпечує велику переносимість коду та зручність у розгортанні програм.

2) Об'єктно-орієнтоване програмування: Java побудована на об'єктно-орієнтованій парадигмі, що дозволяє розробникам створювати класи, об'єкти та використовувати принципи спадкування, поліморфізму та інкапсуляції. Це сприяє модульності, повторному використанню коду та підтримці розширюваності.

3) Велика бібліотека та екосистема: Java має широку бібліотеку стандартних класів, яка надає розробникам доступ до різноманітних функціональностей. Крім того, існує велика кількість сторонніх бібліотек та фреймворків, що допомагають в розробці веб-додатків, наукових обчислень, роботи з базами даних та інших завдань.

4) Безпека: Java має вбудовану систему безпеки, що дозволяє розробникам створювати надійні та захищені програми. Вона включає механізми контролю доступу, обробку виключень та інші заходи безпеки.

5) Підтримка мультипотоковості: Java має вбудовану підтримку мультипотоковості, що дозволяє розробникам створювати багатопотокові

програми. Це корисно для виконання завдань паралельно, підвищення продуктивності та використання багатоядерних процесорів.

6) Простота використання та вивчення: Java має простий та логічний синтаксис, який дозволяє легко вивчити мову та розпочати розробку. Вона також має багато інструментів розробки та інтегрованих середовищ, які полегшують процес розробки та налагодження програм.

Загалом, Java є потужною та розширюваною мовою програмування з великою спільнотою розробників, великою кількістю інструментів та широкою підтримкою. Вона підходить для розробки різноманітних програмних рішень, включаючи веб-додатки, мобільні додатки, вбудовані системи та багато іншого.

При порівнянні мов програмування Java, C++ та Python було зроблено наступні спостереження.

Java є платформою незалежною, що означає, що програми, написані на цій мові, можуть працювати на різних операційних системах без необхідності змінювати код. Вона також пропонує об'єктно-орієнтований підхід до програмування, що полегшує модульність та повторне використання коду. Java має велику екосистему, яка включає багато сторонніх бібліотек та фреймворків, що дозволяє розробникам швидко створювати програми з різноманітною функціональністю. Крім того, вона має вбудовану систему безпеки, яка допомагає забезпечити надійність та безпеку програм.

C++ славиться своєю продуктивністю та швидкодією. Вона дозволяє розробникам прямо маніпулювати пам'яттю та мати низькорівневий доступ до ресурсів. Також, C++ дозволяє розширювати функціональність програми за допомогою сторонніх бібліотек та розширень.

Python відзначається своєю простотою використання та зрозумілим синтаксисом. Вона має велику кількість стандартних бібліотек та сторонніх модулів, що полегшує розробку програм та дозволяє виконувати різноманітні завдання. Python застосовується в багатьох сферах, включаючи веб-розробку, аналіз даних та машинне навчання.

Загалом, використання Java може бути доречнішим та перспективнішим в порівнянні з C++ та Python, завдяки своїй платформо-незалежності, об'єктно-орієнтованому підходу, широкій екосистемі та вбудованій системі безпеки.

2.3.2 Середовище розробки

Для розробки програмного застосунку на мові Java існує кілька популярних середовищ розробки (IDE – Integrated Development Environment): Eclipse, IntelliJ IDEA та NetBeans. Розглянемо їх детальніше.

Eclipse: Eclipse – це відоме середовище розробки Java, яке володіє широким набором функціональних можливостей [27]. Воно має підсвічування синтаксису, автодоповнення коду, вбудований засіб налагодження та можливості керування проектами. Eclipse також дозволяє розширювати свої можливості за допомогою плагінів. Однак, вважається, що налаштування та конфігурація Eclipse можуть бути трохи складними, а інтерфейс може бути не таким інтуїтивно зрозумілим для новачків.

IntelliJ IDEA: IntelliJ IDEA – це потужне та інноваційне середовище розробки Java, розроблене компанією JetBrains [28]. Воно володіє високою продуктивністю та широким набором функцій, які полегшують розробку. IntelliJ IDEA має дуже ергономічний та інтуїтивно зрозумілий інтерфейс, що сприяє швидкому освоєнню середовища. Воно пропонує автодоповнення, рефакторинг, вбудований засіб налагодження, аналіз коду та підтримку систем контролю версій. IntelliJ IDEA також активно підтримується компанією JetBrains, що гарантує часті оновлення та вдосконалення.

NetBeans: NetBeans – це відкрите середовище розробки Java, розроблене компанією Apache [29]. Воно надає інтуїтивний інтерфейс та підтримує такі функції, як автодоповнення, налагодження та візуальна розробка. NetBeans також має можливість розширення за допомогою плагінів. Однак, порівняно з Eclipse та IntelliJ IDEA, NetBeans може бути менш популярним та мати меншу кількість доступних розширень.

Зробивши порівняння, можна зробити висновок, що використання IntelliJ IDEA може бути доречнішим. IntelliJ IDEA пропонує широкий набір

функціональних можливостей, має дружній та інтуїтивно зрозумілий інтерфейс та активно підтримується компанією JetBrains. Це допомагає забезпечити швидку та продуктивну розробку програм на мові Java. Однак, варто зазначити, що вибір середовища розробки є особистою перевагою, і важливо врахувати ваші власні потреби та вимоги проекту перед прийняттям рішення.

2.3.3 Опис програмного засобу

Програмний засіб має наочно показувати результат формування CIP-квазігруп 4-го порядку за формулою канонічного розкладу та результат прямого добутоку для формування квазігруп 8-го та 16-го порядку.

Загальна структура програмного засобу має наступний вигляд представлений на рисунку 2.4.

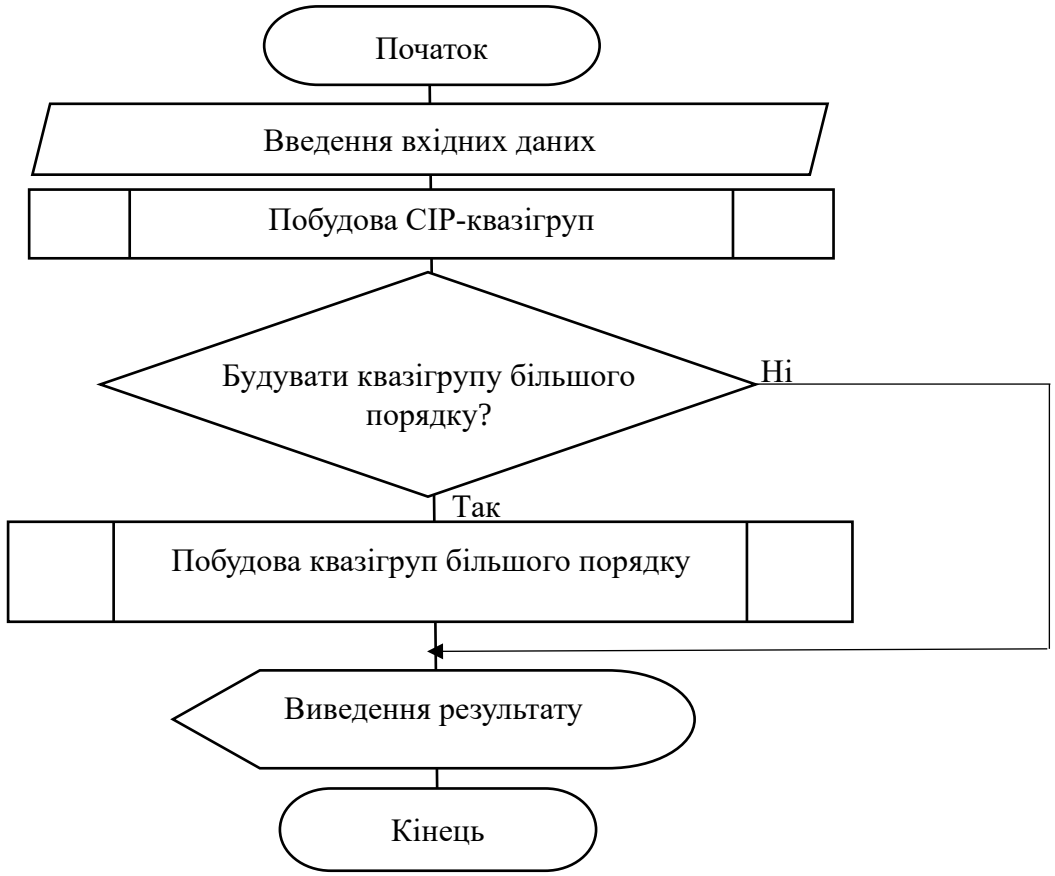


Рисунок 2.4 – Загальна структура програмного засобу

На початку програмного засобу потрібно обрати ціль роботи програми: побудова CIP-квазігруп 4-го порядку, побудова квазігруп 8-го та 16-го порядку за допомогою прямого добутку (рис. 2.5).

```
1.Побудова CIP-квазігруп 4-го порядку
2.Побудова квазігрупи 8 порядку
3.Побудова квазігрупи 16 порядку
4.Кінець
Ваш вибір:
```

Рисунок 2.5 – Початкове меню програмного застосунку

Функція побудови CIP-квазігруп 4-го порядку базується на вище описаній функції канонічного розкладу $x \cdot y = \bar{x}A \oplus \bar{y}A^{-1} \oplus \bar{a}$. Вона є само достатньою та не потребує вхідних даних оскільки всі дані для формування CIP-квазігруп 4-го порядку є сталими у застосунок.

В свою чергу, друга функція створена для побудови CIP-квазігруп 8-го та 16-го порядку на вибір користувача. За основу функція бере CIP-квазігрупи які формує попередня функція. Для побудови квазігруп 8-го порядку застосунок формує квазігрупу 4-го порядку та використовує квазігрупу 2-го порядку яка використовується у попередній функції для формування квазігрупи 4-го порядку. Взявши 2 квазігрупи 4-го порядку, формується квазігрупа 16-го порядку.

2.3.4 Результат роботи та тестування програмного засобу

При виборі першого пункту програмний застосунок за формулою канонічного розкладу сформує на надрукує в консолі всі можливі CIP-квазігрупи 4-го порядку (рис. 2.6).

```
CIP-квазігрупа №1  CIP-квазігрупа №5
0 2 3 1            2 0 1 3
3 1 0 2            1 3 2 0
1 3 2 0            3 1 0 2
2 0 1 3            0 2 3 1

CIP-квазігрупа №2  CIP-квазігрупа №6
0 3 1 2            2 1 3 0
2 1 3 0            0 3 1 2
3 0 2 1            1 2 0 3
1 2 0 3            3 0 2 1

CIP-квазігрупа №3  CIP-квазігрупа №7
1 3 2 0            3 1 0 2
2 0 1 3            0 2 3 1
0 2 3 1            2 0 1 3
3 1 0 2            1 3 2 0

CIP-квазігрупа №4  CIP-квазігрупа №8
1 2 0 3            3 0 2 1
3 0 2 1            1 2 0 3
2 1 3 0            0 3 1 2
0 3 1 2            2 1 3 0
```

Рисунок 2.6 – Сформовані CIP-квазігрупи 4-го порядку

На основі отриманих квазігруп було сформовано таблиці Келі CIP-квазігруп над ізотопами групи Кляйна (рис. 2.7)

1)	0	1	2	3
0	0	3	1	2
1	2	1	3	0
2	3	0	2	1
3	1	2	0	3

2)	0	1	2	3
0	1	2	0	3
1	3	0	2	1
2	2	1	3	0
3	0	3	1	2

3)	0	1	2	3
0	2	1	3	0
1	0	3	1	2
2	1	2	0	3
3	3	0	2	1

4)	0	1	2	3
0	3	0	2	1
1	1	2	0	3
2	0	3	1	2
3	2	1	3	0

5)	0	1	2	3
0	0	2	3	1
1	3	1	0	2
2	1	3	2	0
3	2	0	1	3

6)	0	1	2	3
0	1	3	2	0
1	2	0	1	3
2	0	2	3	1
3	3	1	0	2

7)	0	1	2	3
0	2	0	1	3
1	1	3	2	0
2	3	1	0	2
3	0	2	3	1

8)	0	1	2	3
0	3	1	0	2
1	0	2	3	1
2	2	0	1	3
3	1	3	2	0

Рисунок 2.7 – Таблиці Келі CIP-квазігруп

Для подальшого їх використання у алгоритмах шифрування було сформовано таблицю взаємно оборотних пар CIP-квазігруп (рис. 2.8)

1)	0	1	2	3
0	0	3	1	2
1	2	1	3	0
2	3	0	2	1
3	1	2	0	3

2)	0	1	2	3
0	1	2	0	3
1	3	0	2	1
2	2	1	3	0
3	0	3	1	2

3)	0	1	2	3
0	2	1	3	0
1	0	3	1	2
2	1	2	0	3
3	3	0	2	1

4)	0	1	2	3
0	3	0	2	1
1	1	2	0	3
2	0	3	1	2
3	2	1	3	0

5)	0	1	2	3
0	0	2	3	1
1	3	1	0	2
2	1	3	2	0
3	2	0	1	3

8)	0	1	2	3
0	3	1	0	2
1	0	2	3	1
2	2	0	1	3
3	1	3	2	0

6)	0	1	2	3
0	1	3	2	0
1	2	0	1	3
2	0	2	3	1
3	3	1	0	2

7)	0	1	2	3
0	2	0	1	3
1	1	3	2	0
2	3	1	0	2
3	0	2	3	1

Рисунок 2.8 – Таблиці Келі CIP-квазігруп

Для побудови квазігрупи 8-го порядку потрібно вести початкові дані для формування квазігрупи 4-го порядку та вибору одної з двох квазігруп 2-го порядку. Якщо для формування квазігрупи 4-го порядку ввести вектор під номером один та першу квазігрупу як елемент для формування першого доданку, та в якості другого доданку ми отримаємо наступний результат (рис. 2.9).

3	1	0	2	7	5	4	6
0	2	3	1	4	6	7	5
2	0	1	3	6	4	5	7
1	3	2	0	5	7	6	4
7	5	4	6	3	1	0	2
4	6	7	5	0	2	3	1
6	4	5	7	2	0	1	3
5	7	6	4	1	3	2	0

Рисунок 2.9 – Результат формування квазігрупи 8-го порядку

За схожим алгоритмом але ввівши 2 вектори та 2 квазігрупи 2-го порядку ми отримаємо 2 CIP-квазігрупи 4-го порядку. На основі цих двох квазігруп буде формуватись квазігрупа 16-го порядку (рис. 2.10).

15	12	14	13	7	4	6	5	3	0	2	1	11	8	10	9
13	14	12	15	5	6	4	7	1	2	0	3	9	10	8	11
12	15	13	14	4	7	5	6	0	3	1	2	8	11	9	10
14	13	15	12	6	5	7	4	2	1	3	0	10	9	11	8
3	0	2	1	11	8	10	9	15	12	14	13	7	4	6	5
1	2	0	3	9	10	8	11	13	14	12	15	5	6	4	7
0	3	1	2	8	11	9	10	12	15	13	14	4	7	5	6
2	1	3	0	10	9	11	8	14	13	15	12	6	5	7	4
11	8	10	9	3	0	2	1	7	4	6	5	15	12	14	13
9	10	8	11	1	2	0	3	5	6	4	7	13	14	12	15
8	11	9	10	0	3	1	2	4	7	5	6	12	15	13	14
10	9	11	8	2	1	3	0	6	5	7	4	14	13	15	12
7	4	6	5	15	12	14	13	11	8	10	9	3	0	2	1
5	6	4	7	13	14	12	15	9	10	8	11	1	2	0	3
4	7	5	6	12	15	13	14	8	11	9	10	0	3	1	2
6	5	7	4	14	13	15	12	10	9	11	8	2	1	3	0

Рисунок 2.10 – Результат формування квазігрупи 16-го порядку

Висновки до розділу

В даному розділі бакалаврської роботи були розглянуті та описані важливі аспекти теорії квазігруп. Починаючи з канонічного розкладу CIP-квазігруп, була розкрита його сутність та методика застосування. Канонічний розклад є важливим інструментом у формуванні та аналізі квазігруп, оскільки він дозволяє отримати унікальні розклади для кожної квазігрупи.

Далі, було наведено прямий добуток квазігруп, який є потужним методом для побудови нових квазігруп шляхом комбінації існуючих. Прямий добуток дозволяє злити квазігрупи різних порядків, що розширює можливості утворення більш складних структур.

Після уважного аналізу та порівняння можливостей мов програмування, було прийняте рішення вибрати Java. Java є потужною та широко використовуваною мовою програмування з багатим набором функціональних можливостей. Вона підтримує об'єктно-орієнтований підхід, має велику кількість доступних бібліотек та добре документована. Крім того, Java є платформо незалежною мовою, що дозволяє запускати програмний код на різних операційних системах без змін.

Під час аналізу різних інтегрованих середовищ розробки для Java, було обрано IntelliJ IDEA. Це популярне та потужне середовище розробки, яке надає широкий набір інструментів для комфортної розробки програмного коду. IntelliJ IDEA має розширену функціональність, таку як автодоповнення коду, вбудовану підтримку систем контролю версій, дебагер та інші корисні інструменти, що полегшують процес розробки.

У результаті було успішно реалізовано програмний застосунок, який здатен формувати всі CIP-квазігрупи 4-го порядку. Кількість таких квазігруп становить 8. Також серед них були знайдені оборотні пари які є важливими об'єктами дослідження, оскільки вони мають специфічні властивості та знаходять широке застосування у різних областях.

3 ЛОГІЧНІ СХЕМИ CIP-КВАЗІГРУП

У третьому розділі розглядаються поняття логічних функцій, їх мінімізація, діаграми Вейча, метод мінімізації на основі діаграм Вейча, таблиці істиності. Обчислено логічні та мінімізовані схеми для кожної з восьми CIP-квазігруп 4-го порядку.

3.1 Логічні функції

Логічні функції використовуються в цифрових електронних пристроях, зокрема комп'ютерах, мікросхемах, тощо, для виконання операцій з бітовими сигналами. Ці функції приймають один або більше вхідних сигналів і генерують вихідний сигнал, залежно від встановлених правил логіки.

Деякі з найпоширеніших логічних функцій включають:

1) Логічне "І" (AND): Вихідний сигнал буде "1" тільки тоді, коли всі вхідні сигнали є "1". У протилежному випадку, вихідний сигнал буде "0".

2) Логічне "АБО" (OR): Вихідний сигнал буде "1", якщо хоча б один вхідний сигнал є "1". Якщо всі вхідні сигнали є "0", вихідний сигнал буде "0".

3) Логічне "НЕ" (NOT): Це унарна функція, що приймає тільки один вхідний сигнал і змінює його на протилежне значення. Наприклад, якщо вхідний сигнал є "1", то вихідний сигнал буде "0", і навпаки.

4) Логічне "XOR" (Exclusive OR): Вихідний сигнал буде "1" тільки тоді, коли кількість вхідних сигналів зі значенням "1" є непарною. Якщо кількість вхідних сигналів зі значенням "1" є парною, вихідний сигнал буде "0".

5) Логічні схеми використовують логічні функції для реалізації бажаних логічних операцій. Вони складаються з комбінацій логічних функцій, таких як логічні елементи, які з'єднані між собою, утворюючи складніші операції. Логічні схеми можуть бути представлені у вигляді схематичних діаграм, табличних зображень або у формі булевих функцій.

Наприклад, логічна функція "AND" може бути реалізована за допомогою двох вхідних сигналів і одного логічного елемента "AND". Якщо обидва вхідних сигнали є "1", то вихідний сигнал буде "1", в іншому випадку вихідний сигнал буде "0".

Таким чином, логічні функції є основою для роботи з логічними операціями в цифрових пристроях та електронних системах. Вони дозволяють виконувати різні логічні операції та контролювати поведінку цифрових пристроїв на основі вхідних сигналів.

3.2 Мінімізація на основі діаграм Вейча

Мінімізація логічних схем є процесом спрощення логічних виразів або таблиць істинності з метою зменшення кількості логічних елементів та оптимізації [30]. Це дозволяє скоротити кількість компонентів, знизити складність схеми і покращити ефективність системи. Для мінімізації використовуються різні методи, такі як Квайна-МакКласкі, метод Карно та метод Шеннона, метод Вейча.

Метод Вейча було обрано завдяки можливості візуального представлення результатів та зручність при роботі з малою кількістю змінних.

Основний принцип мінімізації полягає в знаходженні еквівалентних логічних виразів, які мають меншу кількість термів або логічних операторів.

Основні кроки мінімізації логічних функцій:

1) Визначення логічного виразу або таблиці істинності, яку потрібно мінімізувати.

2) Використання методу Вейча для знаходження мінімального набору термів або максимального покриття клітинок в таблиці істинності.

3) Застосування логічних законів та властивостей для спрощення логічного виразу.

4) Перевірка отриманого спрощеного виразу або таблиці істинності на еквівалентність з початковим виразом. Виконання тестів і перевірка, що функція залишається незмінною після мінімізації.

5) Реалізація спрощеного виразу за допомогою логічних елементів.

Важливо враховувати, що мінімізація логічних функцій є завданням, яке може бути складним для складних функцій з великою кількістю входів. Для цього існують спеціалізовані програмні засоби, що допомагають автоматизувати процес мінімізації і забезпечують оптимальні результати.

3.3 Синтез логічних схем

Синтез логічних схем будується на основі таблиць істиності. Таблиця істинності – це логічна таблиця, яка використовується для вивчення та аналізу логічних виразів, функцій та операцій. Дозволяють визначити значення виразів в залежності від можливих комбінацій значень їх складових. Зазвичай в таблиці істинності представлені вхідні змінні, результат операції або виразу та відповідні значення для кожної комбінації.

Таблиця істинності може мати різну кількість рядків, яка визначається кількістю можливих комбінацій значень вхідних змінних. Якщо у таблиці присутні дві вхідні змінні (наприклад, A і B), і кожна змінна може приймати два можливих значення (0 або 1), то кількість рядків у таблиці буде рівна 2^2 = 4.

Найпростіша таблиця істинності використовується для однієї логічної змінної. Наприклад, розглянемо таблицю істинності для логічної змінної P (рис. 3.1).

P
0
1

Рисунок 3.1 – Таблицю істинності змінної P

Таблиці істинності також використовуються для вивчення логічних операцій, таких як "І" (AND), "АБО" (OR), "НЕ" (NOT) тощо, а також для складніших логічних виразів. Наприклад, розглянемо таблицю істинності для операції "І" (AND) з двома вхідними змінними A і B (рис. 3.2).

A	B	A I B
0	0	0
0	1	0
1	0	0
1	1	1

Рисунок 3.2 – Таблиця істинності для операції "I" (AND)

У цій таблиці показані всі можливі комбінації значень A і B, а стовпець "A I B" вказує результат операції "I" для кожної комбінації. Наприклад, коли A = 0 і B = 1, результат операції "I" буде 0.

Таблиці істинності є важливим інструментом при проектуванні та аналізі логічних схем, булевих функцій і систем логічного управління. Вони дозволяють зрозуміти поведінку логічних операцій та визначити значення виразів в залежності від вхідних значень.

У бакалаврській роботі для синтезу логічних схем потрібно пройти 3 кроки:

1. Створити таблиці істинності для кожної квазігрупи.
2. На основі таблиць істинності побудувати діаграми Вейча.
3. Створити логічні вирази та мінімізувати їх.

Кожна таблиця істинності для квазігруп 4-го порядку формується на основі квазігрупової операції: в таблицю записуються всі можливі комбінації вхідних даних. Потім, для кожного набору вхідних даних записується результат операції. Розглянемо квазігрупу №1 на рисунку.3.3 та заповнимо таблицю істиності для неї.

1)	0	1	2	3
0	0	3	1	2
1	2	1	3	0
2	3	0	2	1
3	1	2	0	3

Рисунок 3.3 – Квазігрупи №1

Для синтезу логічних функцій необхідно представити всі змінні в вигляді двійкових чисел. Оскільки використовуються квазігрупи четвертого порядку, то рядки квазігрупи подані як змінна x а стовпчики y:

$$x \in \{0; 1; 2; 3\},$$

$$y \in \{0; 1; 2; 3\}.$$

Кожний елемент для рядків x та стовпчиків y подамо через двійковий код: x=x1x2, y=y1y2. Тобто для представлення кожної змінної необхідні два двійкові розряди, як показано в таблиці 3.1 для рядків та в таблиці 3.2 для стовпців .

Таблиця 3.1 – Представлення змінної *x* в двійковій системі числення

Значення	x_1	x_2
0	0	0
1	0	1
2	1	0
3	1	1

Таблиця 3.2 – Представлення змінної *y* в двійковій системі числення

Значення	y_1	y_2
0	0	0
1	0	1
2	1	0
3	1	1

Перехрестям рядка і стовпчика квазігрупи №1 є функція

$$z \in \{0; 1; 2; 3\}.$$

Функція *z* представляється в двійковому вигляді, відповідно до змінних, як показано в таблиці 3.3

Таблиця 3.3 – Представлення змінної *z* в двійковій системі числення

Значення	z_1	z_2
0	0	0
1	0	1
2	1	0
3	1	1

Далі для кожного набору вхідних даних обчислимо результат. Наприклад, для x=0 та y=0, вхідні дані спочатку переводяться в двійкову систему числення, визначаючи змінні x_1, x_2, y_1, та y_2. В результаті отримуємо операцію z=z1z2 яка на рисунку 3.4 з результатом 0 подана в рядку №0, як зображено на рисунку 3.4.

№	x_1	x_2	y_1	y_2	$1z_1$	$1z_2$
0	0	0	0	0	0	0
1	0	0	0	1	1	1
2	0	0	1	0	0	1
3	0	0	1	1	1	0
4	0	1	0	0	1	0
5	0	1	0	1	0	1
6	0	1	1	0	1	1
7	0	1	1	1	0	0
8	1	0	0	0	1	1
9	1	0	0	1	0	0
10	1	0	1	0	1	0
11	1	0	1	1	0	1
12	1	1	0	0	0	1
13	1	1	0	1	1	0
14	1	1	1	0	0	0
15	1	1	1	1	1	1

Рисунок 3.4 – Таблиця істинності для CIP-квазігрупи 4-го порядку №1

Для квазігрупи 4-го порядку заповнемо таблицю Вейча(рис. 3.5).

	x2	x2	$\overline{x2}$	$\overline{x2}$	
x1	12	13	9	8	$\overline{y1}$
x1	14	15	11	10	y1
$\overline{x1}$	6	7	3	2	y1
$\overline{x1}$	4	5	1	0	$\overline{y1}$
	$\overline{y2}$	y2	y2	$\overline{y2}$	

Рисунок 3.5 – Діаграма Вейча

Використовуючи результати таблиці Вейча випишемо для кожної операції елементи які мають одиницю. Таким чином для квазігрупи №1 маємо дві таблиці значень: таблиця значень z_1 та таблиця значень z_2, зображені на рисунку 3.5.

z_1

	1		1
	1		1
1		1	
1		1	

а)

1			1
	1	1	
1			1
	1	1	

б)

Рисунок 3.6 – Таблиці значень: а – таблиця значень z_1 , б – таблиця значень z_2

З отриманої таблиці, шляхом попарного об’єднання операцій, що мають три спільні стани вхідних змінних, ми отримуємо логічний вираз, який описує визначену змінну. Оскільки в даній таблиці є чотири пари, маємо три операції

логічного АБО, в результаті цього отримуємо логічні вирази, що описують z_1 та z_2 які мають вирази:.

$$z_1 = \bar{x}_1 x_2 \bar{y}_2 + x_1 x_2 y_2 + \bar{x}_1 \bar{x}_2 y_2 + x_1 \bar{x}_2 \bar{y}_2$$

$$z_2 = x_1 y_1 y_2 + \bar{x}_1 \bar{y}_1 y_2 + x_1 \bar{y}_1 \bar{y}_2 + \bar{x}_1 y_1 \bar{y}_2,$$

За допомогою аналогічних дій для наступних семи квазігруп обчислено логічні схеми.

Обчислення логічних схем другої квазігрупи починається з побудови таблиці істинності. Друга квазігрупа зображена на рисунку 3.7.

2)	0	1	2	3
0	1	2	0	3
1	3	0	2	1
2	2	1	3	0
3	0	3	1	2

Рисунок 3.7 – Квазігрупи №2

Згідно таблиці Келі другої квазігрупи, вносимо в таблицю істинності значення, які відповідають результату кожної з 16 операцій, відповідно до чотирьох бінарних змінних, які описують *x* та *y*. Таблиця істинності другої квазігрупи зображена на рисунку 3.8

№	x_1	x_2	y_1	y_2	$2z_1$	$2z_2$
0	0	0	0	0	0	1
1	0	0	0	1	1	0
2	0	0	1	0	0	0
3	0	0	1	1	1	1
4	0	1	0	0	1	1
5	0	1	0	1	0	0
6	0	1	1	0	1	0
7	0	1	1	1	0	1
8	1	0	0	0	1	0
9	1	0	0	1	0	1
10	1	0	1	0	1	1
11	1	0	1	1	0	0
12	1	1	0	0	0	0
13	1	1	0	1	1	1
14	1	1	1	0	0	1
15	1	1	1	1	1	0

Рисунок 3.8 – Таблиця істинності для CIP-квазігрупи 4-го порядку №2

Далі, згідно отриманої таблиці істинності, заповнимо таблиці значень z_1 та z_2. Для цього в кожній позиції діаграми Вейча, що описує набір змінних, який в результаті операції дає результат 1, записується 1. Результат заповнення таблиць зображено на рисунку 3.9.

Рисунок 3.9 – Таблиці значень: а – таблиця значень z1 , б – таблиця значень z_2

Згідно отриманих таблиць значень z_1 та z_2, створюємо логічні вирази, які описують ці змінні:

$$z_1 = \bar{x}_1 x_2 \bar{y}_2 + x_1 x_2 y_2 + \bar{x}_1 \bar{x}_2 y_2 + x_1 \bar{x}_2 \bar{y}_2 = L_1 z_1$$

$$z_2 = x_1 \bar{y}_1 y_2 + x_1 y_1 \bar{y}_2 + \bar{x}_1 y_2 y_1 + \bar{x}_1 \bar{y}_1 \bar{y}_1$$

Таблиця Келі третьої квазігрупи зображена на рисунку 3.10.

3)	0	1	2	3
0	2	1	3	0
1	0	3	1	2
2	1	2	0	3
3	3	0	2	1

Рисунок 3.10 – Квазігрупи №3

Згідно таблиці Келі третьої квазігрупи, вносимо в таблицю істинності значення, які відповідають результату кожної з 16 операцій, відповідно до чотирьох бінарних змінних, які описують *x* та *y*. Таблиця істинності другої квазігрупи зображена на рисунку 3.11.

№	x_1	x_2	y_1	y_2	$3z_1$	$3z_2$
0	0	0	0	0	0	1
1	0	0	0	1	1	1
2	0	0	1	0	1	0
3	0	0	1	1	0	0
4	0	1	0	0	1	0
5	0	1	0	1	0	0
6	0	1	1	0	0	1
7	0	1	1	1	1	1
8	1	0	0	0	0	0
9	1	0	0	1	1	0
10	1	0	1	0	1	1
11	1	0	1	1	0	1
12	1	1	0	0	1	1
13	1	1	0	1	0	1
14	1	1	1	0	0	0
15	1	1	1	1	1	0

Рисунок 3.11 – Таблиця істинності для CIP-квазігрупи 4-го порядку №3.

Далі, згідно отриманої таблиці істинності, заповнимо таблиці значень z_1 та z_2. Для цього в кожній позиції діаграми Вейча, що описує набір змінних, який в результаті операції дає результат 1, записується 1. Результат заповнення таблиць зображено на рисунку 3.12.

Рисунок 3.12 – Таблиці значень: а – таблиця значень z1 , б – таблиця значень z_2

Згідно отриманих таблиць значень z_1 та z_2, створюємо логічні вирази, які описують ці змінні:

$$z_1 = x_2 y_1 y_2 + x_2 \bar{y}_1 \bar{y}_2 + \bar{x}_2 y_1 \bar{y}_2 + \bar{x}_2 \bar{y}_1 y_2$$

$$z_2 = x_1 x_2 \bar{y}_1 + x_1 \bar{x}_2 y_1 + \bar{x}_1 x_2 y_1 + \bar{x}_1 \bar{x}_2 \bar{y}_1$$

Таблиця Келі четвертої квазігрупи, згідно якої буде побудована таблиця істинності, зображена на рисунку 3.13:

4)	0	1	2	3
0	3	0	2	1
1	1	2	0	3
2	0	3	1	2
3	2	1	3	0

Рисунок 3.13 – Квазігрупи №4

Згідно таблиці Келі четвертої квазігрупи, вносимо в таблицю істинності значення, які відповідають результату кожної з 16 операцій, відповідно до чотирьох бінарних змінних, які описують *x* та *y*. Таблиця істинності другої квазігрупи зображена на рисунку 3.14

№	x_1	x_2	y_1	y_2	$4z_1$	$4z_2$
0	0	0	0	0	1	0
1	0	0	0	1	0	1
2	0	0	1	0	1	1
3	0	0	1	1	0	0
4	0	1	0	0	0	0
5	0	1	0	1	1	1
6	0	1	1	0	0	1
7	0	1	1	1	1	0
8	1	0	0	0	0	1
9	1	0	0	1	1	0
10	1	0	1	0	0	0
11	1	0	1	1	1	1
12	1	1	0	0	1	1
13	1	1	0	1	0	0
14	1	1	1	0	1	0
15	1	1	1	1	0	1

Рисунок 3.14 – Таблиця істинності для CIP-квазігрупи 4-го порядку №4.

Далі, згідно отриманої таблиці істинності, заповнимо таблиці значень z_1 та z_2. Для цього в кожній позиції діаграми Вейча, що описує набір змінних, який в результаті операції дає результат 1, записується 1. Результат заповнення таблиць зображено на рисунку 3.15.

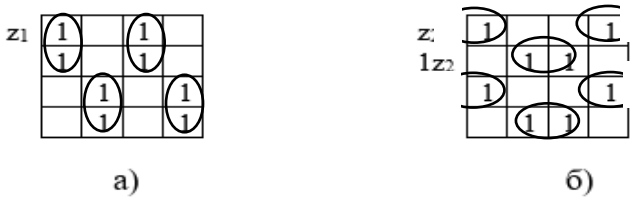


Рисунок 3.15 – Таблиці значень: а – таблиця значень z1 , б – таблиця значень z_2

Згідно отриманих таблиць значень z_1 та z_2, створюємо логічні вирази, які описують ці змінні:

$$z_1 = x_1 x_2 \bar{y}_2 + \bar{x}_1 x_2 y_2 + x_1 \bar{x}_2 y_2 + \bar{x}_1 \bar{x}_2 \bar{y}_2$$

$$z_2 = x_1 y_1 y_2 + \bar{x}_1 \bar{y}_1 y_2 + x_1 \bar{y}_1 \bar{y}_2 + \bar{x}_1 y_1 \bar{y}_2 = L_1 z_2$$

Таблиця Келі п’ятої квазігрупи зображена на рисунку 3.16.

5)	0	1	2	3
0	0	2	3	1
1	3	1	0	2
2	1	3	2	0
3	2	0	1	3

Рисунок 3.16 – Квазігрупи №5

Згідно таблиці Келі п’ятої квазігрупи, вносимо в таблицю істинності значення, які відповідають результату кожної з 16 операцій, відповідно до чотирьох бінарних змінних, які описують *x* та *y*. Таблиця істинності другої квазігрупи зображена на рисунку 3.17

№	x_1	x_2	y_1	y_2	$5z_1$	$5z_2$
0	0	0	0	0	1	0
1	0	0	0	1	0	0
2	0	0	1	0	0	1
3	0	0	1	1	1	1
4	0	1	0	0	0	1
5	0	1	0	1	1	1
6	0	1	1	0	1	0
7	0	1	1	1	0	0
8	1	0	0	0	1	1
9	1	0	0	1	0	1
10	1	0	1	0	0	0
11	1	0	1	1	1	0
12	1	1	0	0	0	0
13	1	1	0	1	1	0
14	1	1	1	0	1	1
15	1	1	1	1	0	1

Рисунок 3.17 – Таблиця істинності для CIP-квазігрупи 4-го порядку №5.

Далі, згідно отриманої таблиці істинності, заповнимо таблиці значень z_1 та z_2. Для цього в кожній позиції діаграми Вейча, що описує набір змінних, який в результаті операції дає результат 1, записується 1. Результат заповнення таблиць зображено на рисунку 3.18.

Рисунок 3.18 – Таблиці значень: а – таблиця значень z_1 , б – таблиця значень z_2

Згідно отриманих таблиць значень z_1 та z_2, створюємо логічні вирази, які описують ці змінні:

$$z_1 = x_2 y_1 \overline{y}_2 + x_2 \overline{y}_1 y_2 + \overline{x}_2 y_1 y_2 + \overline{x}_2 \overline{y}_1 \overline{y}_2$$

$$z_2 = x_1 y_1 x_2 + \overline{x}_1 \overline{y}_1 x_2 + x_1 \overline{x}_2 \overline{y}_1 + \overline{x}_1 \overline{x}_2 y_1$$

Таблиця Келі шостої квазігрупи, згідно якої буде побудована таблиця істинності, зображена на рисунку 3.19:

6)	0	1	2	3
0	1	3	2	0
1	2	0	1	3
2	0	2	3	1
3	3	1	0	2

Рисунок 3.19 – Квазігрупи №6

Згідно таблиці Келі шостої квазігрупи, вносимо в таблицю істинності значення, які відповідають результату кожної з 16 операцій, відповідно до чотирьох бінарних змінних, які описують *x* та *y*. Таблиця істинності другої квазігрупи зображена на рисунку 3.20.

№	x1	x2	y1	y2	6z1	6z2
0	0	0	0	0	1	1
1	0	0	0	1	0	0
2	0	0	1	0	1	0
3	0	0	1	1	0	1
4	0	1	0	0	0	1
5	0	1	0	1	1	0
6	0	1	1	0	0	0
7	0	1	1	1	1	1
8	1	0	0	0	0	0
9	1	0	0	1	1	1
10	1	0	1	0	0	1
11	1	0	1	1	1	0
12	1	1	0	0	1	0
13	1	1	0	1	0	1
14	1	1	1	0	1	1
15	1	1	1	1	0	0

Рисунок 3.20 – Таблиця істинності для CIP-квазігрупи 4-го порядку №6.

Далі, згідно отриманої таблиці істинності, заповнимо таблиці значень z_1 та z_2. Для цього в кожній позиції діаграми Вейча, що описує набір змінних, який в результаті операції дає результат 1, записується 1. Результат заповнення таблиць зображено на рисунку 3.21.

Рисунок 3.21 – Таблиці значень: а – таблиця значень z1 , б – таблиця значень z_2

Згідно отриманих таблиць значень z_1 та z_2, створюємо логічні вирази, які описують ці змінні:

$$z_1 = x_1 x_2 \bar{y}_2 + \bar{x}_1 x_2 y_2 + x_1 \bar{x}_2 y_2 + \bar{x}_1 \bar{x}_2 \bar{y}_2 = L_4 z_1$$

$$z_2 = x_1 \bar{y}_1 y_2 + x_1 y_1 \bar{y}_2 + \bar{x}_1 y_2 y_1 + \bar{x}_1 \bar{y}_1 \bar{y}_1 = L_2 z_2$$

Таблиця Келі сьомої квазігрупи, згідно якої буде побудована таблиця істинності, зображена на рисунку 3.22.

7)	0	1	2	3
0	2	0	1	3
1	1	3	2	0
2	3	1	0	2
3	0	2	3	1

Рисунок 3.22 – Квазігрупи №7

Згідно таблиці Келі шостої квазігрупи, вносимо в таблицю істинності значення, які відповідають результату кожної з 16 операцій, відповідно до чотирьох бінарних змінних, які описують *x* та *y*. Таблиця істинності другої квазігрупи зображена на рисунку 3.23.

№	x1	x2	y1	y2	7z1	7z2
0	0	0	0	0	1	1
1	0	0	0	1	0	1
2	0	0	1	0	0	0
3	0	0	1	1	1	0
4	0	1	0	0	0	0
5	0	1	0	1	1	0
6	0	1	1	0	1	1
7	0	1	1	1	0	1
8	1	0	0	0	1	0
9	1	0	0	1	0	0
10	1	0	1	0	0	1
11	1	0	1	1	1	1
12	1	1	0	0	0	1
13	1	1	0	1	1	1
14	1	1	1	0	1	0
15	1	1	1	1	0	0

Рисунок 3.23 – Таблиця істинності для СІР-квазігрупи 4-го порядку №7.

Далі, згідно отриманої таблиці істинності, заповнимо таблиці значень z_1 та z_2. Для цього в кожній позиції діаграми Вейча, що описує набір змінних, який в результаті операції дає результат 1, записується 1. Результат заповнення таблиць зображено на рисунку 3.24.

Рисунок 3.24 – Таблиці значень: а – таблиця значень z1 , б – таблиця значень z_2

Згідно отриманих таблиць значень z_1 та z_2, створюємо логічні вирази, які описують ці змінні:

$$z_1 = x_2 y_1 y_2 + x_2 \bar{y}_1 \bar{y}_2 + \bar{x}_2 y_1 \bar{y}_2 + \bar{x}_2 \bar{y}_1 y_2 = L_3 z_1$$

$$z_2 = x_1 x_2 \bar{y}_1 + x_1 \bar{x}_2 y_1 + \bar{x}_1 x_2 y_1 + \bar{x}_1 \bar{x}_2 \bar{y}_1 = L_3 z_2$$

Таблиця Келі сьомої квазігрупи, згідно якої буде побудована таблиця істинності, зображена на рисунку 3.25.

8)	0	1	2	3
0	3	1	0	2
1	0	2	3	1
2	2	0	1	3
3	1	3	2	0

Рисунок 3.25 – Квазігрупи №8

Згідно таблиці Келі шостої квазігрупи, вносимо в таблицю істинності значення, які відповідають результату кожної з 16 операцій, відповідно до чотирьох бінарних змінних, які описують *x* та *y*. Таблиця істинності восьмої квазігрупи зображена на рисунку 3.26

№	x_1	x_2	y_1	y_2	$8z_1$	$8z_2$
0	0	0	0	0	0	0
1	0	0	0	1	1	0
2	0	0	1	0	1	1
3	0	0	1	1	0	1
4	0	1	0	0	1	1
5	0	1	0	1	0	1
6	0	1	1	0	0	0
7	0	1	1	1	1	0
8	1	0	0	0	0	1
9	1	0	0	1	1	1
10	1	0	1	0	1	0
11	1	0	1	1	0	0
12	1	1	0	0	1	0
13	1	1	0	1	0	0
14	1	1	1	0	0	1
15	1	1	1	1	1	1

Рисунок 3.26 – Таблиця істинності для CIP-квазігрупи 4-го порядку №8.

Далі, згідно отриманої таблиці істинності, заповнимо таблиці значень z_1 та z_2. Для цього в кожній позиції діаграми Вейча, що описує набір змінних, який в результаті операції дає результат 1, записується 1. Результат заповнення таблиць зображено на рисvнку 3.27.

‘’-

а) б)

Рисунок 3.27 – Таблиці значень: а – таблиця значень z1 , б – таблиця значень z_2

Згідно отриманих таблиць значень z_1 та z_2, створюємо логічні вирази, які описують ці змінні:

$$z_1 = x_2 y_1 y_2 + x_2 \overline{y}_1 \overline{y}_2 + \overline{x}_2 y_1 \overline{y}_2 + \overline{x}_2 \overline{y}_1 y_2 = L_3 z_1$$

$$z_2 = x_1 y_1 x_2 + \overline{x}_1 \overline{y}_1 x_2 + x_1 \overline{x}_2 \overline{y}_1 + \overline{x}_1 \overline{x}_2 y_1 = L_5 z_2$$

Як видно з наведених логічних виразів, результат підлягає мінімізації шляхомскорочення логічних виразів

3.4 Перетворення виразів з урахуванням базису

Для перетворення виразів був обраний базис, що включає логічні елементи «АБО», «І», «НІ» та «Виключне АБО».

Для мінімізації логічних виразів виконаємо операції винесення за дужки спільного множника. Наступним кроком буде визначення операцій додавання за модулем два. Для мінімізації необхідно знайти фрагменти виразу, які описують операцію додавання за модулем два та скоротити їх, шляхом перетворення двох операцій логічного «І» та однієї операції «АБО» в одну операцію «Виключного АБО».

Мінімізація логічних виразів для кожної квазігрупи:

Логічні вирази квазігрупи L_2 складаються з чотирьох доданків, кожен з яких складається з трьох множників:

$$L_1 z_1 = \bar{x}_1 x_2 \bar{y}_2 + x_1 x_2 y_2 + \bar{x}_1 \bar{x}_2 y_2 + x_1 \bar{x}_2 \bar{y}_2$$

$$L_1 z_2 = x_1 y_1 y_2 + \bar{x}_1 \bar{y}_1 y_2 + x_1 \bar{y}_1 \bar{y}_2 + \bar{x}_1 y_1 \bar{y}_2$$

Шляхом винесення за дужки спільних множників $\overline{y_2}$ та y_2, логічні вирази скорочуються:

$$L_1 z_1 = y_2 \overline{(x_1 \oplus x_2)} + \bar{y}_2 (x_1 \oplus x_2)$$

$$L_1 z_2 = y_2 \overline{(x_1 \oplus y_2)} + \bar{y}_2 (x_1 \oplus y_2)$$

Логічні вирази квазігрупи L_2 складаються з чотирьох доданків, кожен з яких складається з трьох множників:

$$L_2 z_1 = \bar{x}_1 x_2 \bar{y}_2 + x_1 x_2 y_2 + \bar{x}_1 \bar{x}_2 y_2 + x_1 \bar{x}_2 \bar{y}_2$$

$$L_2 z_2 = x_1 \bar{y}_1 y_2 + x_1 y_1 \bar{y}_2 + \bar{x}_1 y_2 y_1 + \bar{x}_1 \bar{y}_1 \bar{y}_2$$

Шляхом винесення за дужки спільних множників $\overline{y_2}$ та y_2, логічні вирази скорочуються:

$$L_2 z_1 = y_2 \overline{(x_1 \oplus x_2)} + \bar{y}_2 (x_1 \oplus x_2)$$

$$L_2 z_2 = y_2 (x_1 \oplus y_1) + \bar{y}_2 \overline{(x_1 \oplus y_1)}$$

Логічні вирази квазігрупи L_3 складаються з чотирьох доданків, кожен з яких складається з трьох множників:

$$L_3 z_1 = x_2 y_1 y_2 + x_2 \bar{y}_1 \bar{y}_2 + \bar{x}_2 y_1 \bar{y}_2 + \bar{x}_2 \bar{y}_1 y_2$$

$$L_3 z_2 = x_1 x_2 \bar{y}_1 + x_1 \bar{x}_2 y_1 + \bar{x}_1 x_2 y_1 + \bar{x}_1 \bar{x}_2 \bar{y}_1$$

Шляхом винесення за дужки спільних множників $\overline{x_2}, x_2, \overline{x_1}$ та x_1, логічні вирази скорочуються:

$$L_3 z_1 = x_2 \overline{(y_1 \oplus y_2)} + \bar{x}_2 (y_1 \oplus y_2)$$

$$L_3 z_2 = x_1 (x_2 \oplus y_1) + \bar{x}_1 \overline{(x_2 \oplus y_1)}$$

Логічні вирази квазігрупи L_4 складаються з чотирьох доданків, кожен з яких складається з трьох множників:

$$L_4 z_1 = x_1 x_2 \bar{y}_2 + \overline{x_1} x_2 y_2 + x_1 \bar{x}_2 y_2 + \bar{x}_1 \bar{x}_2 \bar{y}_2$$

$$L_4 z_2 = x_1 y_1 y_2 + \bar{x}_1 \bar{y}_1 y_2 + x_1 \bar{y}_1 \bar{y}_2 + \bar{x}_1 y_1 \bar{y}_2$$

Шляхом винесення за дужки спільних множників $\overline{x_2}, x_2, \overline{y_2}$ та y_2, логічні вирази скорочуються:

$$L_4 z_1 = x_2 (x_1 \oplus y_2) + \bar{x}_2 \overline{(x_1 \oplus y_2)}$$

$$L_4 z_2 = y_2 \overline{(x_1 \oplus y_2)} + \bar{y}_2 (x_1 \oplus y_2)$$

Логічні вирази квазігрупи L_5 складаються з чотирьох доданків, кожен з яких складається з трьох множників:

$$L_5 z_1 = x_2 y_1 \bar{y}_2 + x_2 \bar{y}_1 y_2 + \bar{x}_2 y_1 y_2 + \bar{x}_2 \bar{y}_1 \bar{y}_2$$

$$L_5 z_2 = x_1 y_1 x_2 + \bar{x}_1 \bar{y}_1 x_2 + x_1 \bar{x}_2 \bar{y}_1 + \bar{x}_1 \bar{x}_2 y_1$$

Шляхом винесення за дужки спільних множників $\overline{x_2}$ та x_2, логічні вирази скорочуються:

$$L_5 z_1 = x_2 (y_1 \oplus y_2) + \bar{x}_2 \overline{(y_1 \oplus y_2)}$$

$$L_5 z_2 = x_2 \overline{(x_1 \oplus y_1)} + \bar{x}_2 (x_1 \oplus y_1)$$

Логічні вирази квазігрупи L_6 складаються з чотирьох доданків, кожен з яких складається з трьох множників:

$$L_6z_1 = x_1x_2\bar{y}_2 + \bar{x}_1x_2y_2 + x_1\bar{x}_2y_2 + \bar{x}_1\bar{x}_2\bar{y}_2$$

$$L_6z_2 = x_1\bar{y}_1y_2 + x_1y_1\bar{y}_2 + \bar{x}_1y_2y_1 + \bar{x}_1\bar{y}_1\bar{y}_2$$

Шляхом винесення за дужки спільних множників $\overline{x_2}, x_2, \overline{y_2}$ та y_2, логічні вирази скорочуються:

$$L_6z_1 = x_2(x_1 \oplus y_2) + \bar{x}_2\overline{(x_1 \oplus y_2)}$$

$$L_6z_2 = y_2(x_1 \oplus y_1) + \bar{y}_2\overline{(x_1 \oplus y_1)}$$

Логічні вирази квазігрупи L_7 складаються з чотирьох доданків, кожен з яких складається з трьох множників:

$$L_7z_1 = x_2y_1\bar{y}_2 + x_2\bar{y}_1y_2 + \bar{x}_2y_1y_2 + \bar{x}_2\bar{y}_1\bar{y}_2$$

$$L_7z_2 = x_1x_2\bar{y}_1 + x_1\bar{x}_2y_1 + \bar{x}_1x_2y_1 + \bar{x}_1\bar{x}_2\bar{y}_1$$

Шляхом винесення за дужки спільних множників $\overline{x_2}, x_2, \overline{x_1}$ та x_1, логічні вирази скорочуються:

$$L_7z_1 = x_2(y_1 \oplus y_2) + \bar{x}_2\overline{(y_1 \oplus y_2)}$$

$$L_7z_2 = x_1(x_2 \oplus y_1) + \bar{x}_1\overline{(x_2 \oplus y_1)}$$

Логічні вирази квазігрупи L_8 складаються з чотирьох доданків, кожен з яких складається з трьох множників:

$$L_8z_1 = x_2y_1y_2 + x_2\bar{y}_1\bar{y}_2 + \bar{x}_2y_1\bar{y}_2 + \bar{x}_2\bar{y}_1y_2$$

$$L_8z_2 = x_1y_1x_2 + \bar{x}_1\bar{y}_1x_2 + x_1\bar{x}_2\bar{y}_1 + \bar{x}_1\bar{x}_2y_1$$

Шляхом винесення за дужки спільних множників $\overline{x_2}$ та x_2, логічні вирази скорочуються:

$$L_8z_1 = x_2\overline{(y_1 \oplus y_2)} + \bar{x}_2(y_1 \oplus y_2)$$

$$L_8z_2 = x_2\overline{(x_1 \oplus y_1)} + \bar{x}_2(x_1 \oplus y_1)$$

Як бачимо з мінімізованих схем, деякі логічні вирази повторюються між собою. При групуванні логічних виразів за належністю до основного або побічного набору, можна визначити, що для реалізації квазігруп одного набору достатньо використати чотири унікальні логічні вирази.

Оскільки всі логічні вирази, що реалізують квазігрупи, є подібними, можна провести підрахунок необхідної кількості логічних елементів, обчисливши елементи, необхідні для реалізації одного виразу.

Таким чином, бачимо, що для реалізації одного виразу необхідно використати один логічний елемент «АБО», два логічні елементи «І», два логічні елементи «Виключне АБО» та два логічні елементи «НІ».

Оскільки всі логічні вирази є подібними, для обчислення кількості логічних елементів, необхідних для реалізації квазігруп, помножимо кількість елементів, необхідних для реалізації одного виразу, на кількість виразів, що реалізують квазігрупи.

Таким чином маємо вісім логічних елементів «АБО», шістнадцять логічних елементів «І», шістнадцять логічних елементів «Виключне АБО» та шістнадцять логічних елементів «НІ».

Висновки до розділу

У цьому розділі ми детально розглянули перемикальні функції та логічні схеми, що є основою для реалізації криптографічних алгоритмів. Починаючи з визначення та опису перемикальних функцій, ми проаналізували їх основні властивості та використання.

Окрему увагу було приділено мінімізації перемикальних функцій. Метод мінімізації на основі діаграм Вейча дозволяє ефективно скорочувати кількість вхідних змінних та логічних виразів, забезпечуючи оптимальну логічну схему з меншим числом гейтів та зменшенням витрат на ресурси.

Діаграма Вейча є потужним графічним інструментом для візуалізації логічних функцій та логічних виразів. Вона дозволяє зрозуміти структуру та

взаємозв'язок між вхідними та вихідними сигналами, спрощуючи процес мінімізації та оптимізації логічних схем.

Застосувано метод мінімізації на основі діаграм Вейча до логічних схем 8 CIP-квазігруп. Використовуючи таблиці істиності та принципи мінімізації, успішно зменшили кількість гейтів та оптимізували логічні схеми, що сприяє поліпшенню ефективності та швидкодії цих схем.

При обчисленні кількості логічних елементів, необхідних для реалізації квазігруп, виявилось, що загальна кількість логічних елементів становить 56 гейтів.

Отже, в цьому розділі детально досліджено перемикальні функції та логічні схеми, ознайомлено з методами їх мінімізації на основі діаграм Вейча та успішно застосовано ці методи до мінімізації логічних схем 8 CIP-квазігруп.

ВИСНОВКИ

Під час дослідження інформаційних джерел було визначено що CIP-квазігрупи (Cros Invers Properties) є важливим інструментом у сучасній криптографії з кількох причин, які детально розглянемо:

1) Криптографічна стійкість: CIP-квазігрупи мають специфічні властивості, які роблять їх стійкими до криптоаналітичних атак. Одна з таких властивостей – необоротність, що означає, що зі значень квазігрупи неможливо однозначно відновити початкові дані або ключ. Крім того, CIP-квазігрупи дуже чутливі до навіть малих змін вхідних даних або ключа, що робить атаки з використанням статистичного аналізу менш ефективними. Всі ці фактори сприяють забезпеченню високого рівня конфіденційності та безпеки при передачі та збереженні даних.

2) Ефективність обчислень: Операції, визначені на CIP-квазігрупах, можуть бути ефективно реалізовані на сучасних обчислювальних пристроях, включаючи комп'ютери, мобільні пристрої та мікроконтролери. Це означає, що обробка даних з використанням CIP-квазігруп може відбуватись швидко, що дозволяє їх використання в реальному часі для шифрування, розшифрування та інших криптографічних операцій.

3) Гнучкість та розширюваність: CIP-квазігрупи можуть бути використані для побудови різних криптографічних примітивів, таких як блочні шифри, хеш-функції, генератори псевдовипадкових чисел та інше. Вони можуть бути поєднані з іншими криптографічними алгоритмами для створення складних систем шифрування та автентифікації. Це дає можливість гнучко налаштовувати криптографічні протоколи залежно від конкретних потреб і вимог застосування.

4) Математична основа: CIP-квазігрупи базуються на математичних структурах та алгебраїчних властивостях, що робить їх абстрактними та формальними. Це дозволяє проводити математичний аналіз їхніх властивостей, довести теоретичні твердження та забезпечити вивчення їх стійкості.

Математична основа CIP-квазігруп сприяє розвитку криптографічних алгоритмів та дозволяє проводити формальну перевірку їхньої безпеки.

Враховуючи всі переваги, CIP-квазігрупи є важливим інструментом у сучасній криптографії та допомагають забезпечувати безпеку та конфіденційність в цифровому світі. Вивчення їх властивостей та використання в різних криптографічних системах допомагає розвивати цю науку та забезпечувати захист інформації у сучасному інформаційному суспільстві

Наступним кроком були розглянуті та описані важливі аспекти теорії квазігруп. Починаючи з канонічного розкладу CIP-квазігруп, була розкрита його сутність та методика застосування. Канонічний розклад є важливим інструментом у формуванні та аналізі квазігруп, оскільки він дозволяє отримати унікальні розклади для кожної квазігрупи.

Наведено прямий добуток квазігруп, який є потужним методом для побудови нових квазігруп шляхом комбінації існуючих. Прямий добуток дозволяє злити квазігрупи різних порядків, що розширює можливості утворення більш складних структур.

Після уважного аналізу та порівняння можливостей мов програмування, було прийняте рішення вибрати Java. Java є потужною та широко використовуваною мовою програмування з багатим набором функціональних можливостей. Вона підтримує об'єктно-орієнтований підхід, має велику кількість доступних бібліотек та добре документована. Крім того, Java є платформо незалежною мовою, що дозволяє запускати програмний код на різних операційних системах без змін.

Під час аналізу різних інтегрованих середовищ розробки для Java, було обрано IntelliJ IDEA. Це популярне та потужне середовище розробки, яке надає широкий набір інструментів для комфортної розробки програмного коду. IntelliJ IDEA має розширену функціональність, таку як автодоповнення коду, вбудовану підтримку систем контролю версій, дебагер та інші корисні інструменти, що полегшують процес розробки.

У результаті було успішно реалізовано програмний застосунок, який здатен формувати всі CIP-квазігрупи 4-го порядку. Кількість таких квазігруп становить 8. Також серед них були знайдені оборотні пари які є важливими об'єктами дослідження, оскільки вони мають специфічні властивості та знаходять широке застосування у різних областях.

У цьому розділі ми детально розглянули перемикальні функції та логічні схеми, що є основою для реалізації криптографічних алгоритмів. Починаючи з визначення та опису перемикальних функцій, ми проаналізували їх основні властивості та використання.

Окрему увагу було приділено мінімізації перемикальних функцій. Метод мінімізації на основі діаграм Вейча дозволяє ефективно скорочувати кількість вхідних змінних та логічних виразів, забезпечуючи оптимальну логічну схему з меншим числом гейтів та зменшенням витрат на ресурси.

Діаграма Вейча є потужним графічним інструментом для візуалізації логічних функцій та логічних виразів. Вона дозволяє зрозуміти структуру та взаємозв'язок між вхідними та вихідними сигналами, спрощуючи процес мінімізації та оптимізації логічних схем.

Застосувано метод мінімізації на основі діаграм Вейча до логічних схем 8 CIP-квазігруп. Використовуючи таблиці істиності та принципи мінімізації, успішно зменшили кількість гейтів та оптимізували логічні схеми, що сприяє поліпшенню ефективності та швидкодії цих схем.

При обчисленні кількості логічних елементів, необхідних для реалізації квазігруп, виявилось, що загальна кількість логічних елементів становить 56 гейтів.

Усі сформульовані задачі роботи розв’язано і досягнуто мету дослідження, а саме зменшення апаратних витрат засобу потокового шифрування шляхом використання CIP-квазігруп.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Крайнічук Г.В., Пилявець І.Ю., Радченко Є.В. СІР-квазігрупи 4-го порядку з оборотним елементом x^2 серед ізотопів групи Клейна // Збірник наук. праць Міжн. наук. конф. «Сучасні проблеми мех. та мат. – 2023», ІПММ ім. Я.С.Підстригача. Львів. 2023. – С. 285-286.

2. Лужецький В.А., Крайнічук Г.В., Радченко Є.В., Пилявець І.Ю. алгоритм шифрування на основі СІР-квазігруп // Матеріали тезів IX Міжн. наук.-техн. конф. «ЗАХИСТ ІНФОРМАЦІЇ І БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ», НУ «Львівська політехніка». Львів. 2023. – С.

3. Крайнічук Г.В., Радченко Є.В., Пилявець І.Ю. концепція шифру на основі СІР-квазігруп // Матеріали Всеукр. наук.-практ. конф. «Theoretical and Applied Cybersecurity (TACS-2023)», присвяч. 100-річному ювілею акад. В. М. Глушкова, КПІ ім. Ігоря Сікорського. Київ. 2023. – 3 С.

4. Крайнічук Г.В., Пилявець І.Ю., Радченко Є.В. огляд методів шифрування за допомогою квазігрупових операцій // Матеріали тезів LII наук.-техн. конф. ФІТКІ, ВНТУ. Вінниця. 2023 – 2 С.

5. Комп'ютерна програма "Тестування множини непарних складених чисел на приналежність до Кармайклових чисел" : а. с. 95986 Україна / І.Ю. Пилявець, М.В. Луканов, О.С. Козак, М.В. Маркусович. № 96945 ; заявл. 08.01.2020 ; опубл. 11.02.2020.

6. Сушкевич А. К. Теорія узагальнених груп / А. К. Сушкевич. – К.: Держ. наук.-тех. вид-во України, 1937. – 175 с.

7. Белоусов В.Д. Основи теорії квазігруп і луп / В.Д. Белоусов. – М: Наука. АН Молдовська ССР, 1967. – 225 с.

8. Quasigroups and loops: Theory and applications / ed. by C. O. 1943-, P. H. O, Smith, Jonathan D. H., 1949-. Berlin : Heldermann, 1990. 568 p.

9. Smith J. D. H. Introduction to Quasigroups and Their Representations. Taylor & Francis Group, 2006. 352 p.

10. Keedwell A. D., Dénes J. Latin Squares and Their Applications. Elsevier Science & Technology Books, 2015. 440 p.

11. Shcherbacov V. Elements of Quasigroup Theory and Applications. Taylor & Francis Group, 2017. 600 p.

12. Jaiyeola T., Smarandache F. Inverse Properties in Neutrosophic Triplet Loop and Their Application to Cryptography. Algorithms. 2018. Vol. 11, no. 3. P. 32. URL: https://doi.org/10.3390/a11030032 (date of access: 18.06.2023)

13. Olsson C. Discreet Discrete Mathematics : Secret Communication Using Latin Squares and Quasigroups : thesis. 2017. URL: http://urn.kb.se/resolve?urn=urn:nbn:se:umu:diva-136860(date of access: 18.06.2023)

14. Fawaz M., Zorkta H., Alnazer S. A Public Key Cipher Algorithm Based on Multivariate Cubic Quasigroups (MCQ). The International Conference on Electrical Engineering. 2010. Vol. 7, no. 7. P. 1–11. URL: https://doi.org/10.21608/iceeng.2010.33467(date of access: 18.06.2023)

15. Large quasigroups in cryptography and their properties testing / J. Dvorsky et al. 2009 World Congress on Nature & Biologically Inspired Computing (NaBIC 2009), Coimbatore, 9–11 December 2009.

16. McKay B. D. and Wanless I. M. On the number of Latin Squares // Ann. Combin. − 2005. − No. 9. − P. 335-344.

17. Шелепало Г. В. Класифікація квазігрупових функційних рівнянь і тотожностей мінімальної довжини : кандидатська дисертація. Хмельницький, 2013. 191 с.

18. Сохацький Ф.М. Оборотні бінарні функції і квазігрупи четвертого порядку // XIII Міжн. алгебр. конф. в Україні / Київ – КНУ ім. Т. Шевченка, 2021, 77-78 с.

19. Сохацький Ф.М., Луценко А.В., Фриз І.В .Побудова квазігруп з властивістю оборотності // Мат. методи та фіз.-мех. поля. 64, − 2021. – С.

20. Belousov V. D. Balanced Identities in Algebras of Quasigroups // Aequationes Math. — 1972. — Vol. 8. — P. 1–73.

21. Белоусов В. Д. Сандик М. Д. n-арные квазигруппы и лупы // Сиб. мат. журнал. — 1966. — № 7(1).— С. 31–54

22. Sinha Roy S., Verbauwhede I. Lattice-Based Public-Key Cryptography in Hardware. Singapore : Springer Singapore, 2020. URL: https://doi.org/10.1007/978-981-32-9994-8 (date of access: 18.06.2023)

23. Bjørstad T. E., A note on the Edon 80 s-box | Semantic Scholar. Semantic Scholar | AI-Powered Research Tool. URL: https://www.semanticscholar.org/paper/A-note-on-the-Edon-80-S-box-Bjørstad/fe7114a2ae9c605e026a5cfd61758f3d303f26f6 (accessed: 31.05.2023).

24. Byte of Python. O'reilly Media, 2010.

25. Oualline S. Practical C++ Programming. 2nd ed. Sebastopol, CA : O'Reilly, 2003. 549 p.

26. Spell B. Pro Java programming. 2nd ed. Berkley, Calif : Apress, 2005. 694 p.

27. Eclipse Documentation | The Eclipse Foundation. Eclipse Foundation. URL: https://www.eclipse.org/documentation/ (date of access: 18.06.2023).

28. Documentation | IntelliJ Platform Plugin SDK. IntelliJ Platform Plugin SDK Help. URL: https://plugins.jetbrains.com/docs/intellij/documentation.html (date of access: 18.06.2023).

29. NetBeans Tutorials. Welcome to Apache NetBeans. URL: https://netbeans.apache.org/kb/ (date of access: 18.06.2023).

30. Дичка І. А., Тарасенко В. П., Онай М. В. ОСНОВИ ПРИКЛАДНОЇ ТЕОРІЇ ЦИФРОВИХ АВТОМАТІВ. URL: https://core.ac.uk/download/pdf/32353 1874.pdf (date of access: 18.06.2023).

ДОДАТКИ

Додаток А
ПЕРЕЛІК ПУБЛІКАЦІЙ ЗА ТЕМОЮ

1) Крайнічук Г.В., Пилявець І.Ю., Радченко Є.В. CIP-квазігрупи 4-го порядку з оборотним елементом X2 серед ізотопів групи Клейна // Збірник наук. праць Міжн. наук. конф. «Сучасні проблеми мех. та мат. – 2023», ІПММ ім. Я.С.Підстригача. Львів. 2023. – С. 285-286.

2) Лужецький В.А., Крайнічук Г.В., Радченко Є.В., Пилявець І.Ю. алгоритм шифрування на основі CIP-квазігруп // Матеріали тезів IX Міжн. наук.-техн. конф. «ЗАХИСТ ІНФОРМАЦІЇ І БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ», НУ «Львівська політехніка». Львів. 2023. – С.

3) Крайнічук Г.В., Радченко Є.В., Пилявець І.Ю. концепція шифру на основі CIP-квазігруп // Матеріали Всеукр. наук.-практ. конф. «Theoretical and Applied Cybersecurity (TACS-2023)», присвяч. 100-річному ювілею акад. В. М. Глушкова, КПІ ім. Ігоря Сікорського. Київ. 2023. – 3 С.

4) Крайнічук Г.В., Пилявець І.Ю., Радченко Є.В. огляд методів шифрування за допомогою квазігрупових операцій // Матеріали тезів LII наук.-техн. конф. ФІТКІ, ВНТУ. Вінниця. 2023 – 2 С.

5) Комп'ютерна програма "Тестування множини непарних складених чисел на приналежність до Кармайклових чисел" : а. с. 95986 Україна / І.Ю. Пилявець, М.В. Луканов, О.С. Козак, М.В. Маркусович. № 96945 ; заявл. 08.01.2020 ; опубл. 11.02.2020.

Додаток Б

АПРОБАЦІЯ РЕЗУЛЬТАТІВ ДОСЛІДЖЕНЬ

1) Міжнародна наукова конференція «Сучасні проблеми механіки та математики – 2023», ІПММ ім. Я.С.Підстригача. Львів. 24-26 травня 2023. – С. 285-286.
2) IX Міжнародна науково-технічна конференція «ЗАХИСТ ІНФОРМАЦІЇ І БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ», Національний Університет «Львівська політехніка». Львів 2023.
3) Всеукраїнська науково-практична конференція «Theoretical and Applied Cybersecurity (TACS-2023)», присвячена 100-річному ювілею академіка В. М. Глушкова, Київський Політехнічний Інститут ім. Ігоря Сікорського. Київ 2023
4) LII науково-технічна конференція Факультету інформаційних технологій та комп’ютерної інженерії, Вінницький Національний Технічний Університет. Вінниця, 21-23 червня 2023

Додаток В

КОД ПРОГРАМНОГО ЗАСТОСУНКУ

Main.java

```
import java.util.Scanner;
public class Main {
    public static void main(String[] args) {
        String[][] k_1={
                {"0","1"},
                {"1","0"}
        };
        String[][] k_2={
                {"1","0"},
                {"0","1"}
        };
        while (true){
        System.out.println("1.Побудова CIP-квазігруп 4-го порядку\n2.Побудова квазігрупи
8 порядку\n3.Побудова квазігрупи 16 порядку\n4.Кінець");
        Scanner in = new Scanner(System.in);
        System.out.println("Ваш вибір:");
        int p= in.nextInt();
            switch (p){
                case 1:int q=1;
                    for(int i=0;i<4;i++){
                        for(int w=0;w<2;w++){
                            System.out.println("CIP-квазігрупа №"+(q));
                            bild.CreateQuasigroup(i,w);
                            System.out.println();
                            q++;}}
                    break;
                case 2:
                    System.out.println("Для побудови квазігрупи 8 порядку потрібні
квазігрупи 2-го та 4-го порядку\n" +
                            "Виберіть вектор(1-4) та квазігрупу 2-го порядку(1-2) для
квазігрупи 4-го порядку");
                    System.out.println("Вектор:");
                    int v_1 = in.nextInt();
                    System.out.println("Квазігрупа 2-го порядку:");
                    int kv_1 = in.nextInt();
                    addition.addition(k_1, bild.CreateQuasigroup(v_1, kv_1-1));
                    break;
                case 3:
                    System.out.println("Для побудови квазігрупи 16 порядку потрібно 2
квазігрупи 4-го порядку\n" +
                            "Виберіть вектор(1-4) та квазігрупу 2-го порядку(1-2) для
першої квазігрупи 4-го порядку");
                    System.out.println("Вектор:");
                    v_1 = in.nextInt();
                    System.out.println("Квазігрупа 2-го порядку:");
                    kv_1 = in.nextInt();
                    System.out.println("Виберіть вектор(1-4) та квазігрупу 2-го
порядку(1-2) для другої квазігрупи 4-го порядку");
                    System.out.println("Вектор:");
                    int v_2 = in.nextInt();
                    System.out.println("Квазігрупа 2-го порядку:");
                    int kv_2 = in.nextInt();
                    addition.addition(bild.CreateQuasigroup(v_1,kv_1-1),
bild.CreateQuasigroup(v_2,kv_2-1));
                    break;
                case 4:
                    System.exit(0);
                    break;
            }
        }
    }}
```

addition.java

```
public class addition {
    public static int[][] addition(String[][] kvaz_1, String[][] kvaz_2) {

        String[] G = new String[kvaz_1.length];
        String[] H= new String[kvaz_2.length];

        for(int i=0; i<kvaz_1.length; i++){
            G[i] = kvaz_1[0][i];}
        for(int i=0; i<kvaz_2.length; i++){
            H[i] = kvaz_2[0][i];
        }
        String[] sum = new String[G.length*H.length];
        for(int e=0; e<sum.length;){
            for(int i=0; i<G.length; i++){
                for(int w=0; w<H.length; w++){
                    String _1 = G[i];
                    String _2 = H[w];
                    String _1_2 = _1+_2;
                    sum[e]=_1_2;
                    e++;
                }
            }
        }

        String[][] demo_kvaz = new String[sum.length][sum.length];

        for(int i=0; i<sum.length; i++){
            String numberSt_1 = String.valueOf(sum[i]);
            char[] digits_1 = numberSt_1.toCharArray();
            for(int w=0; w<sum.length; w++){
                String numberSt_2 = String.valueOf(sum[w]);
                char[] digits_2 = numberSt_2.toCharArray();
                String st_1
=kvaz_1[Integer.parseInt(String.valueOf(digits_1[0]))][Integer.parseInt(String.valueOf(di
gits_2[0]))];
                String st_2
=kvaz_2[Integer.parseInt(String.valueOf(digits_1[1]))][Integer.parseInt(String.valueOf(di
gits_2[1]))];

                demo_kvaz[i][w]= st_1+st_2;
            }
        }
        for(int i=0; i< demo_kvaz.length; i++){
            for(int w=0; w< demo_kvaz.length; w++){
                //System.out.print(demo_kvaz[i][w]+"  ");
            }
        }
        int[][] kvaz_fin=new int[sum.length][sum.length];

        for(int i=0; i < demo_kvaz.length; i++){
            for(int w=0; w < demo_kvaz.length; w++){
                for(int q=0; q<sum.length;q++){
                    if(demo_kvaz[i][w].equals(sum[q])){
                        kvaz_fin[i][w]=q;
                        q++;
                    }
                }
            }        }

        for(int i=0; i< kvaz_fin.length; i++){
            for(int w=0; w< kvaz_fin.length; w++){
                System.out.print(kvaz_fin[i][w]+"  ");
            }
            System.out.println("\n");
        }

  return kvaz_fin;}}
```

bild.java

```
import static java.lang.Integer.parseInt;
public class bild {
    public static String[][] CreateQuasigroup(int aNumerical, int StateA) {
        int[][][] A = {
                {
                        /*A*/ {0, 1},
                        {1, 1}},
                {
                        /*A^-1*/ {1, 1},
                        {1, 0}}
        };

        int[] a = new int[2];
        a[0] = aNumerical > 1 ? 1 : 0;
        a[1] = aNumerical % 2 == 1 ? 1 : 0;

        int[][] bufx = new int[2][2];
        int[][] bufy = new int[2][2];
        String[][] res = new String[4][4];
        int[] bufVector = new int[2];
        for (int x = 0; x < 4; x++) {
            bufx[0][0] = x > 1 ? 1 : 0;
            bufx[0][1] = x % 2 == 1 ? 1 : 0;
            bufx = multiplyMatrices(bufx, A[StateA]);
            for (int y = 0; y < 4; y++) {
                bufy[0][0] = y > 1 ? 1 : 0;
                bufy[0][1] = y % 2 == 1 ? 1 : 0;
                bufy = multiplyMatrices(bufy, A[(StateA + 1) % 2]);
                bufVector[0] = bufx[0][0] + bufy[0][0] % 2;
                bufVector[1] = bufx[0][1] + bufy[0][1] % 2;
                bufVector[0] = (bufVector[0] + a[0]) % 2;
                bufVector[1] = (bufVector[1] + a[1]) % 2;

                res[x][y] = String.valueOf((char) (bufVector[0] + '0')) + (char)
(bufVector[1] + '0');
                System.out.print( parseInt (String.valueOf(res[x][y]),2) +" ");
            }
            System.out.println();
        }
        String[][] QWE= new String[4][4];
        for (int i = 0; i < res.length; i++) {
            for (int j = 0; j < res[0].length; j++) {
                QWE[i][j]= String.valueOf(parseInt (String.valueOf(res[i][j]),2));
            }
        }
        return QWE;
    }

   private static int[][] multiplyMatrices(int[][] matrix1, int[][] matrix2) {
        int[][] result = new int[matrix1.length][matrix2[0].length];

        for (int i = 0; i < matrix1.length; i++) {
            for (int j = 0; j < matrix2[0].length; j++) {
                for (int k = 0; k < matrix1[0].length; k++) {
                    result[i][j] += matrix1[i][k] * matrix2[k][j];
                }
            }
        }
        return result;
    }
}
```

Додаток Г
ПРОТОКОЛ ПЕРЕВІРКИ
БАКАЛАВРСЬКОЇ ДИПЛОМНОЇ РОБОТИ
НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: Засіб шифрування на основі квазігрупи. Частина 1. Реалізація квазігрупи

Автор роботи: Пилявець Ігор Юрійович

Тип роботи: бакалаврська дипломна робота .

Підрозділ кафедра захисту інформації ФІТКІ .

Показники звіту подібності Unicheck

Оригінальність – 84.5%. Схожість – 15.5%.

Аналіз звіту подібності (відмітити потрібне):

√ 1. Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.

□ 2. Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.

□ 3. Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку _____ (підпис) Каплун В. А. (прізвище, ініціали)

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи _____ (підпис) _____ (прізвище, ініціали)

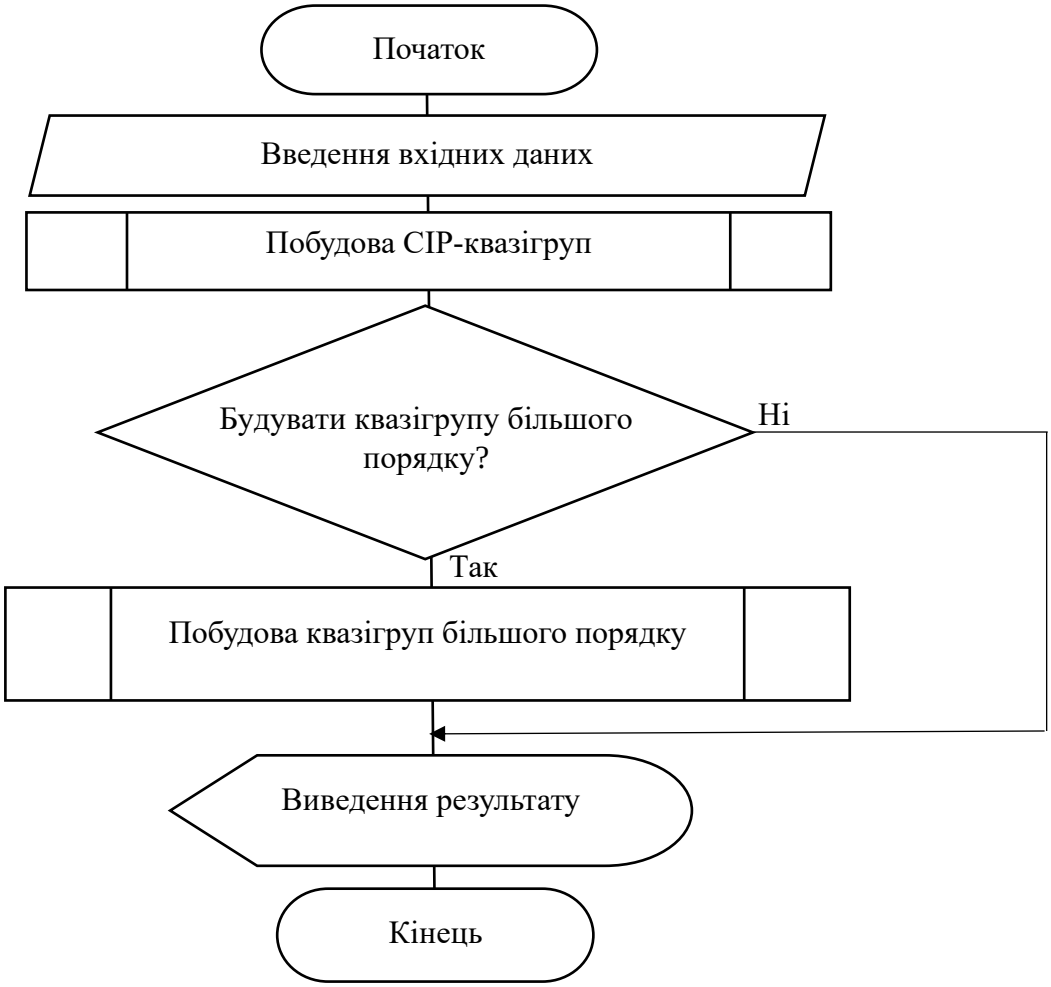
Керівник роботи _____ (підпис) _____ (прізвище, ініціали)

ІЛЮСТРАТИВНА ЧАСТИНА

ЗАСІБ ШИФРУВАННЯ НА ОСНОВІ КВАЗІГРУПИ.
ЧАСТИНА 1. РЕАЛІЗАЦІЯ КВАЗІГРУПИ

Виконав: студент 4 курсу групи 1БС-19б
спеціальності 125 Кібербезпека
_____ Пилявець І.Ю.
17 червня 2023 р.
Керівник: к.ф.-м.н., доцент каф. ЗІ
_____ Шелепало Г.В.
17 червня 2023 р.

СХЕМА РОБОТИ ПРОГРАМНОГО ЗАСОБУ



ТАБЛИЦІ КЕЛІ СІР-КВАЗІГРУП 4-ГО ПОРЯДКУ

1)	0	1	2	3
0	0	3	1	2
1	2	1	3	0
2	3	0	2	1
3	1	2	0	3

2)	0	1	2	3
0	1	2	0	3
1	3	0	2	1
2	2	1	3	0
3	0	3	1	2

3)	0	1	2	3
0	2	1	3	0
1	0	3	1	2
2	1	2	0	3
3	3	0	2	1

4)	0	1	2	3
0	3	0	2	1
1	1	2	0	3
2	0	3	1	2
3	2	1	3	0

5)	0	1	2	3
0	0	2	3	1
1	3	1	0	2
2	1	3	2	0
3	2	0	1	3

6)	0	1	2	3
0	1	3	2	0
1	2	0	1	3
2	0	2	3	1
3	3	1	0	2

7)	0	1	2	3
0	2	0	1	3
1	1	3	2	0
2	3	1	0	2
3	0	2	3	1

8)	0	1	2	3
0	3	1	0	2
1	0	2	3	1
2	2	0	1	3
3	1	3	2	0

ТАБЛИЦЯ ВЗАЄМНО ОБОРОТНИХ ПАР СІР-КВАЗІГРУП

1)	0	1	2	3
0	0	3	1	2
1	2	1	3	0
2	3	0	2	1
3	1	2	0	3

2)	0	1	2	3
0	1	2	0	3
1	3	0	2	1
2	2	1	3	0
3	0	3	1	2

3)	0	1	2	3
0	2	1	3	0
1	0	3	1	2
2	1	2	0	3
3	3	0	2	1

4)	0	1	2	3
0	3	0	2	1
1	1	2	0	3
2	0	3	1	2
3	2	1	3	0

5)	0	1	2	3
0	0	2	3	1
1	3	1	0	2
2	1	3	2	0
3	2	0	1	3

8)	0	1	2	3
0	3	1	0	2
1	0	2	3	1
2	2	0	1	3
3	1	3	2	0

6)	0	1	2	3
0	1	3	2	0
1	2	0	1	3
2	0	2	3	1
3	3	1	0	2

7)	0	1	2	3
0	2	0	1	3
1	1	3	2	0
2	3	1	0	2
3	0	2	3	1

КВАЗІГРУПА 16-ГО ПОРЯДКУ

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	11	8	10	9	7	4	6	5	15	12	14	13	3	0	2	1
1	9	10	8	11	5	6	4	7	13	14	12	15	1	2	0	5
2	8	11	9	10	4	7	5	6	12	15	13	14	0	3	1	2
3	10	9	11	8	6	5	7	4	14	13	15	12	2	1	3	0
4	3	0	2	1	15	12	14	13	7	4	6	5	11	8	10	9
5	1	2	0	3	13	14	12	15	5	6	4	7	9	10	8	11
6	0	3	1	2	12	15	13	14	4	7	5	6	8	11	9	10
7	2	1	3	0	14	13	15	12	6	5	7	4	10	9	11	8
8	7	4	6	5	11	8	10	9	3	0	2	1	15	12	14	13
9	5	6	4	7	9	10	8	11	1	2	0	3	13	14	12	15
10	4	7	5	6	8	11	9	10	0	3	1	2	12	15	13	14
11	6	5	7	4	10	9	11	8	2	1	3	0	14	13	15	12
12	15	12	14	13	3	0	2	1	11	8	10	9	7	4	6	5
13	13	14	12	15	1	2	0	3	9	10	8	11	5	6	4	7
14	12	15	13	14	0	3	1	2	8	11	9	10	4	7	5	6
15	14	13	15	12	2	1	3	0	10	9	11	8	6	5	7	4

ТАБЛИЦЯ КЕЛІ ГРУПИ КЛЯЙНА

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

ТАБЛИЦЯ ІСТИНОСТІ ДЛЯ ВСІХ СІР-КВАЗІГРУП 4-ГО ПОРЯДКУ

№	x_1	x_2	y_1	y_2	$1z_1$	$1z_2$	$2z_1$	$2z_2$	$3z_1$	$3z_2$	$4z_1$	$4z_2$	$5z_1$	$5z_2$	$6z_1$	$6z_2$	$7z_1$	$7z_2$	$8z_1$	$8z_2$
0	0	0	0	0	0	0	0	1	0	1	1	0	1	0	1	1	1	1	0	0
1	0	0	0	1	1	1	1	0	1	1	0	1	0	0	0	0	0	1	1	0
2	0	0	1	0	0	1	0	0	1	0	1	1	0	1	1	0	0	0	1	1
3	0	0	1	1	1	0	1	1	0	0	0	0	1	1	0	1	1	0	0	1
4	0	1	0	0	1	0	1	1	1	0	0	0	0	1	0	1	0	0	1	1
5	0	1	0	1	0	1	0	0	0	0	1	1	1	1	1	0	1	0	0	1
6	0	1	1	0	1	1	1	0	0	1	0	1	1	0	0	0	1	1	0	0
7	0	1	1	1	0	0	0	1	1	1	1	0	0	0	1	1	0	1	1	0
8	1	0	0	0	1	1	1	0	0	0	0	1	1	1	0	0	1	0	0	1
9	1	0	0	1	0	0	0	1	1	0	1	0	0	1	1	1	0	0	1	1
10	1	0	1	0	1	0	1	1	1	1	0	0	0	0	0	1	0	1	1	0
11	1	0	1	1	0	1	0	0	0	1	1	1	1	0	1	0	1	1	0	0
12	1	1	0	0	0	1	0	0	1	1	1	1	0	0	1	0	0	1	1	0
13	1	1	0	1	1	0	1	1	0	1	0	0	1	0	0	1	1	1	0	0
14	1	1	1	0	0	0	0	1	0	0	1	0	1	1	1	1	1	0	0	1
15	1	1	1	1	1	1	1	0	1	0	0	1	0	1	0	0	0	0	1	1

ДІАГРАМА ВЕЙЧА

	x2	x2	$\overline{x2}$	$\overline{x2}$	
x1	12	13	9	8	$\overline{y1}$
x1	14	15	11	10	y1
$\overline{x1}$	6	7	3	2	y1
$\overline{x1}$	4	5	1	0	$\overline{y1}$
	$\overline{y2}$	y2	y2	$\overline{y2}$	